The least prime with a given factorization type

Peter Jaehyun Cho
Department of Mathematical Sciences, Ulsan National Institute of Science and Technology

1 Introduction

This article reviews the paper "The least prime with a given cycle type" [1] by the author, Lemke Oliver and Zaman. Let k be a number field, and K/k be a Galois extension with Galois group G. The Frobenius density theorem (a precursor to the Chebotarev density theorem) implies that as the prime ideal $\mathfrak{p}$ of the field k varies, the cycle type of $\mathrm{Frob}_\mathfrak{p}$ is equidistributed; more concretely, it states for any cycle type λ occuring in G that

$$\frac{\#\{\mathrm{N}\mathfrak{p} \le x : \mathrm{Frob}_\mathfrak{p} \text{ has cycle type } \lambda\}}{\#\{\mathrm{N}\mathfrak{p} \le x\}} \sim \frac{\#\{\sigma \in G : \sigma \text{ has cycle type } \lambda\}}{|G|}$$

as $x \to \infty$. Our interest is to bound the smallest prime $\mathfrak{p}$ for which $\mathrm{Frob}_\mathfrak{p}$ has cycle type λ. Among the results in [1], in this review paper, we introduce the following main result only.

Theorem 1.1. *Let K/k be a Galois extension of number fields with $\mathrm{Gal}(K/k) \cong S_n$ for some $n \ge 2$. For a conjugacy class $C \subset S_n$, let $\ell_1, \dots, \ell_m \ge 2$ denote the lengths of the nontrivial cycles in C, and define*

$$\alpha(S_n, C) := 2^{m-1} \prod_{i=1}^{m} \frac{(\ell_i - 2)2^{\ell_i - 2} + 1}{\ell_i!}.$$

Then for any $\epsilon > 0$, there is a prime $\mathfrak{p}$ of k, unramified in K, with $\mathrm{Frob}_\mathfrak{p} \in C$ satisfying

$$\mathrm{N}\mathfrak{p} \ll_{n,[k:\mathbb{Q}],\epsilon} |\mathrm{Disc}(K)|^{\alpha(S_n,C)+\epsilon}.$$

The implied constant is effectively computable if $\epsilon > \frac{2^m \prod_{i=1}^{m}(\ell_i - 1)}{n![k:\mathbb{Q}]}$.

Due to space constraints and the expository nature of this paper, most theorems and lemmas used here will only be stated, and their proofs will be omitted. However, we have clearly highlighted the underlying logic and essential ideas behind the main theorem.

2 The outline and ideas for the Proof of Theorem 1.1

People used to take advantage of zero-free regions for appropriate L-functions to bound the smallest prime. In [1], we reduce this problem to First Sign Change problem. First, let us introduce a new term: rational equivalence class. Given a finite group G, two elements $g, h \in G$ are *rationally equivalent* if they generate conjugate cyclic subgroups. If g and h are conjugate, then they are also rationally equivalent, so each rational equivalence class breaks up as a union of conjugacy classes. In the symmetric group S_n, two elements are rationally equivalent if and only if they are conjugate, so each rational equivalence class consists of a single conjugacy class, but this need not be true for arbitrary G.

The following theorem states that if we can find characters with certain desirable properties, we can obtain a strong bound.

Theorem 2.1. *Let K/k be a Galois extension of number fields with $G = \mathrm{Gal}(K/k)$. For a rational equivalence class $C \subset G$, assume there exists characters Ψ_+ and Ψ_- of G such that:*

1. *the difference $\Psi_+ - \Psi_-$ is supported on elements of the rational class C;*
2. *the Artin L-function $L(s, \Psi_+)$ is entire apart from a simple pole at $s = 1$; and*
3. *the Artin L-function $L(s, \Psi_-)$ is entire.*

For $A \geq 2$ and $0 < \epsilon < 1$, there exists a sufficiently small constant $b > 0$ and sufficiently large constant $B > 0$ which depend at most on $\Psi_+(1), \Psi_-(1), [k : \mathbb{Q}], A$, and ϵ, such that if

$$x \geq B\Big(\big(\operatorname*{Res}_{s=1} L(s, \Psi_+) \big)^{-A} \max\{q(\Psi_+), q(\Psi_-)\}^{1/2} \Big)^{1+\epsilon}, \tag{2.1}$$

then there exists at least $b(\log x)^A$ prime ideals $\mathfrak{p}$ of k whose norm $\mathrm{N}\mathfrak{p}$ is a rational prime not dividing $|\mathrm{Disc}(K)|$ (and hence $\mathfrak{p}$ is unramified in K), and $\sigma_{\mathfrak{p}} = C$.

To obtain an effective constant for the smallest prime problem using Theorem 2.1, we need an effective lower bound on the residue of Artin L-function $L(s, \Psi_+)$ at $s = 1$. For this, we appeal to the following lemma.

Lemma 2.2. *Let K/k be a Galois extension of number fields with $G = \mathrm{Gal}(K/k)$. Let χ be any character of G with $\langle \chi, \mathbf{1}_G \rangle = 1$. Let $\nu(\chi)$ be the maximum multiplicity $\langle \chi, \psi \rangle$ over all trivial or quadratic characters ψ of G whose Artin L-function $L(s, \psi)$ has a real zero $\beta_\psi > 1 - \frac{1}{4 \log |\mathrm{Disc}(K)|}$. For $\epsilon > 0$,*

$$\operatorname*{Res}_{s=1} L(s, \chi) \gg_{\chi(1), |G|, [k:\mathbb{Q}], \epsilon} |\mathrm{Disc}(K)|^{-\epsilon},$$

where the implied constant is effectively computable if $\epsilon > \frac{\nu(\chi)}{[K:\mathbb{Q}]}$.

From Theorem 2.1, we can see that the crucial thing is to construct such characters with small analytic conductors. The following lemma enables us to find candidates.

Lemma 2.3. *Let G be a finite group, let $g \in G$, and let $\langle g \rangle \leq G$ be the cyclic subgroup generated by g. Let $\xi \colon \langle g \rangle \to \mathbb{C}^\times$ be the unique irreducible character of $\langle g \rangle$ such that $\xi(g) = \exp\left(\frac{2\pi i}{n}\right)$, where $n := |g|$. Define a class function ϕ_g of $\langle g \rangle$ by means of the expression*

$$\phi_g := \prod_{p \mid n} \left(1 - \xi^{\frac{n}{p}}\right), \tag{2.2}$$

and let $\Delta_g := \mathrm{Ind}_{\langle g \rangle}^G \phi_g$.

Then, as a class function of G, Δ_g is a non-zero function supported on the rational equivalence class of g. Moreover, $\langle \Delta_g, \chi \rangle$ is an integer for every irreducible character χ of G.

Proof. We first observe that $\phi_g(g^i) = 0$ unless $\gcd(i, n) = 1$, for if not, there is some prime $p \mid \gcd(i, n)$, and we would have $\xi^{n/p}(g^i) = 1$ and hence that $1 - \xi^{n/p}(g^i) = 0$. As a result, ϕ_g is supported on the generators of the cyclic group $\langle g \rangle$, and hence its induction Δ_g is supported on the conjugates of these generators, which together comprise exactly the rational equivalence class of g. To see that Δ_g is non-zero, we observe that $\langle \phi_g, \mathbf{1}_{\langle g \rangle} \rangle_{\langle g \rangle} = 1$, so that, by Frobenius reciprocity, we find that $\langle \Delta_g, \mathbf{1}_G \rangle_G = 1$ as well. This implies that $\Delta_g \neq 0$. The final claim follows on observing that ϕ_g is a difference of characters, so Δ_g must be too. □

By Lemma 2.3, we can take

$$\Psi_+ := \mathrm{Ind}_{\langle g\rangle}^G \left[\sum_{d|n} \frac{\mu(d)^2 + \mu(d)}{2} \xi^{\sum_{p|d} \frac{n}{p}} \right]$$

and

$$\Psi_- := \mathrm{Ind}_{\langle g\rangle}^G \left[\sum_{d|n} \frac{\mu(d)^2 - \mu(d)}{2} \xi^{\sum_{p|d} \frac{n}{p}} \right].$$

The drawback of these two characters is that they may share a common component. However, even if we remove them, the property that the two characters take the same values—except on our fixed rational equivalence class—is preserved. Under this observation, we may take

$$\Psi_+ = \sum_{\chi \in \mathrm{Irr}(G)} \max\{\langle \chi, \Delta_g\rangle, 0\} \cdot \chi$$

and

$$\Psi_- = -\sum_{\chi \in \mathrm{Irr}(G)} \min\{\langle \chi, \Delta_g\rangle, 0\} \cdot \chi$$

If we know that $L(s, \Psi_+)$ is entire except at $s = 1$ and $L(s, \Phi_-)$ is entire, we can use them. In general, however, we cannot guarantee their holomorphicity. In S_n case, we overcome this issue by adding a suitable character to them.

In some cases, we can determine the multiplicities $< \chi, \Delta_g >$ of characters χ in Δ_g explicitly.

Lemma 2.4. *Let G, g, and Δ_g be as in Lemma 2.3. Then for any irreducible character χ of G that is constant on the rational class of g, we have*

$$\langle \Delta_g, \chi\rangle = \chi(g).$$

In particular, if the rational class of g comprises a single conjugacy class, then Δ_g is $|C_G(g)|$ times the indicator function of the conjugacy class of g, where $C_G(g)$ denotes the centralizer of g in G.

Also, we need a good upper bound for analytic conductors $q(\psi)$ of the character ψ over k. We can reply on the following lemma.

Lemma 2.5. *Let χ be a character of the finite group G. Then*

$$v_{\mathfrak{p}}(\mathfrak{f}_\chi) \le \frac{2\chi(1)}{|G|} v_{\mathfrak{p}}(\mathfrak{D}_{K/k}).$$

Proof. For a general character χ of G, not necessarily irreducible, the Artin conductor $\mathfrak{f}_\chi$ is an ideal of k defined locally by

$$\mathfrak{f}_\chi = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{f}_\chi)}, \tag{2.3}$$

where

$$v_{\mathfrak{p}}(\mathfrak{f}_\chi) = \sum_{i \ge 0} \frac{|G_i|}{|G_0|} \left(\chi(1) - \frac{1}{|G_i|} \sum_{\sigma \in G_i} \chi(\sigma) \right), \tag{2.4}$$

with G_i for $i \geq 0$ being the (lower) ramification groups associated with a prime of K lying over $\mathfrak{p}$ [3, VI §2 Corollary 1]. Using the trivial inequality $|\chi(\sigma)| \leq \chi(1)$, it follows from (2.4) that

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{f}_\chi) &= \frac{1}{|G_0|} \sum_{i \geq 0} \left((|G_i| - 1)\chi(1) - \sum_{\substack{\sigma \in G_i \\ \sigma \neq 1}} \chi(\sigma) \right) \\ &\leq \frac{1}{|G_0|} \sum_{i \geq 0} 2\chi(1)(|G_i| - 1) \\ &= \frac{2\chi(1)}{|G|} v_{\mathfrak{p}}(\mathfrak{D}_{K/k}), \end{aligned}$$

as claimed. □

We are ready to prove Theorem 1.1. We consider only the case of n-cycle $C = [(1, 2, 3, 4, \ldots, n)]$ only. For a general conjugacay class, we refer the reader to the original article [1] under review.

By means of their cycle decomposition, conjugacy classes of S_n are in correspondence with partitions μ of n. As is standard, we will write $\mu \vdash n$ to denote that μ is a partition of n.

The irreducible characters of S_n are also naturally in correspondence with partitions of n, and if $\lambda \vdash n$, then the *hook length formula* gives a formula for the degree of the character χ_λ associated with λ. Consider the Ferrers diagram associated with λ. A *hook* η in λ is associated with a cell in the Ferrers diagram, and consists of the cell, all cells below it in the same column, and all cells to its right in the same row. The length of the hook is the number of cells in the hook, which we shall denote by $|\eta|$. There are n hooks $\eta_1, \ldots, \eta_n$ associated with any partition $\lambda \vdash n$, and the hook length formula [2, Formula 4.12] states that

$$\chi_\lambda(1) = \frac{n!}{\prod_{i=1}^n |\eta_i|}.$$

As examples of particular importance to us, for any $0 \leq i \leq n-1$, let $\lambda_i \vdash n$ be the partition consisting of the single part $n - i$, together with i 1's. Thus, the Ferrers diagram of λ_i is itself a single hook, and the characters associated with these λ_i are sometimes referred to as hook characters. Let $\chi_i := \chi_{\lambda_i}$ be the character of λ_i, we find by the hook length formula that

$$\chi_i(1) = \binom{n-1}{i}.$$

In particular, χ_0 is the trivial character, and χ_{n-1} is the sign character.

Lemma 2.6. *Let $n \geq 2$ and let $g \in S_n$ be an n-cycle. Let χ be an irreducible character of S_n. Then $\chi(g) = 0$ unless there is $0 \leq i \leq n-1$ such that $\chi = \chi_i$ is the character of S_n associated with the partition $\lambda_i \vdash n$ given by $\lambda_i := (n-i) + 1 + 1 + \cdots + 1$, where there are i 1's. Moreover, for any $0 \leq i \leq n-1$, we have $\chi_i(g) = (-1)^i$ and $\chi_i(1) = \binom{n-1}{i}$.*

Lemmas 2.4 Lemma 2.6 imply

Lemma 2.7. *Let $n \geq 2$ and for each $0 \leq i \leq n-1$, let χ_i be the irreducible character of S_n from Lemma 2.6. Define characters Ψ_+ and Ψ_- of S_n by*

$$\Psi_+ = \sum_{\substack{0 \leq i \leq n-1 \\ i \text{ even}}} \chi_i \quad \text{and} \quad \Psi_- = \sum_{\substack{0 \leq i \leq n-1 \\ i \text{ odd}}} \chi_i.$$

Then the difference $\Psi_+ - \Psi_-$ is supported on the conjugacy class of an n-cycle, and we have $\Psi_+(1) = \Psi_-(1) = 2^{n-2}$.

At this point, we cannot guarantee that the Artin L-functions $L(s, \chi_i)$ and $L(s, \Psi_-)$ are holomorphic. We resolve this issue via the following lemma.

Lemma 2.8. *Let $n \geq 2$, and for each $0 \leq i \leq n-1$, let χ_i be the character of S_n as in Lemma 2.7. Then $\chi_{i-1} + \chi_i$ is a monomial character of S_n for every $1 \leq i \leq n-1$.*

We define

$$\begin{aligned}\Psi_+ &= \chi_0 + \sum_{1 \leq i \leq n-1} 2\left\lceil \frac{i-1}{2} \right\rceil \cdot \chi_i \\ &= \chi_0 + 2(\chi_2 + \chi_3) + 4(\chi_4 + \chi_5) + \dots,\end{aligned}$$

where the summation above ends with $(n-3) \cdot (\chi_{n-3} + \chi_{n-2}) + (n-1)\chi_{n-1}$ if n is odd and with $(n-2) \cdot (\chi_{n-2} + \chi_{n-1})$ if n is even. In either case, since both χ_0 and χ_{n-1} are 1-dimensional characters of S_n and hence monomial, it follows from Lemma 2.8 that Ψ_+ is a non-negative integral linear combination of monomial characters. We also define

$$\begin{aligned}\Psi_- &= \sum_{1 \leq i \leq n-1} \left(2\left\lfloor \frac{i-1}{2} \right\rfloor + 1\right) \cdot \chi_i \\ &= (\chi_1 + \chi_2) + 3(\chi_3 + \chi_4) + \dots,\end{aligned}$$

where the summation ends with $(n-2)(\chi_{n-2} + \chi_{n-1})$ if n is odd and with $(n-3)(\chi_{n-3} + \chi_{n-2}) + (n-1)\chi_{n-1}$ if n is even. As with Ψ_+, Lemma 2.8 implies that Ψ_- is a non-negative linear combination of monomial characters. Moreover, the difference $\Psi_+ - \Psi_- = \chi_0 - \chi_1 + \chi_2 - \dots$ is Δ_g by construction (where g is an n-cycle), so the difference $\Psi_+ - \Psi_-$ is supported on the conjugacy class C. Finally, we observe that

$$\Psi_+(1) = \Psi_-(1) = \frac{\Psi_+(1) + \Psi_-(1)}{2}$$

and that

$$\Psi_+(1) + \Psi_-(1) = 1 + \sum_{i=1}^{n-1} (2i-1)\binom{n-1}{i} = 2 + (n-2)2^{n-1}.$$

Hence, $\Psi_+(1) = \Psi_-(1) = 1 + (n-2)2^{n-2}$, nearly completing the proof if C is an n-cycle. It remains only to note that, since $\mathrm{sgn} = \chi_{n-1}$, $\langle \Psi_+, \mathrm{sgn} \rangle = 2\lceil \frac{n-2}{2} \rceil \leq n-1$. However, we also find it convenient to note here that $\langle \Psi_-, \mathrm{sgn} \rangle = 2\lfloor \frac{n-2}{2} \rfloor + 1 \leq n-1$ as well.

References

[1] P. J. Cho, R. J. Lemke Oliver, and A. Zaman, *The Least Prime with a Given Cycle Type*, preprint, https://doi.org/10.48550/arXiv.2512.24963

[2] W. Fulton and J. D. Harris, *Representation theory*, Graduate Texts in Mathematics Readings in Mathematics, 129, Springer, New York, 1991.

[3] J.-P. Serre, *Local fields*, translated from the French by Marvin Jay Greenberg, Graduate Texts in Mathematics, 67, Springer, New York-Berlin, 1979.

Department of Mathematical Sciences
Ulsan National Institute of Sciecen and Technology
Ulsan 44919
S. Korea
E-mail address: petercho@unist.ac.kr