Arithmetic Group Determinants
ProDoc Seminar 2009

Daniel Haase
D-MATH ETH Zürich

daniel.haase@math.ethz.ch

26.11.2009

Definition

Let P be the set of natural prime numbers. The prime number counting function is

$$\pi(x) \;=\; \#\{p \in P \,:\, p \leq x\} \;=\; \sum_{p \leq x} 1\,.$$

Usually one works with the Chebyshev counting function

$$\psi(x) \;=\; \sum_{p^k \leq x} \log(p)$$

which has a simpler structure.

The famous prime number theorem reads

$$\pi(x) \;=\; \mathrm{li}(x) \;+\; E(x) \;\text{ or equivalently }\; \psi(x) \;=\; x \;+\; E(x)$$

for error terms $E(x)$.

One investigates the properties of ψ by complex analysis of $\zeta(s)$:

Definition

Riemann's zeta function is defined on the half plane $\mathrm{Re}(s) > 1$ *by*

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} n^{-s} \;=\; \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \,.$$

It is absolutely convergent for $\mathrm{Re}(s) > 1$.

The functional equation for the completed zeta function

$$Z(s) \;=\; \pi^{-\frac{s}{2}} \cdot \Gamma(\frac{s}{2}) \cdot \zeta(s)$$

reads $Z(1-s) = Z(s)$, and provides a meromorphic continuation of $\zeta(s)$ to the complex plane, which has a simple pole at $s = 1$, trivial zeros for $s = -2, -4, -6, \ldots$, and nontrivial zeros in the strip $0 < \mathrm{Re}(s) < 1$.

Consider the Mellin pairing

$$F(s) \;=\; \int_0^\infty f(x)x^s\frac{dx}{x} \quad\leftrightarrow\quad f(x) \;=\; \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(s)x^{-s}dx\,.$$

The negative logarithmic derivative of $\zeta(s)$ is

$$F(s) \;=\; -\frac{\zeta'(s)}{\zeta(s)} \;=\; s\int_0^\infty \psi(x)x^{-s-1}dx$$

Classical explicit formula

$$\psi(x) \;=\; -\log(2\pi) + \sum_\varrho{}^{*}\,\mathrm{ord}(\varrho)\frac{x^\varrho}{\varrho} \;\;,\;\; \mathrm{ord}_\zeta(\varrho) \;=\; \mathrm{Res}_F(\varrho)\,.$$

So the orders of $\zeta(s)$ (the residues of F) control the prime distribution.

This formula translates knowledge of larger zero free regions of $\zeta(s)$ to smaller error terms $E(x)$.

- Hadamard/de la Vallée Poussin 1896: Pole at $s = 1$, no zeros on line $\mathrm{Re}(s) = 1$, gives asymptotic $\psi(x) = x + o(x)$ with small o, using a trigonometric identity on $\sum n^{-s}$.

- Best known approximation today comes from the zero free region which gives

$$\psi(x) \;=\; x \;+\; O\left(x \cdot \exp\left(-c \cdot \frac{\log(x)^{\frac{3}{5}}}{\log(\log(x))^{\frac{1}{5}}}\right)\right) .$$

  This was obtained by Vinogradov and Korobov in the 1960's, using mean value theorems on exponential sums.

- Riemann's Hypothesis is $\mathrm{Re}(\varrho) = \frac{1}{2}$ for every nontrivial zero, which implies the best possible approximation $\psi(x) = x + O(x^{\frac{1}{2}+\varepsilon})$ or $\pi(x) = \mathrm{li}(x) + O(\sqrt{x}\log(x))$ for the counting function $\pi(x)$.

Explicit formula holds for more general arithmetic data:

Dedekind zeta functions

Distribution of prime ideals norms of a number field K as given by the counting function

$$\psi_K(x) \;=\; \sum_{N(\mathfrak{p})^k \leq x} \log(N(\mathfrak{p}))$$

is encoded in the Dedekind zeta function

$$\zeta_K(s) \;=\; \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} \;=\; \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \,.$$

Prime ideal theorem: $\psi_K(x) = x + o(x)$.

Artin L-series

Distribution of prime ideals norms weighted by characters $\chi = \mathrm{Tr}(\varrho)$ of the Galois group of L/K

$$\psi_\chi(x) \;=\; \sum_{N(\mathfrak{p})^k \leq x} \log(N(\mathfrak{p}))\chi(\mathfrak{p}^k)$$

is encoded in the Artin L-series

$$L(s,\chi) \;=\; \prod_{\mathfrak{p}} \frac{1}{\det(\mathrm{id} - f_{\mathfrak{p}})(N(\mathfrak{p}))^{-s}} \,.$$

Tate's Thesis

For a character χ, $L(s,\chi)$ has a meromorphic continuation to $\mathbb{C}$ with (at most) a simple pole at $s=1$, trivial zeros on the real line, and nontrivial zeros in the strip $0<\mathrm{Re}(s)<1$.

A. Weil's explicit formula

For suitable $f:(0,\infty)\to\mathbb{C}$ and Weil's summation technique,

$$\sum_{\mathfrak{p},n}\log(N(\mathfrak{p}))\chi(\mathfrak{p}^n)f(N(\mathfrak{p})^n) \;=\; \sum_{\varrho}^{*}\mathrm{ord}_L(\varrho)F(\varrho)$$

holds where ϱ runs over the zeros/poles of $L(s,\chi)$.

Counting functions satisfy $\psi(x)=x+E(x)$ as in the classical case, error terms $E(x)$ unknown until location of the zeros is discovered.

We call these zeta functions analytic zeta functions, because

- they have a convergent Euler product expansion (hence no zeros for $\mathrm{Re}(s) > 1$),
- they have a meromorphic continuation to the complex plane,
- its zeros and poles control the counting function,
- the zeta function behaves nicely, so tools from complex calculus apply.

Usually these properties follow from a convenient functional equation like $Z(s,\chi) = Z(1-s,\chi^*)$, which in turn comes from the fact that the zeta function is a Mellin transform of some modular function (or form).

But that's not mandatory, for example the pair

$$\psi_p(x) \;=\; \sum_{p^k \le x} \log(p) \;=\; \left\lfloor \frac{\log(x)}{\log(p)} \right\rfloor \quad , \quad \zeta_p(s) \;=\; \frac{1}{1-p^{-s}}$$

also has these properties, also if p is any positive real number.

Some arithmetic questions have no analytic or geometric background:

Chebyshev's bias hypothesis

There are more primes $p \equiv 3 \bmod 4$ *then* $p \equiv 1 \bmod 4$.

We have to examine the functions

$$\psi_{a,m}(x) \;=\; \sum_{\substack{p^k \leq x \\ p \equiv a \bmod m}} \log(p) \;\;,\;\; \zeta_{a,m}(s) \;=\; \prod_{p \equiv a \bmod m} \frac{1}{1-p^{-s}} \;.$$

Dirichlet's density theorem

$\psi_{a,m}(x) = \frac{x}{\phi(m)} + o(x)$, *which for the zeta function reads*

$$\zeta_{a,m}(s) \;\sim\; (s-1)^{-\frac{1}{\phi(m)}}$$

for $s \to 1+$.

Not enough to answer Chebyshev's question since the main term does not depend on a. Moreover, we cannot look behind the line $\mathrm{Re}(s) = 1$ because there is no meromorphic continuation.

That is quite unfortunate: Loss of regularity means

- most tools of analytic number theory just don't work anymore,
- function behaviour for $\mathrm{Re}(s) > 1$ no longer related to critical strip,
- we cannot speak of poles/zeros in the critical strip.

Idea to attack such problems (Sarnak 1990's): Use strong assumptions on the distribution of the zeros of the functions $L(s, \chi)$ (GRH and GSH, both far out of reach) to proof a normal distribution of the primes in progressions. If both assumptions hold, there is indeed a bias in a more general setting. It is too small to turn up in the main term of the density theorem.

H. 2008: Relate these restricted products to analytic zeta functions using a functional equation system instead of a single functional equation to transfer analytic properties.

Chebyshev's question is a about arithmetic of the quadratic field $K = \mathbb{Q}(i)$:

- Prime numbers $p \equiv 1 \bmod 4$ are those which decompose in K: $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, $N(\mathfrak{P}_j) = p$, decomposition type $(e, f, g) = (1, 1, 2)$.
- Prime numbers $p \equiv 2 \bmod 4$ are those which ramify in K: $p\mathcal{O}_K = \mathfrak{P}^2$, $N(\mathfrak{P}) = p$, decomposition type $(e, f, g) = (2, 1, 1)$.
- Prime numbers $p \equiv 3 \bmod 4$ are those which are inert in K: $p\mathcal{O}_K = \mathfrak{P}$, $N(\mathfrak{P}) = p^2$, decomposition type $(e, f, g) = (1, 2, 1)$.

We use this to factorise the Dedekind zeta function of K

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \left(\frac{1}{1 - p^{-fs}} \right)^g .$$

Hence we have a decomposition

$$\zeta_K(s) = \left(\prod_{1 \bmod 4} \frac{1}{1-p^{-s}} \right)^2 \cdot \prod_{2 \bmod 4} \frac{1}{1-p^{-s}} \cdot \prod_{3 \bmod 4} \frac{1}{1-p^{-2s}} \cdot$$

Which we simply write as $\zeta_K(s) = \zeta_1(s)^2 \cdot \zeta_2(s) \cdot \zeta_3(2s)$.

We also have the trivial decomposition $\zeta_{\mathbb{Q}}(s) = \zeta_1(s)\zeta_2(s)\zeta_3(s)$.

We write this as a functional equation system:

	ζ_1	ζ_3	ζ_2
ζ_K	$2[1]$	$[2]$	$[1]$
$\zeta_{\mathbb{Q}}$	$[1]$	$[1]$	$[1]$

where $g[f]$ is a formal symbol, which acts on complex functions by $(f[g]) * L(s) = L(fs)^g$.

We can invert this system because its determinant $2[1] - [2]$ is not zero. Thus ζ_1 and ζ_3 are combinations of the analytic functions $\zeta_{\mathbb{Q}}$, ζ_K and ζ_2 ...but over which field and in which vector space?

So the main problems of this talk are

- Properly define the operators and the field in which they live.
  The field will be similar to a local field in many aspects, but it will not operate on meromorphic functions (we cannot hope for this, because already ζ_1 from the previous example is not meromorphic). We have to switch to the counting functions instead.

- Properly define the functional equation system for general settings.
  We have to choose n analytic zeta functions and relate them to precisely n arithmetic zeta functions using operators from our field. There will be multiple ways to do that.

- Show that the determinant does not vanish.
  For this we compute the principal component decomposition of the system. The eigenvalues turn out to be 1-units in the field.

  In fact this is a purely group theoretic phenomenon, which does not depend on number theoretic context.

A tool used frequently in analytic number theory is the Dirichlet algebra of arithmetic functions:

Definition

A function $f : \mathbb{N} \to \mathbb{C}$ is called arithmetic function. The set of these functions form a $\mathbb{C}$-algebra using addition of functions and Dirichlet's convolution

$$(f * g)(n) \;=\; \sum_{\substack{a,b\in\mathbb{N}\\ ab=n}} f(a)g(b)\,.$$

We have Dirichlet's identity

$$F(s) \;=\; \sum_{n=1}^{\infty} f(n)n^{-s} \;\;,\;\; G(s) \;=\; \sum_{n=1}^{\infty} g(n)n^{-s}$$

$$\Rightarrow \;\; F(s)\cdot G(s) \;=\; \sum_{n=1}^{\infty}(f*g)(n)n^{-s}\,.$$

Important arithmetic functions:

- The neutral element

$$\varepsilon(n) \;=\; \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases} \;,\; \sum_{n=1}^{\infty} \varepsilon(n) n^{-s} \;=\; 1\,.$$

- The 1-function

$$1(n) \;=\; 1 \;,\; \sum_{n=1}^{\infty} 1(n) n^{-s} \;=\; \zeta(s)\,.$$

- The Möbius inversion function $\mu = 1^{-1}$

$$\mu(n) \;=\; \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r \\ 0 & \text{otherwise} \end{cases} \;,\; \sum_{n=1}^{\infty} \mu(n) n^{-s} \;=\; \frac{1}{\zeta(s)}\,.$$

Idea for our field of operators: Turn this algebra into a field.

Definition

An extended arithmetic function is a function $f : (0, \infty) \to \mathbb{C}$ which has countable support which accumulates at most at 0. We form the extended convolution

$$(f * g)(x) = \sum_{\substack{a,b>0 \\ ab=x}} f(a)g(b)$$

which turns the set Q of these functions into a field.

Functions which are supported on a single point are denoted by

$$[m](x) = \begin{cases} 1 & \text{if } x = \frac{1}{m} \\ 0 & \text{otherwise} \end{cases}.$$

We have $[a] * [b] = [ab]$, and obtain the desired operation $[m] * f(x) = f(mx)$.

Definition

The absolute value $|f|$ of $f \in Q$ is the maximum of its support in $(0, \infty)$. We endow Q with the induced topology.

We have ultrametric inequality $|f+g| \leq \max(|f|, |g|)$, and call

- $R = \{f \in Q \ : \ |f| \leq 1\}$ the ring of integers of Q,
- $\mathfrak{m} = \{f \in Q \ : \ |f| < 1\}$ the maximal ideal of R,
- $U^{(1)} = [1] + \mathfrak{m}$ the group of 1-units contained in $Q^\times$.

Indeed $\mathfrak{m}$ is the unique maximal ideal of R. But Q is not a local field, unfortunately we have $\mathfrak{m}^n = \mathfrak{m}$ for every $n \in \mathbb{N}$, so the topology of Q is quite different from the classical local topology.

Analogue of the unit group decomposition: $Q^\times = (0, \infty) \times \mathbb{C}^\times \times U^{(1)}$, so $(0, \infty)$ plays the role of the valuation group.

The field Q is a nice and safe playground:

- The analogue of an infinite series

$$\sum_{n=1}^{\infty} a_n [b_n]$$

converges always in Q whenever (b_n) tends to infinity.

- Infinite products like

$$\prod_{n=1}^{\infty} \frac{1}{1-[b_n]}$$

converge always in Q whenever (b_n) tends to infinity.

- Especially, the inverse of a 1-unit always has a geometric series expansion

$$\frac{1}{1-f} = \sum_{k=0}^{\infty} f^{*k} .$$

The operation of most elements of Q on meromorphic functions is not well defined, either for convergence reasons or because complex powers z^w depend on the choice of a branch.

Enabling complex powers:
We switch to the negative logarithmic derivative

$$F(s) \;=\; -\frac{L'(s)}{L(s)}$$

which again is meromorphic, but now has only simple poles with $\mathrm{ord}_L(z) = \mathrm{Res}_F(z)$. Weil's explicit formula holds, we just have to replace ord by Res.

The operation of Q is now the linear continuation of the rule

$$[m].F(s) \;=\; mF(ms)$$

for $m > 0$, which is well defined.

Deposing convergence problems:

The connection between the negative logarithmic derivative $F(s)$ and the counting function $\psi(x)$ is given by the Mellin transform

$$F(s) \;=\; -\frac{L'(s)}{L(s)} \;=\; s\int_0^\infty \psi(x)x^{-s-1}dx$$

as seen at the beginning. The action $[m].F(s) = mF(ms)$ corresponds to

$$[m].\psi(x) \;=\; m\psi(x^{\frac{1}{m}})$$

on the right hand side.

This action is well defined for every $f \in Q$ whenever ψ is locally constant and its support is bounded away from 1.

The set of counting functions $\psi : (1,\infty) \to \mathbb{C}$ which

- are piecewise constant,
- have support bounded away from 1,

forms a Q-vector space with operation

$$\left(\sum a_j[b_j]\right).\psi(x) \;=\; \sum a_j b_j \psi(x^{\frac{1}{b_j}}) \,.$$

Note that for fixed $x > 1$ only finitely many terms contribute.

The equivalent series for complex functions

$$\left(\sum a_j[b_j]\right).F(s) \;=\; \sum a_j b_j F(b_j s)$$

does not converge in general.
We have to do Q-computations behind the Mellin integral.

The functional equation system from the introduction

	ζ_1	$\cdots$	ζ_n	E_1	$\cdots$	E_m
L_1	t_{11}	$\cdots$	t_{1n}	r_{11}	$\cdots$	r_{1m}
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
L_n	t_{n1}	$\cdots$	t_{nn}	r_{n1}	$\cdots$	r_{nm}

for the counting functions reads

$$\begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} = T. \begin{pmatrix} \varphi_1 \\ \vdots \\ \varphi_n \end{pmatrix} + R. \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix}$$

which is an inhomogeneous Q-linear equation system

- in indeterminates $\varphi_1, \ldots, \varphi_n$,
- with a square matrix T with components in Q,
- and the right hand side $\psi - R.\phi$, where each component is a counting function which has a Mellin transform which is meromorphic on $\mathbb{C}$ and satisfies Weil's formula.

The first nontrivial choice:

- Pick a normal number field K, and let
- $K_1, \ldots, K_n$ be the conjugation classes of cyclic subfields of K,
- $P_1, \ldots, P_n$ be the partition of the unramified prime numbers according to their decomposition behaviour in K.

The match is given by a bijection $\{P_1, \ldots, P_n\} \to \{K_1, \ldots, K_n\}$:

For a set P, $M = M(P)$ is the maximal subextension of $K/\mathbb{Q}$ in which every $p \in P$ is totally decomposed.

Inverse bijection:
An intermediate field M selects those prime numbers p, which have M as their decomposition field in $K/\mathbb{Q}$: for every $\mathfrak{p}|p$ the decomposition group $D_{\mathfrak{p}} = \{\sigma \in G(K/\mathbb{Q}) \ : \ \sigma(\mathfrak{p}) = \mathfrak{p}\}$ has fixed field M up to conjugation.

Well defined, because decomposition groups are always cyclic, and do not depend on the choice $\mathfrak{p}|p$ up to conjugation.

Enumerating the prime sets and intermediate fields according to the bijection we get

	ζ_1	$\cdots$	ζ_n	E_1	$\cdots$	E_m
L_1	t_{11}	$\cdots$	t_{1n}	r_{11}	$\cdots$	r_{1m}
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
L_n	t_{n1}	$\cdots$	t_{nn}	r_{n1}	$\cdots$	r_{nm}

where we put

$$\zeta_j(s) \;=\; \prod_{p\in P_j} \frac{1}{1-p^{-s}}$$

on the arithmetic side, and

$$L_j(s) \;=\; \zeta_{K_j}(s) \;=\; \prod_{\mathfrak{p}\trianglelefteq \mathcal{O}_{K_j}} \frac{1}{1-N(\mathfrak{p})^{-s}}$$

on the analytic side. The finitely many primes $p_1,\ldots,p_m$ which ramify in K are attached to single Euler factors

$$E_j(s) \;=\; \frac{1}{1-p_j^{-s}} \;\; \text{(on the analytic side)}.$$

The component $t_{ij} \in Q$ then is given by the decomposition type of $p \in P_j$ in the intermediate field K_i:

$$p\mathcal{O}_{K_i} \;=\; \mathfrak{p}_1 \cdots \mathfrak{p}_g \;\;,\;\; N(\mathfrak{p}_k) \;=\; p^{f_k} \quad \Rightarrow \quad t_{ij} \;=\; \sum_{k=1}^{g} [f_k] \,.$$

For the ramified primes we have to put

$$p\mathcal{O}_{K_i} \;=\; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \;\;,\;\; N(\mathfrak{p}_k) \;=\; p^{f_k} \quad \Rightarrow \quad r_{ij} \;=\; \sum_{k=1}^{g} [f_k] \,.$$

Then we obtain for row each intermediate field K_i the equation

$$L_i(s) \;=\; \prod_{j=1}^{n} t_{ij}.\zeta_j(s) \;\cdot\; \prod_{j=1}^{m} r_{ij}.E_j(s)$$

which is just the i-th row of our system.

Pre-Theorem

For every normal number field K and the partition $P_1, \ldots, P_n$ given above, the partial zeta functions

$$\zeta_j(s) = \prod_{p \in P_j} \frac{1}{1 - p^{-s}}$$

are formal Q-linear combinations of Dedekind zeta functions and single Euler factors.

...only formal because the action of Q has no meaning on zeta functions.

Note that the components t_{ij} and r_{ij} have finite support, so their action is defined. But we will see that the determinant is not $[1]$, so the linear combinations have non-finite components.

The inversion is well defined for $\mathrm{Re}(s) > 1$, because the Euler factors drop very fast as $\mathrm{Re}(s) \to \infty$. Sadly that is precisely the half plane which we are not interested in.

Theorem (H. 2009)

For every normal number field K and the partition $P_1, \ldots, P_n$ given above, the partial counting functions

$$\psi_j(x) = \sum_{\substack{p^k \leq x \\ p \in P_j}} \log(p)$$

are Q-linear combinations of Chebyshev's counting functions of intermediate fields of $K/\mathbb{Q}$ and single prime numbers.

Remember that Riemann and Chebyshev were interested in $\psi(x)$ in the first place, the Dirichlet series $\zeta(s)$ is just a tool to analyse it.

Proof of theorem: Determinant of the functional equation system is not zero, and Q is a field.

For the example $K = \mathbb{Q}(i)$ from the introduction, we obtain

$$F_1(x) \;=\; \frac{1}{2[1]-[2]} \cdot (F_K(s) - 2F_{\mathbb{Q}}(2s) - F_2(s) + 2F_2(2s))$$

and

$$F_3(x) \;=\; \frac{1}{2[1]-[2]} \cdot (-F_K(s) + 2F_{\mathbb{Q}}(s) - F_2(s))$$

for the logarithmic derivatives of the partial Euler products by solving the Q-linear equation system. These are identities of analytic functions on the half plane $\mathrm{Re}(s) > 1$.

A refinement of this theorem is obtained by the following choice:

- Pick a normal number field K,
- Let $L_1, \ldots, L_n$ be the Artin L-series on $\mathbb{Q}$ defined by the $n = [K : \mathbb{Q}]$ irreducible group characters $\chi : G(K/\mathbb{Q}) \to \mathbb{C}^\times$.
- Let $P_1, \ldots, P_n$ be the partition of the unramified prime numbers given by the characters.

For a prime number p and a character χ we put

$$\chi(p) = \chi(\left[\frac{K/\mathbb{Q}}{\mathfrak{p}}\right])$$

for the Artin symbol and any $\mathfrak{p}|p$, and form the partition $P_1, \ldots, P_n$ induced by the map $\chi_1, \ldots, \chi_n : P \to \mathbb{C}^n$.

Here the bijection and the formulation of the operators is difficult: We have to formulate the insertion of a character

$$\prod \frac{1}{1 - p^{-s}} \mapsto \prod \frac{1}{1 - \chi(p)p^{-s}}$$

as the action of an element of Q which must not depend on p, but on the set P_j.

Note that the counting function for L_j now is defined by

$$\psi(x) \;=\; \sum_{p^n \leq x} \log(p)\chi(p^n)$$

so the power of p enters χ, hence it is not constant even if the prime number comes from a fixed set P_j.

We encode the powers in a series in Q. But how to define it?

For the trivial character $\chi(n) = 1(n)$ we want it to be $\varepsilon(n)$, so we convolute χ with the Möbius function $\mu = 1^{-1}$:

$$t_{\chi,j} \;=\; \sum_{k=1}^{\infty} \frac{[n]}{n} \sum_{ab=k} \mu(a)\chi(p)^b \,.$$

Here $\chi(p)$ only depends on the set P_j, not p itself.

$$t_{\chi,j}.\psi_j(x) \;=\; \left(\sum_{k=1}^{\infty}\frac{[k]}{k}\sum_{ab=k}\mu(a)\chi(p)^b\right)\;.\sum_{\substack{p^k\leq x\\ p\in P_j}}\log(p)$$

$$=\sum_{k=1}^{\infty}\sum_{ab=k}\mu(a)\chi(p)^b\sum_{\substack{p^n\leq x^{\frac{1}{k}}\\ p\in P_j}}\log(p)$$

$$=\sum_{p\in P_j}\sum_{n=1}^{\infty}\sum_{a,b=1}^{\infty}\mu(a)1[p^{abn}\leq x]\chi(p)^b\log(p)\;=\;\sum_{p\in P_j}\sum_{n=1}^{\infty}\sum_{a=1}^{\infty}\mu(a)\psi_{\chi,p}(x^{\frac{1}{an}})$$

$$=\sum_{p\in P_j}\sum_{m=1}^{\infty}\psi_{\chi,p}(x^{\frac{1}{m}})\underbrace{\sum_{an=m}\mu(a)1(n)}_{=\varepsilon(m)}\;=\;\psi_{\chi,j}(x)\,.$$

Theorem (H. 2009)

For every normal number field K and the partition $P_1, \ldots, P_n$ induced by the characters, the partial weighted counting functions

$$\psi_{\chi,j}(x) = \sum_{\substack{p^k \leq x \\ p \in P_j}} \log(p)\chi(p^k)$$

are Q-linear combinations of counting functions associated to Artin L-series.

We have to take some additional care if K is not abelian. Then the insertion of the Frobenius determinant is more complex.

So far, we have just played around with counting functions. How can we translate the poles from the analytic side to the arithmetic side?

Different actions of $[m]$ on functions:

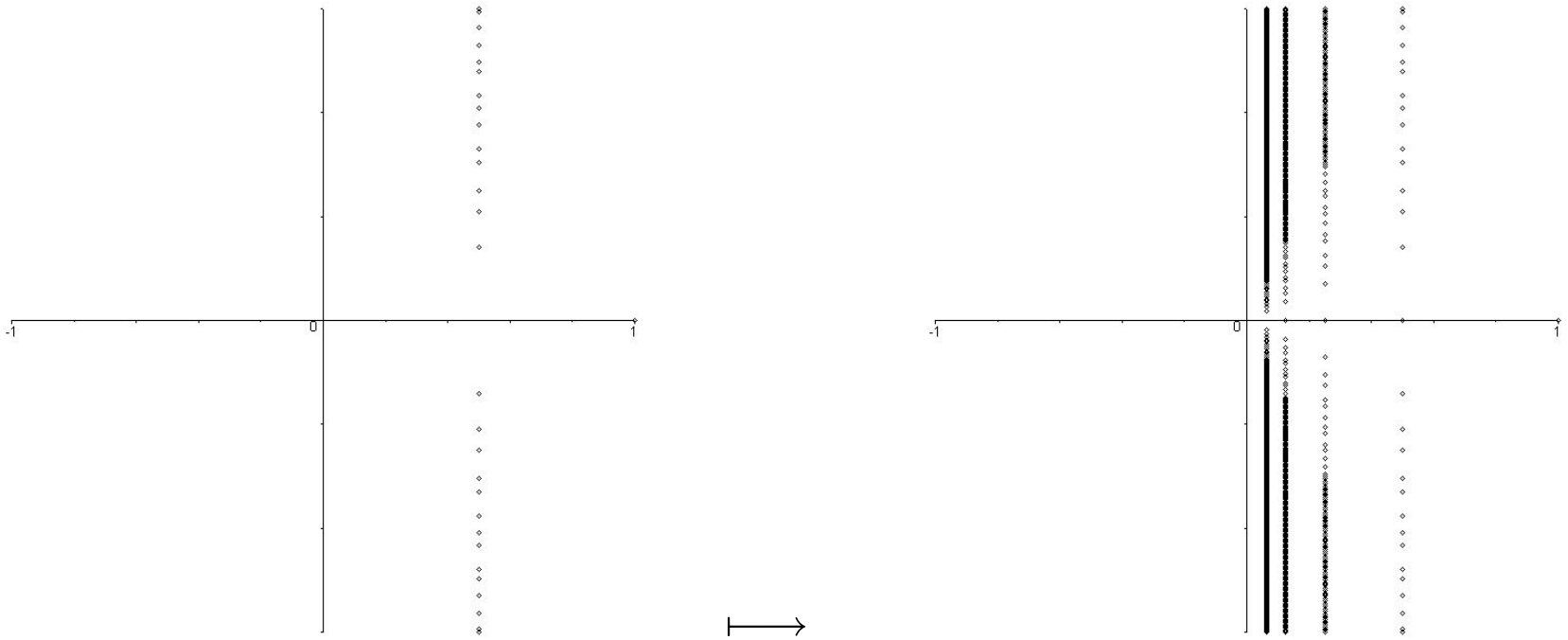
- On zeta functions $[m].\zeta(s) = ([m] * \zeta)(s) = \zeta(ms)$ inserts an exponent by definition,
- on logarithmic derivatives the action $[m].F(s) = mF(ms)$ moves simple poles

$$[m] \, . \, \frac{1}{s-\varrho} \quad = \quad \frac{m}{ms-\varrho} \quad = \quad \frac{1}{s-\varrho/m}$$

  and preserves their residues.

So a Q-linear combination of functions $\psi_\chi(x)$ is attached to a pole set with residues, also if the associated zeta function has no meromorphic continuation.

Thus we can visualise the asymptotic behaviour by a pole set:



This action comes from the geometric series expansion

$$\frac{1}{[1]-\frac{1}{2}[2]} = \sum_{k=0}^{\infty} 2^{-k}\left[2^k\right] .$$

$\Rightarrow$ Q translates zero free regions from analytic to arithmetic side.

Give and take: Arithmetic zeta functions have some properties that would be nice to have for analytic zeta functions.

Gel'fond-Schneider theorem implies that zeta functions $\zeta_1, \ldots, \zeta_n$ belonging to arbitrary prime number partitions are linearly independent if we put $Q = \mathbb{C}(\mathbb{Q}^+)$ instead of $Q = \mathbb{C}((0, \infty))$.

Corollary

Given a normal number field K and the set $\{K_j\}$ of cyclic subextensions of $K/\mathbb{Q}$ up to conjugation, then the zeta functions $\zeta_{K_j}(s)$ are formally Q-linearly independent (proper version for the counting functions).

$\mathbb{C}$-linear independence was already known.
But Q-operations also stretch and squeeze the pole set.

Much weaker then GSH, because Q operates on all poles simultaneously.

Give and take: Arithmetic zeta functions have some properties that would be nice to have for analytic zeta functions.

In the author's opinion, the theorem which comes closest to Riemann's hypothesis is

Bombieri-Vinogradov

We have the asymptotic

$$\sum_{m \leq y} \max_{\substack{a \bmod m \\ \gcd(a,m)=1}} \left| \psi_{a,m}(x) - \frac{x}{\phi(m)} \right| = O\left(y x^{\frac{1}{2}} \log(x) \right)$$

for $\sqrt{x} \log^{-c}(x) \leq y \leq \sqrt{x}$.

which means that Riemann's hypothesis is true on the average over the arithmetic progressions.

What does it imply for the zeros of the functions $L(s, \chi)$?
...still work in progress, nonlinear operation max is main obstruction.

A nontrivial example: Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be a D_6-extension of $\mathbb{Q}$.

Analytic side:

Its cyclic subextensions are K, $K' = \mathbb{Q}(\omega)$ and the conjugate fields $K_j = \mathbb{Q}(\sqrt[3]{2} \cdot \omega^j)$.

Arithmetic side:

The possible unramified decomposition types are

- Decomposition field K: $p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_6$.
- Decomposition field K': $p\mathcal{O}_{K'} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{P}_i$.
- Decomposition field K_j: $p\mathcal{O}_{K_j} = \mathfrak{p}$ (fixed j) with $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$.

Arithmetic determinant is

$$\begin{vmatrix} 6[1] & 3[2] & 2[3] \\ 3[1] & [1]+[2] & [3] \\ 2[1] & [2] & 2[1] \end{vmatrix} = 2^2 \cdot 3 \cdot \left([1] - \frac{[2]}{2}\right) \cdot \left([1] - \frac{[3]}{3}\right).$$

For a finite group, form the extended matrix $T = (t_{gh})$ over Q with

$$t_{gh} = \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a) 1[g^b = h] \quad , \quad g, h \in G$$

where the elements of G have a fixed ordering. The characteristic polynomial of the matrix associated to the Artin-L-series is a divisor of $\det(T - \lambda \mathrm{id})$ in $Q[\lambda]$: Using Q-elementary row transformations we can construct the characters $G \to \mathbb{C}$ from the indicator functions, and group them in a block matrix. Other choices of matches result in other groupings.

T itself corresponds to the finest matching possible.
It therefore suffices to show $\det(T) \neq 0$ over the field Q.

Theorem (H. 2009), Part I

For every finite group G, the extended matrix has a principal component decomposition

$$T = F \cdot D \cdot E \cdot F^{-1}$$

with

$$D = \begin{pmatrix} 1 & & & \\ * & \ddots & & \\ \vdots & \ddots & \ddots & \\ * & \cdots & * & 1 \end{pmatrix}, \quad E = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

for $\lambda_j \in Q$ which are 1-units, a unitary matrix $F \in \mathbb{C}^{n \times n}$, and $D \in R_f^{n \times n}$.

Theorem (H. 2009), Part II

The eigenvalues have a convergent product expansion

$$\lambda \;=\; \lambda_\varphi \;=\; \prod_p \frac{[1]-\frac{1}{p}[p]}{[1]-\frac{\varphi(p)}{p}[p]}$$

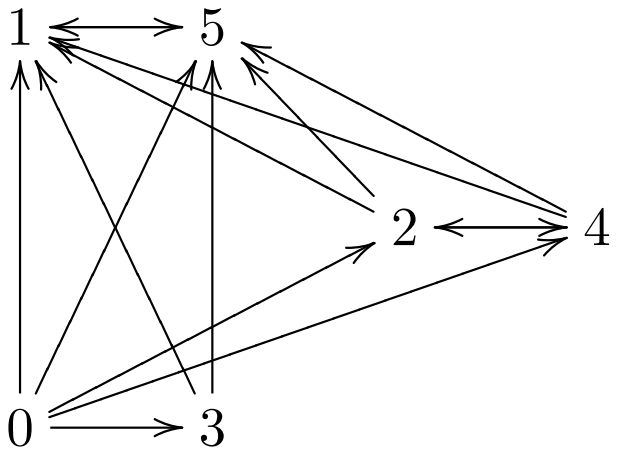
for Dirichlet characters φ. The eigenvalue has finite support if and only if φ is a principal character, in this case we have

$$\lambda \;=\; \lambda_m \;=\; \prod_{p|m}\left([1]-\frac{1}{p}[p]\right)\;.$$

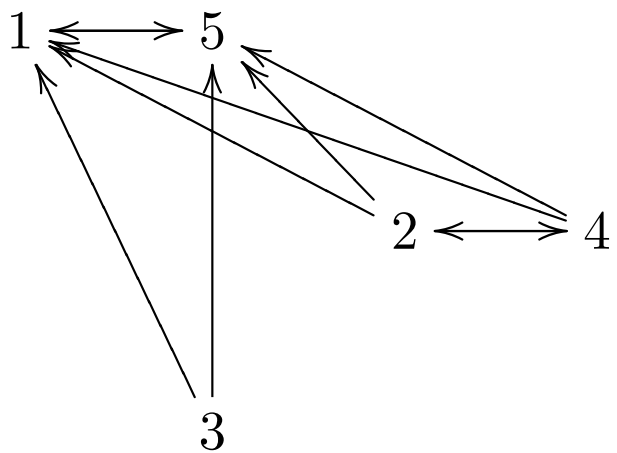
For the proof, we need the generator graph of the group G:

- Its vertices are the elements of G,
- (g, h) is an edge if and only if $g \in \langle h \rangle$.
- A prime subgraph is a subgraph which is fully associated, and has no ingoing edges.
- The factorisation of G is computed by removing such subgraphs iteratively. Each subgraph is associated to a set of principal vectors.

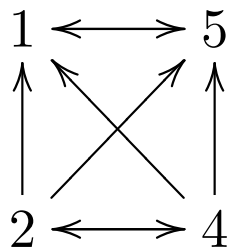
An example: $G = \mathbb{Z}/6\mathbb{Z}$. The generator graph of this group is



where we exclude the reflexive edges (g, g).
We remove the root 0. In the next step, the graph is



Now we remove the root 3, which is itself a prime subgraph.



Here $\{2,4\}$ is a totally associated subgraph with no ingoing edges. We remove these vertices, the remaining graph now is $1 \leftrightarrow 5$.

So the factorisation of $\mathbb{Z}/6\mathbb{Z}$ is given by the sets

$$\{0\}\ ,\ \{3\}\ ,\ \{2,4\}\ ,\ \{1,5\}\ .$$

Components of T are

$$t_{gh} = \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a) 1[g^b = h] \, .$$

Lemma

Eigenvectors are of the form

$$f = \big(f(g)\big)_{g \in G}$$

where $f : G \to \mathbb{C}$ satisfies a functional equation $f(g^k) = \varphi(k) f(g)$ for some Dirichlet character mod m.

Principal vectors are of this form, but satisfy the functional equation only on some prime subgraph of G, and are zero on the complement.

Proof of the lemma: Multiplying T with f we get

$$\forall g \in G: \ (Tf)_g \ = \ \sum_{h\in G} t_{gh} f(h) \ = \ \sum_{h\in G} \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a) \underbrace{1[g^b = h] f(h)}_{\text{selects } f(g^b)}$$

$$= \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a) f(g^b) \ \underset{\text{FEQ}}{=} \ \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a)\varphi(b) f(g) \ = \ \lambda \cdot f_g$$

for the eigenvalue

$$\lambda \ = \ \lambda_\varphi \ = \ \sum_{k=1}^{\infty} \frac{[k]}{k} \sum_{ab=k} \mu(a)\varphi(b) \ = \ \prod_p \frac{[1] - \frac{1}{p}[p]}{[1] - \frac{\varphi(p)}{p}[p]}$$

which is always a 1-unit of Q.

For the theorem, it remains to show that the principal f form a basis.

We use the following enumeration argument:

- A prime subgraph S containing an element g of order m satisfies $S = \{g^k \ : \ \gcd(k, m) = 1\}$, so it has precisely $\phi(m)$ vertices.

- For each every S, we fix a vertex $g_S \in S$ and put $f(g_S) = 1$. Each of the $\phi(m)$ Dirichlet characters mod m then defines the function f on the subgraph by the functional equation, and we put $f(g) = 0$ for $g \notin S$.

- We obtain for every subgraph S precisely $|S| = \phi(m)$ principal vectors, so in total we get $|G| = \sum |S|$ principal vectors. There cannot be more.

- These functions f are linearly independent in Q^n. This is obvious if a selection of them is defined on different subgraphs, otherwise we use that different Dirichlet characters on the same group are linearly independent.

Basic rule for every prime subgraph: Order of elements is modulus m, number of elements is $\phi(m)$.

- $S = \{0\}$: We have $f(g) = 1$ if $g = 0$ and $f(g) = 0$ otherwise. Case $m = 1$, the eigenvalue is $\lambda_1 = [1]$.
- $S = \{3\}$: We have $f(g) = 1$ if $g = 3$ and $f(g) = 0$ otherwise. Case $m = 2$ and $\phi(m) = 1$, eigenvalue is $\lambda_2 = 1 - \frac{1}{2}[2]$.
- $S = \{2, 4\}$: Here the functions

$$f_1(g) = \begin{cases} 1 & \text{if } g = 2, 4 \\ 0 & \text{otherwise} \end{cases}, \quad f_2(g) = \begin{cases} 1 & \text{if } g = 2 \\ -1 & \text{if } g = 4 \\ 0 & \text{otherwise} \end{cases}$$

  are associated to the two Dirichlet characters mod 3.
- $S = \{1, 5\}$: Here the functions

$$f_1(g) = \begin{cases} 1 & \text{if } g = 1, 5 \\ 0 & \text{otherwise} \end{cases}, \quad f_2(g) = \begin{cases} 1 & \text{if } g = 1 \\ -1 & \text{if } g = 5 \\ 0 & \text{otherwise} \end{cases}$$

  are associated to the two Dirichlet characters mod 6.

So we compute the arithmetic determinant $\det(T) = \det(\mathbb{Z}/6\mathbb{Z})$ as follows:

$$\det(T) \;=\; \lambda_1 \cdot \lambda_2 \cdot \lambda_3\lambda_3' \cdot \lambda_6\lambda_6' \,.$$

For the decomposition matching, we have to select the principal characters:

$$\lambda_1 \cdot \lambda_2 \cdot \lambda_3 \cdot \lambda_6 \;=\; [1] \cdot \left(1 - \frac{[2]}{2}\right) \cdot \left(1 - \frac{[3]}{3}\right) \cdot \left(1 - \frac{[2]}{2}\right)\left(1 - \frac{[3]}{3}\right)$$

$$= \left(1 - \frac{[2]}{2}\right)^2 \cdot \left(1 - \frac{[3]}{3}\right)^2$$

times a complex constant (coming from the matrix block grouping operations).

Examples computed using a computer:

Isomorphism type	$\det$
$\{1\}$ (trivial)	$[1]$
C_2 (cyclic)	$2 \cdot ([1] - \frac{1}{2}[2])$
C_4 (cyclic)	$2^3 \cdot ([1] - \frac{1}{2}[2])^2$
C_8 (cyclic)	$2^6 \cdot ([1] - \frac{1}{2}[2])^3$
C_3 (cyclic)	$3 \cdot ([1] - \frac{1}{3}[3])$
C_9 (cyclic)	$3^3 \cdot ([1] - \frac{1}{3}[3])^2$
C_6 (cyclic)	$2^2 3^2 \cdot ([1] - \frac{1}{2}[2])^2 \cdot ([1] - \frac{1}{3}[3])^2$
C_{12} (cyclic)	$2^6 3^3 \cdot ([1] - \frac{1}{2}[2])^4 \cdot ([1] - \frac{1}{3}[3])^3$
C_{24} (cyclic)	$2^{12} 3^4 \cdot ([1] - \frac{1}{2}[2])^6 \cdot ([1] - \frac{1}{3}[3])^4$
C_2^2 (abelian)	$2^5 \cdot ([1] - \frac{1}{2}[2])^3$
C_2^3 (abelian)	$2^{17} \cdot ([1] - \frac{1}{2}[2])^7$
C_2^4 (abelian)	$2^{49} \cdot ([1] - \frac{1}{2}[2])^{15}$
$C_2 \times C_4$ (abelian)	$2^{11} \cdot ([1] - \frac{1}{2}[2])^5$
D_8 (dihedral)	$2^8 \cdot ([1] - \frac{1}{2}[2])^4$
Q_8 (quaternion)	$2^8 \cdot ([1] - \frac{1}{2}[2])^4$
$\mathcal{A}_4$ (alternating)	$2^3 3 \cdot ([1] - \frac{1}{2}[2]) \cdot ([1] - \frac{1}{3}[3])$

Some side effects (computational aspect):

- Determinants don't get too complicated, for example the sporadic Mathieu group M_{12} of 7920 elements has arithmetic determinant (with respect to the decomposition matching)

$$c \cdot \left([1] - \frac{[2]}{2}\right)^8 \cdot \left([1] - \frac{[3]}{3}\right)^2 \cdot \left([1] - \frac{[5]}{5}\right) \cdot \left([1] - \frac{[11]}{11}\right) .$$

- Algorithm to compute $\det$ symbolically is quite simple and, surprisingly, involves no linear algebra at all.

The algorithm sets up the generator graph of the group G, and for each prime subgraph of elements of order n, adds the $\phi(n)$ Dirichlet characters mod n to the list of eigenvalues.

The difficult part is to find those which belong to the chosen matching of analytic and arithmetic functions.

For the matching subfield$\leftrightarrow$decomposition it is simple: Select finitely supported eigenvalues, i.e. those belonging to principal characters.

Some side effects (number theoretic aspect):

- Matching exists and $\det(G) \neq 0$ for every finite group G, even if there is no number field satisfying $G(K/\mathbb{Q}) = G$.
- Finest possible matching associated to the unmodified extended matrix exists, but what is its number theoretic interpretation? Some L-function formed using arbitrary group functions instead of characters, but the left hand side is no longer analytic, or is it?
- Be careful: Topology of Q is quite weak, so „convergence of pole locations“ should be treated with care. No problems if there is no accumulation on the half plane $\mathrm{Re}(s) > 0$, but on the line $\mathrm{Re}(s) = 0$ strange things happen...
- Every discrete set is in the Q-span of P and vice versa: In a certain sense Weil's formula holds true for every set of numbers, and does not depend on any number theoretic conditions, but we loose the analytic properties of the right hand side.

Some last remarks:

- It's a technique to relate analytic and arithmetic sides, it has to be fitted to the problem at hand.
- Chebyshev's question remains open until someone comes up with the zeros of $L(s, \chi)$. But then they will determine $\psi_{a,m}(x)$ without error term, GSH is not required. In some sense, the Q-linear independence of the zeta functions is enough.
- Concepts of arithmetic group determinants may have other uses: for example an algorithm that decides if two groups are isomorphic.

.....thanks for your patience.