A supplement to Chebotarev's density theorem

(based on joint work with K. Soundararajan)

Gergely Harcos

Alfréd Rényi Institute of Mathematics
https://users.renyi.hu/∼gharcos/

18 July 2023
1st Analytic Number Theory &
Automorphic Forms Conference in Patras

The original papers of Chebotarev (1923 & 1925)

Известия Российской Академии Наук. 1923.

(Bulletin de l'Académie des Sciences de Russie).

Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок.

Н. Чеботарева.

Представлено академиком Я. В. Успенским в заседании Отделения Физико-Математических Наук 7 марта 1923 года.

I.

Задача, решение которой является целью настоящей работы, была поставлена Frobenius'ом («Über Beziehungen u. s. w.», Sitzungsber. der Berl. Akad., 1896, S. 689). Она состоит в следующем. Дано неприводимое нормальное уравнение n-ой степени

(1) $$f(x) = 0.$$

Обозначим область, полученную от присоединения к области рациональных чисел его корня, через $\Omega(x)$, а через $\mathfrak{p}$ простой идеал внутри $\Omega(x)$, взаимно простой с дискриминантом уравнения (1). Тогда имеют место сравнения:

(2) $$x_1{}^p \equiv x_{\alpha_1},\ x_2{}^p \equiv x_{\alpha_2}, \ldots\ x_n{}^p \equiv x_{\alpha_n} \pmod{\mathfrak{p}},$$

если через $x_1, x_2, \ldots x_n$ обозначить сопряженные корни уравнения (1), а

$$S = \begin{pmatrix} 1 & 2 & 3 \cdots n \\ \alpha_1 & \alpha_2 & \alpha_3 \cdots \alpha_n \end{pmatrix}$$

является подстановкой над $1, 2, 3, \ldots n$, которая, как известно, входит в группу G уравнения (1) (см. Dedekind, Zur Theorie der Ideale, Gött. Nachr., 1894; также Frobenius, loc. cit.). Тогда будем говорить, что простой идеал $\mathfrak{p}$ *принадлежит* к подстановке S, а рациональное простое число p, кратное $\mathfrak{p}$, *принадлежит* к классу подстановок TST^{-1}, где T пробегает все подстановки группы G.

Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören.

Von

N. Tschebotareff in Odessa.

Das Problem, dessen Lösung der Zweck der vorliegenden Abhandlung ist, rührt von Frobenius her[1]). Es besteht im folgenden. Es sei eine irreduzible normale Gleichung n-ten Grades

(1) $$f(x) = 0$$

gegeben. Ist dann $\mathfrak{K}(x)$ der durch Adjunktion ihrer Wurzeln zum Körper der rationalen Zahlen entstandene Körper, und $\mathfrak{P}$ ein in seine Diskriminante nicht aufgehendes Primideal in $\mathfrak{K}(x)$, so gelten die Kongruenzen:

(2) $$x_1^p \equiv x_{\alpha_1},\ x_2^p \equiv x_{\alpha_2}, \ldots, x_n^p \equiv x_{\alpha_n} \pmod{\mathfrak{P}},$$

wenn man mit $x_1, x_2, \ldots, x_n$ das System aller Wurzeln der Gleichung (1) bezeichnet, und

$$S = \begin{pmatrix} 1 & 2 & 3 \ldots n \\ \alpha_1 & \alpha_2 & \alpha_3 \ldots \alpha_n \end{pmatrix}$$

eine gewisse Substitution ist, welche, wie bekannt (siehe unten, § 1, Satz 2), in die Galoissche Gruppe der Gleichung (1) eingeht. Dann sagen wir, daß das Primideal $\mathfrak{P}$ zur Substitution S, und die rationale Primzahl p, deren Faktor $\mathfrak{P}$ ist, zur Substitutionsklasse von S *gehört*. Nehmen wir nun die Menge aller zur Substitutionsklasse von S gehörenden Primzahlen p, so nennt man den Limes

(3) $$\lim_{s=1} \frac{\sum_p p^{-s}}{\lg \frac{1}{s-1}},$$

[1]) Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe (Sitzber. Berl. Akad. 1896, S. 689–705).

The density of split primes (1 of 2)

Notation

$$\mathcal{H}_\sigma := \{s \in \mathbb{C} : \Re(s) > \sigma\}$$

Dedekind (1894) associated a zeta function to any number field L:

$$\zeta_L(s) := \sum_{\mathfrak{I}} \frac{1}{N(\mathfrak{I})^s} = \prod_{\mathfrak{P}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}, \qquad s \in \mathcal{H}_1.$$

As proved by Hecke (1918), this function is meromorphic on $\mathbb{C}$ with a simple pole at $s = 1$ and no other pole. Moreover, it satisfies a functional equation, generalizing the work of Riemann (1859).

By taking the logarithmic derivative of both sides, we obtain

$$-\frac{\zeta_L'}{\zeta_L}(s) = \sum_{\mathfrak{P}} \sum_{r=1}^{\infty} \frac{\log N(\mathfrak{P})}{N(\mathfrak{P})^{rs}} \approx \sum_{\mathfrak{P}} \frac{\log N(\mathfrak{P})}{N(\mathfrak{P})^s},$$

where $f(s) \approx g(s)$ means that $f(s) - g(s)$ is a Dirichlet series converging absolutely in $\mathcal{H}_{1/2}$.

The density of split primes (2 of 2)

Let $L/\mathbb{Q}$ be a Galois extension. Then with a bit of algebraic number theory we see that

$$-\frac{\zeta_L'}{\zeta_L}(s) \approx \sum_{\mathfrak{P}} \frac{\log N(\mathfrak{P})}{N(\mathfrak{P})^s} \approx \sum_{p \text{ splits completely in } L} [L:\mathbb{Q}] \frac{\log p}{p^s}.$$

In particular, the right-hand side is meromorphic on $\mathcal{H}_{1/2}$ with simple poles, and $s = 1$ is a pole:

$$\sum_{p \text{ splits completely in } L} \frac{\log p}{p^s} \sim \frac{1}{[L:\mathbb{Q}]} \cdot \frac{1}{s-1}, \qquad s \to 1.$$

Compare with the special case $L = \mathbb{Q}$. The other poles are the zeros of $\zeta_L(s)$ in $\mathcal{H}_{1/2}$. According to the generalized Riemann hypothesis, there is no such zero. This is equivalent to:

$$\sum_{\substack{p \leqslant x \\ p \text{ splits completely in } L}} \log p = \frac{x}{[L:\mathbb{Q}]} + O_{L,\varepsilon}(x^{1/2+\varepsilon}), \qquad \varepsilon > 0.$$

Dirichlet's theorem on primes (1 of 2)

Now let $L = \mathbb{Q}(e^{2\pi i/q})$. Then the previous findings become a special case of Dirichlet's theorem on primes:

$$\sum_{p \equiv 1 \pmod{q}} \frac{\log p}{p^s} \approx \frac{1}{\varphi(q)} \cdot -\frac{\zeta_L'}{\zeta_L}(s) \sim \frac{1}{\varphi(q)} \cdot \frac{1}{s-1}, \qquad s \to 1.$$

Question

How about the density of $p \equiv a \pmod{q}$ for $(a, q) = 1$?

Hint

$$\frac{\zeta_L(s)}{\zeta_{\mathbb{Q}}(s)} = \prod_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} L(s, \chi_{\mathrm{prim}}).$$

The factors on the right-hand side are entire functions, hence so is the left-hand side. They do not vanish at the point $s = 1$.

Dirichlet's theorem on primes (2 of 2)

Dirichlet (1837) realized that the non-vanishing at $s = 1$ of the Dirichlet L-functions $L(s, \chi)$ is the key to the equidistribution of primes in reduced residue classes modulo q:

$$\begin{aligned}
\sum_{p \equiv a \pmod{q}} \frac{\log p}{p^s} &= \sum_p \frac{\log p}{p^s} \left(\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \chi(p) \overline{\chi}(a) \right) \\
&= \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \left(\sum_p \frac{\chi(p) \log p}{p^s} \right) \overline{\chi}(a) \\
&\approx \frac{1}{\varphi(q)} \sum_{\chi \bmod q} -\frac{L'}{L}(s, \chi) \overline{\chi}(a) \\
&\approx \frac{1}{\varphi(q)} \sum_{\chi \bmod q} -\frac{L'}{L}(s, \chi_{\mathrm{prim}}) \overline{\chi}(a) \\
&\sim \frac{1}{\varphi(q)} \cdot \frac{1}{s-1}, \qquad s \to 1.
\end{aligned}$$

The left-hand side is meromorphic on $\mathcal{H}_{1/2}$ with simple poles.

A supplement to Dirichlet's theorem on primes (1 of 2)

Assume that $s_0 \in \mathcal{H}_{1/2}$ is not a zero of the entire function

$$\frac{\zeta_L(s)}{\zeta_{\mathbb{Q}}(s)} = \prod_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} L(s, \chi_{\mathrm{prim}}).$$

Then the point s_0 is not a zero of any of the factors on the right-hand side. We can reformulate this observation as follows.

Proposition

Assume that $s_0 \in \mathcal{H}_{1/2}$ is not a pole of

$$\sum_{p \equiv 1 \pmod q} \frac{\log p}{p^s} - \frac{1}{\varphi(q)} \sum_p \frac{\log p}{p^s} \approx \frac{1}{\varphi(q)} \left(\frac{\zeta_{\mathbb{Q}}'}{\zeta_{\mathbb{Q}}}(s) - \frac{\zeta_L'}{\zeta_L}(s) \right).$$

Then, for $(a, q) = 1$, the point s_0 is not a pole of

$$\sum_{p \equiv a \pmod q} \frac{\log p}{p^s} - \frac{1}{\varphi(q)} \sum_p \frac{\log p}{p^s} \approx \frac{1}{\varphi(q)} \sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} -\frac{L'}{L}(s, \chi_{\mathrm{prim}}) \overline{\chi}(a).$$

In particular, by standard Mellin transform techniques, we obtain:

Corollary

Suppose $\sigma \geqslant 1/2$ *is such that for any* $\varepsilon > 0$ *we have*

$$\sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod q}} \log p = \frac{1}{\varphi(q)} \sum_{p \leqslant x} \log p + O(x^{\sigma+\varepsilon}).$$

Then for $(a, q) = 1$ *and any* $\varepsilon > 0$ *we have*

$$\sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \log p = \frac{1}{\varphi(q)} \sum_{p \leqslant x} \log p + O(x^{\sigma+\varepsilon}).$$

Chebotarev's density theorem

Chebotarev (1923) proved a far-reaching generalization of Dirichlet's theorem, originally conjectured by Frobenius (1896).

To fix ideas, let L/K be a Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. To an unramified prime ideal $\mathfrak{p}$ in K, we associate a conjugacy class $\mathrm{Frob}(\mathfrak{p}) \subset G$ as follows. For any prime divisor $\mathfrak{P} \mid \mathfrak{p}$ in L, there is a unique $\mathrm{Frob}(\mathfrak{P}) \in G$ satisfying

$$x^{\mathrm{Frob}(\mathfrak{P})} \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for all integers x in L. The class $\mathrm{Frob}(\mathfrak{p})$ is the set of $\mathrm{Frob}(\mathfrak{P})$'s.

Theorem

For each conjugacy class $C \subset G$, consider the Dirichlet series

$$D_G(s, C) := \sum_{\mathrm{Frob}(\mathfrak{p})=C} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s}, \qquad s \in \mathcal{H}_1.$$

This function is meromorphic on $\mathcal{H}_{1/2}$ with simple poles, and it has a simple pole at $s = 1$ with residue $|C|/|G|$.

Artin L-functions

In order to prove Chebotarev's density theorem (and more), we shall use the L-functions introduced by Artin (1923). These Artin L-functions are associated to (characters of) Galois representations.

Basic properties

1. *For the trivial character χ_0 of G, we have $L(s,\chi_0) = \zeta_K(s)$.*
2. $L(s,\chi_1+\chi_2) = L(s,\chi_1)L(s,\chi_2)$.
3. *For a subgroup $H \leqslant G$ and a character ψ of H, we have $L(s, \mathrm{Ind}_H^G \psi) = L(s,\psi)$.*

Corollary

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \prod_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi\neq\chi_0}} L(s,\chi)^{\chi(1)}.$$

Artin (1923) conjectured that the L-functions $L(s,\chi)$ on the right-hand side are entire. It follows from the celebrated reciprocity law of Artin (1927) that the conjecture is true when G is abelian.

Chebotarev's density theorem via Artin reciprocity (1 of 2)

The definition of $L(s, \chi)$ yields readily that

$$-\frac{L'}{L}(s, \chi) \approx \sum_{\mathfrak{p}} \frac{\chi(\mathrm{Frob}(\mathfrak{p})) \log N(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Hence if $g_C \in C$ is any element, then we get by Schur orthogonality

$$\begin{aligned} D_G(s, C) &= \sum_{\mathfrak{p}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s} \left(\frac{|C|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(\mathrm{Frob}(\mathfrak{p})) \overline{\chi}(g_C) \right) \\ &= \frac{|C|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{\mathfrak{p}} \frac{\chi(\mathrm{Frob}(\mathfrak{p})) \log N(\mathfrak{p})}{N(\mathfrak{p})^s} \right) \overline{\chi}(g_C) \\ &\approx \frac{|C|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} -\frac{L'}{L}(s, \chi) \overline{\chi}(g_C). \end{aligned}$$

We claim that the last sum is meromorphic on $\mathbb{C}$ with simple poles, and it has a simple pole at $s = 1$ with residue 1. By Artin reciprocity, the claim holds when G is abelian. Hence it suffices to show that the last sum doesn't change when G is replaced by $\langle g_C \rangle$.

Chebotarev's density theorem via Artin reciprocity (2 of 2)

Notation

$$U_G(s,g) := \sum_{\chi \in \mathrm{Irr}(G)} \frac{L'}{L}(s,\chi)\overline{\chi}(g), \qquad s \in \mathcal{H}_1, \quad g \in G.$$

Master relation

For any subgroup $H \leqslant G$, we have $\mathrm{Res}^G_H U_G(s,*) = U_H(s,*)$.

Proof.

Let us fix $s \in \mathcal{H}_1$. For any character χ of G, we have

$$\langle U_G(s,*), \overline{\chi} \rangle_G = \frac{L'}{L}(s,\chi).$$

Hence for any character ψ of H, Frobenius reciprocity gives that

$$\langle \mathrm{Res}^G_H U_G(s,*), \overline{\psi} \rangle_H = \langle U_G(s,*), \mathrm{Ind}^G_H \overline{\psi} \rangle_G = \\ = \frac{L'}{L}(s, \mathrm{Ind}^G_H \psi) = \frac{L'}{L}(s,\psi) = \langle U_H(s,*), \overline{\psi} \rangle_H.$$

□

The meromorphicity of $L'(s,\chi)/L(s,\chi)$

The previous proof used a fundamental idea of Heilbronn (1973).

Corollary

For any character $\chi \in \mathrm{Irr}(G)$, the function $L'(s,\chi)/L(s,\chi)$ is meromorphic on $\mathbb{C}$ with simple poles. Moreover, for $\chi \neq \chi_0$, the point $s = 1$ is not a pole.

Proof.

We have seen that

$$U_G(s,g) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{L'}{L}(s,\chi)\overline{\chi}(g)$$

is meromorphic on $\mathbb{C}$ with simple poles, and it has a simple pole at $s = 1$ with residue -1. Hence we are done upon noting that

$$\frac{L'}{L}(s,\chi) = \langle U_G(s,*), \overline{\chi}\rangle_G.$$

□

A supplement to Chebotarev's density theorem

Theorem

For each conjugacy class $C \subset G$, consider the Dirichlet series

$$F_G(s, C) := \sum_{\mathrm{Frob}(\mathfrak{p})=C} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s} - \frac{|C|}{|G|} \sum_{\mathfrak{p}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s}, \qquad s \in \mathcal{H}_1.$$

This function is meromorphic on $\mathcal{H}_{1/2}$ with simple poles. For any point $s_0 \in \mathcal{H}_{1/2}$, the following statements are equivalent:

- a. s_0 *is a zero of* $\zeta_L(s)/\zeta_K(s)$;
- b. s_0 *is a pole of* $F_G(s, \{1\})$;
- c. s_0 *is a pole of* $F_G(s, C)$ *for some conjugacy class* $C \subset G$;
- d. s_0 *is a pole of* $L'(s, \chi)/L(s, \chi)$ *for some nontrivial* $\chi \in \mathrm{Irr}(G)$.

Moreover,

$$\sum_C \frac{|G|}{|C|} \left| \operatorname*{res}_{s=s_0} F_G(s, C) \right|^2 \leqslant \left(\operatorname*{ord}_{s=s_0} \zeta_L(s) \right)^2 - \left(\operatorname*{ord}_{s=s_0} \zeta_K(s) \right)^2. \qquad (*)$$

The Foote–Murty inequality (1 of 2)

First we prove the key bound $(*)$. Proceeding as in the proof of Chebotarev's density theorem, we see that

$$F_G(s, C) \approx -\frac{|C|}{|G|} V_G(s, g_C),$$

where

Notation

$$V_G(s,g) := \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq \chi_0}} \frac{L'}{L}(s,\chi)\overline{\chi}(g), \qquad s \in \mathcal{H}_1, \quad g \in G.$$

Hence it suffices to prove the following inequality that is essentially due to Foote–Murty (1989):

$$\frac{1}{|G|} \sum_{g \in G} \left| \operatorname*{res}_{s=s_0} V_G(s,g) \right|^2 \leqslant \left(\operatorname*{ord}_{s=s_0} \zeta_L(s) \right)^2 - \left(\operatorname*{ord}_{s=s_0} \zeta_K(s) \right)^2.$$

The Foote–Murty inequality (2 of 2)

Let us work with an arbitrary $s_0 \in \mathbb{C}$. Since

$$V_G(s,g) = U_G(s,g) - \frac{\zeta_K'}{\zeta_K}(s),$$

the bound is clear when $s_0 = 1$ (cf. Chebotarev's density theorem):

$$\operatorname*{res}_{s=1} V_G(s,g) = \operatorname*{res}_{s=1} U_G(s,g) + 1 = 0.$$

For $s_0 \neq 1$, we combine the Master relation with Artin reciprocity:

$$\left|\operatorname*{res}_{s=s_0} U_G(s,g)\right| = \left|\operatorname*{res}_{s=s_0} U_{\langle g\rangle}(s,g)\right| \leqslant$$
$$\leqslant \operatorname*{res}_{s=s_0} U_{\langle g\rangle}(s,1) = \operatorname*{res}_{s=s_0} U_{\{1\}}(s,1) = \operatorname*{ord}_{s=s_0} \zeta_L(s).$$

We square this bound and average over G. We get that

$$\frac{1}{|G|}\sum_{g\in G}\left|\operatorname*{res}_{s=s_0} V_G(s,g) + \operatorname*{ord}_{s=s_0}\zeta_K(s)\right|^2 \leqslant \left(\operatorname*{ord}_{s=s_0}\zeta_L(s)\right)^2.$$

This is what we need, since the average of $V_G(s,g)$ over G is zero.

The final equivalences

The Foote–Murty inequality yields in particular that

$$\operatorname*{ord}_{s_0} \zeta_K(s) \leqslant \operatorname*{ord}_{s_0} \zeta_L(s), \qquad s_0 \in \mathbb{C},$$

hence $\zeta_L(s)/\zeta_K(s)$ is an entire function. This is originally due to Aramata (1931), and re-discovered by Brauer (1947).

Now we can prove that the statements (a), (b), (c) are equivalent. If (a) holds, then s_0 is a pole of the logarithmic derivative

$$\frac{\zeta_L'}{\zeta_L}(s) - \frac{\zeta_K'}{\zeta_K}(s) = U_{\{1\}}(s,1) - \frac{\zeta_K'}{\zeta_K}(s) = U_G(s,1) - \frac{\zeta_K'}{\zeta_K}(s) = V_G(s,1),$$

which then implies (b). Now (b) trivially implies (c), while (c) implies (a) by $(*)$. Finally, (c) is equivalent to (d), because the functions $V_G(s,g)$ for $g \in G$ span the same $\mathbb{C}$-vector space as the functions $L'(s,\chi)/L(s,\chi)$ for $\chi \neq \chi_0$.

A supplement to Chebotarev's density theorem (cont.)

In particular, by standard Mellin transform techniques, we obtain:

Corollary

Suppose $\sigma \geqslant 1/2$ *is such that for any* $\varepsilon > 0$ *we have*

$$\sum_{\substack{N(\mathfrak{p}) \leqslant x \\ \mathrm{Frob}(\mathfrak{p}) = \{1\}}} \log N(\mathfrak{p}) = \frac{1}{|G|} \sum_{N(\mathfrak{p}) \leqslant x} \log N(\mathfrak{p}) + O(x^{\sigma+\varepsilon}).$$

Then for any conjugacy class $C \subset G$ *and any* $\varepsilon > 0$ *we have*

$$\sum_{\substack{N(\mathfrak{p}) \leqslant x \\ \mathrm{Frob}(\mathfrak{p}) = C}} \log N(\mathfrak{p}) = \frac{|C|}{|G|} \sum_{N(\mathfrak{p}) \leqslant x} \log N(\mathfrak{p}) + O(x^{\sigma+\varepsilon}).$$

Enter Brauer's theorem

Theorem

For each conjugacy class $C \subset G$, consider the Dirichlet series

$$F_G(s, C) := \sum_{\mathrm{Frob}(\mathfrak{p})=C} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s} - \frac{|C|}{|G|} \sum_{\mathfrak{p}} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^s}, \qquad s \in \mathcal{H}_1.$$

This function is meromorphic on $\mathcal{H}_{1/2}$ with simple poles. For any point $s_0 \in \mathcal{H}_{1/2}$, the following statements are equivalent:

- a. *s_0 is a zero of $\zeta_L(s)/\zeta_K(s)$;*
- b. *s_0 is a pole of $F_G(s, \{1\})$;*
- c. *s_0 is a pole of $F_G(s, C)$ for some conjugacy class $C \subset G$;*
- d. *s_0 is a pole of $L'(s, \chi)/L(s, \chi)$ for some nontrivial $\chi \in \mathrm{Irr}(G)$;*
- e. *s_0 is a zero or pole of $L(s, \chi)$ for some non-trivial $\chi \in \mathrm{Irr}(G)$;*
- f. *s_0 is a zero of $L(s, \chi)$ for some non-trivial $\chi \in \mathrm{Irr}(G)$.*