Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

ON THE INFLUENCE OF THE GALOIS GROUP STRUCTURE ON THE CHEBYSHEV BIAS IN NUMBER FIELDS

Mounir Hayani

Tome 153
Fascicule 3

2025

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 793-829

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 3, tome 153, septembre 2025

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
`commandes@smf.emath.fr`

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 50 € ($ 75)
Abonnement électronique : 165 € ($ 247),
avec supplément papier : Europe 251 €, hors Europe 289 € ($ 433)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
`bulletin@smf.emath.fr` • `smf.emath.fr`

ISSN 0037-9484 (print) 2102-622X (electronic)

Directrice de la publication : Isabelle GALLAGHER

Bull. Soc. Math. France
153 (3), 2025, p. 793-829

ON THE INFLUENCE OF THE GALOIS GROUP STRUCTURE ON THE CHEBYSHEV BIAS IN NUMBER FIELDS

BY MOUNIR HAYANI

ABSTRACT. — In this paper, we produce unconditionally new instances of Galois number field extensions exhibiting strong discrepancies in the distribution of Frobenius elements among conjugacy classes of the Galois group. We first prove an inverse Galois theoretical statement showing a dichotomy between "extreme Chebyshev biases" and "equal prime ideal counting". We further introduce a group theoretic property that implies extreme biases. In the case of abelian extensions, this leads to a complete characterization of Galois groups enabling extreme biases. In the case where the Galois group is a p-group, a simple criterion is deduced for the existence of extreme biases, and associated effective statements of Linnik type are obtained.

RÉSUMÉ (*Sur l'influence de la structure du groupe de Galois sur le biais de Tchebychev dans les corps de nombres*). — Dans cet article, nous produisons inconditionnellement de nouveaux exemples d'extensions galoisiennes de corps de nombres qui présentent de fortes disparités dans la répartition des éléments de Frobenius parmi les classes de conjugaison du groupe de Galois. Nous prouvons d'abord un énoncé de théorie inverse de Galois mettant en évidence une dichotomie entre "biais de Tchebychev extrêmes" et "comptage égal d'idéaux premiers". Nous introduisons ensuite une propriété de théorie des groupes qui implique de tels biais extrêmes. Dans le cas des extensions abéliennes, cela conduit à une caractérisation complète des groupes de Galois pour lesquels ces biais extrêmes peuvent exister. Lorsque le groupe de Galois est un p-groupe, nous établissons un critère simple assurant l'existence de biais extrêmes et obtenons des énoncés effectifs de type Linnik correspondants.

Texte reçu le 14 mai 2024, modifié le 3 novembre 2024, accepté le 26 novembre 2024.

MOUNIR HAYANI, Institut de mathématiques de Bordeaux, Université de Bordeaux, Talence, 33400, France • *E-mail :* `mounir.hayani@math.u-bordeaux.fr`

Mathematical subject classification (2010). — 11K38, 11N05, 11R32, 11R42, 20B30.

Key words and phrases. — Chebyshev's bias, prime number races, Artin L-functions, inverse Galois theory.

doi:10.24033/bsmf.2911

1. Introduction and statement of results

1.1. Background on Chebyshev's bias. — In 1896, de La Vallée Poussin proved that for every $q \geq 2$, prime numbers are uniformly distributed among invertible residue classes modulo q. More precisely, denoting

$$\pi(x; q, a) = \#\{p \text{ prime} \colon p \leq x,\ p \equiv a \bmod q\} \quad (x \geq 2),$$

where $(a, q) = 1$, the prime number theorem in arithmetic progressions asserts that

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

Half a century before, examining the specific case of $q = 4$, Chebyshev sought to conduct a more detailed comparison between prime numbers $p \equiv 1 \bmod 4$ and prime numbers $p \equiv 3 \bmod 4$. In a letter sent to Fuss [5], Chebyshev noted that for a given $x \geq 2$, the quantity $\pi(x; 4, 3)$ seems to be greater than $\pi(x; 4, 1)$. Since then, this discrepancy has been referred to as *Chebyshev's bias.*

In [15] Rubinstein and Sarnak studied, for any $q \geq 3$, the general question of Chebyshev's bias between invertible classes modulo q. Under the generalized Riemann hypothesis and a linear independence assumption on non-trivial zeros of Dirichlet L-functions, they proved that for $q \geq 3$ and $a \neq b$ two invertible classes modulo q, the *logarithmic density*

$$\delta(q; a, b) := \lim_{X \to +\infty} \frac{1}{\log(X)} \int_2^X \mathbb{1}_{\pi(x;q,a) > \pi(x;q,b)}(t) \frac{\mathrm{d}t}{t}$$

exists. Moreover, they confirmed Chebyshev's original observation of the existence of a bias towards a (that is, $\delta(q; a, b) > \frac{1}{2}$) if and only if a is not a quadratic residue mod q, and b is a quadratic residue mod q.

Following the ideas of Rubinstein and Sarnak, Ng [14] studied Chebyshev's bias in the context of number fields. Let L/K be a Galois extension of number fields, with group G. Consider $t \colon G \to \mathbb{C}$ a class function on G. Define the prime ideal counting function for any $x \geq 2$:

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

Here, the sum runs over non-zero prime ideals $\mathfrak{p}$ of O_K, and $\varphi_{\mathfrak{p}}$ denotes the corresponding Frobenius conjugacy class defined up to inertia. In order to unify the treatment of ramified and unramified prime ideals we use the standard definition (*e.g.*, used in [9, page 28]) valid for any $k \geq 1$:

$$t(\varphi_{\mathfrak{p}}^k) := \frac{\sum_{s \in I_{\mathfrak{P}/\mathfrak{p}}} t(\varphi_{\mathfrak{p}}^k s)}{|I_{\mathfrak{P}/\mathfrak{p}}|}\,,$$

where $\mathfrak{P}$ is a prime of O_L lying above $\mathfrak{p}$, and $I_{\mathfrak{P}/\mathfrak{p}}$ denotes the inertia group attached to $\mathfrak{P}/\mathfrak{p}$.

For two conjugacy classes C_1, C_2 of G we define the class function on G:

$$t_{C_1,C_2} = \frac{|G|}{|C_1|}\mathbb{1}_{C_1} - \frac{|G|}{|C_2|}\mathbb{1}_{C_2}\,, \tag{1}$$

where $\mathbb{1}_{C_i}$ is the indicator function of C_i. Denoting $\mathcal{P}_{C_1,C_2} := \{x \geq 2\colon \pi\,(x; L/K; t_{C_1,C_2}) > 0\}$, the logarithmic density of $\mathcal{P}_{C_1,C_2}$ (when it exists) is the generalization to Galois extensions of number fields of $\delta(q;a,b)$, that is,

$$\delta(\mathcal{P}_{C_1,C_2}) := \lim_{X\to+\infty}\frac{1}{\log X}\int_2^X \mathbb{1}_{\mathcal{P}_{C_1,C_2}}(x)\frac{\mathrm{d}x}{x}\,.$$

In his thesis [14], Ng studied densities of type $\delta(\mathcal{P}_{C_1,C_2})$. Assuming Artin's holomorphy conjecture, GRH, as well as a linear independence assumption on the set of zeros of Artin L-functions, in [14] Ng proved the existence of $\delta(\mathcal{P}_{C_1,C_2})$ and computed its value in several explicit cases. Since then, the study of $\delta(\mathcal{P}_{C_1,C_2})$ has seen numerous developments (see, *e.g.*, [6, 1, 9]). Devin ([6, Th. 2.5]) established conditionally to assumptions of the same type (although substantially weaker than the hypotheses made in [14]) that $0 < \delta(\mathcal{P}_{C_1,C_2}) < 1$. In particular, the expected (but unproved) diophantine properties of Artin L-function zeros prevent extreme biases occurring (see Definition 1.1).

In this paper, we will study in the context of normal number field extensions, settings where the assumptions of [6, Th. 2.5] are not met, thereby producing the following phenomenon.

Definition 1.1 (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, one has $\pi(x; L/K; t_{C_1,C_2}) > 0$ for big enough x, and hence, in particular, $\delta(\mathcal{P}_{C_1,C_2})$ exists and is equal to 1.

In [1, §1.3], Bailleul explains that Ng's linear independence (LI) assumption cannot hold in general for a relative extension of number fields L/K. Instead, Bailleul suggests in the case $K = \mathbb{Q}$ a refined version of LI under which he computes $\delta(\mathcal{P}_{C_1,C_2})$ for some families of normal extensions (with dihedral and quaternion Galois groups). In [9], Fiorilli and Jouve give a detailed probabilistic study of the fluctuations of the error term in the Chebotarev density theorem within families of normal number field extensions and obtain general estimates for $\delta(\mathcal{P}_{C_1,C_2})$ that they apply (under assumptions analogous to those used in [14] or [1]) to various Galois group structures (Abelian, supersolvable, $\mathfrak{S}_n$,...).

In strong contrast with the framework of [6, 1, 9], Fiorilli and Jouve ([8]) show unconditionally that there exist infinitely many Galois extensions of number fields having an extreme Chebyshev bias. More precisely, they prove, for a tower $L/K/\mathbb{Q}$ of number fields such that $L/\mathbb{Q}$ is Galois with group G^+, that if two conjugacy classes C_1 and C_2 in $G = \mathrm{Gal}(L/K)$ *do not* have the same number of square roots[1] in G but are contained in a common conjugacy class C^+ of G^+, then L/K has an extreme Chebyshev bias with respect to C_1 and C_2 (see [8, Th. 1.1]). Natural questions that arise are the following.

a) Can we produce extreme Chebyshev biases in the case of conjugacy classes with *the same* number of square roots and contained in a common conjugacy class of G^+?

b) Is it possible to classify the group structures enabling such extreme biases (see [8, §2, Remark])?

The main goal in this paper is to answer these questions. We now state our main results.

1.2. Statement of the main results. — Our main contributions can be split into two different settings: first we let k be an arbitrary number field and G be an arbitrary finite group. Denoting by $\mathfrak{S}(G)$ the group of all permutations of elements of G, our first results are stated in the setting of the *Cayley embedding* of G into $\mathfrak{S}(G)$, (*i.e.*, we let G act on itself by left translation giving rise to an injective group homomorphism $G \to \mathfrak{S}(G)$). Letting L be a Galois extension of k of group $G^+ \simeq \mathfrak{S}(G)$ and denoting $K = L^G$, we obtain unconditional results on discrepancies for the distribution of Frobenius elements in conjugacy classes of $G = \mathrm{Gal}(L/K)$. The second framework for our main results aims at relaxing the assumption according to which $G \hookrightarrow G^+$ is the Cayley embedding. For example, we will produce an infinite family of abelian groups G exhibiting an extreme Chebyshev bias that is Galois groups of an extension L/K such that the degree of K over $\mathbb{Q}$ is exactly 4. We will also produce extreme Chebyshev biases for subextensions of Galois extensions L/k of prime power degree.

We will use the following notation: given a group G and $g \in G$, we denote by $\mathrm{ord}(g)$ the order of g in G. Moreover, if $D \subset G$ is a conjugacy invariant subset, we will write $\pi(x; L/K, D)$ as a shorthand for $\pi(x; L/K, \mathbb{1}_D)$.

1.2.1. *Cayley embedding and Chebyshev biases in number fields.* — Our first main result uncovers the following dichotomy phenomenon.

Theorem 1.2. — *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 $a, b \in G$ such that* $\mathrm{ord}(a) = \mathrm{ord}(b)$, *with respective conjugacy classes C_a and C_b, one of the following cases occurs:*

1. *Either for all $x \geq 2$:*

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

1. One can easily see that the count of square roots is a class function on any group.

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 with respect to C_a and C_b.

When G is not isomorphic to the symmetric groups $\mathfrak{S}_1, \mathfrak{S}_2, \mathfrak{S}_3$, then G always contains two elements a and b of the same order that are not in the same conjugacy class (see [7, Corollary B.2]). Thus, given any group G of order at least 3 and not isomorphic to $\mathfrak{S}_3$, Theorem 1.2 answers a non-trivial Chebyshev bias question in a specific Galois extension L/K with Galois group G.

Remark 1.3. — Having distinct prime counting functions coincide at every value of x (as in Theorem 1.2(1)) is counterintuitive. Certainly, such a phenomenon does not occur when counting rational primes in distinct arithmetic progressions. In our setting, however, one must keep in mind that multiple prime ideals can share the same norm. Furthermore, in certain situations, a purely algebraic proof of this equality is possible (see, for instance, Corollary 2.4 and its proof).

The proof of Theorem 1.2 will be obtained as a consequence of a more general statement (Theorem 2.9) that makes precise under which condition (1) (resp. (2)) of Theorem 1.2 occurs. This distinction relies entirely on group theoretic properties of the conjugacy classes C_1 and C_2. The following statement gives an instance of both alternatives appearing in Theorem 1.2.

Corollary 1.4. — *With notation as in Theorem 1.2, we have:*

1. *If $G = Q_8$ is the quaternion group of order 8, then, for all $a, b \in G$ such that* $\mathrm{ord}(a) = \mathrm{ord}(b)$*, with respective conjugacy classes C_a and C_b, we have for all $x \geq 2$:*
$$\pi(x; L/K; C_a) = \pi(x; L/K; C_b)\,.$$
2. *If $G = Q_8 \times \mathbb{Z}/4\mathbb{Z}$, then denoting $a = (1, \bar{2})$,$b = (-1, 0)$ and C_a, C_b their respective conjugacy classes, the extension L/K has an extreme Chebyshev bias relatively to (C_a, C_b). More precisely, for all x sufficiently large, we have:*
$$\pi(x; L/K; C_a) > \pi(x; L/K; C_b)\,.$$

As a second illustration, we present another family of groups giving rise to an extreme Chebyshev bias.

Corollary 1.5. — *With notation as in Theorem 1.2, assume that $G = (\mathbb{Z}/p^m\mathbb{Z} \rtimes \mathbb{Z}/p^n\mathbb{Z}) \times H$, where p is a prime, $1 \leq n < m$ and $(H, +)$ is a finite group (e.g., G is a dihedral group). Let $a = (0, 1, 0)$, $b = (p^{m-n}, 0, 0)$ and*