Montréal Summer School

Typical and Atypical values of some number theoretic functions

This minicourse is intended to be a high level overview of many important results taking place at the intersection of number theory and probability. Some of what is covered is classical, whilst others have appeared in recent years

These notes have been heavily influenced and inspired by many authors, and I direct the interested reader to their excellent resources including (but not limited to!)

Elliott, Tenenbaum, Koukoulopoulos,

Kowalski, Harper (particularly the Bourbaki notes)

Finally I have also created a Jupyter notebook with various exercises/plots included. The aim of the notebook is to be able to visualise some of the results mentioned henceforth. It is available on Github under

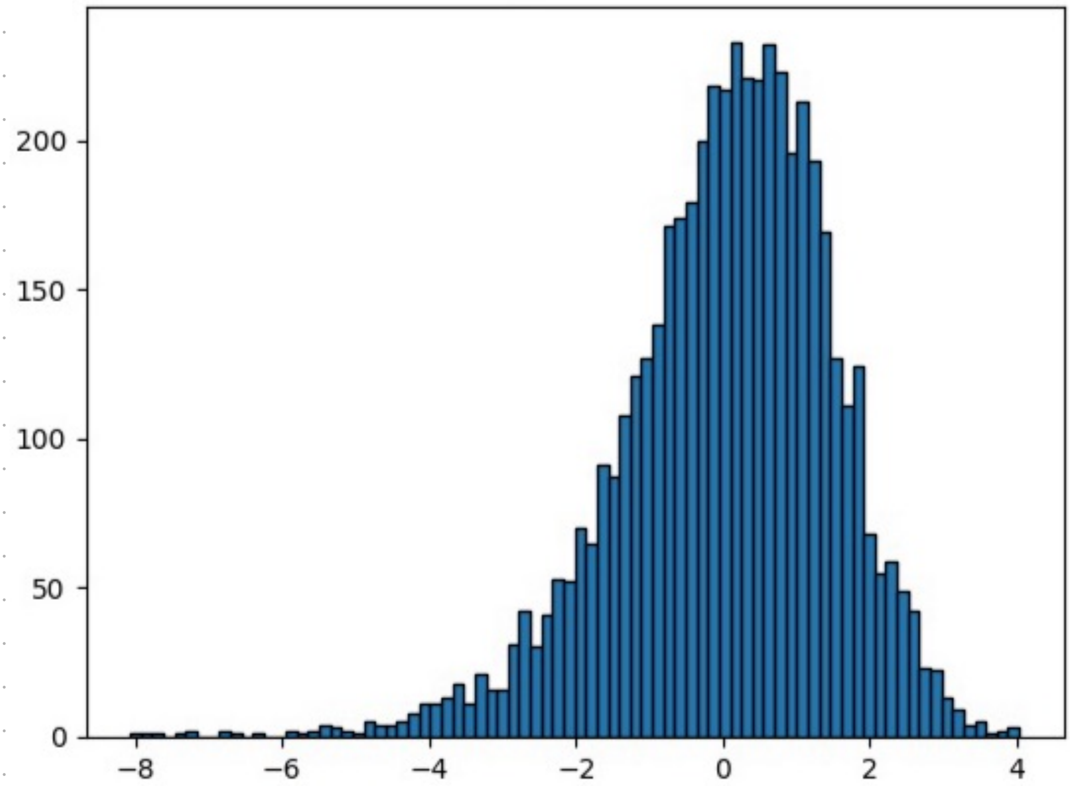
ecbaile/pnt_exercises.

Section 1 Classical results in NT and PNT.

Looking forward: By the end of this mini-course, I will explain some of the fundamental ideas behind recent progress in understanding atypical values of the Riemann ζ-f^n

All relevant number theoretic ideas will be introduced. Many of the ideas apply much more widely (e.g. atypical values of characteristic polynomials) and come from probability.

One of the key themes of the course is understanding the following picture:



This is a plot of 5000 values of

$$\mathrm{Re}\left(\log \zeta\left(\tfrac{1}{2} + i\gamma\right)\right)$$

where $\gamma \sim \mathrm{Unif}\,[10^6, 2 \times 10^6]$.

Try to recreate it yourself! (There will be a link to a Google Colab file where you can run through the code used to produce the images in this course.)

Related questions are therefore:

* Does the random variable
$$X = \mathrm{Re}\left(\log \zeta\left(\tfrac{1}{2}+i\tau\right)\right)$$
for $\tau \sim \mathrm{Unif}[T, 2T]$ satisfy a CLT?

* What implications does this have for $\zeta(s)$?

* What about atypical values (e.g. those beyond the standard deviation)?

First, some introductory results from probabilistic number theory.

Def. A function $f: \mathbb{N} \to \mathbb{C}$ is *additive* if
$$f(ab) = f(a) + f(b)$$
whenever a and b are coprime.
If the property holds for all a, b then

f is said to be completely additive.

↳ This means that if f is additive then it is sufficient to understand the value of f at the prime powers

$$f(n) = \sum_{i=1}^{r} f(p_i^{a_i})$$

if n's prime factorisation is $p_1^{a_1} \cdots p_r^{a_r}$.

Ex Two useful arithmetic functions are

additive

$$\omega(n) = \sum_{p|n} 1$$

$= \#\{$ prime factors of n without multiplicity $\}$

completely additive

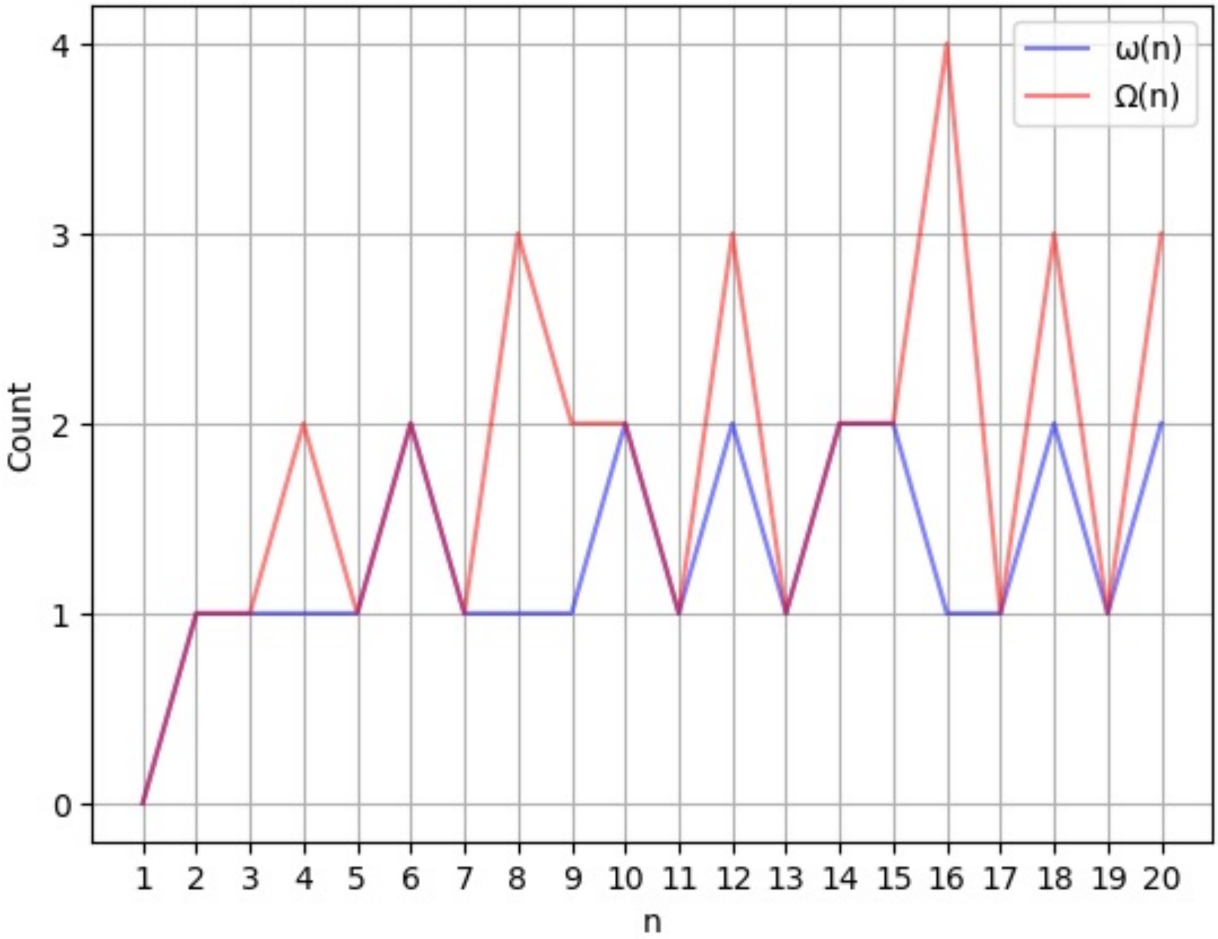
$$\Omega(n) = \sum_{p^k|n} 1$$

$= \#\{$ prime factors of n with multiplicity $\}$

So if $n = p_1^{a_1} \cdots p_r^{a_r}$ then

$\omega(n) = r$ $\qquad$ $\Omega(n) = \sum_{i=1}^{r} a_i$

Here are some plots of the first few values of $\omega(n)$, $\Omega(n)$:



<u>Q</u> If I pick an integer at random, how many distinct prime factors will it have?

In the notation above, what is

$$\mathbb{E}_N[\omega]$$

where the expectation is with respect to the discrete uniform dist on $\{1, \dots, N\}$ for some large N?

The answer to this question is due to Kac (and we will learn even more about ω through the Erdős-Kac theorem shortly).

Let f be additive. Then for $n \leq N$,

$$f(n) = \sum_{p \leq N} \sum_{k \geq 1} f(p^k) \mathbb{1}\{p^k \text{ exactly divides } n\}$$

Hence, can we first understand the likelihood of a given set of prime powers dividing a given integer n?

exactly div.

$$\mathbb{P}_N \left(p_1^{k_1} \| n \text{ and } p_2^{k_2} \| n \text{ and} \cdots p_r^{k_r} \| n \right)$$

discrete unif on $\{1, \dots, N\}$

Assume $p_1, \dots, p_r$ distinct

$$= \frac{1}{N}\#\{n \le N : p_i^{k_i} \mid n \text{ for } i=1,\dots,r \text{ but } p_i^{k_i+1} \nmid n \text{ for } i=1,\dots,r\}$$

So we want the number of $n \le N$ s.t. n is indivisible by $p_i^{k_i+1}$ for $i=1,\dots,r$ but divisible by all $p_i, p_i^2, \dots, p_i^{k_i}$.

So think of breaking N up in to multiples of $p_1^{k_1+1}\cdots p_r^{k_r+1}$. Within each block, there are exactly

$$\phi(p_1\cdots p_r) = (p_1-1)\cdots(p_r-1)$$

such values (see below for an example) and hence the above is

$$= \frac{1}{N}\left(\underbrace{\overbrace{\left[\frac{N}{p_1^{k_1+1}\cdots p_r^{k_r+1}}\right]}^{\text{integer part}}}_{\#\text{blocks}} \underbrace{\phi(p_1\cdots p_r)}_{\#\text{'good' ints per block}} + \underbrace{\left\{\frac{N}{\prod_{i=1}^r p_i^{k_i+1}}\right\}}_{\text{fractional part}} \phi(p_1\cdots p_r) \right)$$

(for distinct $p_1,\dots,p_r$ and positive ints $k_1,\dots,k_r$)

Ex $N=100$, $p_1^{k_1}=2^2$, $p_2^{k_2}=3$ How many $n\le 100$ are there such that $4|n$ and $3|n$ but $8\nmid n$ nor does $9|n$?

Divide in to blocks of $p_1^{k_1+1}\cdot p_2^{k_2+1}=72$:

1 2 3 4 5 6 7 8 ...... 67 68 69 70 71 72

73 74 75 76 ---- 94 95 96 97 98 99 100

In the top block there are $\dfrac{p_1^{k_1+1}\,p_2^{k_2+1}}{p_1^{k_1}p_2^{k_2}}=p_1p_2$ candidates for integers divisible by both $p_1^{k_1}$ and $p_2^{k_2}$ (hence by $p_1^{k_1}p_2^{k_2}$). How many of these multiples are themselves divisible by $p_1^{k_1+1}$ or $p_2^{k_2+1}$?

Suppose for $1\le m\le p_1p_2$

$$p_1^{k_1+1}\mid m\cdot p_1^{k_1}\cdot p_2^{k_2} \implies p_1\mid m$$

and similarly for p_2.

So the "bad" options amongst $1 \leq m \leq p_1 p_2$ are those multiples of p_1, p_2. Not over-counting we get $p_1 p_2 - p_2 - p_1 + 1 = (p_1 - 1)(p_2 - 1)$.

Scaling up to general $p_1^{k_1} \cdots p_r^{k_r}$ we see that we want the integers $1 \leq a \leq p_1 \cdots p_r$ that are coprime to $p_1, \ldots, p_r$, i.e.

$$\phi(p_1 \cdots p_r) = p_1 \cdots p_r \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

$$= (p_1 - 1) \cdots (p_r - 1)$$

Euler totient f^n.

Overall therefore there are <u>two</u> values between 1 and 72 s.t. $4 \mid n$, $3 \mid n$ but $8 \nmid n$, $9 \nmid n$, and between 73 and 100 we find <u>one</u> extra value (84).

Therefore

exactly divides

$$\mathbb{P}_N\left(\bigcap_{i=1}^{r}\{p_i^{k_i} \| n\}\right) = \prod_{i=1}^{r} \frac{\phi(p_i)}{p_i^{k_i+1}} + O\left(\frac{\phi(p_1\cdots p_r)}{N}\right)$$

as $x = [x] + \{x\}$
and $\{x\} \in [0,1)$

Thus, if $\frac{\phi(p_1\cdots p_r)}{N} = O\left(\frac{p_1\cdots p_r}{N}\right)$ is small

then we effectively have

$$\boxed{\mathbb{P}_N\left(\bigcap_{i=1}^{r}\{p_i^{k_i} \| n\}\right) \approx \prod_{i=1}^{r} \mathbb{P}_N\left(p_i^{k_i} \| n\right)}$$

$\Rightarrow$ effectively independence for different primes!

and since if f is additive and $n = p_1^{a_1}\cdots p_r^{a_r}$

$$f(n) = \sum_{i=1}^{r} f(p_i^{a_i}) = \sum_{p\leq n}\sum_{a\geq 1} f(p^a)\mathbb{1}\{p^a \| n\}$$

If n is drawn randomly from $\{1,\dots,N\}$ then f is effectively the sum of independent variables.

$$f(n) = \sum_{p\leq N} f_p(n)$$

$$f_p(n) =: \sum_{a\geq 1} f(p^a)\mathbb{1}\{p^a \| n\}$$

We can then find the corresponding expectation:

Lemma Let $f: \mathbb{N} \to \mathbb{C}$ be additive, then

$$\mathbb{E}_N[f] = \sum_{p^k \leq N} \frac{f(p^k)\,\phi(p)}{p^{k+1}} + \Theta\left(\frac{1}{N}\sum_{p^k \leq N} |f(p^k)|\right)$$

sum over all primes and their powers below N

In particular, if we take $\omega: \mathbb{N} \to \mathbb{C}$ as the additive function then

$$\mathbb{E}_N[\omega] = \sum_{p \leq N} \frac{1}{p}\left(1 - \frac{1}{p}\right) + \sum_{p \leq \sqrt{N}} \frac{1}{p^2}\left(1 - \frac{1}{p}\right) + \dots + \Theta\left(\frac{1}{N}\sum_{p^k \leq N} 1\right)$$

$$= \sum_{p \leq N} \frac{1}{p} + \Theta(1)$$

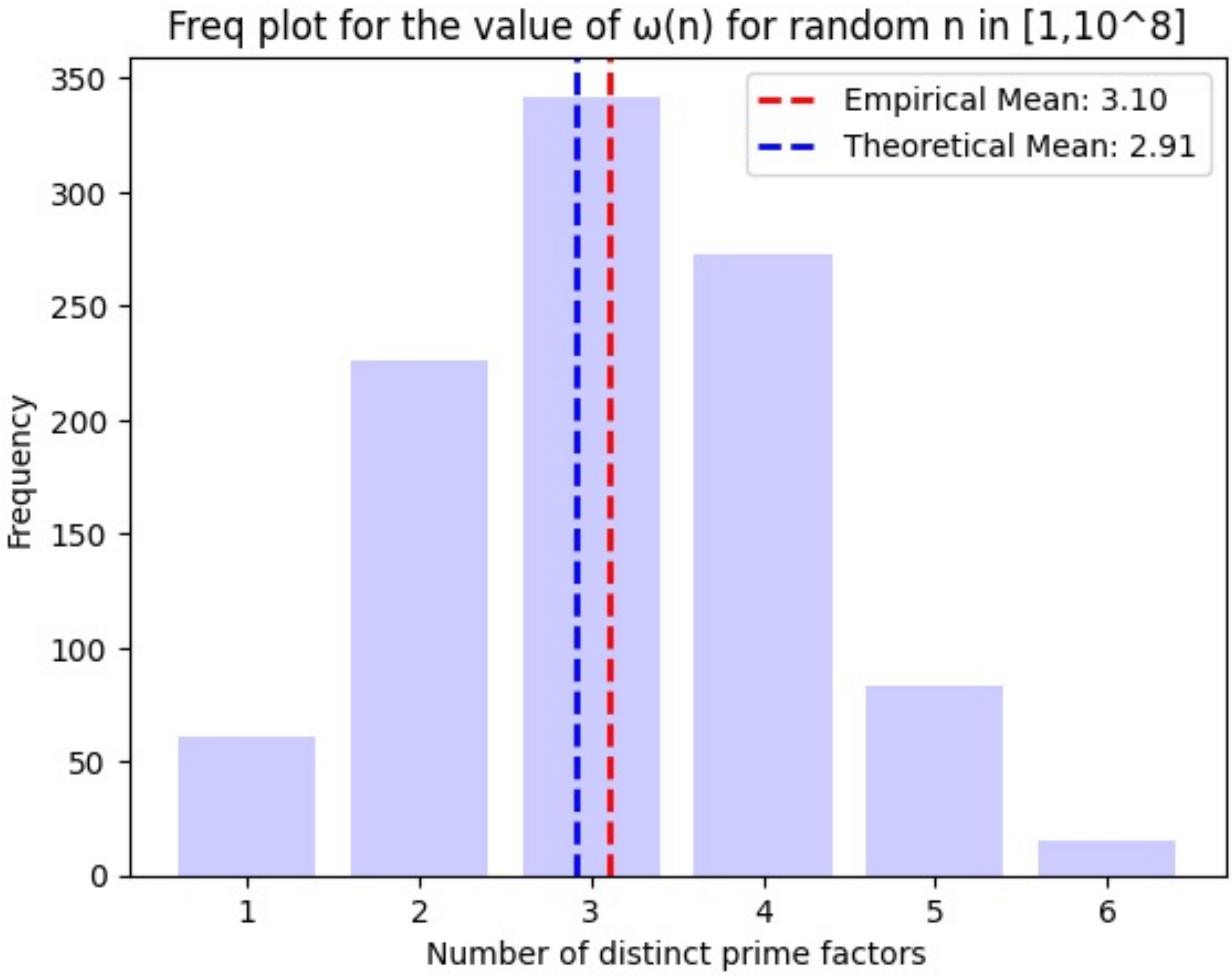
Then applying Merten's (second) theorem

$$\sum_{p \leq N} \frac{1}{p} = \log\log N + \Theta(1)$$

means

$$\boxed{\mathbb{E}_N[\omega] \sim \log\log N}$$

i.e. a random integer typically has loglog N distinct prime factors



Outline of proof of the lemma:

Just use linearity of expectation on f using its additive structure to get

$$\mathbb{E}_N[f] = \sum_{p \le N} \sum_{\substack{k \ge 1 \\ p^k \le N}} f(p^k)\, \mathbb{P}_N(p^k \| n)$$

Then use the previously derived expression for the probability.

As may be inspired by the plot, one may ask about the variance of $\omega(n)$ (and more generally additive $f(n)$'s).

Thm (Hardy-Ramanujan) "Most numbers $n \leq N$ have about $\log\log N$ prime factors"

↳ * $\omega(n)$ has "normal order" $\log\log N$

* $$\mathbb{P}_N\left(|\omega(n) - \log\log N| \geq V(N)\sqrt{\log\log N}\right) \ll \frac{1}{V(N)^2}$$

$f(x) \ll g(x)$ if $|f(x)| \leq Cg(x)$

for any $V(N) \geq 1$.

This was originally proved (non-"probabilistically") by Hardy and Ramanujan.

A very nice and succinct proof follows

quickly from the Turán-Kubilius ineq:

Thm Turán-Kubilius inequality

If f is an additive function, then

$$\mathbb{E}_N\left[\,|f - \mathbb{E}_N[f]|^2\right] \ll \sum_{p^k \leq N} \frac{|f(p^k)|^2}{p^k}$$

We omit the proof though it is a reasonably straightforward manipulation of the LHS, considering the contribution of different prime powers in $\mathbb{E}_N[f^2]$.

From this, the statement that "most integers $\leq N$ have about $\log\log N$ prime factors" follows: firstly,

prev. lemma

$$\mathbb{E}_N[\,|\omega - \log\log N|^2] = \mathbb{E}_N[\,|\omega - \mathbb{E}_N[\omega] + O(1)|^2]$$

$$\overset{\text{T-K}}{\ll} \sum_{p^k \leq N} \frac{1}{p^k} + O(1)$$

$$\Rightarrow \quad \overset{\text{Mertens}}{\ll} \log\log N$$

So by Markov/Chebyshev:

$$\mathbb{P}_N\left(|\omega - \log\log N| \geq V(N)\sqrt{\log\log N} \right)$$

$$\leq \frac{\mathbb{E}_N[|\omega - \log\log N|^2]}{V(N)^2 \log\log N}$$

$$\ll \frac{1}{V(N)^2}$$

Finally for this introduction, we'll see the beautiful refinement of the above due to Erdős-Kac.

So far we understand the first and second moments of $\omega(n)$ for n uniform:

$$\mathbb{E}_N[\omega] \sim \log\log N$$

$$\mathrm{Var}[\omega] \ll \log\log N$$

Erdős-Kac proved a beautiful improvement of the above, showing $\omega(n)$, suitably normalised, is Gaussian

Thm (Erdős-Kac) Take n uniformly from $\{1, \dots, N\}$. Then

$$\frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \xrightarrow[N\to\infty]{} \mathcal{N}(0,1)$$

where the convergence is in law.

- The theorem can be generalised to permit more general additive functions, though not all (e.g. Lindeberg's condition should be satisfied)
- Turán understood that since $\omega(n)$ can be thought of as a sum of essentially independent r.v. $\sum_{p\leq N} \left(\sum_{k\geq 1} \omega(p^k) \mathbb{1}\{p^k \| n\} \right)$ then a CLT "should hold".
- Following a lecture in which Erdős was in attendance, Kac and Erdős established the above result (using fairly sophisticated number theoretic tools – the Brun sieve).

Arguably the most popular way to prove Erdős-Kac is to use the method of moments (i.e. show the moments of $\omega(n)$ match those of the Gaussian).

This idea was used by Billingsley (also Granville & Soundararajan, Harper) who relied on work of Delange and Halberstam.
Many clear proofs can be found in these references (also Kowalski, Koukoulopoulos etc).

A crash course in $\zeta(s)$

References: Titchmarsh, Edwards, inline refs.

Before progressing, let's lay some of the number theoretic groundwork for studying ζ.

Def The Riemann zeta function is
$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad \text{for } \operatorname{Re}(s) > 1.$$

The connection to prime numbers is perhaps most simply seen through applying the fundamental theorem of arithmetic to the above:

$$\sum_{n\geq 1} \frac{1}{n^s} = 1 + \sum_{\substack{n\geq 1:\\ \Omega(n)=1}} \frac{1}{n^s} + \sum_{\substack{n\geq 1:\\ \Omega(n)=2}} \frac{1}{n^s} + \cdots$$

$$= 1 + \sum_{p\geq 1} \frac{1}{p^s} + \sum_{p,q\geq 1} \frac{1}{(pq)^s} + \cdots$$

$$= \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)$$

$$= \prod_p \sum_{k\geq 0} \left(\frac{1}{p^s}\right)^k$$

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

So for $\mathrm{Re}(s) > 1$

$$\boxed{\zeta(s) = \underbrace{\sum_{n\geq 1} \frac{1}{n^s}}_{\text{Dirichlet series}} = \underbrace{\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}}_{\text{Euler product}}}$$

We can analytically continue $\zeta(s)$ in s, progressively covering the whole plane

(Titchmarsh reviews a host of methods for the continuation): first notice

$$\sum_{n=1}^{N} \frac{1}{n^s} = Nf(N) - \int_1^N f'(x)[x]\,dx \qquad \boxed{f(x) = x^{-s}}$$

partial summation

$$= \frac{1}{N^{s-1}} + s\int_1^N \frac{[x]}{x^{s+1}}\,dx$$

$$= \frac{1}{N^{s-1}} + \frac{s}{1-s}\left(\frac{1}{N^{s-1}} - 1\right) - s\int_1^N \frac{\{x\}\,dx}{x^{s+1}}$$

$$\xrightarrow[\substack{N\to\infty \\ Re(s)>1}]{} \boxed{\frac{s}{s-1} - s\int_1^\infty \frac{\{x\}\,dx}{x^{s+1}}}$$

this however is valid meromorphically for $Re(s)>0$, so this defines $\zeta(s)$ for this half plane.

Continuing the continuation, one may find an integral expression for $\zeta(s)$ defining a meromorphic continuation to $\mathbb{C}$. The only pole is at $s=1$ (residue 1). Further, the following "functional equation" holds for all $s \in \mathbb{C}$

$$\boxed{\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{s}{2}\pi\right)\Gamma(1-s)\zeta(1-s)}$$

↳ so $\zeta(-2n) = 0$ for all $n \in \mathbb{N}$

↳ Also implies that the only other places $\zeta(s)=0$ lie in $Re(s) \in [0,1]$

If $\zeta(s)=0$ for some $Re(s)>1$ then $\prod_p (1-\frac{1}{p^s})^{-1} = 0$ but since each local term is bounded away from 0 (p is of course at least 2) this cannot hold. Then use that $\zeta(1-s) = \chi(s)\zeta(s)$ to conclude.

↳ In fact showing all other zeros lie in $Re(s) \in (0,1)$ is equivalent to showing

$$\pi(x) = \sum_{p \leq x} 1 \sim \frac{x}{\log x} \quad \text{(Prime number theorem)}$$

↳ Conjecture (Riemann hypothesis) All zeros of $\zeta(s)$ are of the form $s=-2n$, $n \in \mathbb{N}$ ("trivial zeros") or $s = \frac{1}{2}+it$, $t \in \mathbb{R}$ ("non-trivial zeros")

Let's apply some similar ideas to those applied to Erdös-Kac to understand

ζ "probabilistically", first in the half-plane of convergence.

Write $s = \sigma + it$ (n.b. unfortunately number theoretic and probabilistic notation sometimes clashes. It is very common to write σ for the real part of the argument of ζ, not to be confused with the – soon to come – standard dev.!)

Let $\sigma > 1$ so we are in the region of convergence. Then let's consider

$$\log \zeta(\sigma + it) = \log \prod_p (1 - p^{-\sigma - it})^{-1}$$

$$= -\sum_p \log(1 - p^{-\sigma - it})$$

$$= \sum_p \sum_{k \geq 1} \frac{p^{-k(\sigma + it)}}{k}$$

which is an absolutely convergent (double) series.