The influence of the structure of the Galois group on Chebyshev biases in number fields

Mounir Hayani

Introduction

Let L/K be a Galois extension of number fields with group G and let C be a conjugacy class in G. For $x \geq 2$, define

$$\pi(x; L/K, C) := \sum_{N\mathfrak{p} \leq x} \mathbb{1}_C(\varphi_\mathfrak{p}) .$$

where $\varphi_\mathfrak{p}$ is the class of Frobenius, which is a conjugacy class in G when $\mathfrak{p}$ is unramified.

Introduction

Let L/K be a Galois extension of number fields with group G and let C be a conjugacy class in G. For $x \geq 2$, define

$$\pi(x; L/K, C) := \sum_{N\mathfrak{p} \leq x} \mathbb{1}_C(\varphi_{\mathfrak{p}}) .$$

where $\varphi_{\mathfrak{p}}$ is the class of Frobenius, which is a conjugacy class in G when $\mathfrak{p}$ is unramified.
The Chebotarev density Theorem states that

$$\pi(x; L/K, C) \sim \frac{|C|}{|G|} \frac{x}{\log x} \text{ as } x \to +\infty .$$

Introduction

In the particular case where $L = \mathbb{Q}(\zeta_q)$, $q \geq 2$. We have $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$. If $a \in \mathbb{Z}$ is coprime to q we have

$$\pi(x; L/\mathbb{Q}, \{\bar{a}\}) = \#\{p \leq x \ : \ p \equiv a \bmod q\} =: \pi(x; q, a)\,.$$

Introduction

In the particular case where $L = \mathbb{Q}(\zeta_q)$, $q \geq 2$. We have $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^{\times}$. If $a \in \mathbb{Z}$ is coprime to q we have

$$\pi(x; L/\mathbb{Q}, \{\bar{a}\}) = \#\{p \leq x \ : \ p \equiv a \bmod q\} =: \pi(x; q, a)\,.$$

Applying the Chebotarev Theorem, we recover the prime number theorem in Arithmetic progressions :

$$\pi(x; q, a) \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \text{ as } x \to +\infty\,.$$

Introduction

In the particular case where $L = \mathbb{Q}(\zeta_q)$, $q \geq 2$. We have $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$. If $a \in \mathbb{Z}$ is coprime to q we have

$$\pi(x; L/\mathbb{Q}, \{\bar{a}\}) = \#\{p \leq x \ : \ p \equiv a \bmod q\} =: \pi(x; q, a)\,.$$

Applying the Chebotarev Theorem, we recover the prime number theorem in Arithmetic progressions :

$$\pi(x; q, a) \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \text{ as } x \to +\infty\,.$$

If $a, b \in \mathbb{Z}$ are distinct modulo q, what can we say about the set

$$\mathcal{P}(q; a, b) := \{x \geq 2 \ : \ \pi(x; q, a) > \pi(x; q, b)\}\,?$$

Theorem (Rubinstein-Sarnack, 1994)

Assuming GRH and LI, the set $\mathcal{P}(q;a,b)$ admits a logarithmic density. That is, the limit

$$\delta(q;a,b) := \lim_{X\to\infty} \frac{1}{\log X}\int_2^X \mathbb{1}_{\mathcal{P}(q;a,b)}(x)\frac{dx}{x}$$

exists. Moreover, we have :

1. $0 < \delta(q;a,b) < 1$
2. $\delta(q;a,b) > \frac{1}{2}$ *if and only if a is a non-square modulo q and b is a square modulo q.*

Introduction

Theorem (Rubinstein-Sarnack, 1994)

Assuming GRH and LI, the set $\mathcal{P}(q;a,b)$ admits a logarithmic density. That is, the limit

$$\delta(q;a,b) := \lim_{X\to\infty} \frac{1}{\log X} \int_2^X \mathbb{1}_{\mathcal{P}(q;a,b)}(x) \frac{dx}{x}$$

exists. Moreover, we have :

1. $0 < \delta(q;a,b) < 1$
2. $\delta(q;a,b) > \frac{1}{2}$ *if and only if a is a non-square modulo q and b is a square modulo q.*

Several results have extended the study of $\delta(q;a,b)$.
D. Fiorilli and G. Martin : giving an asymptotic formula to $\delta(q;a,b)$.
Y. Lamzouri : generalizing their result to more competitors $\delta(q;a_1,\cdots,a_r)$.

Introduction

More generally, what can we say about the set

$$\mathcal{P}(L/K; C_1, C_2) = \left\{ x \geq 2 \ : \ \frac{1}{|C_1|}\pi(x; L/K, C_1) > \frac{1}{|C_2|}\pi(x; L/K, C_2) \right\} ?$$

Introduction

More generally, what can we say about the set

$$\mathcal{P}(L/K; C_1, C_2) = \left\{ x \geq 2 \ : \ \frac{1}{|C_1|}\pi(x; L/K, C_1) > \frac{1}{|C_2|}\pi(x; L/K, C_2) \right\} ?$$

Theorem (Ng, 2000)

Assuming GRH, AC and LI, the set $\mathcal{P}(L/K; C_1, C_2)$ admits a logarithmic density $\delta(L/K; C_1, C_2)$.

More generally, what can we say about the set

$$\mathcal{P}(L/K; C_1, C_2) = \left\{ x \geq 2 \ : \ \frac{1}{|C_1|}\pi(x; L/K, C_1) > \frac{1}{|C_2|}\pi(x; L/K, C_2) \right\} ?$$

Theorem (Ng, 2000)

Assuming GRH, AC and LI, the set $\mathcal{P}(L/K; C_1, C_2)$ admits a logarithmic density $\delta(L/K; C_1, C_2)$.

A. Bailleul, Fiorilli and Jouve, Lucile Devin.

The property $0 < \delta(q; a, b) < 1$ is not valid in the general case of number fields.

Definition (Extreme Chebyshev bias)

We say that the Galois extension L/K has an extreme Chebyshev bias relatively to (C_1, C_2) where C_1, C_2 are two conjugacy classes of $\mathrm{Gal}(L/K)$, if up to exchanging C_1 with C_2, $\delta(L/K; C_1, C_2)$ exists and is equal to 1.

Unconditional Chebyshev bias

If $a \in G$ and $\ell \geq 2$ denote

$$r_\ell(a) := \#\{g \in G \ : \ g^\ell = a\}\,.$$

Theorem (Fiorilli-Jouve, 2020)

Let L/K be a Galois extension of number fields with group G, and assume that L is a Galois extension over $\mathbb{Q}$ with group G^+. Let $a, b \in G$ with respective conjugacy classes $C_a \neq C_b$ in G. Assume that a and b are conjugates in G^+ and that $r_2(a) < r_2(b)$. Then, there exists $A \geq 2$ such that for all $x \geq A$ we have

$$\frac{1}{|C_a|}\pi(x; L/K, C_a) > \frac{1}{|C_b|}\pi(x; L/K, C_b)\,.$$

In particular, L/K has an extreme Chebyshev bias relatively to (C_a, C_b).

Unconditional Chebyshev bias

Example

Let $G := \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle \subset \mathfrak{S}_4 =: G^+$. Then G is isomorphic to the Dihedral group D_8 of order 8. If $a = (1\ 2)(3\ 4)$ and $b = (1\ 3)(2\ 4)$, then a has no square roots ($r_2(a) = 0$) and b has 2 square roots ($r_2(b) = 2$). Also, a and b are conjugates in G^+. Thus, if L is a Galois extension over $\mathbb{Q}$ with group $\mathfrak{S}_4$ and $K = L^G$, applying the Theorem of Fiorilli and Jouve we see that L/K has an extreme Chebyshev bias relatively to (C_a, C_b).

Unconditional Chebyshev bias

Example

Let $G := \langle (1\ 2\ 3\ 4), (1\ 2)(3\ 4) \rangle \subset \mathfrak{S}_4 =: G^+$. Then G is isomorphic to the Dihedral group D_8 of order 8. If $a = (1\ 2)(3\ 4)$ and $b = (1\ 3)(2\ 4)$, then a has no square roots ($r_2(a) = 0$) and b has 2 square roots ($r_2(b) = 2$). Also, a and b are conjugates in G^+. Thus, if L is a Galois extension over $\mathbb{Q}$ with group $\mathfrak{S}_4$ and $K = L^G$, applying the Theorem of Fiorilli and Jouve we see that L/K has an extreme Chebyshev bias relatively to (C_a, C_b).

Can we generalize the Theorem of Fiorilli and Jouve to more groups ?

Unconditional Chebyshev bias

Theorem (H. 2024)

Let G be a finite group and let k be a number field. Consider the injection $G \hookrightarrow \mathfrak{S}(G) =: G^+$ (the group of permutations of G), given by the action of G on itself by left translation. Let L denote a Galois extension of k with group G^+ and let $K = L^G$ be the subextension of L/k fixed by G. Then, for all $a, b \in G$ with the same order, with respective conjugacy classes C_a and C_b, one of the following cases occurs :

1. *either for all $x \geq 2$:*
$$\frac{1}{|C_a|}\pi(x; L/K; C_a) = \frac{1}{|C_b|}\pi(x; L/K; C_b)\,,$$
2. *or there exists $A > 0$ such that, up to exchanging C_a and C_b, we have for all $x \geq A$,*
$$\frac{1}{|C_a|}\pi(x; L/K; C_a) > \frac{1}{|C_b|}\pi(x; L/K; C_b)\,.$$

Thus, L/K has an extreme Chebyshev bias relatively to (C_a, C_b)

Unconditional Chebyshev bias

1. If G is not isomorphic to $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{S}_3$, then there exists elements $a, b \in G$ with the same order such that $C_a \neq C_b$.

Unconditional Chebyshev bias

1. If G is not isomorphic to $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{S}_3$, then there exists elements $a, b \in G$ with the same order such that $C_a \neq C_b$.
2. The first case is true if and only if for all square-free $\ell \geq 2$ we have $r_\ell(a) = r_\ell(b)$.

Unconditional Chebyshev bias

1. If G is not isomorphic to $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{S}_3$, then there exists elements $a, b \in G$ with the same order such that $C_a \neq C_b$.
2. The first case is true if and only if for all square-free $\ell \geq 2$ we have $r_\ell(a) = r_\ell(b)$.
3. When the first case hold we have $\delta(L/K; C_a, C_b) = \delta(L/K; C_b, C_a) = 0$.

Unconditional Chebyshev bias

1. If G is not isomorphic to $\mathfrak{S}_1$, $\mathfrak{S}_2$ or $\mathfrak{S}_3$, then there exists elements $a, b \in G$ with the same order such that $C_a \neq C_b$.
2. The first case is true if and only if for all square-free $\ell \geq 2$ we have $r_\ell(a) = r_\ell(b)$.
3. When the first case hold we have $\delta(L/K; C_a, C_b) = \delta(L/K; C_b, C_a) = 0\,.$
4. When the second case hold we have

$$1 \in \{\delta(L/K; C_a, C_b), \delta(L/K; C_b, C_a)\}\,.$$

Unconditional Chebyshev bias

Theorem (H.)

Let G be a finite abelian group and let k be a number field. Consider the injection $G \hookrightarrow \mathfrak{S}(G) =: G^+$ (the group of permutations of G), given by the action of G on itself by left translation. Let L denote a Galois extension of k with group G^+ and let $K = L^G$ be the subextension of L/k fixed by G. Then there exists elements $a, b \in G$ with $\mathrm{ord}(a) = \mathrm{ord}(b)$ such that L/K has an extreme Chebyshev bias relative to $(C_a = \{a\}, C_b = \{b\})$ if and only if $G \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times H$ where $1 \leq n < m$ and H is a finite group.

Unconditional Chebyshev bias

Theorem (H.)

Let G be a finite abelian group and let k be a number field. Consider the injection $G \hookrightarrow \mathfrak{S}(G) =: G^+$ (the group of permutations of G), given by the action of G on itself by left translation. Let L denote a Galois extension of k with group G^+ and let $K = L^G$ be the subextension of L/k fixed by G. Then there exists elements $a, b \in G$ with $\mathrm{ord}(a) = \mathrm{ord}(b)$ such that L/K has an extreme Chebyshev bias relative to $(C_a = \{a\}, C_b = \{b\})$ if and only if $G \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times H$ where $1 \leq n < m$ and H is a finite group.

Example

Let p be a prime and assume that G is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^m$. Let $L/K/k$ as in the previous theorem. Then, for all $a, b \in G$ such that $\mathrm{ord}(a) = \mathrm{ord}(b)$ and for all $x \geq 2$, we have

$$\pi(x; L/K; \{a\}) = \pi(x; L/K; \{b\}) \,.$$

Elements of the proof

Consider a tour $L/K/k$ of number fields such that L/k is Galois of group G^+ and denote $G = \mathrm{Gal}(L/K)$. If $t : G \to \mathbb{C}$ is a class function, that is for all $a, g \in G$ we have $t(gag^{-1}) = t(a)$, we denote

$$\pi(x; L/K, t) := \sum_{N\mathfrak{p} \leq x} t(\varphi_{\mathfrak{p}}),$$

$$\theta(x; L/K, t) := \sum_{N\mathfrak{p} \leq x} t(\varphi_{\mathfrak{p}}) \log N\mathfrak{p},$$

$$\psi(x; L/K, t) := \sum_{\substack{\mathfrak{p}, m \\ N\mathfrak{p}^m \leq x}} t(\varphi_{\mathfrak{p}}^m) \log N\mathfrak{p}\,.$$

Elements of the proof

We denote $t^+ := \mathrm{Ind}_G^{G^+} t$ the induced class function by t on G^+. Recall that for all $a \in G^+$ we have :

$$t^+(a) := \frac{1}{|G|} \sum_{\substack{g \in G^+ \\ g^{-1}ag \in G}} t(g^{-1}ag)$$

Elements of the proof

We denote $t^+ := \mathrm{Ind}_G^{G^+} t$ the induced class function by t on G^+. Recall that for all $a \in G^+$ we have :

$$t^+(a) := \frac{1}{|G|} \sum_{\substack{g \in G^+ \\ g^{-\mathbf{1}} ag \in G}} t(g^{-1}ag)$$

Lemma

For all $x \geq 2$ we have $\psi(x; L/K, t) = \psi(x; L/k, t^+)$.

Elements of the proof

We denote $t^+ := \mathrm{Ind}_G^{G^+} t$ the induced class function by t on G^+. Recall that for all $a \in G^+$ we have :

$$t^+(a) := \frac{1}{|G|} \sum_{\substack{g \in G^+ \\ g^{-1}ag \in G}} t(g^{-1}ag)$$

Lemma

For all $x \geq 2$ we have $\psi(x; L/K, t) = \psi(x; L/k, t^+)$.

Let $a, b \in G$ and denote C_a, C_b their respective conjugacy classes. We denote $t_{a,b} = \frac{|G|}{|C_a|} \mathbb{1}_{C_a} - \frac{|G|}{|C_b|} \mathbb{1}_{C_b}$. We note that a and b are conjugates in G^+ if and only if $t^+_{a,b} = 0$. Define $f_\ell : G \to G$ by $f_\ell(g) = g^\ell$.

Elements of the proof

Lemma

With the previous notations, we have :

1. *Assume there exists $d \geq 2$ square-free such that $r_d(a) \neq r_d(b)$ and that for $1 \leq \ell < d$ square-free, one has $(t_{a,b} \circ f_\ell)^+ = 0$. Then we have :*

$$\pi(x; L/K; t_{a,b}) = \mu(d)(r_d(a) - r_d(b))\frac{x^{\frac{1}{d}}}{\log x} + o\left(\frac{x^{\frac{1}{d}}}{\log x}\right)$$

   where μ is the Möbius function.

2. *Assume that for all square-free $\ell \geq 1$ we have $(t_{a,b} \circ f_\ell)^+ = 0$. Then, for every $x \geq 2$, we have :*

$$\pi(x; L/K; t_{a,b}) = 0\,.$$

Elements of the proof

Lemma

With the previous notations, we have :

1. *Assume there exists $d \geq 2$ square-free such that $r_d(a) \neq r_d(b)$ and that for $1 \leq \ell < d$ square-free, one has $(t_{a,b} \circ f_\ell)^+ = 0$. Then we have :*

$$\pi(x; L/K; t_{a,b}) = \mu(d)(r_d(a) - r_d(b))\frac{x^{\frac{1}{d}}}{\log x} + o\left(\frac{x^{\frac{1}{d}}}{\log x}\right)$$

   where μ is the Möbius function.

2. *Assume that for all square-free $\ell \geq 1$ we have $(t_{a,b} \circ f_\ell)^+ = 0$. Then, for every $x \geq 2$, we have :*

$$\pi(x; L/K; t_{a,b}) = 0\,.$$

To conclude our main theorems, we consider the case where $G^+ \simeq \mathfrak{S}(G)$. We relate conditions $(t_{a,b} \circ f_\ell)^+ = 0$ to $r_\ell(a) = r_\ell(b)$, then we apply the previous Lemma.

Elements of the proof

Démonstration.

Applying the inclusion-exclusion principle we see that

$$\theta(x; L/K, t) = \sum_{\ell \geq 1} \mu(\ell)\psi(x^{\frac{1}{\ell}}; L/K, t \circ f_\ell)\,. \tag{1}$$

Démonstration.

Applying the inclusion-exclusion principle we see that

$$\theta(x; L/K, t) = \sum_{\ell \geq 1} \mu(\ell) \psi(x^{\frac{1}{\ell}}; L/K, t \circ f_\ell) . \tag{1}$$

By the induction property for all square-free $\ell \geq 1$ such that $(t_{a,b} \circ f_\ell)^+ = 0$ we have for all $x \geq 2$ $\psi(x^{\frac{1}{\ell}}; L/K, t_{a,b} \circ f_\ell) = 0$.

Elements of the proof

Démonstration.

Applying the inclusion-exclusion principle we see that

$$\theta(x; L/K, t) = \sum_{\ell \geq 1} \mu(\ell)\psi(x^{\frac{1}{\ell}}; L/K, t \circ f_\ell)\,. \tag{1}$$

By the induction property for all square-free $\ell \geq 1$ such that $(t_{a,b} \circ f_\ell)^+ = 0$ we have for all $x \geq 2$ $\psi(x^{\frac{1}{\ell}}; L/K, t_{a,b} \circ f_\ell) = 0$.
If $d \geq 2$ is a square-free integer such that $r_d(a) \neq r_d(b)$, applying the Chebotarev Theorem we deduce that $\psi(x^{\frac{1}{d}}; L/K; t_{a;b} \circ f_d) = (r_d(a) - r_d(b))x^{\frac{1}{d}} + o(x^{\frac{1}{d}})\,.$

Elements of the proof

Démonstration.

Applying the inclusion-exclusion principle we see that

$$\theta(x; L/K, t) = \sum_{\ell \geq 1} \mu(\ell)\psi(x^{\frac{1}{\ell}}; L/K, t \circ f_\ell)\,. \tag{1}$$

By the induction property for all square-free $\ell \geq 1$ such that $(t_{a,b} \circ f_\ell)^+ = 0$ we have for all $x \geq 2$ $\psi(x^{\frac{1}{\ell}}; L/K, t_{a,b} \circ f_\ell) = 0$.
If $d \geq 2$ is a square-free integer such that $r_d(a) \neq r_d(b)$, applying the Chebotarev Theorem we deduce that $\psi(x^{\frac{1}{d}}; L/K; t_{a;b} \circ f_d) = (r_d(a) - r_d(b))x^{\frac{1}{d}} + o(x^{\frac{1}{d}})\,.$
It is easy to see that $\sum_{\ell > d} \mu(\ell)\psi(x^{\frac{1}{\ell}}; L/K, t_{a,b} \circ f_\ell) = o(x^{\frac{1}{d}})$.
Thus,

$$\theta(x; L/K, t_{a,b}) = \mu(d)(r_d(a) - r_d(b))x^{\frac{1}{d}} + o(x^{\frac{1}{d}})\,.$$

We conclude by a summation by parts.

□

Thank you.