Effective Chebotarev density theorems for families of number fields without GRH

Melanie Matchett Wood

University of Wisconsin-Madison

joint with Lillian Pierce and Caroline Turnage-Butterbaugh

The Chebotarev density theorem

The Chebotarev density theorem

K a Galois number field

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$\pi_C(X, K) =$

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X, K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \leq X\}$$

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X,K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \leq X\}$$

$\left[\frac{K/\mathbb{Q}}{p}\right]$ Artin symbol

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X, K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \leq X\}$$

$\left[\frac{K/\mathbb{Q}}{p}\right]$ Artin symbol

C a fixed conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X, K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \leq X\}$$

$\left[\frac{K/\mathbb{Q}}{p}\right]$ Artin symbol

C a fixed conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$

Theorem (Chebotarev Density Theorem, 1926)

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X, K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \leq X\}$$

$\left[\frac{K/\mathbb{Q}}{p}\right]$ Artin symbol

C a fixed conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X, K) \sim \frac{|C|}{|G|} \mathrm{Li}(X)$$

The Chebotarev density theorem

K a Galois number field
Count primes based on their behavior in K

$$\pi_C(X,K) = \#\{p \text{ prime} : p \text{ unramified in } K, \left[\frac{K/\mathbb{Q}}{p}\right] = C, p \le X\}$$

$\left[\frac{K/\mathbb{Q}}{p}\right]$ Artin symbol

C a fixed conjugacy class in $\mathrm{Gal}(K/\mathbb{Q})$

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X,K) \sim \frac{|C|}{|G|}\mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

An effective Chebotarev density theorem

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X, K) \sim \frac{|C|}{|G|}\mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

An effective Chebotarev density theorem

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X, K) \sim \frac{|C|}{|G|}\mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

But I want primes now!

An effective Chebotarev density theorem

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X, K) \sim \frac{|C|}{|G|}\mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

But I want primes now!

How big does X have to be to get any such primes?

An effective Chebotarev density theorem

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X,K) \sim \frac{|C|}{|G|}\mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

But I want primes now!

How big does X have to be to get any such primes? many?

An effective Chebotarev density theorem

Theorem (Chebotarev Density Theorem, 1926)

$$\pi_C(X, K) \sim \frac{|C|}{|G|} \mathrm{Li}(X)$$

$\mathrm{Li}(X) = \int_2^X dt/\log t = X/\log X + O(X/\log^2 X)$

But I want primes now!

How big does X have to be to get any such primes? many?

"Effective": error term and lower bound on X

An effective Chebotarev density theorem

$n_F := [F : \mathbb{Q}]$

An effective Chebotarev density theorem

$n_F := [F : \mathbb{Q}]$

$D_F := |\operatorname{Disc} F|$

An effective Chebotarev density theorem

$n_F := [F : \mathbb{Q}]$

$D_F := |\,\mathrm{Disc}\, F|$

Theorem (Lagarias and Odlyzko ’75, Serre ’82)

$n_F := [F : \mathbb{Q}]$

$D_F := |\operatorname{Disc} F|$

Theorem (Lagarias and Odlyzko '75, Serre '82)

If $K \neq \mathbb{Q}$, then $\zeta_K(s)$ has at most one zero β_0 in a standard zero-free region.

An effective Chebotarev density theorem

$n_F := [F : \mathbb{Q}]$

$D_F := |\operatorname{Disc} F|$

Theorem (Lagarias and Odlyzko '75, Serre '82)

If $K \neq \mathbb{Q}$, then $\zeta_K(s)$ has at most one zero β_0 in a standard zero-free region. We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2} (\log X)^{1/2})$$

An effective Chebotarev density theorem

$n_F := [F : \mathbb{Q}]$

$D_F := |\operatorname{Disc} F|$

Theorem (Lagarias and Odlyzko '75, Serre '82)

If $K \neq \mathbb{Q}$, then $\zeta_K(s)$ has at most one zero β_0 in a standard zero-free region. We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2} (\log X)^{1/2})$$

for all $X \geq \exp(10 n_K (\log D_K)^2)$.

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \geq \exp(10 n_K (\log D_K)^2)$,

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \geq \exp(10 n_K (\log D_K)^2)$,

- want to apply in families,

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \geq \exp(10 n_K (\log D_K)^2)$,

- want to apply in families, β_0 not uniform,

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \le \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \ge \exp(10 n_K (\log D_K)^2)$,

- want to apply in families, β_0 not uniform, need to remove effect of exceptional zero

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \le \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2} (\log X)^{1/2})$$

for all $X \ge \exp(10 n_K (\log D_K)^2)$,

- want to apply in families, β_0 not uniform, need to remove effect of exceptional zero
- need to apply to smaller X,

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \geq \exp(10 n_K (\log D_K)^2)$,

- want to apply in families, β_0 not uniform, need to remove effect of exceptional zero
- need to apply to smaller X, e.g. $X = D_K^{\epsilon}$,

An effective Chebotarev density theorem

Theorem (Lagarias and Odlyzko '75, Serre '82)

We have

$$\left|\pi_C(X) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \le \frac{|C|}{|G|}\mathrm{Li}(X^{\beta_0}) + C_1 X \exp(-C_2 n_K^{-1/2}(\log X)^{1/2})$$

for all $X \ge \exp(10 n_K (\log D_K)^2)$,

- want to apply in families, β_0 not uniform, need to remove effect of exceptional zero
- need to apply to smaller X, e.g. $X = D_K^{\epsilon}$, need bigger zero-free region

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields,

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ *of number fields, for every* $A \geq 2$*, and* $\epsilon > 0$*,*

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$,

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|} \mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left|\pi_C(X, K) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\frac{X}{(\log X)^A},$$

for

$$X \geq D_K^{\epsilon}.$$

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left|\pi_C(X, K) - \frac{|C|}{|G|}\mathrm{Li}(X)\right| \leq \frac{|C|}{|G|}\frac{X}{(\log X)^A},$$

for

$$X \geq D_K^{\epsilon}.$$

- dihedral D_p fields without order p ramification

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|}\mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

for

$$X \geq D_K^{\epsilon}.$$

- dihedral D_p fields without order p ramification
- S_3, S_4 fields with square-free discriminant

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|} \mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

for

$$X \geq D_K^{\epsilon}.$$

- dihedral D_p fields without order p ramification
- S_3, S_4 fields with square-free discriminant
- A_4 fields, all ramification order 3

Our main result

Theorem (Pierce, Turnage-Butterbaugh, W. '17)

For each appropriate family $\mathscr{F}(G)$ of number fields, for every $A \geq 2$, and $\epsilon > 0$, for almost all $K \in \mathscr{F}(G)$, (except a power saving exceptional family), we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|} \mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

for

$$X \geq D_K^{\epsilon}.$$

- dihedral D_p fields without order p ramification
- S_3, S_4 fields with square-free discriminant
- A_4 fields, all ramification order 3
- cyclic fields, all ramification total

Theorem (PTW)

The Chebotarev theorem

Theorem (PTW)

Given G, for every $A \geq 2$, and $\epsilon > 0$, and $0 < \delta \leq 1/(2A)$,

The Chebotarev theorem

Theorem (PTW)

Given G, *for every* $A \geq 2$, *and* $\epsilon > 0$, *and* $0 < \delta \leq 1/(2A)$, *for any number field* K *with* $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ *and* $D_K \geq D_0$ *and*

The Chebotarev theorem

Theorem (PTW)

Given G, for every $A \geq 2$, and $\epsilon > 0$, and $0 < \delta \leq 1/(2A)$, for any number field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ and $D_K \geq D_0$ and

- $\zeta_K(s)/\zeta(s)$ *has no zero in the region* $[1-\delta, 1] \times [-(\log D_K)^{2/\delta}, (\log D_K)^{2/\delta}]$

The Chebotarev theorem

Theorem (PTW)

Given G, for every $A \geq 2$, and $\epsilon > 0$, and $0 < \delta \leq 1/(2A)$, for any number field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ and $D_K \geq D_0$ and

- *$\zeta_K(s)/\zeta(s)$ has no zero in the region $[1-\delta, 1] \times [-(\log D_K)^{2/\delta}, (\log D_K)^{2/\delta}]$*

we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|} \mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

The Chebotarev theorem

Theorem (PTW)

Given G, for every $A \geq 2$, and $\epsilon > 0$, and $0 < \delta \leq 1/(2A)$, for any number field K with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ and $D_K \geq D_0$ and

- $\zeta_K(s)/\zeta(s)$ *has no zero in the region* $[1-\delta, 1] \times [-(\log D_K)^{2/\delta}, (\log D_K)^{2/\delta}]$

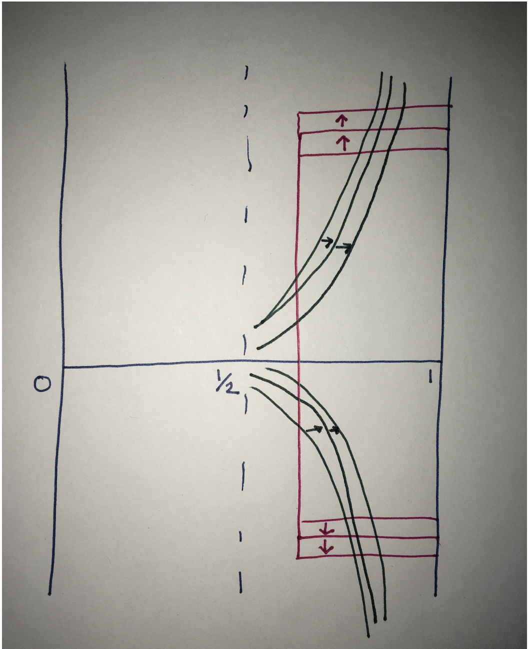
we have

$$\left| \pi_C(X, K) - \frac{|C|}{|G|} \mathrm{Li}(X) \right| \leq \frac{|C|}{|G|} \frac{X}{(\log X)^A},$$

for all

$$X \geq D_K^{\epsilon}.$$

Zero-free regions



Theorem (Kowalski and Michel, '02)

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions,

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Conditions:

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Conditions:

- size of family

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Conditions:

- size of family
- control of conductors

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Conditions:

- size of family
- control of conductors
- Ramanujan-Petersson conjecture

Theorem (Kowalski and Michel, '02)

Let $S(X)$ be a family of cuspidal automorphic representations of $\mathrm{GL}_m(\mathbb{Q})$ satisfying several conditions, then the total number of zeroes of all their L functions in the box

$$[1-\delta, 1] \times [-T, T]$$

is at most $O(X^\gamma)$.

Choose δ so almost all have no zeroes

Conditions:

- size of family
- control of conductors
- Ramanujan-Petersson conjecture
- convexity and joint convexity bounds

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Strong Artin Conjecture: each $L(s, \rho, K)$ is cuspidal

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Strong Artin Conjecture: each $L(s, \rho, K)$ is cuspidal

Kowalski-Michel fails for products of cuspidal L-functions

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Strong Artin Conjecture: each $L(s, \rho, K)$ is cuspidal

Kowalski-Michel fails for products of cuspidal L-functions

- One bad cuspidal L-function L_{bad}

Our L-functions

$$\zeta_K(s) = \prod_{\substack{\rho \\ \text{irrep. of } G}} L(s, \rho, K)$$

product of Artin L-functions

Strong Artin Conjecture: each $L(s, \rho, K)$ is cuspidal

Kowalski-Michel fails for products of cuspidal L-functions

- One bad cuspidal L-function L_{bad}
- Consider the family $L_{bad} L_i$ for cuspidal L_i

Extending to products of cuspidal L-functions

Extending to products of cuspidal L-functions

Key:

Extending to products of cuspidal L-functions

Key: ensuring any bad cuspidal L-function does not propogate into too many $\zeta_L(s)$

Extending to products of cuspidal L-functions

Key: ensuring any bad cuspidal L-function does not propogate into too many $\zeta_L(s)$

Task:

Extending to products of cuspidal L-functions

Key: ensuring any bad cuspidal L-function does not propogate into too many $\zeta_L(s)$

Task: counting number fields with fixed subfields (corresponding to $\ker \rho$)

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem
- lower: more subtle

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem
- lower: more subtle

Harder—need to count with fixed subfields

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem
- lower: more subtle

Harder—need to count with fixed subfields

- in some cases what we need is not true

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem
- lower: more subtle

Harder—need to count with fixed subfields

- in some cases what we need is not true (a positive proportion of $\mathbb{Z}/4\mathbb{Z}$ fields contain any given quadratic field)

Counting number fields

Asymptotics of $\#\{G\text{-number fields } K : |D_K| \leq X\}$?

Some G known, many G wide open

Dihedral groups D_p open

Easier—only need upper and lower bounds

- upper: no problem
- lower: more subtle

Harder—need to count with fixed subfields

- in some cases what we need is not true (a positive proportion of $\mathbb{Z}/4\mathbb{Z}$ fields contain any given quadratic field)
- main tool: pointwise upper bounds on $\#\{K : |D_K| = X\}$ and control ramification

Example arguments

Example arguments

(as many arguments as there are families)

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x,t)$ Galois group G over $\mathbb{Q}(t)$

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$
- $f(x, t_1)$ must have produced many different fields

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$
- $f(x, t_1)$ must have produced many different fields

Upper bounds with fixed discriminant, for dihedral D_p:

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$
- $f(x, t_1)$ must have produced many different fields

Upper bounds with fixed discriminant, for dihedral D_p:

- cyclic p extensions of quadratic fields

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$
- $f(x, t_1)$ must have produced many different fields

Upper bounds with fixed discriminant, for dihedral D_p:

- cyclic p extensions of quadratic fields
- class field theory to count cyclic p-extensions

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x, t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x, t_1)f(x, t_2)$ typically has Galois group $G \times G$
- $f(x, t_1)$ must have produced many different fields

Upper bounds with fixed discriminant, for dihedral D_p:

- cyclic p extensions of quadratic fields
- class field theory to count cyclic p-extensions
- reduce to local counting question

Example arguments

(as many arguments as there are families)

Lower bounds (e.g. A_n):

- $f(x,t)$ Galois group G over $\mathbb{Q}(t)$
- show $f(x,t_1)f(x,t_2)$ typically has Galois group $G \times G$
- $f(x,t_1)$ must have produced many different fields

Upper bounds with fixed discriminant, for dihedral D_p:

- cyclic p extensions of quadratic fields
- class field theory to count cyclic p-extensions
- reduce to local counting question
- (not a tight upper bound)

Application to ℓ-torsion in class groups

Application to ℓ-torsion in class groups

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

Application to ℓ-torsion in class groups

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

Conjecture

$$|\mathrm{Cl}_K[\ell]| \ll_{n_K,\ell,\epsilon} D_K^{\epsilon}$$

Application to ℓ-torsion in class groups

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

Conjecture

$$|\mathrm{Cl}_K[\ell]| \ll_{n_K,\ell,\epsilon} D_K^{\epsilon}$$

Theorem (PTW)

Let $\mathscr{F}(G)$ be an appropriate family of number fields of degree n.

Application to ℓ-torsion in class groups

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

Conjecture

$$|\mathrm{Cl}_K[\ell]| \ll_{n_K,\ell,\epsilon} D_K^{\epsilon}$$

Theorem (PTW)

Let $\mathscr{F}(G)$ be an appropriate family of number fields of degree n. Then almost every $K \in \mathscr{F}(G)$ (except power saving exceptions) satisfies

Application to ℓ-torsion in class groups

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

Conjecture

$$|\mathrm{Cl}_K[\ell]| \ll_{n_K,\ell,\epsilon} D_K^{\epsilon}$$

Theorem (PTW)

Let $\mathscr{F}(G)$ be an appropriate family of number fields of degree n. Then almost every $K \in \mathscr{F}(G)$ (except power saving exceptions) satisfies

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

for all $\epsilon > 0$.

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K-1)}$

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K - 1)}$ and suppose that there are at least M rational primes with $p \leq D_K^{\delta}$ that are unramified and split completely in K.

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K - 1)}$ and suppose that there are at least M rational primes with $p \leq D_K^{\delta}$ that are unramified and split completely in K. Then for any $\epsilon > 0$,

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

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K - 1)}$ and suppose that there are at least M rational primes with $p \leq D_K^{\delta}$ that are unramified and split completely in K. Then for any $\epsilon > 0$,

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

Note the requirement for small primes

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K-1)}$ and suppose that there are at least M rational primes with $p \le D_K^{\delta}$ that are unramified and split completely in K. Then for any $\epsilon > 0$,

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

Note the requirement for small primes

Assuming GRH, Ellenberg and Venkatesh get

Application to ℓ-torsion in class groups

Theorem (Ellenberg and Venkatesh '07)

Let $\delta < \frac{1}{2\ell(n_K-1)}$ and suppose that there are at least M rational primes with $p \leq D_K^{\delta}$ that are unramified and split completely in K. Then for any $\epsilon > 0$,

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

Note the requirement for small primes

Assuming GRH, Ellenberg and Venkatesh get

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

Application to number fields with small generators

Application to number fields with small generators

Theorem (Vaaler and Widmer, '13)

Application to number fields with small generators

Theorem (Vaaler and Widmer, '13)

Assuming GRH, every K of degree n has a generator of height $O(D_K^{\frac{1}{2n}})$.

Application to number fields with small generators

Theorem (Vaaler and Widmer, '13)

Assuming GRH, every K of degree n has a generator of height $O(D_K^{\frac{1}{2n}})$.

Theorem (PTW)

Application to number fields with small generators

Theorem (Vaaler and Widmer, '13)

Assuming GRH, every K of degree n has a generator of height $O(D_K^{\frac{1}{2n}})$.

Theorem (PTW)

Let $\mathscr{F}(G)$ be an appropriate family of number fields of degree n.

Application to number fields with small generators

Theorem (Vaaler and Widmer, '13)

Assuming GRH, every K of degree n has a generator of height $O(D_K^{\frac{1}{2n}})$.

Theorem (PTW)

Let $\mathscr{F}(G)$ be an appropriate family of number fields of degree n. Almost every $K \in \mathscr{F}(G)$ has a generator of height $O(D_K^{\frac{1}{2n}})$.