PAIR CORRELATION AND THE CHEBOTAREV DENSITY THEOREM

V. Kumar Murty
University of Toronto

Analytic number theory is about the problem of explicating the relationship between analytic properties of L-functions and distribution of prime numbers.

Analytic number theory is about the problem of explicating the relationship between analytic properties of L-functions and distribution of prime numbers.

- The Riemann zeta function is the prototype.

Analytic number theory is about the problem of explicating the relationship between analytic properties of L-functions and distribution of prime numbers.

- The Riemann zeta function is the prototype.

- However, it does not reveal all phenomena.

Analytic number theory is about the problem of explicating the relationship between analytic properties of L-functions and distribution of prime numbers.

• The Riemann zeta function is the prototype.

• However, it does not reveal all phenomena.

• In fact, perhaps it is impossible to understand it in isolation.

Analytic number theory is about the problem of explicating the relationship between analytic properties of L-functions and distribution of prime numbers.

• The Riemann zeta function is the prototype.

• However, it does not reveal all phenomena.

• In fact, perhaps it is impossible to understand it in isolation.

• The study of non-Abelian Artin L-functions may help.

Let K/F be a finite Galois extension of number fields with group G.

Fundamental problem: The distribution of primes in conjugacy classes.

Example 1. If $F = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_m)$, then the Frobenius conjugacy class associated to a prime p (that does not divide m) is the automorphism

$$\zeta_m \ \mapsto \zeta_m^a$$

where $p \equiv a (mod\ m)$.

Example 2. Let f be a monic polynomial of degree d with integer coefficients whose Galois group is the symmetric group S_d. The Frobenius conjugacy class of a prime p that does not divide the discriminant of f is determined by the factorization of f modulo p. Indeed, if

$$f \equiv f_1 \cdots f_t \ mod\ p$$

with f_i irreducible of degree r_i, then the Frobenius conjugacy class of p is the conjugacy class of permutations with cycle structure (r_1-cycle)(r_2-cycle)$\cdots$(r_t-cycle).

Let C be a conjugacy subset of G.

Denote by $\pi_C(x)$ the number of prime ideals $\mathfrak{p}$ of F that are unramified in K and whose Frobenius symbol lies in C.

The Chebotarev Density theorem asserts that

$$\pi_C(x) \ = \ (\frac{|C|}{|G|} + \mathbf{o}(1))\mathsf{Li}\ x$$

where, as usual,

$$\mathsf{Li}x \ = \ \int_2^x \frac{dt}{\log t}.$$

To be useful in many applications, we need a uniform and effective version of this. This means an explicit error term.

Such error terms usually reflect knowledge of the zeros and poles of various L-functions.

In this case, there is the Dedekind zeta function defined for $Re(s) > 1$ by

$$\zeta_F(s) \ = \ \sum_{\mathfrak{a}} (\mathbf{N}\mathfrak{a})^{-s}$$

where the sum is over integral ideals $\mathfrak{a}$ of $\mathcal{O}_F$ (the ring of integers of F).

A recent result of Ram Murty and Benjamin Ju is that the "elementary proof" of the prime number theorem can be extended to F provided we know that

$$\#\{\mathfrak{a} : \mathbf{N}\mathfrak{a} \leq x\} \;=\; c_F x \;+\; \mathcal{O}(x^\theta)$$

for some $\theta < 1$.

This is equivalent to knowing that $\zeta_F(s)$ has a continuation to $Re(s) > \theta$, analytic in that region apart from a simple pole at $s = 1$.

In fact, we know that $\zeta_F(s)$ has such a continuation to the entire s-plane.

The Generalized Riemann Hypothesis (GRH) for ζ_F asserts that its "nontrivial" zeros are on the line $Re(s) = \frac{1}{2}$.

An effective version of the Chebotarev Density Theorem was obtained by Lagarias and Odlyzko.

Assuming the GRH for $\zeta_F(s)$, they showed that

$$|\pi_C(x, F/K) - \frac{|C|}{|G|}\mathsf{Li}(x)| \ll |C|x^{1/2}[K:\mathbb{Q}](\log d_F x).$$

The challenge is to manage the dependence of the error term on all the "constants" (such as d_F, $[F:K]$, etc.)

The challenge is to manage the field constants in the error term. Can we get rid of them altogether?

The challenge is to manage the field constants in the error term. Can we get rid of them altogether?

For example, could we expect that

$$|\pi_C(x, F/K) \; - \; \frac{|C|}{|G|}\mathsf{Li}(x)| \; \ll \; x^{1/2}(\log x)?$$

The challenge is to manage the field constants in the error term. Can we get rid of them altogether?

For example, could we expect that

$$|\pi_C(x, F/K) \; - \; \frac{|C|}{|G|}\mathsf{Li}(x)| \; \ll \; x^{1/2}(\log x)?$$

No! This is not even true in the Abelian case $K = \mathbb{Q}$ and F a quadratic extension of K.

The challenge is to manage the field constants in the error term. Can we get rid of them altogether?

For example, could we expect that

$$|\pi_C(x, F/K) \; - \; \frac{|C|}{|G|}\mathsf{Li}(x)| \; \ll \; x^{1/2}(\log x)?$$

No! This is not even true in the Abelian case $K = \mathbb{Q}$ and F a quadratic extension of K.

Correct size of the error term is an open question.

The challenge is to manage the field constants in the error term. Can we get rid of them altogether?

For example, could we expect that

$$|\pi_C(x, F/K) \; - \; \frac{|C|}{|G|}\mathsf{Li}(x)| \; \ll \; x^{1/2}(\log x)?$$

No! This is not even true in the Abelian case $K = \mathbb{Q}$ and F a quadratic extension of K.

Correct size of the error term is an open question.

For example, is it possible that

$$|\pi_C(x, F/K) \; - \; \frac{|C|}{|G|}\mathsf{Li}(x)| \; \ll \; x^{1/2}(\log d_F x)?$$

To improve on the Lagarias-Odlyzko estimate, we observe that the Dedekind zeta function is not "primitive" (in the sense of Selberg). It factors

$$\zeta_F(s) \;=\; \prod_{\chi \in \mathrm{Irr}(G)} L(s,\chi)^{\chi(1)}.$$

Here $L(s,\chi)$ is the Artin L-function associated to the character χ of the Galois group.

In analytic number theory, whenever a zeta or L-function factors, one expects better results by working directly with the factors.

In this case, the Artin L-functions have a meromorphic continuation for all s and a functional equation.

Artin's conjecture (AC) is that they are entire apart from a pole at $s = 1$ of multiplicity equal to $< \chi, 1 >$.

One can also ask the Riemann Hypothesis for the $L(s, \chi)$. This actually follows from the GRH for $\zeta_F(s)$.

More generally, the set of zeros and poles of $L(s, \chi)$ are a subset of the zeros of the $\zeta_F(s)$.

If we assume the GRH and AC, Ram Murty, Saradha and KM showed that

$$|\pi_C(x, F/K) \ - \ \frac{|C|}{|G|}Li(x)|$$

$$\ll \ |C|^{1/2}x^{1/2}[F : K](\log d_F x).$$

Here, GRH means the Riemann Hypothesis for $\zeta_F(s)$ and AC means the Hypothesis that all $L(s, \chi)$ are analytic for $s \neq 1$.

In fact, the above bound can be essentially proved even if AC is replaced by a weaker hypothesis involving the growth of Artin L-functions in $Re(s) > 1/2$. All we need is that for $Re(s) > \frac{1}{2} + \epsilon$, we have the bound

$$L(s, \chi) \ \ll \ (|s| + 1)^{c\chi(1)[K:\mathbb{Q}]}$$

for some absolute constant $c > 0$.

This is very useful when dealing with problems in which conjugacy classes are very large.

An example of this is the Lang-Trotter conjecture. Let f be a holomorphic cusp form for some congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that is a normalized eigenform for the Hecke algebra. Write

$$f(z) \;=\; \sum_{n=1}^{\infty} a_f(n) e^{2\pi i n z}$$

for its Fourier expansion at infinity. Suppose that the Fourier coefficients all lie in $\mathbb{Z}$.

The Lang-Trotter conjecture asserts that if $a \neq 0$, then

$$\#\{p \leq x : a_f(p) = a\} \;=\; (c(f,a) \;+\; \mathbf{o}(1)) \frac{\sqrt{x}}{\log x}.$$

Using the Galois representations associated with f, this is translated into a Chebotarev problem with group $G = \mathrm{GL}_2(\mathbb{Z}/\ell)$ (for some large prime ℓ) and C the conjugacy subset consisting of elements of G of trace equal to $a \mod \ell$. We see that

$$|C| \sim \ell^3.$$

Using the Lagarias-Odlyzko estimate, one finds that

$$\#\{p \leq x : a_f(p) = a\} \ll x^{7/8}$$

while using the $|C|^{\frac{1}{2}}$ estimate, one obtains

$$\#\{p \leq x : a_f(p) = a\} \ll x^{4/5}$$

However, there are three defects in this:

• Even with these powerful assumptions, we do not get close to the actual Lang-Trotter estimate.

Indeed, it is only if we assume an estimate like the question raised earlier:

$$|\pi_C(x, F/K) \ - \ \frac{|C|}{|G|}\mathsf{Li}(x)| \ \ll \ x^{1/2}(\log d_F x)$$

that we can employ it in the above manner to deduce an upper bound of the right order for Lang-Trotter.

• The improvement obtained by using GRH and AC are not useful if the conjugacy class is small.

For example, suppose we are dealing with the problem of primes splitting completely in a field of large discriminant.

This situation arises in the Artin primitive root conjecture.

In this case improving the $|C|$ to $|C|^{\frac{1}{2}}$ will not have much impact.

• These estimates do not completely reflect the intuition that it is easier for a prime to fall into a larger conjugacy class than a smaller one.

We can apply each to get a bound for the least prime which lies in a given conjugacy class (analogue of the least prime in an arithmetic progression).

The Lagarias-Odlyzko estimate gives a bound of

$$(\log d_F)^2.$$

In particular this is independent of the size of the conjugacy class.

The $|C|^{\frac{1}{2}}$ estimate gives a bound of

$$\frac{[K:\mathbb{Q}]^2}{|C|}(n\log n + \log d_F)^2$$

where $n = [F:K]$.

This is better, but probably still does not reflect the truth. It is possible that the bound of

$$\left(\frac{1}{|C|}\log d_F\right)^2$$

or a slightly weaker variant might hold.

Notice that this entire issue is invisible over $\mathbb{Q}$.

There is a large gap between what we can prove or even conjecture and what might be the truth.

We are still looking for a path.

Can we use finer information about the zeros of Artin L-functions to improve the bounds?

Pair correlation is a natural candidate.

This is not very effective in the distribution of rational primes.

Assuming the RH, one has

$$\pi(x) \;=\; \mathrm{Li}x \;+\; \mathbf{O}(x^{\frac{1}{2}}(\log x)).$$

Assuming a pair correlation conjecture for the zeros of the Riemann zeta function improves this to

$$\pi(x) \;=\; \mathrm{Li}x \;+\; \mathbf{O}(x^{\frac{1}{2}}(\log x)^{\frac{1}{2}}).$$

However, it does seem to give a step forward in the non-Abelian setting.

This is joint work with Ram Murty.

The quantity to study is

$$\psi_C(x) \;=\; \sum_{\substack{\mathbf{N}\mathfrak{p}^m \le x \\ \mathsf{Frob}_{\mathfrak{p}} \subseteq C}} \log \mathbf{N}\mathfrak{p}.$$

Using the spectral decomposition of the characteristic function of C, we have

$$\psi_C(x) \;=\; \frac{|C|}{|G|} \sum_{\chi} \overline{\chi}(C) \psi(x, \chi)$$

where

$$\psi(x, \chi) \;=\; \sum_{\substack{\mathbf{N}\mathfrak{p}^m \le x \\ \mathsf{Frob}_{\mathfrak{p}} \subseteq C}} \chi(\mathsf{Frob}_{\mathfrak{p}}^m) \log \mathbf{N}\mathfrak{p}.$$

Assuming that $L(s,\chi)$ is entire, and using the explicit formula, we deduce that

$$\psi(x,\chi) \;=\; \delta(\chi)x \;-\; \sum_{|\gamma|\le T} \frac{x^\rho}{\rho} \;+\; E(x,\chi)$$

where the sum is over zeros $\rho = \rho_\chi \;=\; \beta + i\gamma$ of $L(s,\chi)$ and E is an error term that can be estimated easily.

In fact, we have

$$E(x,\chi)$$

$$\ll \frac{x\log x}{T}\log A_\chi T \;+\; \chi(1)n_F x^{1/2}\log x \;+\; \cdots$$

where $\cdots$ represents small terms that are easily managed.

Here A_χ is the Artin conductor of χ. It is defined by

$$A_\chi \;=\; d_K^{\chi(1)}\mathbf{N}\mathfrak{f}_\chi$$

where $\mathfrak{f}_\chi$ is an ideal of K supported at primes where χ is ramified.

To analyze the sum over zeros, we set

$$S(T,X) \;=\; S_\chi(T,X) \;=\; \sum_{0\le\gamma\le T} \exp(2\pi i\gamma X)$$

with the sum ranging over the imaginary parts of the nontrivial zeros of $L(s,\chi)$.

Assuming the GRH, the sum to estimate is

$$\sum_{|\gamma_\chi|\le T} \frac{x^{i\gamma}}{\frac12+i\gamma} \;=\; \int_0^T \frac{dS(t,(\log x)/2\pi)}{\frac12+it}.$$

Integrating by parts, the right hand side is

$$\ll\; T^{-1}S(T,(\log x)/2\pi) + 1 + \int_2^T \frac{S(t,(\log x)/2\pi)}{t^2}dt.$$

We formulate a pair correlation conjecture to estimate the sum $S(T, X)$.

Let us set

$$w(u) \ = \ \frac{4}{4+u^2}.$$

Let us also define

$$P(T,X) \ = \ P_\chi(T,X) \ =$$

$$= \sum_{|\gamma_1|,|\gamma_2|\leq T} w(\gamma_1-\gamma_2)\exp(2\pi i(\gamma_1-\gamma_2)X).$$

Conjecture. Let $A > 0$. For

$$0 \leq Y \leq A\chi(1)[K:\mathbb{Q}]\log T$$

we have

$$P(T,Y) \ \ll_A \ T(\log A_\chi \ + \ \chi(1)[K:\mathbb{Q}]\log T).$$

Conjecture. Let $A > 0$. For

$$0 \leq Y \leq A\chi(1)[K : \mathbb{Q}] \log T$$

we have

$$P(T, Y) \ \ll_A \ T(\log A_\chi \ + \ \chi(1)[K : \mathbb{Q}] \log T).$$

Using this, we deduce that

$$S(T, X) \ \ll \ T^{3/4} \log A_\chi(T) \ + \ T(\log A_\chi(T))^{\frac{1}{2}}.$$

Here

$$\log A_\chi(T) \ = \ \log A_\chi \ + \ \chi(1)[K : \mathbb{Q}] \log T.$$

Applying this in the formula for $\psi(x,\chi)$ we get

$$\psi(x,\chi) - \delta(\chi)x \ \ll \ x^{\frac{1}{2}}\{E_1 + E_2\}$$

where

$$E_1 \ = \ 1 \ + \ T^{-1}S(T, \log x/2\pi) \ +$$

$$+ \ \int_2^T t^{-2}S(t, \log x/2\pi)dt$$

and

$$E_2 \ \ll xT^{-1}(\log x)(\log A_\chi(T)).$$

Applying the estimate above for $S(T,X)$, we deduce that

$$\psi(x,\chi) - \delta(\chi)x \ \ll \ x^{\frac{1}{2}}(\log A_\chi(x))^{\frac{1}{2}} \log x \ + \ \cdots .$$

Now to apply this to $\psi_C(x)$, we use the identity

$$\sum_{C \subseteq G} \frac{1}{|C|} \left(\psi_C(x) - \frac{|C|}{|G|} x \right)^2 \;=\; \frac{1}{|G|} \sum_{\chi \neq 1} |\psi(x, \chi)|^2.$$

Using the estimate of the previous slide, we see that

$$\sum_{\chi \neq 1} |\psi(x, \chi)|^2 \;\ll\; x (\log x)^2 \sum \log A_\chi(x).$$

Recall that

$$\log A_\chi(x) \;=\; \log A_\chi \;+\; \chi(1)[K : \mathbb{Q}] \log x.$$

We also have the estimate

$$\log A_\chi \;\ll\; \chi(1)[K : \mathbb{Q}] \log M$$

where M is a quantity defined in terms of the ramified primes.

Hence,

$$\sum_{\chi} \log A_{\chi}(x) \ll [K : \mathbb{Q}](\log Mx)|G^{\#}|^{\frac{1}{2}}|G|^{\frac{1}{2}}$$

where $G^{\#}$ denotes the set of number of irreducible characters of G. Equivalently, it is the number of conjugacy classes of G.

Thus,

$$\sum_{C\subseteq G}\frac{1}{|C|}\left(\psi_C(x)-\frac{|C|}{|G|}x\right)^2 \ll$$

$$\ll \ [K:\mathbb{Q}]\frac{|G^{\#}|^{\frac{1}{2}}}{|G|^{\frac{1}{2}}}x(\log x)^2(\log Mx)+\cdots .$$

Now choosing an individual C, we deduce that

$$\psi_C(x)-\frac{|C|}{|G|}x \ll$$

$$\ll \ [K:\mathbb{Q}]^{\frac{1}{2}}|C|^{\frac{1}{2}}\left(\frac{|G^{\#}|}{|G|}\right)^{1/4}x^{\frac{1}{2}}(\log x)(\log Mx)+\cdots .$$

Notice that the quantity $|G|/|G^{\#}|$ is the average size of a conjugacy class.

To summarize the above discussion, we have outlined a proof of the following result.

Theorem. Assume the GRH, AC and the Pair Correlation conjecture for F/K. Then

$$\pi_C(x) \ - \ \frac{|C|}{|G|}\mathsf{Li}x \ \ll$$

$$\ll \ [K:\mathbb{Q}]^{\frac{1}{2}}|C|^{\frac{1}{2}}\left(\frac{|G^{\#}|}{|G|}\right)^{1/4} x^{\frac{1}{2}}(\log x)(\log Mx)+\cdots .$$

If we apply this to the Lang-Trotter problem, we find (using the same notation as before)

$$\#\{p \leq x : a_f(p) \ = \ a \ \} \ \ll \ x^{2/3+\epsilon}.$$

It is also instructive to see what bound this gives for the least prime in a conjugacy class:

$$\ll \frac{[K:\mathbb{Q}]}{|C|}\frac{1}{|C^{av}|^{\frac{1}{2}}}(\log d_F)^2.$$

Here, we are writing $|C^{av}|$ for the average size of a conjugacy class. If we are in a group where most conjugacy classes are the same size, then this can be rewritten as

$$\ll \frac{[K:\mathbb{Q}]}{|C|^{3/2}}(\log d_F)^2.$$

Finally, let us look at the implications of the above theorem to the error term in the Artin primitive root conjecture.

Let $a \neq 0, 1$ be an integer that is not a square. Set

$N_a(x) = \#\{p \leq x : a \text{ is a primitive root mod } p\}$.

Artin's primitive root conjecture asserts that

$$N_a(x) \sim c(a)\mathrm{Li}x.$$

Hooley proved this assuming the GRH (RH for Dedekind zeta functions of Kummer extensions.)

In fact, he proved

$$N_a(x) \;=\; c(a)\mathrm{Li}x \;+\; \mathbf{O}(x(\log\log x)^2/(\log x)^2).$$

We expect the error term to be $\mathbf{O}(x^{\frac{1}{2}+\epsilon})$.

Theorem. Assume the GRH and PC. Then

$$N_a(x) \;=\; c(a)\mathrm{Li}x \;+\; \mathbf{O}(x^{10/11}(\log x)^2(\log a)).$$

Sketch of Proof. Consider the Kummer extension

$$L_m \;=\; \mathbb{Q}(\zeta_m, a^{1/m}).$$

It is Galois over $\mathbb{Q}$ with group a semidirect product $(\mathbb{Z}/m)^\times \ltimes (\mathbb{Z}/m)$ AC is known for this group.

For m prime, this group has about m conjugacy classes of which $m-1$ are singletons and one has size m. Thus, the size of an average conjugacy class is m.

Denote by $\pi_m(x)$ the number of primes $p \leq x$ that split completely in L_m.

By our main result

$$L_m(x) \;=\; \frac{1}{m\phi(m)}\mathrm{Li}x \;+\; \mathbf{O}(x^{\frac{1}{2}}m^{-1/4}\log amx).$$

By inclusion-exclusion,

$$N_a(x) \;=\; \sum_{m=1}^{\infty} \mu(m)\pi_m(x)$$

as a is a primitive root modulo p if and only if p does not split completely in any L_m.

Using this, we see that

$$\sum_{m\le y} \mu(m)\left(\pi_m(x) - \frac{\mathrm{Li}x}{m\phi(m)}\right)$$

$$\ll\; x^{1/2}y^{3/4}(\log x)^2(\log a).$$

Also,

$$\sum_{y\le m\le x} \pi_m(x) \ll \sum_{p\le x} \sum_{\substack{y\le m\le x \\ m|(p-1),p|a^{(p-1)/m}-1}} 1.$$

This is bounded by

$$\sum_{v\le x/y} \sum_{p|a^v-1} 1 \ll (x/y)^2(\log a).$$

Choosing $y = x^{6/11}$ gives the result.

Remark 1. The PC assumption is that for $0 \leq Y \ \leq A\chi(1)[K:\mathbb{Q}]\log T$, we have

$$P(T,Y) \ \ll_A T(\log A_\chi \ + \ \chi(1)[K:\mathbb{Q}]\log T).$$

Note that we only need an upper bound and in the application, we need it only for *some* value of $A > 0$.

Remark 2. The trivial estimate is

$$P(T,Y) \ll_A T(\log A_\chi \ + \ \chi(1)[K:\mathbb{Q}]\log T)^2.$$

Remark 3. Following the work of R. Murty and Zaharescu, it should be possible to formulate the above PC hypothesis without the GRH and to study its implication for the Chebotarev density theorem.