Math 229 - Introduction to Analytic Number Theory

(Fabian Gundlach)

0. Introduction

A few things that can be proved using analysis:

Thm 0.1 (Prime Number Theorem)

$$\#\{p \le X \text{ prime}\} \underset{X\to\infty}{\sim} \frac{X}{\log X}$$

More precise estimate:

$$\#\{p \le x \text{ prime}\} \sim \int_2^x \frac{1}{\log t}\, dt.$$

⇝ Heuristic: The set $\{2,3,5,\dots\}$ of prime numbers behaves a little like a random set of natural numbers containing $n \ge 2$ with probability $\frac{1}{\log n}$.

Notation

$f(x) \underset{x\to\infty}{\sim} g(x)$:	$\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$
$f(x) = o_{x\to\infty}(g(x))$:	$\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 0$
$f(x) \ll g(x)$ or: $f(x) = \mathcal{O}(g(x))$:	$\exists C>0 : \forall x : \ \lvert f(x)\rvert \le C \cdot g(x)$
$f(k,x) \ll_k g(k,x)$:	$\forall k : \exists C_k > 0 : \forall x : \ \lvert f(k,x)\rvert \le C_k \cdot g(k,x)$
$f(x) \asymp g(x)$:	$f(x) \ll g(x)$ and $f(x) \gg g(x)$
$f(x) = \Omega_{x\to\infty}(g(x))$:	not $f(x) = o_{x\to\infty}(g(x))$ or: $\limsup\limits_{x\to\infty} \frac{\lvert f(x)\rvert}{g(x)} > 0$.

Thm 0.2 (Dirichlet's Thm on primes in arithmetic progressions)

$$\#\{p \le X \text{ prime} : p \equiv a \bmod k\} \sim \frac{1}{\varphi(k)} \cdot \#\{p \le X \text{ prime}\}$$

if a is relatively prime to k, where $\varphi(k) = \#(\mathbb{Z}/k\mathbb{Z})^\times$ is the nr. of residue classes a mod k that are relatively prime to k (invertible). "All invertible res. cl. are equally likely!")

E.g., half the primes are $\equiv 1 \bmod 4$, half are $\equiv 3 \bmod 4$.

Thm 0.3

$$\#\{1 \le n \le X : \exists a, b \in \mathbb{Z} : n = a^2 + b^2\} \sim C \cdot \frac{X}{\sqrt{\log X}}$$ for some $C > 0$.

Thms 0.1–0.3 are proved using *complex analysis* (Dirichlet series).

Thm 0.4 (special case of Waring's problem) Every positive integer is the sum of at most 19 fourth powers.

This is proved using the circle method.

Thm 0.5

$$\#\{1 \leq n \leq x \text{ squarefree}\} \sim \frac{6}{\pi^2} \cdot x$$

This is proved using a sieve.

Thm 0.6 (Zhang + polymath)
There are infinitely many pairs of primes that differ by ~~exactly 2 (twin prime conjecture)~~ at most 246.

Prerequisites: - Complex analysis

- Fourier analysis

- a little bit of number theory

Grade: 70% weekly homework (probably due Wednesdays)
(dropping two lowest scores)
30% take-home final exam

OH this week: Mo, Th 3-4pm in room 233

Course assistant: [redacted] Yujie [redacted] Xu (yujiex@math.harvard.edu)

1. Initiation

1.1. Divisor sum

Def For any integer $n \geq 1$, let $d(n)$ be the number of positive divisors of n:

$$d(n) = \#\{a \mid n\} = \sum_{a \mid n} 1.$$

Ex

n	1	2	3	4	5	6
$d(n)$	1	2	2	3	2	4

Goal Estimate $\sum_{n \leq X} d(n)$ for large X.

Heuristic

$$\sum_{n \leq X} d(n) = \sum_{n \leq X} \sum_{a \mid n} 1 \underset{\overset{\uparrow}{n = a \cdot b}}{=} \sum_{\substack{a,b \geq 1: \\ ab \leq X}} 1$$

$$\overset{(I)}{\approx} \sum_{1 \leq a \leq X} \underset{\overset{\uparrow}{\#\{b:\, ab \leq X\}}}{\frac{X}{a}}$$

$$\overset{(II)}{\approx} \int_1^X \frac{X}{t}\, dt = \left[X \log t\right]_{t=1}^{X} = X \log X.$$

Making (I) rigorous:

$$\#\{1 \leq b \leq \tfrac{X}{a}\} = \left\lfloor \frac{X}{a} \right\rfloor = \frac{X}{a} + O(1),$$

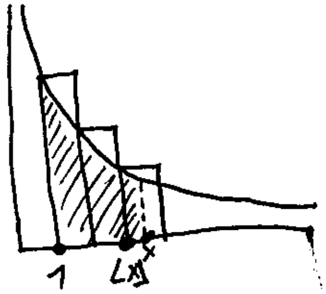
so

$$\sum_{\substack{a,b \geq 1: \\ ab \leq X}} 1 = \sum_{1 \leq a \leq X} \left(\frac{X}{a} + O(1)\right) = \sum_{1 \leq a \leq X} \frac{X}{a} + O(X).$$

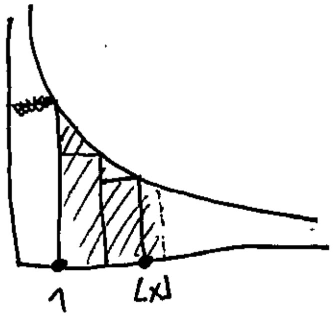
Making (II) rigorous:

Claim $\displaystyle\sum_{1\le n\le X} \frac{1}{n} = \log X + O(1)$ for $X \ge 1$.

Pf



$$\sum_{1\le n\le X} \frac{1}{n} \ge \int_1^X \frac{1}{t}\,dt = \log X$$



$$\sum_{2\le n\le X} \frac{1}{n} \le \int_1^X \frac{1}{t}\,dt = \log X$$

□

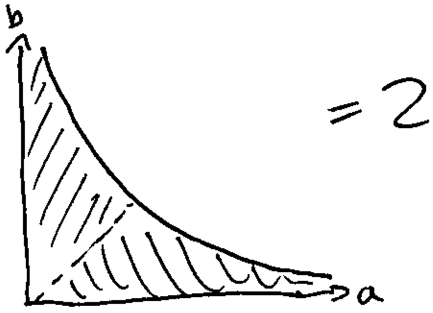
Summary $\displaystyle\sum_{1\le n\le X} d(n) = X\log X + O(X)$,

so the average number of divisors of a random $n \le X$ is $\sim \log X$ for $X \to \infty$.

We can improve the estimate!

Improving (I): ("Dirichlet hyperbola method")

$$\sum_{\substack{a,b\ge 1:\\ ab\le x}} 1 = \sum_{\substack{a\ge b\ge 1:\\ ab\le x}} 1 + \sum_{\substack{b\ge a\ge 1:\\ ab\le x}} 1 - \sum_{\substack{a=b\ge 1:\\ ab\le x}} 1$$



$$= 2\cdot \sum_{\substack{b\ge a\ge 1:\\ ab\le x}} 1 - \sum_{\substack{a\ge 1:\\ a^2\le x}} 1$$

$$= 2\cdot \sum_{1\le a\le x^{1/2}} \sum_{1\le b\le \frac{x}{a}} 1 - \sum_{1\le a\le x^{1/2}} 1$$

$$= 2\cdot \sum_{1\le a\le x^{1/2}} \left(\frac{x}{a} - a + O(1)\right) - \left(x^{1/2} + O(1)\right)$$

$$= 2\cdot \sum_{1\le a\le x^{1/2}} \frac{x}{a} - x + O(x^{1/2}).$$

↑ better than $O(x)$

1.2. Abel summation

<u>Reminder</u> (Integration by parts)

Let $f, g : [a,b] \to \mathbb{C}$ be continuously differentiable. $(a \le b)$

Then,

$$\int_a^b f'(t)g(t)\,dt + \int_a^b f(t)g'(t)\,dt = \underset{\left(f(b)g(b) - f(a)g(a)\right)}{\overset{}{\left[f(t)g(t)\right]_{t=a}^{b}}} \underset{}{.}$$

Rmk This continues to hold if f, g are continuous and piecewise continuously differentiable, ignoring points t where $f'(t)$ or $g'(t)$ doesn't exist.

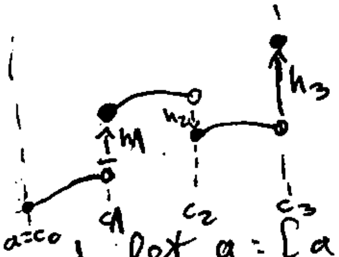
It fails if f, g are not continuous.

<u>Thm 1.2.1</u> (Abel summation)

Let $a = c_0 \le c_1 \le \dots \le c_k = b$, let $f : [a,b] \to \mathbb{C}$ be continuously differentiable on $[c_i, c_{i+1})$ with a jump of height $h_i = f(c_i) - \lim\limits_{\substack{t \nearrow c_i \\ \uparrow}} f(t)$ at c_i

limit from below

$= $ " $f(c_i) - f(c_i - \varepsilon)$ " $(i \ge 1)$



and let $g : [a,b] \to \mathbb{C}$ be continuously differentiable.

Then,

$$\underbrace{\int_a^b f'(t)\,g(t)\,dt}_{\text{ignore pts. } t = c_i} + \sum_{1 \le i \le k} h_i\, g(c_i) + \int_a^b f(t)g'(t)\,dt = \left[f(t)g(t)\right]_{t=a}^{b}.$$

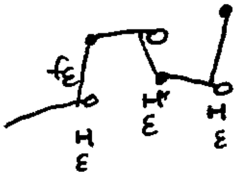
Pf 1 Apply integration by parts to the continuous extension of each $f|_{[c_i, c_{i+1})}$ to $[c_i, c_{i+1}]$ and add the results:

$$\int_a^b f'(t)g(t)\,dt + \int_a^b f(t)g'(t)\,dt = \sum_{i=0}^{n-1}\Big(\underbrace{f(c_{i+1})g(c_{i+1})}_{(f(c_{i+1})-h_{i+1})g(c_{i+1})} - f(c_i)g(c_i)\Big)$$

$$= f(b)g(b) - f(a)g(a) - \sum_{i=1}^{n} h_i g(c_i)$$

□

Pf 2 Apply int. by parts to f_ε, g and let $\varepsilon \to 0$.



□

Pf 3 Look up Riemann-Stieltjes integration. "□"

Use
- Apply liberally
- Normally, $\sum h_i g(c_i)$ is what you want to estimate.
- For best results try making $f(x)$ small. (Usually, $\int f'(t)g(t)dt$ is the main term.)
- Try applying integration by parts (backwards) to $\int f g'$ after plugging in an upper bound for f.

Example:

Thm 1.2.2 Assume Thm 0.1 (PNT). Then:

$$\sum_{\substack{p \le x \\ \text{prime}}} \frac{1}{p} \sim \log\log x \quad \text{for } x \ge 2.$$

Pf Use $f(x) = \sum_{\substack{p \le x \\ \text{prime}}} 1 - \int_2^x \frac{1}{\log t} dt = o\left(\int_2^x \frac{1}{\log t} dt\right)$

(jumps of height 1 at primes, $f'(x) = -\frac{1}{\log(x)}$ elsewhere)

and $g(x) = \frac{1}{x}$.

$$\int_2^x \left(-\frac{1}{\log t}\right) \cdot \frac{1}{t} dt + \sum_{2 < p \le x} 1 \cdot \frac{1}{p} + \int_2^x f(t) \cdot g'(t) dt = \left[f(t) \cdot \frac{1}{t}\right]_{t=a}^{b}$$

$$\left[f(t) \cdot \frac{1}{t}\right]_{t=a}^{b} = O(1)$$

$$\int_2^x \frac{1}{t \log t} dt = \left[\log\log t\right]_{t=2}^{x} = \log\log x + O(1)$$

Let $\varepsilon > 0$. For suff. large C_{ε}, we have

$$|f(t)| \le \varepsilon \cdot \int_2^x \frac{1}{\log t} dt \quad \text{for all } x \ge C.$$

$$\Rightarrow \left|\int_2^x f(t)\cdot g'(t)\,dt\right| \le \underbrace{\left|\int_2^{c_\varepsilon} f(t)\, g'(t)\right|}_{=:\, D_\varepsilon} + \underbrace{\left|\int_2^x \left(\varepsilon\cdot \int_2^t \frac{1}{\log s}\,ds\right)\cdot g'(t)\,dt\right|}_{=:\, E_\varepsilon(x)}$$

$$E_\varepsilon(x) + \underbrace{\int_2^x \varepsilon\cdot \frac{1}{\log t}\cdot \underbrace{g(t)}_{\frac{1}{t}}\,dt}_{\varepsilon\cdot [\log\log t]_{t=2}^{x}} = \underbrace{\Big[\varepsilon\cdot \underbrace{\underbrace{\int_2^t \frac{1}{\log s}\,ds}_{\sim \frac{t}{\log t}} \cdot \frac{1}{t}}_{\frac{\varepsilon}{\log t}}\Big]_{t=2}^{x}}_{\mathcal{O}(\varepsilon)}$$

Summary:

$$\sum_{\substack{p\le x\\ \text{prime}}} \frac{1}{p} = \log\log x + \mathcal{O}_\varepsilon(1) + \mathcal{O}(\varepsilon\cdot \log\log x)$$

For any $\delta > 0$, we can choose $\varepsilon > 0$ so that

$$\mathcal{O}(\varepsilon\cdot \log\log x) < \frac{\delta}{2}\cdot \log\log x.$$

Then, for sufficiently large x,

$$\mathcal{O}_\varepsilon(1) < \frac{\delta}{2}\cdot \log\log x.$$

Hence, $\displaystyle\sum_{\substack{p\le x\\ \text{prime}}} \frac{1}{p} = \log\log x + \delta\cdot \log\log x$ for suff. large x.

In other words, $\displaystyle\sum_{\substack{p\le x\\ \text{prime}}} \frac{1}{p} \sim \log\log x.$ □

1.3. Euler - Maclaurin formulas

Def The Bernoulli polynomials $b_0, b_1, \ldots$ are defined by

i) $b_0(x) = 1$

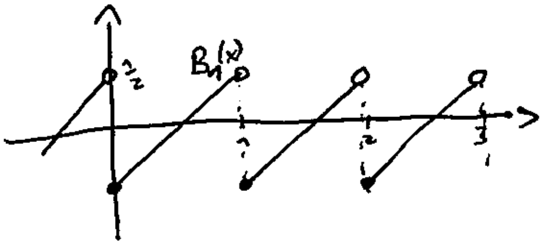
ii) $b'_k(x) = \underset{\substack{\uparrow \\ \boxed{\text{“artificial normalization”}}}}{k} \cdot b_{k-1}(x)$ for $k \geq 1$.

iii) $\int_0^1 b_k(x)\, dx = 0$ for $k \geq 1$.

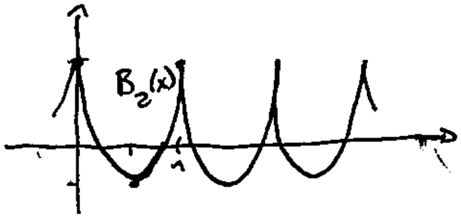
Ex
$$b_0(x) = 1$$
$$b_1(x) = x - \tfrac{1}{2}$$
$$b_2(x) = x^2 - x + \tfrac{1}{6}$$
$$\vdots$$

Def The k-th Bernoulli function is $B_k(x) = b_k(\{x\})$.

Rmk Each B_k is periodic and in particular bounded.



Rmk $B_2, B_3, \ldots$ are continuous due to iii).



Thm 1.3.1 (Euler-Maclaurin formula)

Let $k \geq 0$, and assume that $f : [a,b] \longrightarrow \mathbb{C}$ is $k+1$ times continuously differentiable. Then,

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\,dt + \sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!}\left[B_{r+1}(t)\, f^{(r)}(t)\right]_{t=a}^{b}$$

$$+ \int_a^b \frac{(-1)^{k}}{(k+1)!} B_{k+1}(t)\, f^{(k+1)}(t)\,dt$$

Ex ($k=0$) If $a,b \in \mathbb{Z}$, then $B_1(a)=B_1(b)=B_1(0)=-\frac{1}{2}$, so

$$\sum_{a \underset{\overset{\uparrow}{!}}{\leq} n\leq b} f(n) = \int_a^b f(t)\,dt + \frac{1}{2}\left(f(b) \underset{\overset{\uparrow}{!}}{+} f(a)\right) + \int_a^b B_1(t) f'(t)\,dt$$

Ex ($k=1$) If $a,b \in \mathbb{Z}$, then

$$\sum_{a\leq n\leq b} f(n) = \int_a^b f(t)\,dt + \frac{1}{2}\left(f(b)+f(a)\right) + \frac{1}{12}\left[f'(t)\right]_{t=a}^{b} - \frac{1}{2}\int_a^b B_2(t) f''(t)\,dt.$$

Rmk $\left| \int_a^b B_{k+1}(t)\, f^{(k+1)}(t)\,dt \right| \underset{\substack{\uparrow \\ B_{k+1}(t) \ll_k 1}}{\ll_k} \int_a^b |f^{(k+1)}(t)|\,dt.$

Often, this integral is smaller / has better convergence properties for larger k.

Pf Induction over k:

k=0: Apply Abel summation to $B_1(t)$, $f(t)$:

($B_1(t)$ has jumps of height -1 at $t\in\mathbb{Z}$, $B_1'(t)=1$ for $t\notin\mathbb{Z}$.)

$$\int_a^b 1\cdot f(t)\,dt + \sum_{a<n\le b} (-1)\cdot f(n) + \int_a^b B_1(t) f'(t)\,dt$$

$$= \left[B_1(t)\cdot f(t)\right]_{t=a}^{b}$$

k-1 → k: Apply integration by parts to $B_{k+1}(t)$, $f^{(k)}(t)$:

(no jumps, $B_{k+1}'(t)=(k+1)\cdot B_k(t)$ for all $t\in\mathbb{Z}$).

$$\int_a^b (k+1)\cdot B_k(t) f^{(k)}(t)\,dt + \int_a^b B_{k+1}(t) f^{(k+1)}(t)\,dt$$

$$= \left[B_{k+1}(t)\, f^{(k)}(t)\right]_{t=a}^{b} .$$

Plug this into the induction hypothesis. □

Cor 1.3.2. For $x \geq 1$,

$$\sum_{1 \leq n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

for some constant $\gamma = 0.577\ldots$ called Euler's constant or the Euler-Mascheroni constant.

Pf
$$\sum_{1 \leq n \leq x} \frac{1}{n} = \underbrace{\int_1^x \frac{1}{t}\,dt}_{\log x} + \underbrace{B_1(x)}_{O(1)} \cdot \frac{1}{x} + \frac{1}{2} \cdot \frac{1}{1} + \int_1^x B_2(t) \cdot \left(-\frac{1}{t^2}\right) dt$$

$$= \log x + \left(\frac{1}{2} + \int_1^\infty B_2(t) \cdot \left(-\frac{1}{t^2}\right) dt\right) - \underbrace{\int_x^\infty \underbrace{B_2(t)}_{O(1)} \left(-\frac{1}{t^2}\right) dt}_{O\left(\frac{1}{x}\right)} + O\left(\frac{1}{x}\right)$$

□

Combining this with the improved version of (I) gives:

Thm 1.3.3 $\sum_{n \leq x} d(n) = x(\log x + 2\gamma - 1) + O(x^{1/2})$.

Pf
$$LHS = 2 \cdot \sum_{a \leq x^{1/2}} \frac{x}{a} - x + O(x^{1/2})$$
$$= 2x\left(\log x^{1/2} + \gamma + O\left(\frac{1}{x^{1/2}}\right)\right) - x + O(x^{1/2})$$
$$= RHS.$$

□

Rmk It is conjectured that the error is actually only $O_\varepsilon(x^{1/4+\varepsilon})$ for any $\varepsilon > 0$.

Known (Huxley): $O_\varepsilon(x^{\frac{131}{416}+\varepsilon})$.

2. Smoothing

2.1. Using Euler-Maclaurin

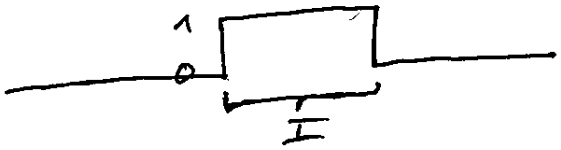
Root of all evil

Let I be an interval of length L.

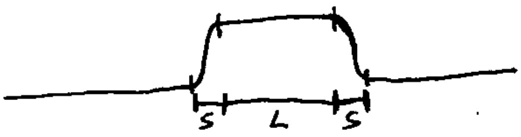
In general, only $\#(I \cap \mathbb{Z}) = L + O(1)$,

not $\#(I \cap \mathbb{Z}) = L$.

Write $\#(I \cap \mathbb{Z}) = \sum_{n \in \mathbb{Z}} 1\!\!1_I(n)$, where $1\!\!1_I$ is the characteristic function of I.



Idea: Replace $1\!\!1_I$ by a smooth function f.



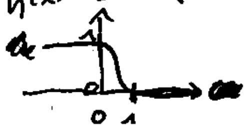
For example, say $I = [0, L]$,

$$f(x) = \begin{cases} 1, & 0 \le x \le 1, \\ \eta\left(\frac{x-1}{s}\right), & 1 \le x, \\ \eta\left(\frac{-x}{s}\right), & x \le 0, \end{cases}$$

where $\eta: \mathbb{R} \to \mathbb{R}$ is a smooth function with

$\eta(x) = 1$ for $x \le 0$

$\eta(x) = 0$ for $x \ge 1$



Thm 2.1.1 we then have

$$\sum_{n\in\mathbb{Z}} f(n) = \int_{\mathbb{R}} f(t)\,dt + O_{\eta,k}(S^{-k})$$ for any η as above and $k \geq 0$.

Pf apply Euler-Maclaurin on an interval $[a,b]$ containing the support of f:

$$\sum_{n\in\mathbb{Z}} f(n) = \int_{\mathbb{R}} f(t)\,dt + \sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!} \underbrace{\left[B_{r+1}(t) f^{(r)}(t)\right]_{t=a}^{b}}_{0}$$

$$+ \underbrace{\int_a^b \frac{(-1)^k}{(k+1)!} B_{k+1}(t) f^{(k+1)}(t)\,dt}$$

$$\ll_k \int_{\mathbb{R}} |f^{(k+1)}(t)|\,dt$$

$$= 2 S^{-k} \underbrace{\int_{\mathbb{R}} |\eta^{(k+1)}(t)|\,dt}_{<\infty \text{ (indep. of } L,S)}$$

□

2.2. Fourier transforms

Def Let $f \in L^1(\mathbb{R}^n)$ (measurable function $f:\mathbb{R}^n \to \mathbb{C}$ s.t. $\int_{\mathbb{R}^n} |f(x)|dx < \infty$

Its Fourier transform is the function $\hat{f}:\mathbb{R}^n \to \mathbb{C}$ given by:

$$\hat{f}(t) = \int_{\mathbb{R}^n} f(x) e^{-2\pi i \overset{\uparrow \text{ inner (dot) product on } \mathbb{R}^n}{(x \cdot t)}} dx$$

Thm 2.2.1 (Riemann-Lebesgue Lemma)

If $f \in L^1(\mathbb{R}^n)$, then $\hat{f} \in C_0(\mathbb{R}^n)$ (continuous function with $\hat{f}(t) \xrightarrow{|t|\to\infty} 0$)

Ex Let $I = [a,b]$. The Fourier transform of the indicator function $\mathbb{1}_I$ is

$$\hat{\mathbb{1}}_I(t) = \int_a^b e^{-2\pi i x t} dx = \left[-\frac{1}{2\pi i t} e^{-2\pi i x t} \right]_{x=a}^{b}$$

(If $a=-b$, this is $\frac{1}{\pi t} \sin(2\pi i b t)$.)

Lemma 2.2.2 (Basic properties of Fourier transforms)

a) $\hat{f}(0)=\int_{\mathbb{R}} f(x)\,dx$

b) If $g_\lambda(x)=f\left(\frac{x}{\lambda}\right)$ $(\lambda>0)$, then

$$\hat{g}_\lambda(t)=\lambda^n\cdot\hat{f}(\lambda t).$$

c) Let $n=1$.
If f is absolutely continuous (f differentiable a.e, f' integrable, $f(b)-f(a)=\int_a^b f'(t)\,dt \ \forall a<b$,
e.g.: continuous and piecewise continuously differentiable),
then $\widehat{f'}(t)=2\pi i t\cdot\hat{f}(t)$.

Pf a) clear

b) clear

c) integration by parts

□

Thm 2.2.3

If $f \in L^1(\mathbb{R}^n)$ and $\hat{f} \in L^1(\mathbb{R}^n)$, then

$$f(x) = \hat{\hat{f}}(-x) \text{ for } \underbrace{\text{almost all } x \in \mathbb{R}^n}_{\substack{\text{set of bad } x \\ \text{has measure } 0}}.$$

If f is continuous, this holds for all $x \in \mathbb{R}^n$.

__Def__ A smooth function $f: \mathbb{R}^n \to \mathbb{C}$ is a __Schwartz function__ if all derivatives of f decay faster than any power of $\frac{1}{|x|}$ for $|x| \to \infty$:

$$|x|^k \left(\frac{\partial}{\partial x_1}\right)^{b_1} \cdots \left(\frac{\partial}{\partial x_n}\right)^{b_n} f(x) \xrightarrow{|x|\to\infty} 0 \quad \text{for all } k, b_1, \dots, b_n \geq 0.$$

The set of Schwartz functions is denoted by $\mathcal{S}(\mathbb{R}^n)$.

__Ex__ Any smooth fct. with compact support.

__Rmks__ $\mathcal{S}(\mathbb{R}^n) \subseteq L^1(\mathbb{R}^n)$

$\mathcal{S}(\mathbb{R}^n) \subseteq C_0(\mathbb{R}^n)$

__Thm 2.2.4__

If $f \in \mathcal{S}(\mathbb{R}^n)$, then $\hat{f} \in \mathcal{S}(\mathbb{R}^n)$.

(In particular, $|t|^k \hat{f}(t) \xrightarrow{|t|\to\infty} 0$ for all $k \geq 0$.)

__Thm 2.2.5__ (Poisson summation formula)

If $f \in \mathcal{S}(\mathbb{R}^n)$, then

$$\sum_{x \in \mathbb{Z}^n} f(x) = \sum_{t \in \mathbb{Z}^n} \hat{f}(t).$$

(Note: Both sides are absolutely convergent.)

__Rmk__ $\hat{f}(0) = \int_{\mathbb{R}^n} f(x)\,dx$ is the naive estimate for $\sum_{x \in \mathbb{Z}^n} f(x)$.

So $\sum_{0 \neq t \in \mathbb{Z}^n} \hat{f}(t)$ is the error term.

Def The *convolution* $f*g$ of $f, g \in L^1(\mathbb{R}^n)$ is given by

$$(f*g)(x) = \int_{\mathbb{R}^n} f(x-y)g(y)\,dy = \int_{\mathbb{R}^n} f(y)g(x-y)\,dy.$$

Lemma 2.2.6 We have $f*g \in L^1(\mathbb{R}^n)$ and

$$\widehat{f*g}\,(t) = \hat{f}(t)\cdot\hat{g}(t) \qquad \forall t \in \mathbb{R}^n.$$

Rmk You can make any $f \in L^1(\mathbb{R}^n)$ smooth by taking the convolution with a smooth fct.

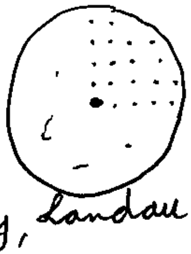
2.3. Gauß circle problem

<u>Goal</u> Estimate $N(R) := \#\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2\le R^2\}$

$$= \#(\underset{\substack{\uparrow \\ \text{closed ball} \\ \text{of radius } R}}{B}(R) \cap \mathbb{Z}^2)$$

<u>Rmk</u> The strategy from chapter 1 proves

$$N(R) = \pi R^2 + O(R)$$



<u>Rmk</u> Hardy, Landau showed that $N(R) = \pi R^2 + \Omega(R^{\frac{1}{2}}(\log R)^{\frac{1}{4}})$.

<u>Conjecture</u> $N(R) = \pi R^2 + O_\varepsilon(R^{\frac{1}{2}+\varepsilon})$ $\forall \varepsilon>0$.

<u>Known</u> (Huxley) $- - -$ $O_\varepsilon(R^{131/208+\varepsilon})$ $\forall \varepsilon>0$.

We'll show $O(R^{2/3})$.

__Lemma 2.3.1__ Let $R \geq 0$.

a) $\displaystyle\sum_{\substack{0\neq x\in\mathbb{Z}^2:\\ |x|\leq R}} |x|^k \sim \frac{2\pi}{k+2}R^{k+2}$ for any real number $k>-2$.

b) $\displaystyle\sum_{\substack{x\in\mathbb{Z}^2:\\ |x|\geq R}} |x|^k \sim \frac{2\pi}{k+2}R^{k+2}$ for any real number $k<-2$.

__Pf__ Apply Abel summation to $\underbrace{N(t)-\pi t^2}_{=o_{t\to\infty}(t^2)}$, t^k:

trivial estimate $N(t)\sim\pi t^2$

$$a) \underbrace{-\int_0^R 2\pi t\cdot t^k\,dt}_{\left[\frac{2\pi}{k+2}t^{k+2}\right]_{t=0}^R} + \sum_{\substack{0\neq x\in\mathbb{Z}^2\\ |x|\leq R}} |x|^k + \underbrace{\int_0^R \underbrace{(N(t)-\pi t^2)}_{o(t^2)}\cdot k t^{k-1}\,dt}_{o_{R\to\infty}(R^{k+2})}$$

$$= \underbrace{\left[(N(t)-\pi t^2)\,t^k\right]_{t=0}^R}_{o_{R\to\infty}(R^{k+2})}$$

b) similar

□

Lemma 2.3.2

$\hat{\mathbb{1}}_{B(1)}(t) \ll |t|^{-3/2}$ (for $|t| \to \infty$)

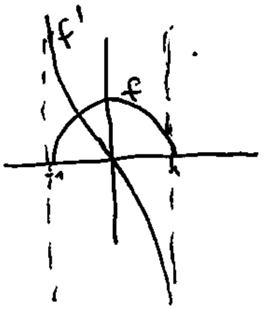
Rmk $\hat{\mathbb{1}}_{B(1)}(t) = \frac{J_1(\pi|t|)}{|t|}$, where $J_1(x)$ is the Bessel function of order 1 of the first kind.

Pf By rotational symmetry, we can assume w.l.o.g. that t lies on the positive x-axis: $t = \binom{a}{0}$, $a > 0$.

$$\Rightarrow \hat{\mathbb{1}}_{B(1)}(t) = \int_{B(1)} e^{-2\pi i x a} \, d\binom{x}{y} = 2\int_{\mathbb{R}} f(x) e^{-2\pi i x a} \, dx$$

$$= 2\hat{f}(a)$$

for $f(x) = \begin{cases} \sqrt{1-x^2}, & -1 \le x \le 1, \\ 0, & \text{otherwise.} \end{cases}$



f is abs. cont., so we can apply Lemma 2.2.2 d):

$$\hat{f}(a) = \frac{1}{2\pi i a} \underbrace{\hat{f'}(a)}_{(\ll 1)} \underbrace{\left(\ll \frac{1}{a} = \frac{1}{|t|}\right)}_{\text{not good enough!}}$$

Problem: f' is not abs. cont. near ±1, so we can't apply Lemma 2.2.2 c) again.

Instead, break up the integral

$$\hat{f'}(a) = \int_{-1}^{1} f'(x)\, e^{-2\pi i x a}\, dx \qquad \text{into:}$$

- a piece away from ±1:

$$\int_{-(1-\frac{1}{a})}^{1-\frac{1}{a}} f'(x) e^{-2\pi i x a} dx \underset{\text{IBP}}{=\!=} \underbrace{\left[f'(x) \cdot \frac{e^{-2\pi i x a}}{-2\pi i a} \right]_{x=-(1-\frac{1}{a})}^{1-\frac{1}{a}}}_{\ll \frac{1}{a^{1/2}}} - \underbrace{\int_{-(1-\frac{1}{a})}^{1-\frac{1}{a}} f''(x) \cdot \underbrace{\frac{e^{-2\pi i x a}}{-2\pi i x a}}_{\ll \frac{1}{a}} dx}_{\ll \frac{1}{a^{1/2}}}$$

- pieces near ±1:

$$\int_{1-\frac{1}{a}}^{1} \underbrace{f'(x)}_{<0} \underbrace{e^{-2\pi i x a}}_{\ll 1} dx \ll -\left[f(x) \right]_{x=1-\frac{1}{a}}^{1} \ll \frac{1}{a^{1/2}}$$

$$\int_{-1}^{-(1-\frac{1}{a})} \; - \; - \; - \qquad \ll \frac{1}{a^{1/2}}.$$

□

Thm 2.3.3 (Sierpinski)

$$\mathcal{N}(R) = \pi R^2 + \mathcal{O}(R^{2/3}).$$

Rmk Applying Poisson summation to $\mathbb{1}_{B(R)}$ would give an error bound of

$$\sum_{0 \neq t \in \mathbb{Z}^2} \hat{\mathbb{1}}_{B(R)}(t) \underset{\substack{\uparrow \\ \mathbb{1}_{B(R)}(x) = \mathbb{1}_{B(1)}\left(\frac{x}{R}\right)}}{=} \sum_{0 \neq t \in \mathbb{Z}^2} R^2 \, \hat{\mathbb{1}}_{B(1)}(Rt)$$

$$\ll \sum_{0 \neq t \in \mathbb{Z}^2} R^{1/2} |t|^{-3/2} \underset{\substack{\uparrow \\ -\frac{3}{2} > -2}}{=} \infty .$$

Pf Let $\eta : \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ be a smooth (radially symmetric) function with $\int_{\mathbb{R}^2} \eta(x)dx = 1$ and $\mathrm{supp}(\eta) \subseteq B(1)$.

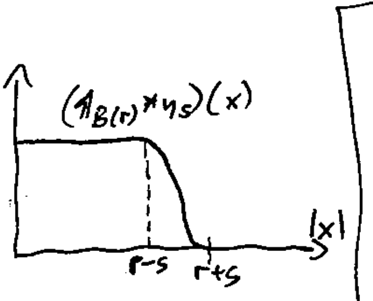
Let $\eta_s(x) = \frac{1}{s^2}\eta\left(\frac{x}{s}\right)$. $(0 < s < R)$

$$\Rightarrow \int_{\mathbb{R}^2} \eta_s(x)dx = 1, \quad \hat{\eta}_s(t) = \hat{\eta}(st), \quad \mathrm{supp}(\eta_s) \subseteq B(s)$$

$$\Rightarrow \mathbb{1}_{B(R-s)} * \eta_s \leq \mathbb{1}_{B(R)} \leq \mathbb{1}_{B(R+s)} * \eta_s \qquad (I)$$

$$(\mathbb{1}_{B(R-s)} * \eta_s)(x) = \int_{\mathbb{R}^2} \underbrace{\mathbb{1}_{B(R-s)}(x-y)}_{\leq 1} \eta_s(y)dy \leq 1 \ \forall x \in B(R)$$

$$\text{---}\,''\,\text{---} = \int_{\mathbb{R}^2} \underbrace{\underbrace{\mathbb{1}_{B(R-s)}(x-y)}_{\substack{0 \text{ unless} \\ x-y \in B(R-s)}} \underbrace{\eta_s(y)}_{\substack{0 \text{ unless} \\ y \in B(s)}}}_{0 \text{ unless } x \in B(R)} dy = 0 \ \forall x \notin B(R)$$



We will later let $s \overset{=s(R)}{\longrightarrow} 0$ as $R \to \infty$.

$$\widehat{(\mathbb{1}_{B(r)} * \eta_s)}(0) = \widehat{\mathbb{1}}_{B(r)}(0) \cdot \hat{\eta}_s(0) = \pi r^2 \cdot 1 = \pi r^2$$

$$\sum_{0 \neq t \in \mathbb{Z}^2} \widehat{(\mathbb{1}_{B(r)} * \eta_s)}(t) = \sum_{0 \neq t \in \mathbb{Z}^2} \widehat{\mathbb{1}}_{B(r)}(t) \cdot \hat{\eta}_s(t)$$

$$= \sum_{0 \neq t \in \mathbb{Z}^2} r^2 \cdot \underbrace{\widehat{\mathbb{1}}_{B(1)}(rt)}_{\ll (r|t|)^{-3/2}} \cdot \underbrace{\hat{\eta}(st)}_{\ll_k (s|t|)^{-k} \text{ for } k \geq 0 \atop \text{and } \ll 1}$$

$$\ll_k \sum_{\substack{0 \neq t \in \mathbb{Z}^2: \\ s|t| \geq 1}} r^2 (r|t|)^{-3/2} (s|t|)^{-k}$$

$$+ \sum_{\substack{0 \neq t \in \mathbb{Z}^2: \\ s|t| \leq 1}} r^2 (r|t|)^{-3/2}$$

$$\underset{\substack{\uparrow \\ \text{Lemma}}}{\ll} r^{1/2} s^{-k} (s^{-1})^{\frac{1}{2}-k} + r^{1/2} (s^{-1})^{1/2} \qquad \text{for } k \geq 1$$

$$\asymp r^{1/2} s^{-1/2}$$

$$\Rightarrow \sum_{x \in \mathbb{Z}^2} (\mathbb{1}_{B(r)} * \eta_s)(x) = \pi r^2 + \mathcal{O}(r^{1/2} s^{-1/2}).$$

With (I): $(S \to 0)$

$$\pi\underbrace{(R-S)^2}_{R^2+O(RS)} + O(R^{1/2}S^{-1/2}) \le N(R) \le \pi\underbrace{(R+S)^2}_{\underset{\text{increasing in } S}{\underset{\uparrow}{R^2+O(RS)}}} + \underset{\text{decreasing in } S}{\underset{\nwarrow}{O(R^{1/2}S^{-1/2})}}$$

$O(RS) + O(R^{1/2}S^{-1/2})$ is smallest (up to bounded factor) when $RS = R^{1/2}S^{-1/2}$, i.e. $S = R^{-1/3}$.

The error term is then $O(R^{2/3})$. □

3. Dirichlet series

In combinatorics, one associates to a sequence $a_0, a_1, \ldots \in \mathbb{C}$ the <u>ordinary generating function</u>

$$F(a,X) = \sum_{n=0}^{\infty} a_n X^n \quad \text{(a formal power series)}$$

Ignoring convergence:

$$F(a,X) + F(b,X) = \sum a_n X^n + \sum b_n X^n = \sum (a_n + b_n) X^n = F(a+b, X)$$

$$F(a,X) \cdot F(b,X) = \left(\sum a_n X^n\right)\left(\sum b_m X^m\right) := \sum_{k=0}^{\infty} \Big(\sum_{\substack{n,m \geq 0: \\ k = n+m}} a_n b_m\Big) X^k = F(a \circledast b, X)$$

$$\frac{d}{dX} F(a,X) = \frac{d}{dX} \sum_{n=0}^{\infty} a_n X^n := \sum_{n=1}^{\infty} n a_n X^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} X^n = F(a', X)$$

$(a'_n = (n+1) a_{n+1})$

<u>Rmk</u> These identities hold for any $X \in \mathbb{C}$ for which the LHS is absolutely convergent.

Similarly:
In (multiplicative) number theory, one associates to a sequence $\overset{=a(1)}{a_1}, \overset{=a(2)}{a_2}, \ldots \in \mathbb{C}$ the <u>Dirichlet series</u>

$$D(a, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad \text{(a formal series)}$$

Ignoring convergence:

$$D(a, s) + D(b, s) = D(a+b, s)$$

$$D(a,s) \cdot D(b,s) = \left(\sum \frac{a_n}{n^s}\right)\left(\sum \frac{b_m}{m^s}\right) = \sum_k \underbrace{\Big(\sum_{\substack{n,m\geq 1:\\ k=nm}} a_n b_m\Big)}_{(a*b)_k} \cdot \frac{1}{k^s} = D(a*b, s),$$

where $a * b$ is the <u>~~number-theoretic~~ convolution</u> of a and b

$$\frac{d}{ds} D(a,s) = \sum_{n=1}^{\infty} \frac{-a_n \log n}{n^s} = D(-a \underset{\substack{\uparrow\\ \text{pointwise mult.}}}{\cdot} \log, s)$$

$$D(a, s-r) = \sum \frac{a_n}{n^{s-r}} = \sum \frac{a_n \cdot n^r}{n^s} = D(a \cdot \underset{\substack{\uparrow\\ \text{identity sequence:}\\ id_n = n}}{id^r}, s)$$

<u>Rmk</u> Again, the identities hold if the LHS is abs. conv.

<u>Rmk</u> The above operations $+, \cdot$ give the set of Dirichlet series (or equivalently, (+, $*$ on) the set of sequences) the structure of a ring.

<u>Rmk</u> The mult. identity is $1 = D(\delta, s)$, where $\delta = (1, 0, 0, \ldots)$.

Rmk $D(a,s)$ is (formally) invertible if and only if $a_1 \neq 0$.

Pf "$\Rightarrow$" $(a*b)_1 = a_1 b_1$

"$\Leftarrow$" ~~let $b(n) :=$~~

~~let $b(n) := \frac{1}{a(1)}$~~

Let $b_1 := \frac{1}{a_1}$,

$$b_k := -\frac{1}{a_1}\cdot \sum_{\substack{n,m\geq 1:\\ k=nm\\ m<k}} a_n b_m \qquad \text{(inductively).}$$

$\Rightarrow a*b = \delta.$ □

Def We'll denote the conv. inverse of a sequence a by $\hat{a}$.

Def The Riemann zeta function is

$$\zeta(s) = D(\mathbb{1}, s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{for } \mathbb{1} = (1,1,\dots).$$

We can use it to make lots of more interesting sequences:

$d = \mathbb{1} * \mathbb{1}$ $\qquad$ $D(d,s) = D(\mathbb{1}*\mathbb{1},s) = D(\mathbb{1},s)\cdot D(\mathbb{1},s) = \zeta(s)^2$

$d_k = \sum_{\substack{n,m\geq 1:\\ nm=k}} 1\cdot 1 =$ nr. of divisors of k

$d^{(k)} = \underbrace{\mathbb{1} * \dots * \mathbb{1}}_{k \text{ times}}$ $\qquad$ $D(d^{(k)},s) = \zeta(s)^k$

$id = (1,2,\dots)$ $\qquad$ $D(id,s) = \zeta(s-1)$

$D(id^r,s) = \zeta(s-r)$

$\sigma = id * \mathbb{1}$ $\qquad$ $D(\sigma, s) = \zeta(s-1)\,\zeta(s)$

$\sigma_k = \sum_{\substack{n,m: \\ k=nm}} n \cdot 1$ = sum of divisors of k

$\mu = \tilde{\mathbb{1}}$ Möbius function $\qquad$ $D(\mu, s) = \frac{1}{\zeta(s)}$

$$\mu_n = \begin{cases} (-1)^k, & n \text{ prod. of } k \text{ distinct primes} \\ 0, & n \text{ not squarefree} \end{cases}$$

$\varphi * \mathbb{1} = id$ $\qquad$ $D(\varphi, s) \cdot \zeta(s) = \zeta(s-1)$

$\varphi_n = \#(\mathbb{Z}/n\mathbb{Z})^\times$ (Euler's phi function)

= nr. of inv. res. cl. mod n

$$(\mathbb{1}_{square})_n = \begin{cases} 1, & n \text{ square} \\ 0, & \text{otherwise} \end{cases}$$

$D(\mathbb{1}_{square}, s) = \zeta(2s)$

$\vdots$

Def A sequence $a=(a_1, a_2, \ldots)$ is multiplicative if

i) $a_1 = 1$ and

ii) $a_{nm} = a_n a_m$ for all $n,m \geq 1$ with $\gcd(n,m)=1$.

It is completely multiplicative if ii) holds for all $n,m \geq 1$.

Exe $\delta, 1, \mathrm{id}$ ~~[illegible]~~ are completely multiplicative.

$1_{\text{square}}, d, \varphi$ are multiplicative.

Lemma 3.1

a) If a,b are multiplicative, then $a*b$ is.

b) If a is multiplicative and invertible, then $\tilde{a}$ is.

Pf a)
$$(a*b)_{nm} = \sum_{\substack{k,l\geq 1:\\ nm=kl}} a_k b_l \underset{\substack{\uparrow\\ \gcd(n,m)=1}}{=} \sum_{\substack{k_1,l_1,k_2,l_2\geq 1\\ n=k_1l_1\\ m=k_2l_2}} \underbrace{a_{k_1k_2}}_{a_{k_1}a_{k_2}} \underbrace{b_{l_1l_2}}_{b_{l_1}b_{l_2}}$$

$$= a_n b_m$$

b) similar ~~to~~ a); prove it for $\tilde{a}_n$ by ind. over n. □

Rmk If ~~[illegible]~~ a is multiplicative, then formally

$$D(a,s) = \prod_{p \text{ prime}} \underbrace{\sum_{k=0}^{\infty} \frac{a_{p^k}}{p^{sk}}}_{1+\frac{a_p}{p^s}+\frac{a_{p^2}}{p^{2s}}+\ldots = F((1,a_p,a_{p^2},\ldots), \frac{1}{p^s})}$$ (formal power series in $\frac{1}{p^s}$)

Exe $\zeta(s) = \prod_p \left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots\right) = \prod_p \frac{1}{1-\frac{1}{p^s}}$

Ex $\zeta(s)^2 = D(d,s) = \prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \frac{4}{p^{3s}} + \dots\right)$

~~Rmk You can formally verify identities. For example:~~

Rule ~~To check whether two~~ To determine a multiplicative sequence a ~~are equal~~ it suffices to know a_{p^k} for all primes p and $k \geq 1$. For example:

Lemma 3.2 Let $\lambda_n = (-1)^{\sum e_i}$ if $n = \prod_i p_i^{e_i}$. Then,

$$\lambda * \mathbb{1} = \mathbb{1}_{\text{square}}.$$

Pf1 Both sides are completely mult.

$$(\lambda * \mathbb{1})_{p^k} = \sum_{\substack{n,m:\\ p^k = nm}} \lambda_n \cdot 1 = \sum_{\substack{t,u \geq 0:\\ k = t+u}} \underbrace{\lambda_{p^t}}_{(-1)^t} \cdot 1 = \begin{cases} 1, & k \text{ even} \\ 0, & k \text{ odd} \end{cases} = \mathbb{1}_{\text{square}}(p^k). \quad \square$$

Pf2

$$D(\lambda * \mathbb{1}, s) = \prod_p \underbrace{\sum_{k \geq 0} \frac{\lambda_{p^k}}{(p^s)^k}}_{f_p(p^s)} \cdot \prod_p \underbrace{\sum_{c \geq 0} \frac{\mathbb{1}_{p^c}}{(p^s)^c}}_{g_p(p^s)} = \prod_p \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{4s}} + \dots\right) = D(\mathbb{1}_{\text{square}}, s)$$

with $f_p(X) = \sum \lambda_{p^k} X^k$, $g_p(X) = \sum \mathbb{1}_{p^c} X^c$,

$= 1 - X + X^2 - X^3 \pm \dots = \frac{1-X}{1-X^2}$ $\qquad$ $= 1 + X + X^2 + X^3 + \dots = \frac{1}{1-X}$

$$f_p(X) \cdot g_p(X) = \frac{1}{1-X^2} = 1 + X^2 + X^4 + \dots$$

$\square$

Rmk $\tilde{\mathbb{1}} = \mu$, where μ is the Möbius function:

$$\mu(n) = \begin{cases} (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0, & \text{otherwise.} \end{cases}$$

Pf $D(\tilde{\mathbb{1}}, s) = D(\mathbb{1}, s)^{-1} = \prod_p (1-p^s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$. □

Rmk (Möbius inversion)

If $b_n = \sum_{m|n} a_m$ for all $n \geq 1$,

then $a_n = \sum_{m|n} b_m \, \mu(\frac{n}{m})$ for all $n \geq 1$.

Pf

Assumption $\Leftrightarrow$ $b = a * \mathbb{1}$

Conclusion $\Leftrightarrow$ $a = b * \mu$

$\Leftarrow$ $\mu = \tilde{\mathbb{1}}$ is the inverse of $\mathbb{1}$ (w.r.t. convolution)

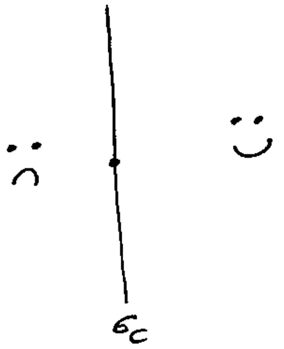
□

3.1. Convergence

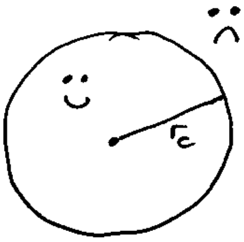
[What does the region of convergence look like?
For power series, it's essentially a disk.
For Dirichlet series, it's essentially a (half-) plane.]

Lemma 3.1.1 Let $s_1, s_2 \in \mathbb{C}$, $\mathrm{Re}(s_1) < \mathrm{Re}(s_2)$.
If $\sum_{n=1}^{\infty} \frac{a_n}{n^{s_1}}$ converges, then $\sum_{n=1}^{\infty} \frac{a_n}{n^{s_2}}$ converges.

Rmk Hence, there is a number $\sigma_c = \sigma_c(a) \in \mathbb{R} \cup \{\pm\infty\}$, called the abscissa of convergence, such that $\sum \frac{a_n}{n^s}$ converges if $\mathrm{Re}(s) > \sigma_c$ and doesn't converge if $\mathrm{Re}(s) < \sigma_c$.



Rmk This is like the radius of convergence for power series.



Pf of Lemma 3.1.1

$$\sum \frac{a_n}{n^{s_1}} \text{ conv.} \Leftrightarrow \sum_{k\le n\le l} \frac{a_n}{n^{s_1}} \xrightarrow[\text{(uniformly in } l)]{k\to\infty} 0$$

$$\sum \frac{a_n}{n^{s_2}} \text{ conv.} \Leftrightarrow \sum_{k\le n\le l} \frac{a_n}{n^{s_2}} \longrightarrow 0$$

Apply Abel summation to $\sum_{k\le n\le x} \frac{a_n}{n^{s_1}}$, $\frac{1}{x^{s_2-s_1}}$ ...

□

Ese $\left(\zeta(s) =\right) \sum_{n=1}^{\infty} \frac{1}{n^s}$ has abscissa of convergence $\sigma_c = 1$.

Pf If $s \in \mathbb{R}$, the sum converges if and only if $s > 1$. □

More precisely:

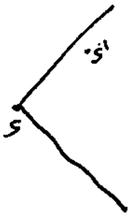
Lemma 3.1.2 ~~For any $\sigma > \sigma_c$, and any $H>0$ $\sum \frac{a_n}{n^s}$ is~~

~~uniformly convergent in~~

~~If~~ If $\sum \frac{a_n}{n^s}$ converges, then $\sum \frac{a_n}{n^{s'}}$ is uniformly convergent in the sector

$\{ s' \in \mathbb{C} : \operatorname{Re}(s') \ge \operatorname{Re}(s),\ |\operatorname{Im}(s'-s)| \le H \operatorname{Re}(s'-s) \}$

for any $H > 0$.



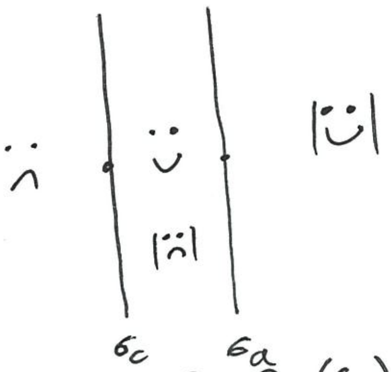
Pf same □

Rmk/Def Similarly, there is a number $\sigma_a = \sigma_a(a) = \sigma_c(|a|) \in \mathbb{R}\cup\{\pm\infty\}$, called the <u>abscissa of absolute convergence</u> such that $\sum \left|\frac{a_n}{n^s}\right|$ converges if $\mathrm{Re}(s) > \sigma_a$

$$= \sum \frac{|a_n|}{n^{\mathrm{Re}(s)}}$$

and doesn't converge if $\mathrm{Re}(s) < \sigma_a$.

Lemma 3.1.3 $\sigma_c \leq \sigma_a \leq \sigma_c + 1$.



Rmk This is unlike for power series, where radius of conv. = radius of abs. conv.

Pf Let $s_1, s_2 \in \mathbb{C}$, $\mathrm{Re}(s_1)+1 < \mathrm{Re}(s_2)$.

$\sum \frac{a_n}{n^{s_1}}$ conv. $\Rightarrow \frac{a_n}{n^{s_1}} = O(1) \Rightarrow \frac{a_n}{n^{s_2}} = O\left(\frac{1}{n^{s_2-s_1}}\right)$

$\Rightarrow \sum \left|\frac{a_n}{n^{s_2}}\right|$ conv. □

Ex $\sum \frac{(-1)^{n-1}}{n^s} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} \pm \dots$ has $\sigma_c = 0$, $\sigma_a = 1$.

(or more generally $\sum \frac{e^{2\pi i n/m}}{n^s}$ for $\overset{\mathbb{Z}}{\overset{\in}{m}} \geq 2$)

(or even more generally $\sum \frac{a_n}{n^s}$ with $a_1, a_2, \dots$ periodic, not all 0, and $\sum_{n\leq x} a_n$ bounded)

~~Remark If $\mathrm{Re}(s) > \sigma_c^{(a)}$, then~~

~~$\frac{d}{ds}\sum_{n\geq 1}\frac{a_n}{n^s} = \underbrace{\sum_{n\geq 1}\frac{-a_n \log n}{n^s}}_{\text{convergent}}$~~

Remark If $\sum \frac{a_n}{n^s} = 0$ for all s with $\mathrm{Re}(s) > \underset{\mathbb{R}}{\overset{\Uparrow}{\sigma}}$,

then $a_n = 0$ for all n.

Pf Assume a_m is the first nonzero entry.

$$\frac{a_m}{\cancel{m^s}} = -\sum_{n>m} \underbrace{\frac{a_n}{(n/m)^s}}_{\xrightarrow[s\to\infty]{} 0}$$ for suff. large $\mathrm{Re}(s)$

$$\Rightarrow |a_m| \leq \sum_{n>m} \underbrace{\frac{|a_n|}{|n/m|^s}}_{\substack{\text{mon.} \\ \text{decreasing,} \\ \to 0 \\ \text{for } s\to\infty}}$$ for suff. large $s \in \mathbb{R}$

↗ converges for $s > \sigma + 1$

$$\xrightarrow{s\to\infty} 0$$

$\Rightarrow a_m = 0$.

□

Lemma 3.1.4 If $D(a,s)$ and $D(b,s)$ are absolutely convergent, then $D(a*b,s)$ is, and $D(a*b,s)=D(a,s)D(b,s)$.

Pf Just rearrange summands. □

Lemma 3.1.5 If a is multiplicative and $D({}^*a,s)$ converges absolutely, then: a) the product

$$\prod_p \sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}} \text{ converges to } D(a,s).$$

b) If $D(a,s)=0$, then at least one factor $\sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}}$ is 0.

Pf a)

$$\prod_{p\leq P} \sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}} = \sum_{\substack{n\geq 1 \\ \text{not divisible} \\ \text{by any } p>P}} \frac{a_n}{n^s} \xrightarrow[P\to\infty]{} D(a,s).$$

b) If $D(a,s)=0$ ~~then~~

$$\overset{\shortparallel}{\prod_p \sum_k \frac{a_{p^k}}{p^{ks}}}$$

and $\sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}} \neq 0$ for all p, then

$$\prod_{p>P} \sum_{k\geq 0} \frac{a_{p^k}}{p^{ks}} = 0 \text{ for all } P.$$

$$\shortparallel$$

$$\sum_{\substack{n\geq 1 \\ \text{only divisible} \\ \text{by } p>P}} \frac{a_n}{n^s} = 1 + \sum_{\substack{n>1 \\ \text{only divisible} \\ \text{by } p>P \\ (\Rightarrow n>P)}} \frac{a_n}{n^s} \xrightarrow{P\to\infty} 1$$

□

Cor 3.1.6 $\zeta(s)$ has no zeros with $\mathrm{Re}(s)>1$.

Pf 1 $\zeta(s) = \prod_p \frac{1}{\underbrace{1-\frac{1}{p^s}}_{\neq 0}}$. □

Pf 2 Later...

Lemma 3.1.7 A Dirichlet series $D(a,s) = \sum \frac{a_n}{n^s}$ is holomorphic in the region $\{s \in \mathbb{C} : \operatorname{Re}(s) > \sigma_c\}$ with derivative $\frac{d}{ds} D(a,s) = \sum \frac{-a_n \log n}{n^s}$.

Pf The sum is locally uniformly convergent in this region according to Lemma 3.1.2. Each summand $\frac{a_n}{n^s}$ is holomorphic with derivative $\frac{-a_n \log n}{n^s}$.

That implies the claim. (See e.g. Thm II.5.2 in Fischer-Lieb: A Course in Complex Analysis)

$\square$

3.2. Meromorphic continuation

Thm 3.2.1 $\zeta(s) = \sum \frac{1}{n^s}$ has a (unique) meromorphic continuation to the entire complex plane, which we will also denote by $\zeta(s)$. Its only singularity is a pole of order 1 and residue 1 at $s = 1$:

$$\zeta(s) - \frac{1}{s-1} \text{ is holomorphic everywhere.}$$

Pf Apply Euler-Maclaurin: For all $k \geq 0$ and $\mathrm{Re}(s) > 1$:

$$\sum_{n=2}^{\infty} \frac{1}{n^s} = \underbrace{\int_1^{\infty} \frac{1}{t^s}\, dt}_{= \left[-\frac{1}{s-1} \cdot \frac{1}{t^{s-1}}\right]_{t=1}^{\infty} = \frac{1}{s-1}}$$

$$+ \underbrace{\sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!} \left[\underbrace{B_{r+1}(t)}_{O(1)} \frac{(-s)\cdots(-s-r+1)}{t^{s+r}} \right]_{t=1}^{\infty}}_{\substack{-B_{r+1}(1)\cdot(-s)\cdots(-s-r+1) \\ \text{(holomorphic in } \mathbb{C})}}$$

$$+ \underbrace{\int_1^{\infty} \frac{(-1)^k}{(k+1)!} \underbrace{B_{k+1}(t)}_{O(1)} \frac{(-s)\cdots(-s-k)}{t^{s+k+1}}\, dt}_{\substack{\text{holomorphic in} \\ \{s \in \mathbb{C} : \mathrm{Re}(s) > -k\}}}$$

$$\Rightarrow \frac{1}{s-1} + \sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!} \cdot \left(-B_{r+1}(1) \cdot (-s) \cdots (-s-r+1)\right)$$

$$+ \int_1^\infty \frac{(-1)^k}{(k+1)!} B_{k+1}(t) \, \frac{(-s) \cdots (-s-k)}{t^{s+k+1}} \, dt$$

is a meromorphic continuation of $\zeta(s)$ to

$\{ s \in \mathbb{C} : \operatorname{Re}(s) > -k \}$ for any $k \geq 0$.

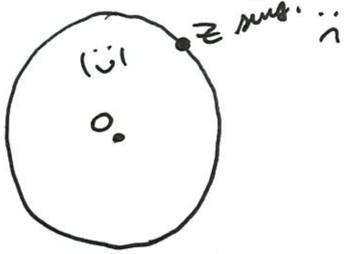
$\wedge$

(with the claimed singularity only)

$\square$

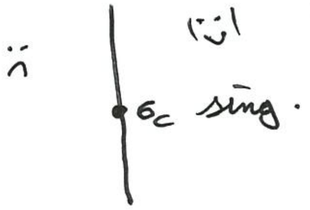
Rmk Power series converge until they cannot due to a singularity:

If $\sum_{n=0}^{\infty} a_n x^n$ has radius of convergence r_c, then it has a singularity $z \in \mathbb{C}$ with $|z| = r_c$.



The same holds for Dirichlet series with nonneg. coeff.:

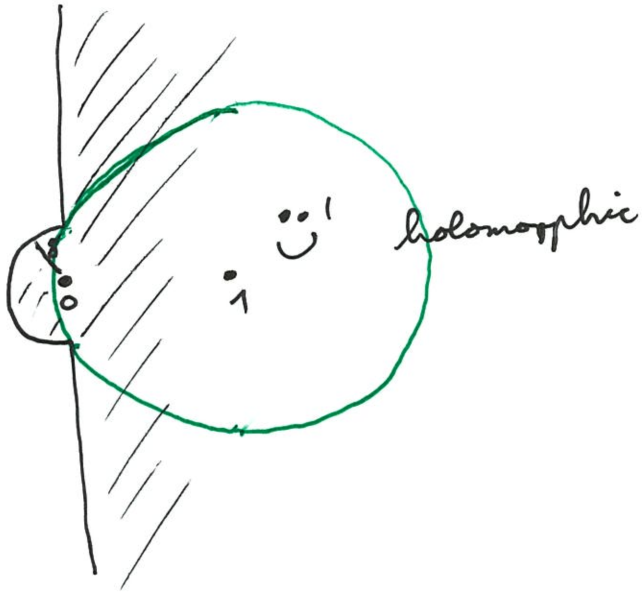
Thm 3.2.2 If $a_1, a_2, \dots \geq 0$ and $\sigma_c \in \mathbb{R}$, then σ_c is a singularity of $D(a,s)$.



Ex $\zeta(s)$ has a pole at $\sigma_c = 1$.

Pf Replacing a_n by $\frac{a_n}{n^{\sigma_c}}$, we can assume w.l.o.g. that $\sigma_c = 0$.

Assume that $D(s) := D(a, s)$ has a holomorphic continuation to a neighborhood $\{ s \in \mathbb{C} : |s| < \delta \}$ of 0.



The Taylor series expansion of $D(s)$ around $s=1$ is:

$$D(s) = \sum_{k \geq 0} \frac{(s-1)^k}{k!} \cdot D^{(k)}(1) = \sum_{k \geq 0} \frac{(s-1)^k}{k!} \cdot \sum_{n \geq 1} \frac{a_n (-\log n)^k}{n}$$

$$= \sum_{k \geq 0} \sum_{n \geq 1} \frac{(1-s)^k}{k!} \cdot \frac{a_n (\log n)^k}{n}$$

According to the remark, it converges in a circle of radius $\sqrt{1+\delta^2} > 1$.

$\Rightarrow$ It converges at some real $s < 0$.

Since $a_1, a_2, \dots \geq 0$, each summand is ≥ 0 for $s \leq 0$.

$\Rightarrow$ We can rearrange:

$$\Rightarrow D(s) = \sum_{n \geq 1} a_n \cdot \underbrace{\sum_{k \geq 0} \frac{(1-s)^k}{k!} \cdot \frac{(\log n)^k}{n}}_{\substack{\text{Taylor series for } \frac{1}{n^s} \\ \text{around } s=1}}$$

$$= \sum_{n \geq 1} \frac{a_n}{n^s} \text{ converges (for some } s<0).$$

$\Rightarrow \sigma_c < 0.$ ↯ □

The assumption that $a_1, a_2, \ldots \geq 0$ is necessary:

Thm 3.2.3 Let the sequence $a_1, a_2, \ldots$ be periodic with period m and assume $a_1 + \ldots + a_m = 0$. Then, $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ (with $\sigma_c \leq \sigma_a \leq 1$ because $a_n = O(1)$) has a holomorphic continuation to $\mathbb{C}$.

Ex $\sum \frac{(-1)^{n-1}}{n^s}$, $\sum \exp(2\pi i n/m) \cdot \frac{1}{n^s}$, ...

Pf Apply Abel summation to $\sum_{n \leq x} a_n$ and $\frac{1}{t^s}$:

$$\sum_{n \leq x} a_n \ \| \leftarrow \text{periodic (because } a_1 + \ldots + a_m = 0) \quad O(1)$$

For $\operatorname{Re}(s) > 1$:

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \Big[\underbrace{\sum_{n \leq t} a_n}_{O(1)} \cdot \frac{1}{t^s} \Big]_{t=1}^{\infty} - \int_1^{\infty} \underbrace{\sum_{n \leq t} a_n}_{O(1)} \cdot \frac{-s}{t^{s+1}} \, dt$$

The RHS is a hol. cont. to $\{s \in \mathbb{C} : \operatorname{Re}(s) > 0\}$.

Keep integrating by parts as in the construction of the Euler-Maclaurin formulas, making sure to keep the first function bounded...

(previously the Bernoulli fcts)

□

4. The functional equation

Def The theta function $\Theta : \mathbb{R}_{>0} \to \mathbb{R}$ is given by
$$\Theta(u) = \sum_{n\in\mathbb{Z}} e^{-\pi u n^2}.$$

Thm 4.1

a) $\Theta(u) - 1 = \mathcal{O}(e^{-u})$ for large u.

b) $\Theta(u^{-1}) = u^{1/2}\,\Theta(u) \quad \forall u>0$

Pf a) easy
b) Poisson summation (Problem 1 on Pset 2) □

Def The gamma function Γ is the meromorphic continuation of the function given by $\Gamma(s) = \int_0^\infty x^{s} e^{-x} \frac{dx}{x}$ for $\operatorname{Re}(s) > 0$.

Thm 4.2

a) $s\Gamma(s) = \Gamma(s+1) \quad \forall s\in\mathbb{C}$

b) $\Gamma(n+1) = n! \quad \forall n\geq 0$.

c) $\Gamma(s)$ has simple poles at $s = 0, -1, -2, \dots$ and no other poles.

d) $\Gamma(s)$ has no zeros.

e) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$

f) $\log\Gamma(s) = s\log s - s - \frac{1}{2}\log s + C + \mathcal{O}_\varepsilon(|s|^{-1})$ if $\arg(s) \in [-\pi+\varepsilon, \pi-\varepsilon]$
(Stirling's approximation) with $C = \frac{1}{2}\log(2\pi)$.

Def The xi function is

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Rmk There are other conventions as well!

Thm 4.3 (Functional equation)

We have $\xi(s) = \xi(1-s)$.

Pf First, note that for $\mathrm{Re}(s)>0$:

$$\int_0^\infty e^{-\pi u n^2} u^{s/2}\frac{du}{u} \underset{\substack{\uparrow \\ \boxed{x=\pi u n^2}}}{=} \pi^{-s/2}\cdot\frac{1}{n^s}\cdot\underbrace{\int_0^\infty x^{s/2}e^{-x}\frac{dx}{x}}_{\Gamma(s/2)}.$$

$\Rightarrow$ For $\mathrm{Re}(s)>1$:

$$\frac{1}{2}\int_0^\infty \underbrace{(\Theta(u)-1)}_{\substack{\sum_{n\neq 0} e^{-\pi u n^2} \\ =\frac{1}{2}\sum_{n\geq 1} e^{-\pi u n^2}}} u^{s/2}\frac{du}{u} = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \xi(s).$$

$$\Rightarrow 2\xi(s) = \int_1^\infty u^{s/2}(\Theta(u)-1)\frac{du}{u} + \int_0^1 u^{s/2}(\Theta(u)-1)\frac{du}{u}$$

$$\underset{\substack{\uparrow \\ \boxed{u=t^{-1}}}}{=} \quad '' \quad + \int_1^\infty t^{-s/2}(t^{1/2}\Theta(t)-1)\frac{dt}{t}$$

$$= \quad '' \quad + \int_1^\infty t^{(1-s)/2}(\Theta(t)-1)\frac{dt}{t} + \int_1^\infty (t^{(1-s)/2}-t^{-s/2})\frac{dt}{t}$$

$$= \quad '' \quad + \quad '' \quad - \frac{2}{1-s} - \frac{2}{s}$$

According to Thm 4.1 a), the RHS is meromorphic for all s, so the equation holds for all s.

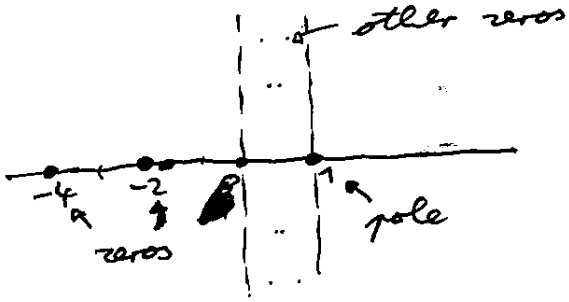
The RHS is unchanged when replacing s by $1-s$. □

Cor 4.4

a) $\zeta(s)$ has a simple zero at $s = -2, -4, \dots$ (trivial zeros)

b) All other (nontrivial) zeros lie in $\{s \in \mathbb{C} : 0 \leq \operatorname{Re}(s) \leq 1\}$.

c) If s is a nontrivial zero, then so are $1-s$, $\bar{s}$, $1-\bar{s}$.



Riemann Hypothesis All nontrivial zeros satisfy $\operatorname{Re}(s) = \frac{1}{2}$.

Pf a) $$\xi(s) = \pi^{-s/2} \underbrace{\Gamma(s/2)}_{\text{simple pole}} \zeta(s) = \xi(1-s) = \pi^{-(1-s)/2} \underbrace{\Gamma((1-s)/2)}_{\text{neither zero nor pole}} \underbrace{\zeta(1-s)}_{\text{neither zero nor pole}}$$

(cf. Cor 3.1.6)

at $s = -2, -4, \dots$

b) $\operatorname{Re}(s) \leq 1$ by Cor 3.1.6.
If $\operatorname{Re}(s) < 0$, then $\operatorname{Re}(1-s) > 1$, so RHS has no zero. Also, $\Gamma(s/2)$ has no pole unless $s = -2, -4, \dots$

c) $\zeta(s) = 0$, $\Gamma(s/2), \Gamma((1-s)/2)$ no zeros/poles $\Rightarrow \zeta(1-s) = 0$.
$\zeta(\bar{s}) = \overline{\zeta(s)} = 0$. □

Thm 45. $\zeta(s)$ has no zeros with $\operatorname{Re}(s)=1$.

Pf By Problem 2c on Pset 3, we have

$$-\frac{\zeta'}{\zeta}(s)=\sum_{n\geq 1}\frac{\Lambda(n)}{n^s}$$

with $\Lambda(n)=\begin{cases}\log p, & n=p^e \quad (e\geq 1),\\ 0, & \text{otherwise.}\end{cases}$

Clearly, $0\leq \Lambda(n)\ll_{\varepsilon} n^{\varepsilon}$.

$\Rightarrow D(\Lambda, s)$ has $\sigma_c\leq 1$.

If $\zeta(s)=f(s)\cdot(s-s_0)^k$ with $f(s)$ holomorphic and nonzero at $s=s_0$

(meaning: $\zeta(s)$ has zero of order k or pole of order $-k$ at $s=s_0$), then

$-\frac{\zeta'}{\zeta}(s)$ has a simple pole at $s=s_0$ with residue $-k$.

Note: Since $-\frac{\zeta'}{\zeta}(s)$ is holomorphic in $\{s\in\mathbb{C}:\operatorname{Re}(s)>1\}$, this again proves that $\zeta(s)$ has no zeros with $\operatorname{Re}(s)>1$.

Now, observe that

$$3+4\cos\theta+\cos 2\theta = 2(1+\cos\theta)^2 \geq 0$$

for all $\theta \in \mathbb{R}$.

$$\Rightarrow 3+4\,\mathrm{Re}\left(\frac{1}{n^{it}}\right)+\mathrm{Re}\left(\frac{1}{n^{2it}}\right) \geq 0 \quad \forall t \in \mathbb{R}.$$

$$\Rightarrow 3\cdot \underbrace{\sum \frac{\Lambda(n)}{n^{\sigma}}}_{-\frac{\zeta'}{\zeta}(\sigma)} + 4\,\mathrm{Re}\Bigg(\underbrace{\sum \frac{\Lambda(n)}{n^{\sigma+it}}}_{-\frac{\zeta'}{\zeta}(\sigma+it)}\Bigg) + \mathrm{Re}\Bigg(\underbrace{\sum \frac{\Lambda(n)}{n^{\sigma+2it}}}_{-\frac{\zeta'}{\zeta}(\sigma+2it)}\Bigg) \geq 0 \qquad (I)$$

$\forall \sigma > 1,\ t \in \mathbb{R}$

Fact. Assume ζ has a zero of order $k \geq 0$ at $1+it$ and of ~~order~~ $l \geq 0$ at $1+2it$.

$$\Rightarrow -\frac{\zeta'}{\zeta}(\sigma) = \frac{1}{\sigma-1} + O_t(1) \quad \text{for } \sigma \to 1,$$

$$\ldots(\sigma+it) = -\frac{k}{\sigma-1} + O_t(1) \quad \text{"} \,,$$

$$\ldots(\sigma+2it) = -\frac{l}{\sigma-1} + O_t(1) \quad \text{"} \,.$$

$$\overset{(I)}{\Rightarrow} 3-4k-l \geq 0 \Rightarrow 4k \leq 3 \Rightarrow k=0.$$

$\Rightarrow \zeta$ has no zero at $1+it$. $\square$

5. The Wiener-Ikehara Theorem

5.1. Statement

Thm 5.1.1 (Wiener-Ikehara)

Let $a_1, a_2, \ldots \geq 0$ and $d > 0$ and assume that $D(a,s)$ can be meromorphically continued to (a neighborhood of) $\{s \in \mathbb{C} : \operatorname{Re}(s) \geq d\}$, holomorphic except for a simple pole at $s=d$ with $\lim_{s \to d} D(a,s)\cdot(s-d) = A$.

Then, $\sum_{n \leq x} a_n \sim \frac{A}{d}\cdot x^d$ for $x \to \infty$.

Ex $D(1,s) = \zeta(s) \rightsquigarrow d=1, \; A=1$

$$\sum_{n \leq x} 1 \sim x$$

Ex $D(id^k, s) = \zeta(s-k)$ with $k > -1$

$\rightsquigarrow d = k+1, \; A = 1$

$$\sum_{n \leq x} n^k \sim \int_1^x t^k \, dt \sim \frac{1}{k+1} x^{k+1}.$$

Ex $D(1_{square}, s) = \zeta(2s) \rightsquigarrow d = \frac{1}{2}, \; A = \frac{1}{2}$

$$\sum_{\substack{n \leq x \\ square}} 1 = \sum_{m \leq x^{1/2}} 1 \sim x^{1/2}$$

Ex $D(\underset{\substack{\uparrow \\ \text{sum} \\ \text{of} \\ \text{divisors}}}{\sigma}, s) = \zeta(s-1)\zeta(s) \rightsquigarrow d=2,\ A=\zeta(2)$

(poles at $s=1,2$)

$$\Rightarrow \sum_{n \le x} \sigma_n \sim \frac{\zeta(s)}{2} \cdot x^2$$

Ex $a_n = \#\{(c,d) : c,d \ge 1,\ n=c^2d\}$

$D(a,s) = \zeta(2s)\zeta(s) \rightsquigarrow d=1,\ A=\zeta(2)$

$$\Rightarrow \sum_{\substack{c,d: \\ c^2d \le x}} 1 \sim \zeta(2) \cdot x$$

Ex $D(\Lambda, s) = -\frac{\zeta'(s)}{\zeta(s)} \rightsquigarrow d=1,\ A=1$

(pole at $s=1$, no other poles with $\mathrm{Re}(s) \ge 1$)

$$\Rightarrow \sum_{n \le x} \Lambda(n) \sim x$$

$$\parallel$$

$$\sum_{\substack{p,e : p^e \le x \\ (p \text{ prime},\ e \ge 1)}} \log p = \sum_{p \text{ prime}} \log p + \underbrace{\mathcal{O}\Big(\sum_{\substack{e \ge 2 \\ \overset{\wedge|}{\log_2 x}}} \underbrace{\sum_{\substack{m \ge 2: \\ m^e \le x}} \log n}_{\mathcal{O}(x^{1/2} \log n)} \Big)}_{\mathcal{O}(x^{1/2} (\log n)^2)}$$

$$\Rightarrow \sum_{p \text{ prime}} \log p \sim x$$

$\Leftrightarrow$ PNT

$\uparrow$

$\boxed{\text{Problem 3 on Pset 3}}$

Thm 5.1.2 (Kato: A remark on the Wiener-Ikehara Tauberian Theorem)

Let $a_1, a_2, \ldots \geq 0$ and $l, m \geq 1$ and $d>0$ and assume that $D(a,s)^m$ can be meromorphically continued to (a nbhd of) $\{s \in \mathbb{C} : \Re(s) \geq d\}$, holomorphic except for a pole of order l at $s=d$ with $\lim_{s \to d} D(a,s)^m \cdot (s-d)^l = A^m$. $(A>0)$

("pole of order l/m")

Then, $\sum_{n \leq X} a_n \sim \frac{A}{d \cdot \Gamma(\frac{l}{m})} \cdot X^d (\log X)^{\frac{l}{m}-1}$.

Ex $D(d,s) = \zeta(s)^2 \rightsquigarrow d=1,\ \frac{l}{m} = \frac{2}{1},\ A=1.$

$\sum_{n \leq X} d_n \sim X \log X$

Ex $D(d^{(3)},s) = \zeta(s)^3 \rightsquigarrow d=1,\ \frac{l}{m} = \frac{3}{1},\ A=1$

$\sum d_n^{(3)} \sim \frac{1}{2} X (\log X)^2$

[Ex with $m>1$: later...]

5.2. Proof

We'll now prove Thm 5.1.1 following chapter 3.3 in Murty.

Rmk It suffices to prove Thm 5.1.1 for $d=1$, [redacted]

Pf Consider the sequence $b_n = a_n \cdot n^{1-d}$.

$D(b,s) = D(a, s+d-1)$ has merom. cont. with pole at $s=1$. $\lim_{s\to 1} D(b,s)\cdot(s-1) = A$.

$$\underset{\boxed{d=1\text{ case}}}{\Longrightarrow} \quad \sum_{n\leq x} b_n \sim A\cdot x$$

Apply Abel summation to estimate

$$\sum_{n\leq x} a_n = \sum_{n\leq x} b_n \cdot n^{d-1}.$$

□

Lemma 5.2.1 Let $a_1, a_2, \ldots \geq 0$ [redacted] and assume that $D(a,s)$ [redacted] has absissa of convergence [redacted] $\sigma_c > 0$.

Then, $\sum_{n\leq x} a_n \ll_q x^{q}$ [redacted] for all $q >$ [redacted] σ_c and $x \geq 1$.

Pf $\sum_{n\leq x} a_n \leq \sum_{n=1}^{\infty} a_n \cdot \left(\frac{x}{n}\right)^{q}$ [redacted] $= x^{q}$ [redacted] $\cdot \underbrace{D(a,q\text{[redacted]})}_{<\infty}$. □

Pf of Thm 5.1.1

W.l.o.g. $d=1$, $A=1$.

Let $f(x) = \sum_{n \le x} a_n$.

Abel summation for $f(x)$, $\frac{1}{x^s}$ shows for $\mathrm{Re}(s)>1$:

$$F(s) := D(a,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \underset{\uparrow}{=} s \cdot \int_1^{\infty} \frac{f(x)}{x^{s+1}}\, dx$$

$$\boxed{\frac{f(x)}{x^s} \to 0 \text{ by Lemma } 5.2.1}$$

$$\underset{\substack{\uparrow \\ x=e^u}}{=} s \cdot \int_0^{\infty} f(e^u)\, e^{-us}\, du$$

$$\Rightarrow H(s) := \frac{F(s)}{s} - \frac{1}{s-1} = \int_0^{\infty} \left(f(e^u)e^{-u} - 1\right) e^{-u(s-1)}\, du$$

$$= \int_0^{\infty} (g(u)-1)\, e^{-u(s-1)}\, du \quad \text{for } \mathrm{Re}(s)>1.$$

with $g(u) := f(e^u)e^{-u} = \dfrac{\sum_{n \le e^u} a_n}{e^u}$.

Goal: $g(u) \xrightarrow{u \to \infty} 0$.

By assumption, $H(s)$ can be holomorphically continued to $\{s \in \mathbb{C} \mid \mathrm{Re}(s) \ge 1\}$.

For any $\delta \geq 0$ and $t \in \mathbb{R}$, let

$$h_\delta(t) = H(1+\delta+2\pi i t).$$

Let $\phi_\delta(u) := \begin{cases} (g(u)-1)e^{-u\delta} & , \quad u \geq 0, \\ 0 & , \quad u < 0. \end{cases}$

$$\Rightarrow h_\delta(t) = \int_0^\infty (g(u)-1)e^{-u\delta}\, e^{-2\pi i u t}\, du$$

$$= \widehat{\phi_\delta}(t).$$

~~Note: $(g(u)-1)e^{-u\delta} \leq C_\delta\, e^{-u\delta/2}$ by Lemma 5.2.1.~~

Fake proof: $h_\delta(t) = \widehat{\phi_\delta}(t) \quad \forall t$

$$\Rightarrow \begin{tikzcd} \phi_\delta(u) \arrow[d] & = & \widehat{h_\delta}(-u) \arrow[d] \arrow[dl, phantom, "\delta \to 0"] & \forall u \\ g(u)-1 & = & \widehat{h_0}(-u) \arrow[r, "u \to \infty", "{(\text{Thm } 2.2.1\text{: Riemann-Lebesgue Lemma})}"'] & 0 \end{tikzcd}$$

Issues: • h_δ converges to h_0 pointwise, but perhaps not uniformly.

$\Rightarrow$ Maybe $\widehat{h_\delta}$ doesn't even converge to $\widehat{h_0}$ pointwise.

• Maybe $\widehat{h_0}$ doesn't even lie in $L^1(\mathbb{R})$.

Maybe $\widehat{h_0}$ — " — .

Note: a) At least h_δ converges to h_0 locally uniformly (because H is continuous).

b) We have $\phi_\delta(v) \ll_\delta e^{-v\delta/2}$ by Lemma 5.2.1, so

in particular $\phi_\delta \in L^1(\mathbb{R})$ and $L^2(\mathbb{R})$.

$$\Rightarrow \quad h_\delta = \widehat{\phi_\delta} \in L^2(\mathbb{R}).$$

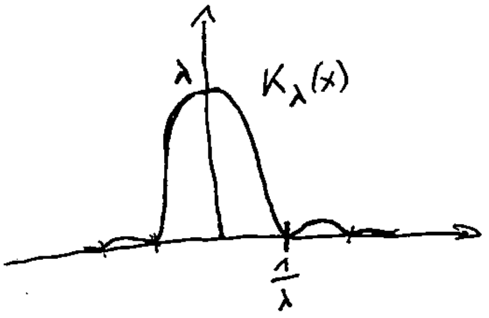
Solution: Use the Fejér kernel

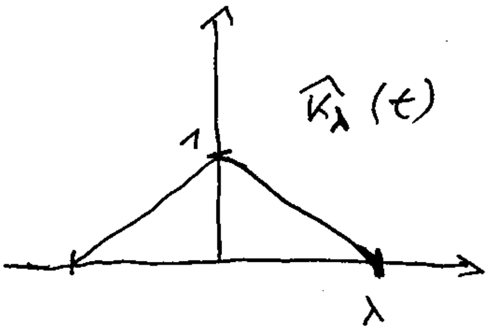
$$K(x) = \left(\frac{\sin(\pi x)}{\pi x}\right)^2 \geq 0 \qquad (K(0)=1)$$

with

$$\widehat{K}(t) = \begin{cases} 1-|t|, & |t| \leq 1, \\ 0, & |t| \geq 0. \end{cases} \qquad \text{(compactly supported, } \geq 0\text{)}$$

Let $K_\lambda(x) = \lambda \cdot K(\lambda x)$. $\Rightarrow$ $\widehat{K_\lambda}(t) = \widehat{K}\left(\frac{t}{\lambda}\right)$.





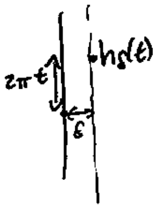
Reminder: $a_1, a_2, \dots \geq 0$

$$f(x) = \sum_{n \leq x} a_n$$

$$g(v) = \frac{f(e^v)}{e^v}$$

Goal: $g(v) \xrightarrow{v \to \infty} 1$

$H(s)$ cont. on $\{\mathrm{Re}(s) \geq 1\}$



$$h_\delta(t) = H(1+\delta+2\pi i t)$$

$$\phi_\delta(v) = \begin{cases} (g(v)-1)e^{-v\delta} & , v \geq 0 \\ 0 & , v < 0 \end{cases}$$

$$h_\delta = \widehat{\phi_\delta}$$

Fake pf:
$$\begin{tikzcd} \phi_\delta(v) \arrow[d] \arrow[r, phantom, "="] & \hat{h}_\delta(-v) \arrow[d] \arrow[l, phantom, "\delta \to 0"', shift left=6] \\ g(v)-1 \arrow[r, phantom, "="] & \hat{h}_0(-v) \arrow[d] \\ & 0 \end{tikzcd}$$

Idea: Smoothen ϕ_δ by taking its convolution with a Fejér kernel K_λ (or a kernel from Problem 1a on Pset 4)

$\phi_\delta * K_\lambda \in L^1(\mathbb{R})$ because $\phi_\delta, K_\lambda \in L^1(\mathbb{R})$.

- $\widehat{\phi_\delta * K_\lambda} = \widehat{\phi_\delta} \cdot \widehat{K_\lambda} = h_\delta \hat{k}_\lambda \in L^1(\mathbb{R})$

because $\widehat{K_\lambda}$ is compactly supported and h_δ is continuous.

$$\underset{\boxed{\text{Thm 2.2.3}}}{\Rightarrow} (\phi_\delta * K_\lambda)(v) = \widehat{h_\delta \cdot \widehat{K_\lambda}}\,(-v)$$

$$\begin{tikzcd}
\Rightarrow \int_{\mathbb{R}} \phi_\delta(v-u)\, K_\lambda(u)\,du \arrow[r, phantom, "="] \arrow[d, "\text{monotone convergence}"', "\delta \to 0"] & \int_{\mathbb{R}} h_\delta(t)\, \underbrace{\widehat{K_\lambda}(t)}_{\text{cpt. support}}\, e^{2\pi i t v}\,dt \arrow[d, "a)"', "(h_\delta \to h_0 \text{ locally uniformly})"] \\
\int_{\mathbb{R}} \underbrace{\phi_0(v-u)} K_\lambda(u)\,du \arrow[r, phantom, "="] & \int_{\mathbb{R}} h_0(t)\, \widehat{K_\lambda}(t)\, e^{2\pi i t v}\,dt \arrow[d, phantom, "\parallel"] \\
 & \widehat{\underbrace{\underbrace{h_0}_{\text{cont.}} \cdot \underbrace{\widehat{K_\lambda}}_{\text{cpt. supp.}}}_{\Rightarrow \in L^1}}\,(-v) \arrow[r, "v \to \infty", "\text{Thm 2.2.1: Riemann-Lebesgue}"'] & 0
\end{tikzcd}$$

$$\Rightarrow \int_{\mathbb{R}} \underbrace{\phi_0(v-u)}_{\begin{cases} g(v-u)-1, & u \le v, \\ 0, & u > v. \end{cases}} K_\lambda(u)\,du \xrightarrow{v \to \infty} 0 \quad \text{for any } \lambda > 0. \quad (\mathrm{I})$$

Hope: $LHS \xrightarrow{\lambda \to \infty} \phi_0(v) = g(v) - 1$. "uniformly"

~~Note: this would be automatic if ϕ_0 were continuous.~~

Note: $f(x) = \sum_{n \le x} a_n$ is increasing, so $g(u) = \frac{f(e^u)}{e^u}$ satisfies

$$g(v+u) \geq g(v)\, e^{-u} \quad \text{for any } u \geq 0.$$

Let $r_\lambda(v) := \int_{-\infty}^{v} g(v-u)\, K_\lambda(u)\,du = \int_{\mathbb{R}} \underbrace{g(v-u)\, K_\lambda(u)}_{\geq 0}\,du.$

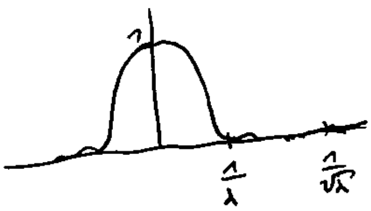
$$(\mathrm{I}) \Leftrightarrow r_\lambda(v) \xrightarrow{v \to \infty} \int_{\mathbb{R}} K_\lambda(u)\,du = \widehat{K_\lambda}(0) = 1.$$

$$\Rightarrow \Gamma_\lambda(v) \geq \int_{-\frac{1}{\sqrt{\lambda}}}^{\frac{1}{\sqrt{\lambda}}} g(v-u)\, K_\lambda(u)\, du$$

$$= \underbrace{g\left(v-\tfrac{1}{\sqrt{\lambda}}\right) e^{-2/\sqrt{\lambda}}} \int_{-\frac{1}{\sqrt{\lambda}}}^{\frac{1}{\sqrt{\lambda}}} K_\lambda(u)\, du$$

$$\downarrow \quad \lambda\to\infty \quad \downarrow$$

$$1 \qquad\qquad 1$$



Let $\varepsilon > 0$. Pick λ large enough so that

$$e^{-2/\sqrt{\lambda}} \int_{\cdot\cdot}^{\cdot\cdot} K_\lambda(u)\, du \geq \frac{1}{1+\varepsilon}$$

$$\Rightarrow (1+\varepsilon)\, \Gamma_\lambda(v) \geq g\left(v-\tfrac{1}{\sqrt{\lambda}}\right) \qquad \forall v$$

$$\Big\downarrow{\scriptstyle v\to\infty}$$

$$1$$

$$\Rightarrow \limsup_{v\to\infty} g(v) \leq 1+\varepsilon \quad \forall \varepsilon > 0$$

$$\Rightarrow \quad \text{---}''\text{---} \quad \leq 1.$$

In particular, $g(v) << 1$.

$$\Rightarrow r_\lambda(v) \le \int_{-\frac{1}{\sqrt{\lambda}}}^{\frac{1}{\sqrt{\lambda}}} g\left(v+\frac{1}{\sqrt{\lambda}}\right) \underset{\substack{\downarrow \\ 1}}{e^{2/\sqrt{\lambda}}} \; {\scriptstyle \lambda \to \infty} \; \underset{\substack{\downarrow \\ 1}}{K_\lambda(u)\,du}$$

$$+ \underset{\substack{\downarrow \lambda\to\infty \\ 0}}{\mathcal{O}\left(\int_{\mathbb{R}\setminus[-\frac{1}{\sqrt{\lambda}},\frac{1}{\sqrt{\lambda}}]} K_\lambda(u)\,du \right)}$$

$$\underset{\substack{\uparrow \\ \text{as before}}}{\Longrightarrow} \liminf_{v\to\infty} g(v) \ge 1.$$

$$\Longrightarrow \lim_{v\to\infty} g(v) = 1.$$

□

6. Dirichlet L-series

Def Let $q \geq 1$. A (multiplicative) character mod q is a group hom. $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$.

Ex The trivial character χ_0 with $\chi_0(x) = 1 \; \forall x \in (\mathbb{Z}/q\mathbb{Z})^\times$.

Ex If $q \neq 2$ is prime:

$$\chi_0(x) = \begin{cases} 1, & x \text{ quadr. res. mod } q, \\ -1, & \text{otherwise}. \end{cases}$$

(Note: $\chi_0(x) \equiv x^{\frac{q-1}{2}} \bmod q$.)

Rmk Each $\chi(x)$ is a (primitive) r-th root of unity for some $r \mid \varphi(q)$.

Pf

$$\chi(x)^{\varphi(q)} = \chi(x^{\varphi(q)}) = \chi(1) = 1. \qquad \square$$

Rmk The finite abelian group $(\mathbb{Z}/q\mathbb{Z})^\times$ is isomorphic to a product of cyclic groups: $(\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_r\mathbb{Z}$.
The group homomorphisms

$$\mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_r\mathbb{Z} \longrightarrow \mathbb{C}^\times$$

are the maps

$$(a_1, \dots, a_r) \longmapsto \zeta_{k_1}^{a_1 i_1} \cdots \zeta_{k_r}^{a_r i_r}$$

for $(i_1, \dots, i_r) \in \mathbb{Z}/k_1\mathbb{Z} \times \dots \times \mathbb{Z}/k_r\mathbb{Z}$.
In particular, $\#\{\chi\} = \#(\mathbb{Z}/q\mathbb{Z})^\times = \varphi(q)$.

Lemma 6.1

a) For any χ,
$$\sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(x) = \begin{cases} \varphi(q), & \chi=\chi_0, \\ 0, & \chi\neq\chi_0. \end{cases}$$

b) For any x,
$$\sum_{\chi} \chi(x) = \begin{cases} \varphi(q), & x=0 \bmod q, \\ 0, & x\neq 0 \bmod q. \end{cases}$$

Pf HW. □

Def The Dirichlet L-series for χ is

$$L(s,\chi) := \sum_{\substack{n\geq 1: \\ \gcd(n,q)=1}} \frac{\chi(n \bmod q)}{n^s}.$$

Rmk Often, people extend χ to $\mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ by letting $\chi(x)=0$ if $x \notin (\mathbb{Z}/q\mathbb{Z})^\times$. Then, $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n \bmod q)}{n^s}$.

Note that the corr. function $\begin{matrix} \mathbb{N} \to \mathbb{C} \\ n \mapsto \chi(n \bmod q) \end{matrix}$ is completely multiplicative.

Rmk Formally, $L(s,\chi) = \prod_{p\nmid q} \frac{1}{1-\frac{\chi(p)}{p^s}}$.

Ex $L(s,\chi_0) = \prod_{p\nmid q} \frac{1}{1-\frac{1}{p^s}} = \zeta(s)\cdot \prod_{p\mid q}\left(1-\frac{1}{p^s}\right)$,

which is holomorphic except for a simple pole at $s=1$ with residue $\prod_{p\mid q}\left(1-\frac{1}{p}\right) = \frac{\varphi(q)}{q}$.

Lemma 6.2 If $\chi \neq \chi_0$, then $L(s,\chi)$ has a holomorphic continuation to $\mathbb{C}$.

Pf χ is periodic, $\sum_x \chi(x) = 0$. Apply Thm 3.2.3. □

Thm 6.3 $L(s,\chi)$ has no zeros with $\mathrm{Re}(s) \geq 1$.

Pf We have

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=p^k} \frac{\chi(n)\log p}{n^s}.$$

Let $f(s) := \prod_{\chi} L(s,\chi)$.

$$\Rightarrow -\frac{f'(s)}{f(s)} = \sum_{\chi}\left(-\frac{L'(s,\chi)}{L(s,\chi)}\right) = \sum_{n=p^k} \frac{\sum_{\chi}\chi(n)\log p}{n^s}$$

$$\underset{\boxed{\text{Lemma 6.1b}}}{=} \sum_{\substack{n=p^k:\\ n\equiv 1 \bmod q}} \frac{\varphi(q)\log p}{n^s}.$$

This Dirichlet series has nonnegative coefficients and satisfies

$$\varphi(q)\cdot\sum_{\substack{m=p^k:\\ \gcd(m,q)=1}} \frac{\log p}{m^{\varphi(q)s}} \overset{\boxed{n=m^{\varphi(q)}\equiv 1 \bmod q}}{\leq} -\frac{f'(s)}{f(s)} \leq \varphi(q)\sum_{n=p^k}\frac{\log p}{n^s} = \varphi(q)\cdot\left(-\frac{\zeta'(s)}{\zeta(s)}\right)$$

for $s \in \mathbb{R}$.

$$\| $$

$$\varphi(q)\cdot\left(-\frac{\zeta'(\varphi(q)s)}{\zeta(\varphi(q)s)}\right) + O_q(1)$$

It therefore has abscissa of convergence $\frac{1}{\varphi(q)} \leq \sigma_c \leq 1$, so must have a pole at σ_c by Thm 3.2.2.

Since the coeff. are ≥ 0 it must be a pole of positive residue. (and therefore $\lim_{s \to \sigma_c^+} \left(-\frac{f'(s)}{f(s)}\right) = \infty$)

$\Rightarrow f(s) = \prod_{\chi} L(s,\chi)$ has a pole.

The only pole of any factor is a simple pole at $s=1$ for $\chi = \chi_0$.

$\Rightarrow f(s)$ has a simple pole at $s=1$, and is holomorphic everywhere else, and $L(1,\chi) \neq 0 \; \forall \chi$.

$\Rightarrow$ By e.g. Problem 4b on Pset 4 (or the same proof as in Thm 4.5), $f(s)$ has no zeros with $\mathrm{Re}(s) \geq 1$.

$\Rightarrow L(s,\chi) = 0$ for $\mathrm{Re}(s) \geq 1$. □

Cor 6.4 (PNT in arithmetic progressions)

Let [redacted] $a \in (\mathbb{Z}/q\mathbb{Z})^\times$. Then,

$$\#\{p \leq X \mid p \equiv a \bmod q\} \sim \frac{1}{\varphi(q)} \cdot \#\{p \leq X\} \text{ for } X \to \infty.$$

Pf Let $g(s) := \sum_{\chi} \left(-\frac{L'(s,\chi)}{L(s,\chi)}\right) \cdot \frac{1}{\chi(a)}$

$$= \sum_{n=p^k} \frac{\sum_{\chi} \chi\left(\frac{n}{a}\right) \log p}{n^s}$$

$$= \sum_{\substack{n=p^k: \\ n \equiv a \bmod q}} \frac{\varphi(q) \log p}{n^s}$$

It is hol. in $\{\operatorname{Re}(s) \geq 1\}$ except for a simple pole at $s=1$ with residue 1 (coming from $-\frac{L'(s,\chi_0)}{L(s,\chi_0)}$, which comes from the simple pole of $L(s,\chi_0)$ at $s=1$).

Wiener - Ikehara $\Rightarrow$ $\displaystyle\sum_{\substack{n=p^k \leq X: \\ n \equiv a \bmod q}} \varphi(q) \log p \sim X.$

$$\| $$

$$\varphi(q) \sum_{\substack{p \leq X: \\ p \equiv a \bmod q}} \log p + \mathcal{O}(X^{1/2}(\log X)^2)$$

Proceed as for the PNT (cf. Problem 3 on Set 1).

□

Cor 6.5

Let $S = \{x^2+y^2 \mid x,y\in\mathbb{Z}\}$.

We have $\#\{n\in S \mid n\leq x\} \sim C\cdot\frac{x}{\sqrt{\log x}}$

for some constant $C>0$.

Pf Algebraic NT tells us that $_{1\leq n} \in S$ if and only if n is divisible by each prime $p\equiv 3 \bmod 4$ an even number of times.

$$\Rightarrow D(1_S, s) = \prod_{p\not\equiv 3 \bmod 4} \underbrace{\frac{1}{1-\frac{1}{p^s}}}_{1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots} \cdot \prod_{p\equiv 3 \bmod 4} \underbrace{\frac{1}{1-\frac{1}{p^{2s}}}}_{1+\frac{0}{p^s}+\frac{1}{p^{2s}}+\dots}$$

Let χ_1 be the nontriv. character mod 4.

$$\chi_1(x) = \begin{cases} 1, & x\equiv 1 \bmod 4,\\ -1, & x\equiv 3 \bmod 4.\end{cases}$$

$$L(s,\chi_0)\cdot L(s,\chi_1) = \prod_{p\equiv 1 \bmod 4} \frac{1}{\left(1-\frac{1}{p^s}\right)^2} \cdot \prod_{p\equiv 3 \bmod 4} \frac{1}{\left(1-\frac{1}{p^s}\right)\left(1+\frac{1}{p^s}\right)}$$

$$= \prod_{p\equiv 1} \left(\frac{1}{\left(1-\frac{1}{p^s}\right)^2}\right) \cdot \prod_{p\equiv 3} \frac{1}{1-\frac{1}{p^{2s}}} .$$

$$\Rightarrow \frac{D(\mathbb{1}_S, s)^2}{L(s,\chi_0)L(s,\chi_1)} = \frac{1}{\left(1-\frac{1}{2^s}\right)^2} \cdot \prod_{p\equiv 1} 1 \cdot \prod_{p \equiv 3} \frac{1}{1-\frac{1}{p^{2s}}},$$

which converges for $\operatorname{Re}(s) > \frac{1}{2}$.

$\Rightarrow D(\mathbb{1}_S, s)^2$ is hol. in $\{\operatorname{Re}(s) \geq 1\}$ except for a simple pole at $s = 1$.

The result follows from Kato's extension of Wiener-Ikehara. $\square$

7. Functional equations

We'll generalise the fct. eq. for $\zeta(s)$ to fct. eq. for $L(s,\chi)$.

First, Poisson summation with a twist:

Lemma 7.1 Let $c : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be any function and let $f \in \mathcal{S}(\mathbb{R})$ (for example). Then,

$$q \cdot \sum_{x \in \mathbb{Z}} c(x \bmod q)\, f(x) = \sum_{t \in \mathbb{Z}} \hat{c}(t \bmod q)\, \hat{f}\left(\frac{t}{q}\right)$$

with $\hat{c} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ the discrete Fourier transform given by $\hat{c}(t) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x)\, e^{2\pi i x t/q}$.

Ex

$$c(x) = 1 \ \forall x \Rightarrow \hat{c}(t) = \begin{cases} 1, & t = 0 \bmod q, \\ 0, & \text{otherwise.} \end{cases}$$

$\rightarrow$ Claim = Poisson summation.

Pf By linearity, it suffices to consider $c = \mathbb{1}_{\{a \bmod q\}}$.

Then, $\text{LHS} = q \sum_{x \equiv a \bmod q} f(x) \underset{x = qy+a}{\overset{\uparrow}{=}} q \cdot \sum_{y \in \mathbb{Z}} g(y)$

with $g(y) = f(qy + a)$.

Poisson summation: $q \sum_{y} g(y) = q \sum_{t \in \mathbb{Z}} \hat{g}(t) = \sum_{t \in \mathbb{Z}} e^{2\pi i a t/q} \hat{f}\left(\frac{t}{q}\right)$

$= \text{RHS}$. □

Rmk $\hat{c}(x) = q\cdot c(-x)$.

Lemma 7.2 Let χ be a primitive character mod q, extended to $\mathbb{Z}/q\mathbb{Z}$ by 0 (outside $(\mathbb{Z}/q\mathbb{Z})^\times$). Its discrete Fourier transform $\hat{\chi}$ satisfies $\hat{\chi}(t) = \overline{\chi(t)}\cdot\hat{\chi}(1)$. for all $t\in\mathbb{Z}/q\mathbb{Z}$. (So the d.F.T. of χ is essentially its complex conjugate.)

Def We write $\tau(\chi) := \hat{\chi}(1) = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} \chi(x)\, e^{2\pi i x/q}$. This is called a Gauß sum.

Pf Case 1: $t\in(\mathbb{Z}/q\mathbb{Z})^\times$

$$\text{LHS} = \sum_{x \bmod q} \chi(x)\, e^{2\pi i x t/q} \underset{\substack{\uparrow\\ xt=y}}{=} \sum_{y \bmod q} \underbrace{\chi\left(\frac{y}{t}\right)}_{\frac{\chi(y)}{\chi(t)} = \overline{\chi(t)}\cdot\chi(y)} e^{2\pi i y/q}$$

$$= \overline{\chi(t)} \cdot \sum_{y \bmod q} \chi(y)\, e^{2\pi i y\cdot 1/q} = \text{RHS}.$$

Case 2: $t\notin(\mathbb{Z}/q\mathbb{Z})^\times$

Let $d = \gcd(t,q)$, $t' = \frac{t}{d}$, $q' = \frac{q}{d}$.

$$\text{LHS} = \sum_{x \bmod q} \chi(x)\, e^{2\pi i x t'/q'}$$

$$= \sum_{x' \bmod q'} \Bigg(\sum_{\substack{x \bmod q:\\ x\equiv x' \bmod q'}} \chi(x) \Bigg) e^{2\pi i x' t'/q'}$$

$= 0 =$ RHS according to the following Lemma. □

Lemma 7.3 Let χ be a ~~primitive~~ character mod q, let $q' \mid q$. Then,

$$\sum_{\substack{x \bmod q:\\ x \equiv x' \bmod q'}} \chi(x) = 0 \qquad \text{for all } x' \in \mathbb{Z}/q'\mathbb{Z}.$$

Pf This is clear if $x' \notin (\mathbb{Z}/q'\mathbb{Z})^\times$.

Otherwise, take any $x_0 \in (\mathbb{Z}/q\mathbb{Z})^\times$ with $x \equiv 1 \bmod q'$.

Mult. by x_0 permutes the summands.

The claim follows, unless $\chi(x_0) = 1$ for all x_0 as above.

But in that case, $\chi(x_1) = \chi(x_2)$ for any $x_1 \equiv x_2 \bmod q'$, which implies that χ is induced by a char. of q', hence not primitive. □

Cor 7.4 $|\tau(\chi)| = \sqrt{q}$ for any primitive character χ mod q.

Pf $\hat{\chi}(t) = \tau(\chi) \cdot \overline{\chi}(t) \quad \forall t$

$$\Rightarrow \underset{\substack{\shortparallel \\ q\cdot\chi(-x)}}{\hat{\hat{\chi}}(x)} = \tau(\chi)\cdot\hat{\overline{\chi}}(x) = \tau(\chi)\cdot\overline{\hat{\chi}}\,(-x)$$

$$= \underbrace{\tau(\chi)\cdot\overline{\tau(\chi)}}_{|\tau(\chi)|^2}\cdot\underbrace{\overline{\overline{\chi}}(-x)}_{\chi(-x)}.$$

□

Thm 7.5 Let χ be a primitive character mod q.

$$\text{Let } a = \begin{cases} 0, & \chi(-1)=1 \quad (\chi \ \underline{\text{even}}), \\ 1, & \chi(-1)=1 \quad (\chi \ \underline{\text{odd}}). \end{cases}$$

Let $\varepsilon(\chi) := \dfrac{\tau(\chi)}{i^a\sqrt{q}} = \dfrac{\tau(\chi)}{\sqrt{\chi(-1)\cdot q}}$.

Let $\xi(s,\chi) := \left(\dfrac{\pi}{q}\right)^{-(s+a)/2} \Gamma\left(\dfrac{s+a}{2}\right) L(s,\chi)$.

~~Then, $\xi(s,\chi) =$ [illegible] $\xi(1-s,\overline{\chi})$.~~

Then, $\xi(s,\chi) = \varepsilon(\chi)\cdot\xi(1-s,\overline{\chi})$.

~~[illegible]~~ Thm-Rmk 7.6

a) $|\varepsilon(\chi)| = 1$

b) $\varepsilon(\chi)\cdot\varepsilon(\overline{\chi}) = 1$.

c) If χ is real (= real-valued), then $\varepsilon(\chi) = 1$.

Pf a), b) easy

c) difficult (see for example Thm 9.15 in Montgomery-Vaughan)

Gauß worked on this for a year...

"Finally, two days ago, I succeeded - not on account of my hard efforts, but by the grace of the Lord. Like a sudden flash of lightning, the riddle was solved. I am unable to say what was the conducting thread that connected what I previously knew with what made my success possible."

Pf of Thm 7.5 for even χ. Let $q>1$.

Define $\Theta_\chi : \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ by $\Theta_\chi(u) = \sum_{n\in\mathbb{Z}} \chi(n) e^{-\pi u n^2}$.

Then: a) $\Theta_\chi(u) = \mathcal{O}(e^{-u})$ for large u.

b) $\Theta_\chi(u) = \frac{\tau(\chi)}{q} \cdot u^{-1/2}\, \Theta_{\overline{\chi}}\left(\frac{1}{q^2 u}\right)$

by Lemma 7.1 (twisted Poisson summation) applied to $f(x) = e^{-\pi u x^2}$ with $\hat{f}(y) = u^{-1/2} e^{-\pi u^{-1} y^2}$

c) $\Theta_\chi(u) = \mathcal{O}_q(e^{-u^{-1}})$ for small $u>0$.

by a), b).

As in the pf of Thm 4.3, $= \int_0^\infty \sum_{n\geq 1} \chi(n) e^{-\pi u n^2} (qu)^{s/2} \frac{du}{u}$

$$\frac{1}{2}\int_0^\infty \Theta_\chi(u)(qu)^{s/2} \frac{du}{u} = \xi(s,\chi) \text{ if } \operatorname{Re}(s)>1.$$

The LHS is holomorphic everywhere, so the eq. holds for all $s\in\mathbb{C}$.

Then, $\xi(s,\chi) = \frac{\tau(\chi)}{\sqrt{q}} \cdot \xi(1-s,\overline{\chi})$ follows from b). □

Pf of Thm 7.5 for odd χ.

Note: The previous argument wouldn't work because

$$\Theta_\chi(u) = \sum_{n\in\mathbb{Z}} \chi(n) e^{-\pi u n^2} = \sum_{n\geq 1} \underbrace{(\chi(n)+\chi(-n))}_{0} e^{-\pi u n^2} = 0.$$

Instead, let $\Theta_\chi(u) = \sum_{n\in\mathbb{Z}} \chi(n)\cdot n\, e^{-\pi u n^2}$.

Then: a), c) as before

b) $\Theta_\chi(u) = \dfrac{\tau(\chi)}{i q^2 u^{3/2}}\, \Theta_{\bar\chi}\left(\dfrac{1}{q^2 u}\right)$

by lemma 7.1 applied to

$$g(x) = x e^{-\pi u x^2} = -\frac{1}{2\pi u} f'(x) \quad (\text{for } f(x) = e^{-\pi u x^2})$$

with $\hat g(y) = -\dfrac{1}{2\pi u}\cdot 2\pi i y \cdot \underbrace{\hat f(y)}_{u^{-1/2} e^{-\pi u^{-1} y^2}}$.

As in the pf of Thm 4.3,

$$\frac{1}{2}\int_0^\infty \Theta_\chi(u)\,(qu)^{(s+1)/2}\,\frac{du}{u} = \xi(s,\chi) \quad \text{if } \operatorname{Re}(s)>1.$$

$\vdots$

$\square$

Cor 7.7 ~~$L(s,\chi)$ has no zeros with Re~~

For primitive characters χ mod q:

a) $L(s,\chi)$ has a simple zero at

$s = 0, -2, -4, \dots$ if χ is even, $q>1$

$s = -1, -3, -5, \dots$ if χ is odd.

(trivial zeros)

b) All other zeros lie in $\{s \in \mathbb{C} : 0 < \mathrm{Re}(s) < 1\}$.

c) ~~If $L(s,\chi)=0$, then L~~

If s is a nontrivial zero of $L(s,\chi)$, then

$1-s$ $\qquad$ $L(s,\overline{\chi})$,

$\overline{s}$ $\qquad$ $L(s,\overline{\chi})$,

$1-\overline{s}$ $\qquad$ $L(s,\chi)$.

Generalized Riemann Hypothesis

For prim. char. χ mod q, the nontriv. zeros of $L(s,\chi)$ satisfy $\mathrm{Re}(s)=\frac{1}{2}$.

Rmk By Thm-Rmk 7.6c), if χ is real, then $L(s,\chi)=L(1-s,\chi)$, which implies that $L(s,\chi)$ can only have a zero of even order at $s=\frac{1}{2}$.

Apparently, it is conjectured that $L(\frac{1}{2},\chi)>0$, though!

Note (Jonas) We have $L(1,\chi)>0$. If the GRH holds, then $L(\frac{1}{2},\chi)\geq 0$.

$$\boxed{L(s,\chi)=\prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}>0 \text{ for } s>1.}$$

8. Connection with Algebraic Number Theory

Def The Dedekind zeta function of a number field K is the Dirichlet series

$$\zeta_K(s) = \sum_{\substack{0\neq \mathfrak{a}\subseteq \mathcal{O}_K\\ \text{ideal}}} \frac{1}{Nm(\mathfrak{a})^s}$$

$$= \sum_{n\geq 1} \frac{\#\{0\neq\mathfrak{a}\subseteq\mathcal{O}_K : Nm(\mathfrak{a})=n\}}{n^s}$$

$$= \prod_{\substack{\mathfrak{p}\text{ prime}\\ \text{of } K}} \frac{1}{1-Nm(\mathfrak{p})^{-s}} .$$

Rmk $\zeta_K(s)$ has a merom. cont. to $\mathbb{C}$ which is hol. except for a simple pole at $s=1$ with residue $\frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{\omega_K \sqrt{|D_K|}}$, (class number formula)

where r_1 = nr. of real emb.
r_2 = nr. of complex emb.
R_K = regulator
h_K = class number
ω_K = nr. of roots of unity
D_K = discriminant.

It satisfies a functional equation. ~~and the~~

Extended Riemann Hypothesis

~~[illegible]~~ Every zero of $\zeta_K(s)$ with $0<\mathrm{Re}(s)<1$ satisfies $\mathrm{Re}(s)=\frac{1}{2}$.

Rmk $$\zeta_{\mathbb{Q}(\zeta_q)}(s) = \prod_{\substack{\chi \\ \text{char.} \\ \text{mod} q}} L(s,\chi) \cdot \prod_{\substack{\mathfrak{q}|q \\ \text{prime} \\ \text{of} K}} \frac{1}{1-Nm(\mathfrak{q})^{-s}} .$$

Rmk If $K \subseteq \mathbb{Q}(\zeta_q)$ is the subfield fixed by

$$H \subseteq (\mathbb{Z}/q\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_q)|\mathbb{Q}),$$
$$a \mapsto (\zeta_q \mapsto \zeta_q^a)$$

then $$\zeta_K(s) = \prod_{\substack{\chi \text{ char} \\ \text{mod} q \\ \text{s.t. } \chi(H)=1}} L(s,\chi) \cdot \prod_{\substack{\mathfrak{q}|q \\ \text{prime} \\ \text{of} K}} \frac{1}{1-Nm(\mathfrak{q})^{-s}} .$$

Rmk let K be a quadratic number field with discriminant D and $q = |D|$ and let χ be the char. mod q given by

$$\chi(p \bmod q) = \begin{cases} 1, & D \text{ quadr. res. mod } p \\ -1, & \text{otherwise} \end{cases}$$

for primes $p \nmid D$. (That this is well-def. uses quadratic reciprocity!)

Then, $$\zeta_K(s) = L(s,\chi_0)L(s,\chi) \cdot \prod_{\mathfrak{q}|q} \frac{1}{1-Nm(\mathfrak{q})^{-s}} .$$

Rmk For any finite Galois extension $L|K$ of number fields and any representation ρ of $\mathrm{Gal}(L|K)$ over $\mathbb{C}$, one can define an *Artin L-function*

$$L(L|K, \rho, s).$$

Ex $L(\mathbb{Q}(\zeta_q)|\mathbb{Q}, \chi, s) = L(s, \chi)$

where we identify a char. χ mod q with a one-dim. representation $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_q)|\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$.

Artin Conjecture

If the triv. representation is not a summand of ρ, then $L(L|K, \rho, s)$ has a hol. cont. to $\mathbb{C}$.

9. Zeros

9.1. Hadamard prod. expansion

Def The order of an entire function $f : \mathbb{C} \to \mathbb{C}$ is

$$\inf\{\alpha \geqslant 0 : f(s) \ll \exp(|s|^\alpha)\} \in [0, \infty].$$

Thm 9.1.1 (Hadamard product expansion)

Let $f \neq 0$ be an entire function of order 1 with $f(0) \neq 0$.

Then, there exist $A, B \in \mathbb{C}$ such that

$$f(s) = e^{A+Bs} \prod_{\substack{\rho \text{ root} \\ \text{of } f \\ \text{(with} \\ \text{mult.)}}} \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \qquad \text{for all } s \in \mathbb{C},$$

where the product is locally uniformly convergent.

Also, $\frac{f'}{f}(s) = B + \sum_{\rho \dots} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right)$,

where the sum is locally uniformly, absolutely convergent.

Warning $\sum_\rho \frac{1}{\rho}$ might not converge!

Cor 9.1.2

$$\Gamma(s)^{-1} = e^{A+Bs} \cdot s \cdot \prod_{n=1}^{\infty} \left(1+\frac{s}{n}\right) e^{-s/n}$$

$$-\frac{\Gamma'}{\Gamma}(s) = B + \frac{1}{s} + \sum_{n=1}^{\infty} \left(\frac{1}{s+n} - \frac{1}{n}\right)$$

Pf $s^{-1}\Gamma(s)^{-1}$ has order 1 by Stirling's formula (for $\Re(s) \geq \frac{1}{2}$) and because $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$.

Its zeros are $-1, -2, \ldots$ □

Cor 9.1.3 If $\Re(s) > 0$, then

$$\frac{\Gamma'}{\Gamma}(s) \ll \log|s| \quad \text{for large } |s|.$$

Pf $$-\frac{\Gamma'}{\Gamma}(s) = \mathcal{O}(1) + \sum_{n=1}^{\infty} \frac{-1}{n\left(1+\frac{n}{s}\right)}$$

Split up the sum:

for $n \leq 2|s|$: $\Re\left(1+\frac{n}{s}\right) > 1$, so $\sum(\ldots) \ll \sum \frac{1}{n} \ll \log|s|$

for $n \geq 2|s|$: $\left|1+\frac{n}{s}\right| \geq \frac{1}{2}\left|\frac{n}{s}\right|$, so $\sum(\ldots) \ll \sum \frac{|s|}{n^2} \ll \frac{|s|}{|s|} = 1$ □

9.2. Riemann zeta function

Reminder: $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ is hol. except for simple poles at $s = 0, 1$ and satisfies $\xi(s) = \xi(1-s)$. Its zeros are the nontrivial zeros of $\zeta(s)$.

Thm 9.2.1 The (entire) function $f(s) := s(s-1)\xi(s)$ has order 1.

~~Pf By the functional equation $f(s) = f(1-s)$, it suffices to consider $s \in \mathbb{C}$ with $\mathrm{Re}(s) \geq \frac{1}{2}$~~

Pf This follows from the functional equation $f(s) = f(1-s)$, Stirling's approximation for $\Gamma(s/2)$, and the following lemma. □

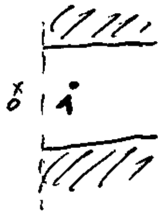
(By the fct. eq., we only need to consider $s \in \mathbb{C}$ with $\mathrm{Re}(s) \geq \frac{1}{2}$)

Lemma 9.2.2 a) $\zeta(s) \geq 1$ for $s > 1$.

For any $\varepsilon > 0$:

b) $\zeta(s) \ll_{\varepsilon} 1$ if $\mathrm{Re}(s) > 1 + \varepsilon$

c) $\zeta(s) \ll |\mathrm{Im}(s)|$ if $\mathrm{Re}(s) \geq \frac{1}{2}$, $|\mathrm{Im}(s)| \geq 1$.



Pf a) clear } from $\zeta(s) = \sum \frac{1}{n^s}$
b) clear }

c) Use Euler-Maclaurin: W.l.o.g. $\mathrm{Re}(s) < 2$. As in the pf. of Thm 3.2

$$\zeta(s) - 1 = \sum_{n=2}^{\infty} \frac{1}{n^s} = \frac{1}{s-1} - \frac{1}{2} + \underbrace{\int_1^{\infty} \underbrace{B_1(t)}_{\ll 1} \cdot \underbrace{\frac{s}{t^{s+1}}}_{\ll \frac{|s|}{t^{\mathrm{Re}(s)+1}}} \, dt}_{\ll |\mathrm{Im}(s)|} .$$

□

Cor 9.2.3

We can write

$$s(s-1)\xi(s) = e^{A+Bs} \cdot \prod_{\substack{\rho \text{ nontriv.} \\ \text{zero of } \xi(s)}} \left(1-\frac{s}{\rho}\right) e^{s/\rho},$$

$$\frac{1}{s} + \frac{1}{s-1} + \frac{\xi'}{\xi}(s) = B + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Rmk We have $\lim_{s\to 1} s(s-1)\xi(s) = \lim_{s\to 1} (s-1)\xi(s) = 1$, so $A=0$.

$\uparrow$

$\boxed{\Gamma(1/2)=\sqrt{\pi}}$

Thm 9.2.4 The number $N(T)$ of nontriv. zeros of $\zeta(s)$

with $0 \leq \mathrm{Im}(s) \leq 2\pi T$ is

$T \log T - T + O(\log T)$ for large T.

Rmk Informally, the nr. of nontriv. zeros

with $2\pi T \leq \mathrm{Im}(s) \leq 2\pi(T+1)$ is

$\approx \frac{d}{dT}(T \log T - T) = \log T$.

~~We first show:~~

~~Lemma 9.2.5~~

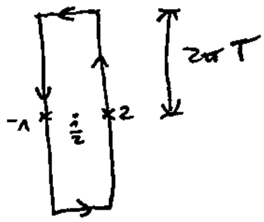
Rmk The Thm implies that this nr. is $\ll \log T$.

Pf of Thm 9.2.4

Let $\mathcal{C}$ be the ccw boundary of

$$[-1,2]\times[-2\pi T, 2\pi T].$$

W.l.o.g. no zeros on $\mathcal{C}$.

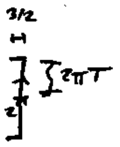


$N(T)+O(1)$

$= \frac{1}{2}$(nr. of zeros minus nr. of poles of $\xi(s)$ in the rectangle, with mult.)

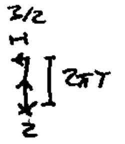
$$= \frac{1}{2}\cdot\frac{1}{2\pi i}\oint_{\mathcal{C}} \frac{\xi'}{\xi}(s)\,ds$$

$$= \frac{1}{2\pi i}\oint_{\mathcal{D}} \frac{\xi'}{\xi}(s)\,ds$$ for $\mathcal{D}$ the right half of $\mathcal{C}$



$$\boxed{\frac{\xi'}{\xi}(1-s) = -\frac{\xi'}{\xi}(s)}$$

$$= \frac{1}{\pi}\operatorname{Im}\oint_{\mathcal{E}} \frac{\xi'}{\xi}(s)\,ds$$ for $\mathcal{E}$ the top half of $\mathcal{D}$



$$\boxed{\frac{\xi'}{\xi}(\bar{s}) = \overline{\frac{\xi'}{\xi}(s)}}$$

Split up $\mathcal{E}$ into the vertical part $\mathcal{E}_1$ and the horizontal part $\mathcal{E}_2$.

Let's first deal with $\mathcal{E}_1$.

Let $f(s)=\pi^{-s}\Gamma(s)$ so that $\xi(s)=f(s)\zeta(s)$.

$$\rightarrow \frac{\xi'}{\xi}(s)=\frac{1}{2}\frac{f'}{f}\left(\frac{s}{2}\right)+\frac{\zeta'}{\zeta}(s).$$

~~[illegible] f has no zeros~~

~~By Stirling's Formula,~~

$$\oint_{\mathcal{E}_1}\frac{1}{2}\frac{f'}{f}\left(\frac{s}{2}\right)ds=\oint_{\mathcal{E}_1/2}\frac{f'}{f}(s)\,ds=\oint_{\mathcal{E}_1/2}d\overbrace{\log f(s)}^{\text{well-def. in }\{\mathrm{Re}(s)>0\}.}$$

$$=\log f\left(\frac{2+2\pi iT}{2}\right)-\log f\left(\frac{2}{2}\right)$$

$$\underset{\substack{\uparrow\\ \text{Stirling}}}{=}-(\cancel{1}+\pi iT)\log\pi+(\cancel{1}+\pi iT)\underbrace{\log(\cancel{1}+\pi iT)}_{\log(\pi T)+\frac{\pi}{2}i}-(\cancel{1}+\pi iT)+\mathcal{O}(\log T)$$

$$=\pi iT\log T-\pi iT-\frac{\pi^2}{2}\cdot T+\mathcal{O}(\log T)$$

has imaginary part $\pi T\log T-\pi T$. This gives the main term.

If $\mathrm{Re}(s) \geq 2$, then $\zeta(s) = 1 + \sum_{n\geq 2} \frac{1}{n^s}$ has

$$\mathrm{Re}(\zeta(s)) \geq 1 - \sum_{n \geq 2} \frac{1}{n^{\mathrm{Re}(s)}} \geq 1 - (\underbrace{\zeta(2)}_{\frac{\pi^2}{6}} - 1) > 0.$$

$\Rightarrow$ $\log \zeta(s)$ is well-def. in $\{\mathrm{Re}(s) \geq 2\}$ with

$|\mathrm{Im} \log \zeta(s)| \leq \frac{\pi}{2}$.

$$\rightarrow \int_{E_1} \frac{\zeta'}{\zeta}(s)\,ds = O(1).$$

Now, deal with E_2.

Problem: E_2 can be arbitrarily close to a nontriv. zero, so $\frac{\zeta'}{\zeta}(s)$ can be arbitrarily large.

But the following lemma implies that

$$\mathrm{Im}\left(\int_{E_2} \frac{\zeta'}{\zeta}(s)\,ds\right) = \sum_{\substack{\rho:\\ |\mathrm{Im}(\rho - s)| \leq 1}} \underbrace{\mathrm{Im}\left(\int_{E_2} \frac{1}{s-\rho}\,ds\right)}_{\ll 1} + O(\log T)$$

$$\ll \log T.$$

□

Lemma 9.2.5

We have $$\frac{\zeta'}{\zeta}(s) = \sum_{\substack{\rho : \\ |\mathrm{Im}(\rho - s)| \le 1}} \frac{1}{s-\rho} + \mathcal{O}(\log \mathrm{Im}(s))$$ for $\frac{1}{2} \le \mathrm{Re}(s) \le 2$ and large $\mathrm{Im}(s)$.

with only $\mathcal{O}(\log T)$ summands

Pf In this region,

$$\frac{\zeta'}{\zeta}(s) = \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) + \mathcal{O}(1) \text{ by Cor 9.2.3.} \qquad (\mathrm{I})$$

$$\| $$

$$\underbrace{\frac{1}{2} \frac{f'}{f}\left(\frac{s}{2}\right)}_{\substack{-\log \pi + \frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) \\ \ll \log |s| \\ \text{by Cor 9.1.3}}} + \underbrace{\frac{\zeta'}{\zeta}(s)}_{\substack{= \sum_{n \ge 1} \frac{\Lambda(n)}{n^s} \ll 1 \\ \text{if } \mathrm{Re}(s) \ge 2}}$$

(with $f(s) = \pi^{-s} \Gamma(s)$ as before)

$\Rightarrow$ For large $t > 0$, (taking $s = 2 + it$)

$$\sum_{\rho} \left(\frac{1}{2+it-\rho} + \frac{1}{\rho} \right) \ll \log t$$

$$\Rightarrow \sum_{\rho} \Bigg(\underbrace{\mathrm{Re}\left(\frac{1}{2+it-\rho} \right)}_{\substack{= \frac{\mathrm{Re}(2-\rho)}{|2+it-\rho|^2} \\ \ge \frac{1}{4 + |t - \mathrm{Im}(\rho)|^2}}} + \underbrace{\mathrm{Re}\left(\frac{1}{\rho} \right)}_{\ge 0} \Bigg) \ll \log t$$

because $0 \le \mathrm{Re}(\rho) \le 1$.

$$\Rightarrow \#\{\rho : |t-\operatorname{Im}\rho|\le 1\} \ll \log t$$

and

$$\sum_{\substack{\rho:\\ |t-\operatorname{Im}\rho|\ge 1}} \frac{1}{|t-\operatorname{Im}\rho|^2} \ll \log t.$$

~~Plug this back into $(I)_\rho$ with $t=\operatorname{Im}(s)$:~~

~~$-\frac{\zeta'}{\zeta}(2+it)+\frac{\zeta'}{\zeta}(s)=\sum_{\rho}\left(\frac{1}{s-\rho}-\frac{1}{2+it-\rho}\right)+O(1)$~~

~~$=\underbrace{\sum_{\substack{\rho:\\ |t-\operatorname{Im}\rho|\le 1}}\left(\underbrace{\frac{1}{s-\rho}}_{\ll 1}-\underbrace{\frac{1}{2+it-\rho}}_{\ll 1}\right)}_{\ll \log t}+\sum_{\substack{\rho:\\ |t-\operatorname{Im}\rho|>1}}\underbrace{(\cdots)}_{\frac{2+it-s}{(s-\rho)(2+it-\rho)}}+O(1)$~~

Let $t = \operatorname{Im}(s)$ and apply (I) to s and $2+it$:

$$\frac{\xi'}{\xi}(s) = \underbrace{\frac{\xi'}{\xi}(2+it)}_{\substack{\ll \log t \\ \text{as before}}} + \sum_{\rho}\left(\frac{1}{s-\rho} - \frac{1}{2+it-\rho}\right) + O(1)$$

$$\sum_{\substack{\rho: \\ |t-\operatorname{Im}(\rho)|\leq 1}} \left(\frac{1}{s-\rho} - \underbrace{\frac{1}{2+it-\rho}}_{\substack{\ll 1 \\ \text{because} \\ \operatorname{Re}(\rho)\leq 1}}\right) = \sum_{\substack{\rho: \\ |\cdot|\leq 1}} \frac{1}{s-\rho} + O(\log t)$$

$\uparrow$

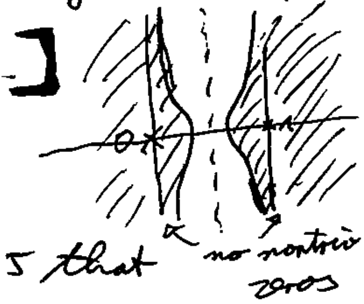
$\boxed{\substack{\ll \log t \\ \text{summands}}}$

$$\sum_{\substack{\rho: \\ |\dots|>1}} \left(\frac{1}{s-\rho} - \frac{1}{2+it-\rho}\right) = \sum_{\substack{\rho: \\ |\dots|>1}} \underbrace{\frac{2+it-s}{(s-\rho)(2+it-\rho)}}_{\ll \frac{1}{|t-\operatorname{Im}(\rho)|^2}} \ll \log t.$$

□

Thm 9.2.6 There is a constant $c>0$ such that $\zeta(s)$ has no (nontrivial) zero $\rho \in \mathbb{C}$ with $\mathrm{Re}(\rho) > 1 - \frac{c}{\log(|\mathrm{Im}(\rho)|+2)}$.

[For large $\mathrm{Im}(\rho)$, we could just write $\log|\mathrm{Im}(\rho)|$, but for small $\mathrm{Im}(\rho)$, that would be negative for $\mathrm{Im}(\rho) \doteq 1$, it would be 0, etc...]



Pf We saw in the pf of Thm 4.5 that for any $\sigma > 1$ and $t \in \mathbb{R}$,

$$\mathrm{Re}\left(-3\cdot\frac{\zeta'}{\zeta}(\sigma) - 4\cdot\frac{\zeta'}{\zeta}(\sigma+it) - \frac{\zeta'}{\zeta}(\sigma+2it)\right) \geq 0. \qquad (I)$$

By Cor 9.2.3 and Cor 9.1.3, for $1 < \mathrm{Re}(s) < 2$,

$$\underbrace{\frac{1}{s}}_{\ll 1} + \frac{1}{s-1} + \underbrace{\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)}_{\ll \log(|\mathrm{Im}(s)|+2)} + \frac{\zeta'}{\zeta}(s) = B + \sum_\rho \left(\underbrace{\frac{1}{s-\rho}}_{\mathrm{Re}(-)>0} + \underbrace{\frac{1}{\rho}}_{\mathrm{Re}(-)>0}\right)$$

Let $t = \mathrm{Im}(\rho)$ and let $L = \log(|t|+2)$.

$\Rightarrow$ For $\sigma > 1$, if $|t| \geq 1$ (so $\frac{1}{\sigma+it-1} \ll 1$), then

$$\mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma)\right) \leq \frac{1}{\sigma-1} + O(L),$$

$$\mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma+it)\right) \leq -\frac{1}{\sigma-\mathrm{Re}(\rho)} + O(L),$$

$$\mathrm{Re}\left(-\frac{\zeta'}{\zeta}(\sigma+2it)\right) \leq O(L).$$

$$\underset{(I)}{\Longrightarrow} \quad \frac{3}{\sigma-1} - \frac{4}{\sigma-\Re(\rho)} + O(L) \geqslant 0$$

Take $\sigma = 1 + \frac{\varepsilon}{L}$ for some small $\varepsilon < L$.

$$\Rightarrow \quad \frac{3}{\varepsilon}L - \frac{4L}{(1-\Re(\rho))L+\varepsilon} + O(L) \geq 0$$

$$\Rightarrow \quad (1-\Re(\rho))L+\varepsilon \geqslant \frac{4}{\frac{3}{\varepsilon}+O(1)}$$

$$\Rightarrow \quad (1-\Re(\rho))L \geqslant \varepsilon \cdot \left(\frac{4}{3+O(\varepsilon)} - 1 \right)$$

For suff. small $\varepsilon > 0$, the RHS is $\geqslant$ some constant $c > 0$.

$$\Rightarrow \quad \Re(\rho) \geqslant 1 - \frac{c}{L}.$$

□

9.3. Dirichlet L-series

Lemma 9.3.1

For primitive characters χ mod $q>1$, we have

$$-\frac{\xi'}{\xi}(s,\chi) = B_\chi + \sum_{\substack{\rho \text{ nontriv} \\ \text{zero of } L(s,\chi)}} \left(\frac{1}{s-\rho}+\frac{1}{\rho}\right).$$

Pf as for $\xi(s)$. □

Lemma 9.3.2 We have $\mathrm{Re}\left(B_\chi + \sum_\rho \frac{1}{\rho}\right)=0$.

Pf HW. □

Lemma 9.3.3 If χ is the char. mod q induced by the char. χ' mod q' (with $q'|q$), then

$$\frac{L'}{L}(s,\chi) = \frac{L'}{L}(s,\chi') + O(\log q) \text{ if } \operatorname{Re}(s) > 1.$$

Pf ~~This follows from~~

$$L(s,\chi) = L(s,\chi') \cdot \prod_{\substack{p|q: \\ p\nmid q'}} \left(1 - \frac{\chi'(p)}{p^s}\right)$$

$$\Rightarrow \frac{L'}{L}(s,\chi) = \frac{L'}{L}(s,\chi') - \underbrace{\sum_{p|q} \underbrace{\sum_{k\geq 1} \frac{\chi'(p^k)\log p}{p^{ks}}}_{\ll \log p}}_{\ll \log q}.$$

□

Thm 9.3.4

There is a constant $c>0$ such that for any character χ mod any q, $L(s,\chi)$ has no (nontriv.) zero $\rho\in\mathbb{C}$ with $\operatorname{Re}(\rho) > 1-\frac{c}{\log(q(|\operatorname{Im}(\rho)|+2))}$,

except possibly one real zero $\rho\in\mathbb{R}$ if χ is real.

Pf W.l.o.g. χ is primitive.

We've already proved the result for $q=1$, so assume $q>1$. ($\Rightarrow \chi\neq\chi_0$)

First attempts: Use the same strategy as before, replacing $\zeta(s)$ by $\prod_\chi L(s,\chi)$. This only proves the above statement with the constant c depending on q. m

~~Let $t=\operatorname{Im}(\rho)$ and $L=\log(q(|t|+2))$.~~

Now, $3+4\cos\theta+\cos 2\theta\geq 0$ implies:

For any $\sigma>1$ and $t\in\mathbb{R}$.

$$\operatorname{Re}\Bigg(-3\cdot \underbrace{\frac{L'}{L}(\sigma,\chi_0)}_{-\sum\limits_{\gcd(n,q)=1}\frac{\Lambda(n)}{n^\sigma}} - 4\cdot \underbrace{\frac{L'}{L}(\sigma+it,\chi)}_{-\sum\limits_{\dots}\frac{\Lambda(n)\chi(n)}{n^{\sigma+it}}} - \underbrace{\frac{L'}{L}(\sigma+2it,\chi^2)}_{-\sum\limits_{\dots}\frac{\Lambda(n)\chi(n)^2}{n^{\sigma+2it}}}\Bigg) \geq 0$$

Let $t = \Im(\rho)$ and $L = \log(q(|t|+2))$. Fix some $\delta > 0$.

For $\sigma > 1$, if $|t| \geq \frac{\delta}{\log q}$ or $\underset{(\chi \text{ nonreal})}{\chi^2 \neq \chi_0}$, then:

$$\Re\left(-\frac{L'}{L}(\sigma,\chi_0)\right) \leq \frac{1}{\sigma-1} + O(L)$$

$$\Re\left(-\frac{L'}{L}(\sigma+it,\chi)\right) \leq -\frac{1}{\sigma - \Re(\rho)} + O(L)$$

$$\Re\left(-\frac{L'}{L}(\sigma+2it,\chi^2)\right) \leq O(L) \qquad \text{if } \chi^2 \neq \chi_0$$

$$\text{—}''\text{—} \qquad \leq \Re\left(\frac{1}{\sigma+2it-1}\right) + O(L) \leq O(L) \qquad \text{if } \underset{(\chi \text{ real})}{\chi^2 = \chi_0}$$

As before, it then follows that

$$\Re(\rho) \geq 1 - \frac{c}{L}. \qquad (c \text{ depends on } \delta.)$$

We now deal with the case $\chi^2 = \chi_0$ and $|\Im(\rho)| < \frac{\delta}{\log q}$

Clearly, $\Re\Big(\underbrace{-\frac{L'}{L}(\sigma,\chi_0)}_{\sum_{\dots} \frac{\Lambda(n)}{n^\sigma}} \underbrace{-\frac{L'}{L}(\sigma,\chi)}_{\sum_{\dots} \frac{\Lambda(n)\chi(n)}{n^\sigma}}\Big) \geq 0$ for any $\sigma > 1$.

We have

$$\mathrm{Re}\left(-\frac{L'}{L}(\sigma,\chi_0)\right) \le \frac{1}{\sigma-1} + O(\log q)$$

$$\mathrm{Re}\left(-\frac{L'}{L}(\sigma,\chi)\right) \le -\sum_{\rho} \mathrm{Re}\left(\frac{1}{\sigma-\rho}\right) + O(\log q)$$

$$\Rightarrow \quad \frac{1}{\sigma-1} - \sum_{\rho} \mathrm{Re}\left(\frac{1}{\sigma-\rho}\right) + O(\log q) \ge 0.$$

Take $\sigma = 1 + \frac{2\delta}{\log q}$

Then, for any ρ with $|\mathrm{Im}(\rho)| < \frac{\delta}{\log q} = \frac{\sigma-1}{2}$

$$\mathrm{Re}\left(\frac{1}{\sigma-\rho}\right) = \frac{\sigma-\mathrm{Re}(\rho)}{|\sigma-\rho|^2} \ge \frac{\sigma-\mathrm{Re}(\rho)}{(\sigma-\mathrm{Re}(\rho))^2 + \left(\frac{\sigma-1}{2}\right)^2}$$

$$\ge \frac{4}{5(\sigma-\mathrm{Re}(\rho))}.$$

$$\Rightarrow \quad \sum_{\substack{\rho: \\ |\mathrm{Im}(\rho)| < \frac{\delta}{\log q}}} \frac{4}{5(\sigma-\mathrm{Re}(\rho))} \le \frac{\log q}{2\delta} + O(\log q)$$

If there are two ρ with $|\mathrm{Im}(\rho)| < \frac{\delta}{\log q}$

and $\mathrm{Re}(\rho) > 1 - \frac{c}{\log q}$, then

$$2 \cdot \frac{4}{5\left(\frac{2\delta+c}{\log q}\right)} \le \frac{\log q}{2\delta} + O(\log q).$$

For suff. small δ, c, this is impossible because $\frac{2\cdot 4}{5\cdot 2} > \frac{1}{2}$.

Hence, $L(s,\chi)$ has at most one bad zero ρ.

Since χ is real, this implies that ρ is real. $\square$

10. Perron's formula

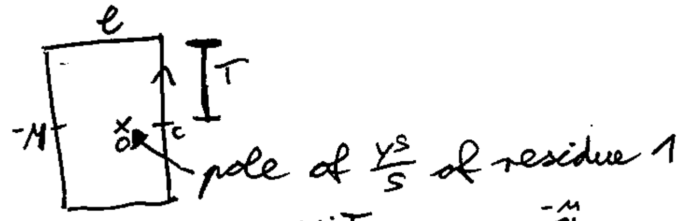
Lemma 10.1 For $y \geq 0$, $c > 0$, we have

$$\lim_{T\to\infty} \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds = \begin{cases} 0, & 0 \leq y < 1, \\ \frac{1}{2}, & y = 1, \\ 1, & y > 1. \end{cases}$$

Pf For $y=1$, $LHS = \lim\limits_{T\to\infty} \frac{1}{2\pi i}\int \frac{ds}{s} = \lim\limits_{T\to\infty} \frac{1}{2\pi i} \underbrace{\left[\log s\right]_{s=c-iT}^{c+iT}}_{\substack{\Re(-)=0 \\ \Im(-)\to\pi}} = \frac{1}{2}.$

For $y > 1$, the integrand $\frac{e^{s\log y}}{s}$ goes to 0 as $\Re(s) \to -\infty$.

$\rightsquigarrow$ Consider the boundary $\mathcal{C}$ of the rectangle $[-M, c] + [-T, T]\cdot i$ in $\mathbb{C}$ for large $M>0$



$$1 \underset{\substack{\uparrow \\ \text{Residue} \\ \text{Theorem}}}{=} \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{y^s}{s}\,ds = \int_{c-iT}^{c+iT} \frac{y^s}{s}\,ds + \underbrace{\int_{c+iT}^{-M+iT} \cdots}_{\substack{O\left(\frac{e^{\Re(s)\log y}}{T}\right) \\ O\left(\frac{y^c}{T\log y}\right) \xrightarrow[T\to\infty]{} 0}} + \underbrace{\int_{-M+iT}^{-M-iT} \underbrace{\cdots}_{O\left(\frac{e^{-M\log y}}{M}\right)}}_{\substack{\xrightarrow{M\to\infty} 0 \\ \text{for fixed } T}} + \underbrace{\int^{\cdots} \cdots}_{\substack{O\left(\frac{y^c}{T\log y}\right) \\ \downarrow T\to\infty \\ 0}}$$

For $y<1$, use the rectangle $[c,M]+[-T,T]\cdot i$ for large M. □

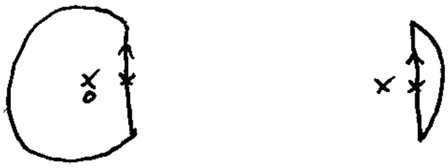
More precisely:

<u>Thm 10.2</u> We have

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\frac{y^s}{s}\,ds - \begin{cases}0 & \cdots\\ \frac{1}{2} & \cdots\\ 1 & \cdots\end{cases}\right| \ll \min\Big(y^c,\ \underbrace{\frac{y^c}{T|\log y|}}_{(\infty \text{ for } y=1)}\Big).$$

<u>Pf</u> The second bound $\left(\cdots \ll \frac{y^c}{T|\log y|}\right)$ follows from the previous proof. The case $y=1$ is HW.

For the first bound $(\cdots \ll y^c)$, use the boundary of $\{s\in\mathbb{C} : |s|\le|c+iT|,\ \Re(s)\le c\}$ if $y\geq 1$ and of $\{s\in\mathbb{C} : |s|\le|c+iT|,\ \Re(s)\ge c\}$ if $0\le y\le 1$.



$y\geq 1$ $\qquad$ $0\le y\le 1$

On the arc, $\frac{y^s}{s} \ll \frac{y^c}{|c+iT|}$ (of length $O(c+iT)$) □

Cor 10.3 Let $c > 0$.

Consider a Dirichlet series $D(a,s) = \sum a_n n^{-s}$ with abscissa of absolute convergence $\sigma_a < c$.

Then,

$$\sum_{n \le x} a_n = \lim_{T \to \infty} \frac{1}{2\pi i} \int_{c-iT}^{c+iT} D(a,s) \frac{x^s}{s} \, ds$$

for any $x > 0$ with $x \notin \mathbb{Z}$.
(otherwise, only count a_x half)

Pf Since $D(a,s)\frac{x^s}{s} \overset{\shortparallel}{} \sum_n a_n \cdot \frac{(x/n)^s}{s}$ is uniformly convergent on the contour,

$$\frac{1}{2\pi i} \int D(a,s) \frac{x^s}{s} \, ds = \sum_n a_n \cdot \frac{1}{2\pi i} \int \frac{(x/n)^s}{s} \, ds$$

$$= \sum_{n \le x} a_n + \mathcal{O}\Big(\underbrace{\sum_n |a_n| \left(\frac{x}{n}\right)^c}_{<\infty} \cdot \frac{1}{T \underbrace{\left|\log \frac{x}{n}\right|}_{\gg 1 \text{ for fixed } x \notin \mathbb{Z}}} \Big)$$

□

We can again bound the error term. For example:

<u>Lemma 10.4</u> If $x - \frac{1}{2} \in \mathbb{Z}$, then

$$\left| \sum_{n \geq 1} \Lambda(n) - \frac{1}{2\pi i} \int_{c-iT}^{c+iT} -\frac{\zeta'}{\zeta}(s) \cdot \frac{x^s}{s} \, ds \right| \ll \frac{x (\log x)^2}{T}$$

for $c = 1 + \frac{1}{\log x}$.

$\uparrow$ (optimal choice!)

<u>Pf</u> Fix $\varepsilon > 0$ suff. small. We bound the error term from the pf of Cor 10.3:

$$\sum_{\substack{n \geq 1 \\ |\log \frac{x}{n}| \geq \varepsilon}} \Lambda(n) \left(\frac{x}{n}\right)^c \cdot \underbrace{\frac{1}{T |\log \frac{x}{n}|}}_{\ll \frac{1}{T}}$$

$$= -\frac{\zeta'}{\zeta}(c) \cdot \frac{x^c}{T} \underset{\substack{\uparrow \\ \text{only a simple} \\ \text{pole at } s=1}}{\ll} \frac{1}{c-1} \cdot \frac{x^c}{T} = \frac{x (\log x) e}{T}$$

$$\sum_{\substack{n \geq 1 \\ |\log \frac{x}{n}| \leq \varepsilon}} \underbrace{\Lambda(n)}_{\leq \log n} \underbrace{\left(\frac{x}{n}\right)^c}_{\ll 1} \cdot \frac{1}{\underbrace{T |\log \frac{x}{n}|}}$$

$$\left|\log \frac{1}{1-(1-\frac{n}{x})}\right| = \left|\sum_{k \geq 1} \frac{1}{k} \left(1 - \frac{n}{x}\right)^k\right| \underset{\substack{\uparrow \\ \varepsilon \text{ suff.} \\ \text{small}}}{\gg} \left|1 - \frac{n}{x}\right|$$

$$\ll \sum_{x e^{-\varepsilon} \leq n \leq x e^{\varepsilon}} (\log x) \cdot \frac{x}{T \underbrace{|n-x|}_{\in \frac{1}{2} \cdot \mathbb{Z}}} \ll \frac{x (\log x)^2}{T}$$

$\square$

Thm 10.5 (PNT with error term)

There is a constant $C>0$ s.t.

$$\sum_{n\leq x} \Lambda(n) = x + \mathcal{O}\left(x e^{-C\sqrt{\log x}}\right) \text{ for large } x.$$

$$\left(= \sum_{p\leq x} \log p + \mathcal{O}\left(x^{1/2}(\log x)^2\right)\right)$$

Rmk For any $k, \varepsilon > 0$,

$$(\log x)^k \ll e^{C\sqrt{\log x}} \ll x^{\varepsilon} \text{ for large } x.$$

~~Set $c = 1 + \frac{1}{\log x}$~~

~~Use the boundary~~ [illegible]

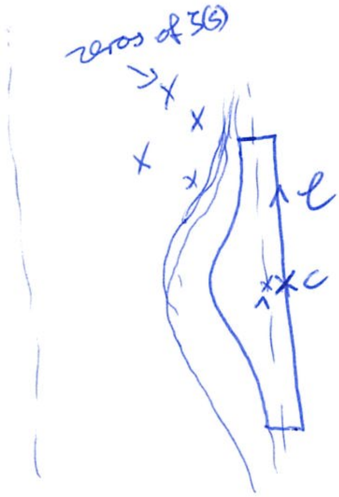
Pf Let $c = 1 + \frac{1}{\log x}$. Let D be the constant from Thm .2.6 so

$\zeta(s)$ has no zero ρ with

$$\Re(\rho) > 1 - \frac{D}{\log(|\Im \rho| + 2)}.$$

Let ℓ be the boundary of

$$\left\{ s \in \mathbb{C} : |\Im s| \le T, \quad 1 - \frac{D}{2\log(|\Im s| + 2)} \le \Re(s) \le c \right\}.$$



By Lemma 10.4,

$$\sum_{n \le x} \Lambda(n) = \frac{1}{2\pi i} \int_{\substack{\text{right}\\\text{edge}}} \underbrace{-\frac{\zeta'}{\zeta}(s) \frac{x^s}{s}}_{\substack{\text{pole of order 1}\\\text{and residue } x\\\text{at } s=1}} ds + O\left(\boxed{\frac{x(\log x)^2}{T}}\right).$$

$\frac{1}{2\pi i} \int_{\ell} \cdots = x$ by the residue theorem.

By Lemma 9.2.5, on ℓ, we have $\frac{\zeta'}{\zeta}(s) \ll (\log T)^2$.

$$\Rightarrow \int_{top} \cdots \ll \int_{top} (\log T)^2 \cdot \frac{x}{T}\, ds \ll \boxed{\frac{x(\log T)^2}{T}}.$$

$$\int_{left} \cdots \ll \int_{left} (\log T)^2 \cdot \frac{x^{Re(s)}}{|s|} |ds|$$

$$\ll \int (\log T)^2 \cdot \frac{x^{1-\frac{D}{2\log T}}}{|Im(s)|+1} |ds|$$

$$\ll x^{1-\frac{D}{2\log T}} \cdot \Big(1 + \underbrace{\int_1^T \frac{1}{y}\, dy}_{\log T}\Big)(\log T)^2$$

$$\ll \boxed{\frac{x(\log T)^3}{x^{D/2\log T}}}.$$

To optimize the error term, solve

$$T = x^{D/2\log T} \quad \text{for } T:$$

$$\Updownarrow$$

$$\log T = \frac{D\log x}{2\log T} \Leftrightarrow \log T = \sqrt{\frac{D\log x}{2}}.$$

$$\rightsquigarrow$$

$$\text{error term } \frac{x(\log T)^3}{e^{\sqrt{\frac{D}{2}\log x}}}.$$

$$\Uparrow$$

$$x e^{-E\sqrt{\log x}} \text{ for any } E < \sqrt{\tfrac{D}{2}}.$$

□

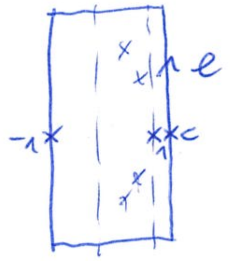
Rmk ~~Using~~ Assuming the RH, we can ~~get~~ a better error bound! (E.g. use a larger region...)

Thm 10.6 ✓ Let x, T be large. Then, have

$$\sum_{\substack{n\le x \\ \text{and } x-\frac{1}{2}\in\mathbb{Z}}} \Lambda(n) = x - \sum_{\rho:|\mathrm{Im}\rho|<T} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) + O\left(\frac{x(\log T)^2}{T} + \frac{(\log T)^2}{x}\right).$$

~~For some $T' = T + O(1)$.~~

Pf Use the boundary ℓ of $[-1, c] + [-T, T]\cdot i$.



$$\frac{1}{2\pi i} \int_\ell \underbrace{-\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}}\,ds = x - \sum_{\substack{\rho: \\ |\mathrm{Im}\rho|<T}} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0)$$

pole of order 1 and residue x at $s=1$

pole of order 1. and residue $-\frac{x^\rho}{\rho}$ at $s=\rho$

pole of order 1 and residue $-\frac{\zeta'}{\zeta}(0)$ at $s=0$

$$\int_{\text{left}} \cdots \ll \frac{(\log T)^2}{x}$$

$-\frac{\zeta'}{\zeta}(s) \ll \log|s|$ for large $|s|$ with $\mathrm{Re}(s) = -1$

$\int_{\text{top}} \cdots$ is problematic because there might be a root very close to the contour.

But we know that there are $\ll \{\log T\}$ roots

with $|\mathrm{Im}\rho - T| < 1$ according to Lemma 9.2.5.

$\Rightarrow$ For some constant $\delta > 0$ (indep. of T),

there is some $T' = T + O(1)$ s.t. there are no

roots with $|\mathrm{Im}\rho - T'| < \frac{\delta}{\log T}$.

Replace T by T' in the above computation. This changes $\sum_\rho \frac{x^\rho}{\rho}$ by $\ll (\log T)\cdot \frac{x}{T}$.

By the pf of Lemma 9.2.5,

$$\frac{\zeta'}{\zeta}(s) \ll (\log T)^2 \text{ on the top contour.}$$

$$\Rightarrow \int_{\text{top}} \cdots \ll \frac{x(\log T)^2}{T}.$$

□

Cor 10.7 Assume the Riemann Hypothesis. Then,

$$\sum_{n\le x} \Lambda(n) = x + O(x^{1/2}(\log x)^2).$$

Pf Take $T = x$.

$$\sum_{\substack{\rho:\\ |\mathrm{Im}\rho|<T}} \frac{x^\rho}{\rho} \underset{\substack{\uparrow \\ \mathrm{Re}(\rho)=\frac{1}{2}}}{\ll} x^{1/2}\cdot \sum \frac{1}{\rho} \underset{\substack{\uparrow \\ \#\{\rho:\,|\mathrm{Im}\rho|<T\} \ll T\log T \\ \text{by Thm 9.2.4} \\ \text{and use Abel summation}}}{\ll} x^{1/2}(\log x)^2.$$

□

We can actually do even better:

Thm 10.8 Let $x - \frac{1}{2} \in \mathbb{Z}$ be large.

Then, $$\sum_{n \le x} \Lambda(n) = x - \sum_{\substack{\rho \text{ nontriv.} \\ \text{zero of } \zeta}} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right).$$

Idea of pf

Use a contour $[-U, c] + [-T, T] \cdot i$.

First, let $U \to \infty$, then $T \to \infty$.

$$\frac{1}{2\pi i} \int_{\mathcal{C}} -\frac{\zeta'}{\zeta}(s) \frac{x^s}{s} ds \longrightarrow x - \sum_{\substack{\rho \\ \text{zero} \\ \text{of } \zeta}} \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0)$$

$$= x - \sum_{\substack{\rho \text{ nontriv.} \\ \text{zero of } \zeta}} \frac{x^\rho}{\rho} - \underbrace{\sum_{k=1}^{\infty} \frac{x^{-2k}}{-2k}}_{-\frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)} - \log(2\pi) \qquad \square$$

Similarly:

Thm 10.9 There exists $c>0$ such that for all a,q with $\gcd(a,q)=1$ and all $x > e^{c(\log q)^2}$, we have

$$\sum_{\substack{n\leq x:\\ n\equiv a \bmod q}} \Lambda(n) = \frac{x}{\varphi(q)} + \mathcal{O}\left(x\, e^{-c\sqrt{\log x}} \right)$$ if no char. χ mod q has a Siegel zero.

and

$$\sum_{\dots} \Lambda(n) = \frac{x}{\varphi(q)} - \frac{\chi(a)\, x^{\beta}}{\beta\varphi(q)} + \mathcal{O}\left(\dots \right)$$ if some char. χ mod q has a Siegel zero at β.

~~If the GRH holds, then the~~

Rmk There can be at most one char. mod q with a Siegel zero! (HW)

Thm 10.10 Assuming the Generalized Riemann Hypothesis, for all a,q with $\gcd(a,q)=1$ and all $x\geq q$, we have

$$\sum_{\dots} \Lambda(n) = \frac{x}{\varphi(q)} + \mathcal{O}\left(x^{1/2} (\log x)^2 \right).$$

11. Sieves

11.1. Basic sieve

Def An integer n is squarefree if it is not divisible by p^2 for any prime p.

Thm 11.1.1 We have

$$\#\{1 \le n \le x \text{ squarefree}\} = \frac{1}{\zeta(2)} \cdot x + \mathcal{O}(x^{1/2}).$$

Rmk $\#\{\dots\} \sim \frac{1}{\zeta(2)} \cdot x$ for $x \to \infty$ follows from $\mu * 1_{\text{square}} = 1_{\text{squarefree}}$ and Wiener-Ikehara.

for large x.

Pf Recall: $\mu * 1 = \delta$, so $\sum_{d \mid m} \mu(d) = \begin{cases} 1, & m = 1, \\ 0, & m \ge 2. \end{cases}$ (I)

$$\Rightarrow \sum_{\substack{d \ge 1: \\ d^2 \mid n}} \mu(d) = \begin{cases} 1, & n \text{ squarefree}, \\ 0, & \text{otherwise} \end{cases}$$

Take the largest m s.t. $m^2 \mid n$. $\Rightarrow (d^2 \mid n \Leftrightarrow d \mid m)$

$\Rightarrow \#\{x \le n \text{ squarefree}\}$

$$= \sum_{1 \le n \le x} \sum_{\substack{d \ge 1: \\ d^2 \mid n}} \mu(d) = \sum_{1 \le d \le x^{1/2}} \mu(d) \sum_{\substack{1 \le n \le x: \\ d^2 \mid n}} 1$$

$$= \sum_{1 \le d \le x^{1/2}} \mu(d) \cdot \left\lfloor \frac{x}{d^2} \right\rfloor$$

$$= \sum_{1 \le d \le x^{1/2}} \underbrace{\frac{\mu(d)}{d^2}}_{\ll \frac{1}{d^2}} \cdot x + \mathcal{O}(x^{1/2})$$

$$= \sum_{d \ge 1} \frac{\mu(d)}{d^2} \cdot x + \mathcal{O}(x^{1/2})$$

$$= \frac{1}{\zeta(2)} \cdot x + \mathcal{O}(x^{1/2}).$$

□

Rmk Another way to look at it:

$\mathbb{P}(p^2 \nmid n : n \in \mathbb{Z} \text{ random}) = 1 - \frac{1}{p^2}$

By the Chinese Remainder Thm, these events $(p^2 \nmid n)$ are independent for finitely many distinct primes $p_1, \dots, p_k$.

If they were indep. for all p, we'd conclude that $\mathbb{P}(n \text{ squarefree}) = \prod_p \mathbb{P}(p^2 \nmid n) = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$,

so $\#\{1 \le n \le x \text{ squarefree}\} \sim \frac{1}{\zeta(2)} \cdot x$.

Rmk More generally, it is conjectured that for any polynomial $f(x) \in \mathbb{Z}[X]$, we have

$$\#\{1 \le n \le x : f(n) \text{ squarefree}\} \sim \prod_p \frac{\#\{a \in \mathbb{Z}/p^2\mathbb{Z} : p^2 \nmid f(a)\}}{p^2} \cdot x.$$

This is only known in some special cases, e.g. $\deg(f) \le 3$, (case deg = 2 easy, deg = 3 due to Hooley) or assuming the ABC conjecture.

In general, we only know $\limsup_{x \to \infty} \frac{LHS}{RHS} \le 1$.

("sieves are better at upper bounds")

Thm 11.1.2 For $K \geq 1$ and any $x \geq 1$, we have

$$\#\{1 \leq n \leq x \text{ not divisible by any } p \leq x\}$$

$$= \prod_{p|K} \left(1 - \frac{1}{p}\right) \cdot x + O(2^{\nu(K)}),$$

where $\nu(K)$ = nr. of primes dividing K.

Pf

$$\#\{\ldots\} = \sum_{d|K} \mu(d) \cdot \#\{1 \leq n \leq x : d|n\}$$

$$= \sum_{d|K} \mu(d) \left(\frac{x}{d} + O(1)\right)$$

$$= \underbrace{\sum_{d|K} \frac{\mu(d)}{d}}_{\prod_{p|K}(1-\frac{1}{p})} \cdot x + O(\underbrace{\#\{d|K \text{ sqfree}\}}_{2^{\nu(K)}})$$

□

11.2. Selberg sieve

Thm 11.2.1 Let $x, z \geq 1$. Then,

$$\pi(x,z) := \#\{1 \leq n \leq x \text{ not divisible by any } p \leq z\}$$

$$\leq \frac{x}{V(z)} + \mathcal{O}(z^2)$$

$$\text{with } V(z) := \sum_{d \leq z} \frac{\mu(d)^2}{\underset{\substack{\uparrow \\ \text{Euler's} \\ \text{totient} \\ \text{function}}}{\phi(d)}} = \sum_{\substack{d \leq z \\ \text{sqfree}}} \frac{1}{\phi(d)}.$$

Rmk

$$\sum_{\substack{d \geq 1 \\ \text{sqfree,} \\ \text{only div.} \\ \text{by primes} \\ p \leq z}} \frac{1}{\phi(d)} \underset{\substack{\uparrow \\ \boxed{\phi \text{ mult.}}}}{=} \prod_{p \leq z} \left(1 + \frac{1}{\phi(p)}\right) = \prod_{p \leq z} \left(1 + \frac{1}{p-1}\right) = \prod_{p \leq z} \frac{1}{1 - \frac{1}{p}}$$

$$= \frac{1}{\prod_{p \leq z} \mathbb{P}(p \nmid n : n \in \mathbb{Z} \text{ random})}$$

Pf Let $\lambda_1, \lambda_2, \dots$ be real numbers with $\lambda_1 = 1$ and $\lambda_n = 0$ for $n > z$.

Let $P_z := \prod_{p \le z} p$.

Note: n not div. by any $p \le z \iff \gcd(n, P_z) = 1$.

$$\Rightarrow \pi(x,z) \le \sum_{1 \le n \le x} \Big(\underbrace{\sum_{d \mid \gcd(n, P_z)} \underbrace{\lambda_d}_{=0 \text{ if } d>z}}_{\substack{=1 \text{ if } \gcd = 1 \\ \ge 0 \text{ always}}} \Big)^2 \qquad (\mathrm{I})$$

$$= \sum_{\substack{d_1, d_2 \le z \\ (\Rightarrow d_1, d_2 \mid P_z)}} \lambda_{d_1} \lambda_{d_2} \, \# \{ 1 \le n \le x : d_1, d_2 \mid n \}$$

$$= \sum_{d_1, d_2 \le z} \lambda_{d_1} \lambda_{d_2} \left(\frac{x}{\operatorname{lcm}(d_1, d_2)} + \mathcal{O}(1) \right) \qquad (\mathrm{II})$$

Note: (I) is an equality if we choose $\lambda_d = \mu(d)$.

We will now choose the numbers $\lambda_2, \dots, \lambda_z$ so that the quadratic form

$$Q(\lambda) := \sum_{d_1, d_2 \le z} \frac{\lambda_{d_1} \lambda_{d_2}}{\operatorname{lcm}(d_1, d_2)}$$ becomes as small as possible.

$$Q(\lambda) = \sum \frac{\lambda_{d_1}}{d_1} \cdot \frac{\lambda_{d_2}}{d_2} \cdot \gcd(d_1, d_2)$$

$$= \sum_{e \le z} \phi(e) \cdot \Big(\underbrace{\sum_{\substack{d \le z : \\ e \mid d}} \frac{\lambda_d}{d}}_{=: \nu_e} \Big)^2 = \sum_{e \le z} \phi(e) \nu_e^2$$

$$\boxed{\begin{matrix} \phi * 1 = \mathrm{id}, \text{ so} \\ \sum_{e \mid t} \phi(e) = t \end{matrix}}$$

(diagonalization of Q)

~~We have~~ For any $d \geq 1$, we have

$$\sum_{k\geq 1} \mu(k)\nu_{dk} = \sum_{k\geq 1}\mu(k)\sum_{dk|f} \frac{\lambda_f}{f} = \sum_{d|f} \frac{\lambda_f}{f} \underbrace{\sum_{k|\frac{f}{d}} \mu(k)}_{\substack{1 \text{ if } \frac{f}{d}=1 \\ 0 \text{ otherwise}}}$$

$$= \frac{\lambda_d}{d}.$$

Hence, $\lambda_1 = 1 \Leftrightarrow \sum_{k\geq 1} \mu(k)\nu_k = 1$

and $\lambda_n = 0 \ \forall n>z \Leftrightarrow \nu_n = 0 \ \forall n > z$.

$\Rightarrow$ We shall minimize $\sum_{e\leq z} \phi(e)\nu_e^2$

subject to the condition $g(\nu) = \sum_{1\leq k\leq z} \mu(k)\nu_k = 1$.

Lagrange multipliers tell us to look at the points $(\nu_k)_k$ where $\sum \mu(k)\nu_k = 1$ and for some $\tau \in \mathbb{R}$, we have $\underset{2\phi(e)\nu_e}{\underset{\shortparallel}{\frac{\partial Q}{\partial \nu_e}}} = \tau \cdot \underset{\mu(e)}{\underset{\shortparallel}{\frac{\partial g}{\partial \nu_e}}}$ for all $1 \leq e \leq z$.

$$\rightsquigarrow \nu_e = \frac{\tau\mu(e)}{2\phi(e)} \quad \rightsquigarrow 1 = \sum \mu(e)\nu_e = \sum \frac{\tau\mu(e)^2}{2\phi(e)} = \frac{\tau}{2}\cdot V(z)$$

$$\Rightarrow \frac{\tau}{2} = \frac{1}{V(z)}, \text{ so } \nu_e = \boxed{\frac{1}{V(z)}\cdot\frac{\mu(e)}{\phi(e)}}, \text{ so}$$

$$Q = \sum_e \phi(e)\nu_e^2 = \frac{1}{V(z)^2}\cdot\sum_e \frac{\mu(e)^2}{\phi(e)} = \frac{1}{V(z)}.$$

(Indeed, for this choice of ν_e, we have $\lambda_1 = 1$ etc.)

~~Also, $\frac{\lambda_d}{d} = \sum_{k\geq 1} \mu(k)\nu_{dk} = \sum_{k\geq 1} \mu(k)\cdot\frac{1}{V(z)}\cdot\frac{\mu(dk)}{\phi(dk)}$~~

~~$\Rightarrow \pi(x,z) \leq \frac{x}{V(z)} + O\Big(\sum_{d_1 d_2 \leq z} |\lambda_{d_1}\lambda_{d_2}|\Big)$~~

Also, $\left|\frac{\lambda_d}{d}\right| = \left|\sum_{k\geq 1} \mu(k)\nu_{dk}\right| = \left|\sum_{\substack{1\leq k\leq z:\\ dk\leq z}} \mu(k)\cdot\frac{1}{V(z)}\cdot\frac{\mu(dk)}{\phi(dk)}\right|$

$$\leq \sum_{\substack{1\leq k\leq z\\ \text{sqfree}:\\ \gcd(d,k)=1\\ dk\leq z}} \frac{1}{V(z)}\cdot\frac{1}{\phi(d)\phi(k)},$$

so $|\lambda_d|\cdot V(z) \leq \Big(\sum_{\substack{1\leq k\leq z\\ \text{sqfree}:\\ dk\leq z\\ \gcd(d,k)=1}} \frac{1}{\phi(k)}\Big)\cdot \underbrace{\frac{d}{\phi(d)}}_{\sum_{e|d}\frac{\mu(e)^2}{\phi(e)}} = \sum_{1\leq k\leq z} \frac{\mu(k)^2}{\phi(k)} = V(z).$

$\Rightarrow |\lambda_d| \leq 1.$

Plugging into $(\#)$:

$\pi(x,z) \leq \frac{x}{V(z)} + O(z^2).$ $\square$

Thm 11.2.2 (Selberg sieve) Let $x, z \geq 1$.

Let $a_1, a_2, \ldots$ be a sequence of integers. Let $b_1, b_2, \ldots > 0$ be multiplicative and

Assume that $\#\{n \leq x : d \mid a_n\} = \frac{x}{b_d} + R_d$ for all $d \geq 1$.

Then,

$$\#\{n \leq x : a_n \text{ not divisible by any } p \leq z\} \leq \frac{x}{U(z)} + O\Big(\sum_{d_1, d_2 \leq z} |R_{\operatorname{lcm}(d_1, d_2)}| \Big),$$

where $U(z) = \sum_{\substack{d \leq z \\ \text{sqfree}}} \frac{1}{c_d}$

with $b = c * 1$

$(\Leftrightarrow b_n = \sum_{d \mid n} c_d \Leftrightarrow c = b * \mu \Leftrightarrow c_n = \sum_{d \mid n} b_d \, \mu(\frac{n}{d}))$.

Pf like the pf of Thm 11.2.1. □

Cor 11.2.3 The number of twin primes $p, p+2 \le x$ is

$$\ll \frac{x}{(\log x)^2}.$$

Pf (sketch) ~~Take $a_n = n(n+2)$.~~

$$\#\{p, p+2 \text{ prime} : z < p < x\}$$

$$\le \#\{n \le \tfrac{x}{2} + 10 : (2n+1)(2n+3) \text{ not div. by any prime } q \le z\}$$

Take $a_n = (2n+1)(2n+3)$

$$\#\{n \le x : d \mid a_n\}$$

$$= \sum_{\substack{d_1, d_2 \ge 1: \\ d = d_1 d_2, \\ \gcd(d_1, d_2) = 1}} \#\{n \le x : \underbrace{d_1 \mid 2n+1,\ d_2 \mid 2n+3}_{\Leftrightarrow\, n \equiv \ldots \bmod d_1 d_2}\}$$

$$= \begin{cases} \sum_{\ldots} \frac{x}{d_1 d_2} + O(1) = \frac{2^{\nu(d)}}{d} \cdot x + O(2^{\nu(d)}), & d \text{ odd}, \\ 0, & d \text{ even}. \end{cases}$$

$$\rightsquigarrow b_d = \begin{cases} \frac{d}{2^{\nu(d)}}, & d \text{ odd} \\ \text{"}\infty\text{"}, & d \text{ even} \end{cases}$$ ~~(multiplicative)~~

$$R_d = O(2^{\nu(d)})$$

$$c_d = \sum_{e \mid d} \frac{e}{2^{\nu(e)}} \cdot \mu\left(\frac{d}{e}\right)$$

$$U(z) = \sum_{\substack{d\le z\\ \text{sqfree}\\ \text{odd}}} \frac{1}{c_d} \ge \sum_{\substack{d\le z\\ \text{sqfree}\\ \text{odd}}} \frac{d}{2^{\nu(d)}}$$

Let $H(z) = \sum_{\substack{d\le z\\ \text{sqfree}\\ \text{odd}}} 2^{\nu(d)}$. We have $H(z) \asymp z\log z$ by Wiener–Ikehara.

By Abel summation,

$$\sum_{\substack{d\le z\\ \text{sqfree}\\ \text{odd}}} \frac{d}{2^{\nu(d)}} - \underbrace{\int_{1/2}^{z} \underbrace{\frac{H(t)}{t^2}}_{\substack{\asymp\\ \frac{\log t}{t}}} dt}_{\substack{\asymp\\ (\log z)^2}} = \underbrace{\left[\frac{H(t)}{t}\right]_{t=1/2}^{z}}_{\substack{\asymp\\ \log z}},$$

so $U(z) \gg (\log z)^2$.

Also,
$$\sum_{d_1,d_2\le z} 2^{\nu(\mathrm{lcm}(d_1,d_2))} \le \sum_{d_1,d_2\le z} 2^{\nu(d_1)}\cdot 2^{\nu(d_2)} = \Big(\sum_{d\le z} 2^{\nu(d)}\Big) = \underset{\substack{\asymp\\ (z\log z)^2}}{H(z)^2}.$$

Summary:

$$\#\{\text{twin primes} \le x\} \ll z + \frac{x}{(\log z)^2} + z^2(\log z)^2$$

For $z = x^{1/4}$, the RHS is $\asymp \frac{x}{(\log x)^2}$. □

Basic heuristic

- The set of primes behaves like a random subset of $\mathbb{Z}_{\geq 2}$ which contains n with prob. $\frac{1}{\log n}$.

$\rightsquigarrow$ (expected nr. of twin primes $\leq x$)

$$\approx \sum_{n \leq x} \frac{1}{(\log(n))(\log(n+2))} \sim \frac{x}{(\log x)^2}.$$

(This heuristic also suggests that there are ∞ many pairs of primes $p, p+1, \ldots$)

Refined heuristic

Fix $z \geq 1$, and let $K_z = \prod_{p \leq z} p$.

The set of primes behaves like a random subset of $\mathbb{Z}_{\geq 2}$ which contains n with prob.

$$\begin{cases} 0, & \gcd(n, K_z) > 1, \\ \dfrac{K_z}{\phi(K_z) \log n}, & \gcd(n, K_z) = 1. \end{cases}$$

$$\frac{K_z}{\phi(K_z) \log n} = \Big(\prod_{p \leq z} \underbrace{\frac{p}{p-1}}_{\frac{1}{1-\frac{1}{p}}}\Big) \cdot \frac{1}{\log n}$$

("The larger z, the better the heuristic.")

$\rightsquigarrow$ (expected nr. of twin primes $\leq x$)

$$\approx \sum_{\substack{n \leq x; \\ \gcd(n, K_z) = 1 \\ \gcd(n+2, K_z) = 1}} \Big(\Big(\prod_{p \leq z} \Big\{\frac{1}{1-\frac{1}{p}}\Big\}\Big) \cdot \frac{1}{\log n}\Big)^2 \approx \frac{\#\{\text{good res. cl. mod } K_z\}}{K_z} \cdot x \cdot \Big(\prod_{p \leq z} \frac{1}{1-\frac{1}{p}} \cdot \frac{1}{\log x}\Big)^2$$

$$= \frac{1}{2} \cdot \prod_{2<p\le z} \left(1 - \frac{2}{p}\right) \cdot 4 \cdot \prod_{2<p\le z} \frac{1}{\left(1-\frac{1}{p}\right)^2} \cdot \frac{x}{(\log x)^2}$$

$$= 2 \cdot \underbrace{\prod_{2<p\le z} \left(1 - \frac{1}{(p-1)^2}\right)}_{\substack{\Big\downarrow z\to\infty \\ C}} \cdot \frac{x}{(\log x)^2}$$

$\rightsquigarrow$ heuristic: $\#(\text{twin primes} \le x) \sim 2C \cdot \frac{x}{(\log x)^2}$,

(Hardy–Littlewood)

References: Murty, Montgomery-Vaughan,

Terence Tao's blog: {254A notes 4: some sieve theory},

Friedlander-Iwaniec: Opera de Cribro

Reminder

Let $n \in \mathbb{Z}$ be a prod. of primes $< z$.

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & n=1 \\ 0, & n \neq 1 \end{cases} \qquad (I)$$

This is an exact sieve for primes $< z$.

If for all $n \in \mathbb{Z}$ prod. of pr. $< z$ $\lambda_1, \lambda_2, \ldots \in \mathbb{R}$ satisfy

$$\sum_{d \mid n} \lambda_d \geq \begin{cases} 1, & n=1, \\ 0, & n \neq 1, \end{cases}$$

we get an upper bound sieve. The numbers $(\lambda_n)_n$ are called upper bound sieve coefficients.

If $\ldots \leq \ldots$, we get a lower bound sieve and the numbers $(\lambda_n)_n$ are called lower bound sieve coefficients.

Rmk (I) follows by expanding the product

$$\prod_{p<z} (1 - a_p) = \begin{cases} 1, & n=1, \\ 0, & n \neq 1, \end{cases}$$

where $a_p = \begin{cases} 1, & p \mid n, \\ 0, & p \nmid n. \end{cases}$

You can "partially expand" a product $\prod_{i=1}^{n}(1+b_i)$

as follows:

<u>Lemma 1.1.3.1</u> Let $b_1, \ldots, b_n \in \mathbb{R}$.

Let $\mathcal{S}$ be a set of subsets of $\{1, \ldots, n\}$ s.t.:

a) $\emptyset \in \mathcal{S}$

b) If $\emptyset \neq A \in \mathcal{S}$, then $A \setminus \{\min(A)\} \in \mathcal{S}$.

Then,

$$\prod_{i=1}^{n}(1+b_i) = \sum_{A \in \mathcal{S}} \prod_{i \in A} b_i + \sum_{\substack{A \subseteq \{1,\ldots,n\} \\ A \notin \mathcal{S} \\ A \setminus \{\min(A)\} \in \mathcal{S}}} \left(\prod_{i \in A} b_i\right) \cdot \prod_{i=1}^{\min(A)-1}(1+b_i).$$

<u>Pf</u> Use induction over n, considering the sets

$$\mathcal{T} := \{B \subseteq \{1, \ldots, n-1\} : B \in \mathcal{S}\},$$

$$\mathcal{U} := \{B \subseteq \{1, \ldots, n-1\} : B \cup \{n\} \in \mathcal{S}\}.$$

...

$\square$

Pf 2 (Jonas) $\quad LHS = \prod_{i=1}^{n} (1+b_i) = \sum_{C \subseteq \{1,\dots,n\}} \prod_{i\in C} b_i.$

$$RHS = \sum_{A\in \mathcal{S}} \prod_{i\in A} b_i + \sum_{\substack{A\subseteq\{1,\dots,n\}\\ A\notin \mathcal{S}\\ A\setminus\{\min(A)\}\in\mathcal{S}}} \left(\prod_{i\in A} b_i\right)\cdot \prod_{i=1}^{\min(A)-1} (1+b_i)$$

$$= \sum_{A\in\mathcal{S}} \prod_{i\in A} b_i + \sum_{A:\dots} \sum_{B\subseteq\{1,\dots,\min(A)-1\}} \prod_{i\in A\cup B} b_i \qquad (I)$$

Consider any subset $C = \{j_1,\dots,j_m\}$ of $\{1,\dots,n\}$, with $j_1 < \dots < j_m$.

By a) and b), there is some $0 \le l \le m$ such that

$\{j_k,\dots,j_m\} \in \mathcal{S}$ if $k > l$,

$\{j_k,\dots,j_m\} \notin \mathcal{S}$ if $k \le l$.

If $l = 0$, then $C \in \mathcal{S}$.

If $l > 0$, then C can be written uniquely as $C = A\cup B$ with $A\notin\mathcal{S}$, $A\setminus\{\min(A)\}\in\mathcal{S}$, $B\subseteq\{1,\dots,\min(A)-1\}$, namely $A = \{j_l,\dots,j_m\}$, $B = \{j_1,\dots,j_{l-1}\}$.

$\Rightarrow$ For every $C\subseteq\{1,\dots,n\}$, the product $\prod_{i\in C} b_i$ appears exactly once on the RHS(I). $\square$

We now translate this to number theory.

<u>Def</u> For $n>1$, denote by $\mathrm{lpf}(n)$ the least prime factor of n.

Let $z \geq 1$. (We'll only consider primes $p<z$ in our sieve.)

Let $\mathcal{D} \subseteq \mathcal{D}_0 := \left\{ d \geq 1 \text{ sqfree, only divisible by primes } < z \right\}$.

such that

a) $1 \in \mathcal{D}$

b) If $1 < d \in \mathcal{D}$, then $\frac{d}{\mathrm{lpf}(d)} \in \mathcal{D}$.

<u>Cor 11.3.2</u> Let $a_1, a_2, \ldots$ be multiplicative.

Then,

$$\prod_{p<z} (1+a_p) = \sum_{d \in \mathcal{D}} a_d + \sum_{\substack{d \in \mathcal{D}_0 \\ d \notin \mathcal{D} \\ \frac{d}{\mathrm{lpf}(d)} \in \mathcal{D}}} a_d \cdot \prod_{p < \mathrm{lpf}(d)} (1+a_p).$$

<u>Pf</u> Let $p_1 < \ldots < p_n$ be the prime numbers $<z$.

Let $\mathcal{S} = \{ A \subseteq \{1, \ldots, n\} \mid \prod_{i \in A} p_i \in \mathcal{D} \}$.

Apply lemma 11.3.1 to the numbers $a_{p_1}, \ldots, a_{p_n}$ and use that $a_{\prod_{i \in A} p_i} = \prod_{i \in A} a_{p_i}$. □

Cor 11.3.3 For any $b \in \mathbb{Z}$,

$$\sum_{\substack{d \in \mathcal{D}: \\ d \mid b}} \mu(d) + \sum_{\substack{d \in \mathcal{D}_0 \\ d \notin \mathcal{D} \\ \frac{d}{\mathrm{lpf}(d)} \in \mathcal{D} \\ d \mid b \\ p \nmid b \ \forall p < \mathrm{lpf}(d) \text{ prime}}} \mu(d) = \begin{cases} 1, & p \nmid b \ \forall p < z, \\ 0, & p \mid b \text{ for some } p < z. \end{cases}$$

Pf Take $a_d = \begin{cases} \mu(d), & d \mid b, \\ 0, & d \nmid b. \end{cases}$

This is multiplicative, with $a_p = \begin{cases} -1, & p \mid b, \\ 0, & p \nmid b. \end{cases}$

$$\prod_{p<z} (1+a_p) = \begin{cases} 1, & p \nmid b \ \forall p < z, \\ 0, & p \mid b \text{ for some } p < z. \end{cases}$$

$\square$

Rmk Hence;

a) If $d \notin \mathcal{D}$, $\frac{d}{\mathrm{lpf}(d)} \in \mathcal{D}$ implies $\mu(d) = -1$, we obtain an upper bound sieve:

For any numbers $a_1, \ldots, a_x \in \mathbb{Z}$,

$$\#\{n : a_n \text{ not div. by any } p < z\} \leq \sum_{d \in \mathcal{D}} \mu(d) \cdot \#\{n : d \mid a_n\}.$$

b) If $---$ implies $\mu(d) = +1$, we obtain a lower bound sieve:

$$\#\{ --- \} \geq \sum \cdots$$

Ex $\mathcal{D} = \mathcal{D}_0 \rightsquigarrow$ basic sieve (inclusion-exclusion)

Ex Let $r \geq 0$.

$\mathcal{D} := \{ d \in \mathcal{D}_0 : \underset{\substack{\uparrow \\ \text{nr. of} \\ \text{primes} \\ \text{dividing } d}}{\nu(d)} \leq r \} \rightsquigarrow$ Brun sieve

(inclusion-exclusion truncated after $r+1$ steps)

$\# = \#\{1 | a_n\} - \sum_p \#\{p | a_n\} + \sum_{p \neq q} \#\{pq | a_n\} \mp \dots$

(upper bound if r is even, lower bound if r is odd)

Ex Let $\beta \geq 1$, $D \geq 1$.

$$\mathcal{D}^+_{\beta,D} := \left\{ p_1 \cdots p_r \;\middle|\; \begin{array}{l} p_1 < \dots < p_r \leq z \text{ prime}, \\ \cancel{p_1^{\beta+1} p_2 \cdots p_r \leq D \text{ if } r \text{ is odd}} \\ \cancel{p_2^{\beta+1} p_3 \cdots p_r \leq D \text{ if } r \text{ is even}} \\ p_k^{\beta+1} p_{k+1} \cdots p_r \leq D \quad \forall\, 1 \leq k \leq r \text{ with } r-k \text{ even} \end{array} \right\}$$

(upper bound)

$$D^-_{\beta,D} := \left\{ p_1 \cdots p_r \;\middle|\; \begin{array}{l} p_1 < \dots < p_r \leq z \text{ prime}, \\ \cancel{p_1^{\beta+1} p_2 \cdots p_r \leq D \text{ if } r \text{ is even},} \\ \cancel{p_2^{\beta+1} p_3 \cdots p_r \leq D \text{ if } r \text{ is odd}} \\ p_k^{\beta+1} p_{k+1} \cdots p_r \leq D \quad \forall\, 1 \leq k \leq r \text{ with } r-k \text{ odd} \end{array} \right\}$$

(lower bound)

$\rightsquigarrow$ beta sieve / Rosser-Iwaniec sieve

Note: $d \in \mathcal{D}^{\pm}_{\beta,D} \Rightarrow d \leq D$

~~Note: $d = p_1 \cdots p_r \in \mathcal{D}^{\pm}_{\beta,D}$ with $p_1 < \dots < p_r \leq z$ prime~~ ~~$\left(\frac{\beta-1}{\beta}\right)^{r-1}$~~

~~Implies~~ [illegible] $d \leq D$ ~~$\leq D$~~

$\beta\left(\frac{\beta-1}{\beta}\right)^{r-1}$

with $p = \beta^{\frac{\beta-1}{\beta}}$

We'll now analyse the main term in the beta sieve.

Def Let $\kappa > 0$. A multiplicative sequence $a_1, a_2, \dots$ of real numbers with $0 \le a_p < 1$ is of sieve dimension $\le \kappa$ if $V(w) := \prod_{p<w} (1-a_p)$

satisfies

$$\frac{V(z)}{V(w)} \gg \left(\frac{\log z}{\log w}\right)^{-\kappa} \quad \underset{\text{all}}{\text{for}}\ 2 \le w \le z.$$

Main example:

Lemma 1.3.4 If $0 \le a_p < 1$, $a_p \le \frac{\kappa}{p}$ for all suff. large p, then $a_1, a_2, \dots$ is of sieve dimension $\le \kappa$.

Pf Assume $a_p \le \frac{\kappa}{p}$ for $p \ge T$.

$$\begin{aligned}
\frac{V(z)}{V(w)} &= \prod_{w \le p < z} (1-a_p) \\
&\gg \prod_{\substack{w \le p < z: \\ T \le p, \\ \kappa \le p}} (1-a_p) \\
&\ge \prod_{\substack{w \le p < z: \\ \kappa \le p}} \left(1-\frac{\kappa}{p}\right) \\
&\gg \prod_{w \le p < z} \left(1-\frac{1}{p}\right)^{\kappa} \\
&= \left(\frac{\prod_{p<z}\left(1-\frac{1}{p}\right)}{\prod_{p<w}\left(1-\frac{1}{p}\right)}\right)^{\kappa} \underset{\substack{\uparrow \\ \text{PNT}}}{\asymp} \left(\frac{\log z}{\log w}\right)^{-\kappa} \quad \text{for large } w, z.
\end{aligned}$$

□

Thm 11.3.5 (Fundamental lemma of sieve theory)

Let $a_1, a_2, \ldots$ be a mult. seq. of sieve dimension $\le \kappa$.

Let $s \ge 1$ be suff. large(depending on the sequence).

Let $D \ge 1$ and $z = D^{1/s}$.

For some $1 \le \beta \le s$, we then have

$$\sum_{d \in \mathcal{D}^{\pm}_{\beta,D}} \mu(d) a_d = V(z) \left(1 + O(e^{-s})\right).$$

(In part., for large s,

$$\sum_{\dots} \mu(d) a_d \asymp V(z).\ )$$

Lemma 11.3.6

If $d = p_1 \cdots p_r \in \mathcal{D}^{\pm}_{\beta,D}$ with $p_1 < \dots < p_r < D^{1/\beta}$,

then $d \le D^{1-\left(\frac{\beta-1}{\beta}\right)^r}$.

Pf by ind. over r.

r=0 : $d = 1 \le D^{1-1}$ ✓

r=1: $d = p_1 < D^{1/\beta} = D^{1-\frac{\beta-1}{\beta}}$ ✓

r≥2: We have

$$p_k^{\beta+1} p_{k+1} \cdots p_r \le D \text{ for } k=1 \text{ or for } k=2$$

(depending on the parity of r).

$$\Rightarrow p_1^{\beta} p_2 \cdots p_r \le D. \qquad (I)$$

Since $p_2 \cdots p_r \in \mathcal{D}^{\pm}_{\beta,D}$ according to axiom b),

we have $p_2 \cdots p_r \le D^{1-\left(\frac{\beta-1}{\beta}\right)^{r-1}}$ by induction.

$$\Rightarrow d^{\beta} = (p_1 \cdots p_r)^{\beta} \underset{(I)}{\le} D \cdot (p_2 \cdots p_r)^{\beta-1}$$

$$\le D^{1+(\beta-1)\left(1-\left(\frac{\beta-1}{\beta}\right)^{r-1}\right)} = D^{\beta\left(1+\left(\frac{\beta-1}{\beta}\right)^{r}\right)}.$$

□

Pf of Thm 11.3.5

$$\sum_{d\in\mathcal{D}^{\pm}_{\beta,D}} \mu(d)\, a_d$$

$$\underset{\substack{\uparrow\\ \boxed{\text{Lemma 11.3.2}}}}{=} V(z) + O\Bigg(\sum_{\substack{d\in\mathcal{D}_0:\\ d\notin\mathcal{D}^{\pm}_{\beta,D}\\ \frac{d}{\mathrm{lpf}(d)}\in\mathcal{D}^{\pm}_{\beta,D}}} a_d \underbrace{V(\mathrm{lpf}(d))}_{\ll V(z)\cdot\left(\frac{\log(z)}{\log(\mathrm{lpf}(d))}\right)^{\kappa}} \Bigg)$$

Write $d = p_1 \cdots p_r$.

If $d \notin \mathcal{D}^{\pm}_{\beta,D}$, $\boxed{\text{but } \frac{d}{p_1}\in\mathcal{D}^{\pm}_{\beta,D}}$ we must have $D^{\frac{\beta+r}{s}} \geq p_1^{\beta+1} p_2 \cdots p_r > D$,

so $r > s-\beta$. Moreover, by Lemma 11.3.6, we have

$p_2 \cdots p_r \leq D^{1-\left(\frac{\beta-1}{\beta}\right)^{r-1}}$, so then

$p_1^{\beta+1} > D^{\left(\frac{\beta-1}{\beta}\right)^{r-1}} > D^{\left(\frac{\beta-1}{\beta}\right)^{r}\cdot\frac{\beta+1}{\beta}}$, so

$p_1 > D^{\left(\frac{\beta-1}{\beta}\right)^{r}\cdot\frac{1}{\beta}} \underset{\substack{\uparrow\\ \boxed{D=z^s,\ s\geq\beta}}}{\geq} z^{\left(\frac{\beta-1}{\beta}\right)^{r}}$. In particular, $\left\{\frac{\log z}{\log p_1}\right\} \leq \left(\frac{\beta}{\beta-1}\right)^{r}$

$$\Rightarrow\quad A := \frac{\sum\limits_{d\in\mathcal{D}^{\pm}_{\beta,D}} \mu(d)a_d}{V(z)} - 1$$

$$\ll \sum_{\substack{d=p_1\cdots p_r:\\ z^{\left(\frac{\beta-1}{\beta}\right)^r}\le p_1<\cdots<p_r<z\\ r> s-\beta}} \underbrace{a_d}_{a_{p_1}\cdots a_{p_r}} \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

$$\le \sum_{r>s-\beta} \frac{1}{r!}\Bigg(\underbrace{\sum_{z^{\left(\frac{\beta-1}{\beta}\right)^r}\le p<z} a_p}_{\rotatebox{90}{$\le$}}\Bigg)^r \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

$$-\log\frac{V(z)}{V\left(z^{\left(\frac{\beta-1}{\beta}\right)^r}\right)} \le \left\{ r\kappa\log\frac{\beta}{\beta-1} + O(1)\right\}$$

$$\le \sum_{r>s-\beta} \underbrace{\frac{r^r}{r!}}_{\le e^r}\cdot\left(\kappa\log\frac{\beta}{\beta-1} + O\left(\frac{1}{r}\right)\right)^r \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

Let $f(\beta) = e\cdot\kappa\log\frac{\beta}{\beta-1}\cdot\left(\frac{\beta}{\beta-1}\right)^{\kappa}$.

We have $f(\beta)\longrightarrow 0$ as $\beta\longrightarrow\infty$.

Choose β so that $f(\beta)\le\frac{1}{2e}$. Then,

$$A \ll \sum_{r\ge s-\beta}\left(\frac{1}{2e}+O_\beta\left(\frac{1}{r}\right)\right)^r \underset{\substack{\uparrow\\ \text{suff. large } s}}{\le} \sum_{r\ge s-\beta}\frac{1}{e^r} \ll_\beta \frac{1}{e^s}.$$

□

Cor 11.3.7 (Weaker form of twin prime conjecture)

Let $t \geq 1$ be suff. large. Then, for large x, we have

$$N(x) := \# \left\{ n \leq x : \begin{array}{l} n, n+2 \text{ aren't divisible by} \\ \text{any } p \leq x^{1/t} \end{array} \right\} \gg \frac{x}{(\log x)^2}.$$

Rmk $n \leq x$ can be divisible by at most t primes $\leq x^{1/t}$.

Pf of Cor Let $D = x^{1/2}$, $z = D^{1/s} = x^{1/2s}$.

$(\rightsquigarrow t := 2s)$.

We've seen in the pf of Cor 11.2.3 that if

$$a_d = \begin{cases} \frac{2^{\nu(d)}}{d}, & d \text{ odd}, \\ 0, & d \text{ even}, \end{cases}$$

then

$$\# \{ n \leq x : d \mid (2n+1)(2n+3) \} = x \cdot a_d + \mathcal{O}(2^{\nu(d)}).$$

$$\Rightarrow$$

$$N(x) \geq \sum_{d \in \mathcal{D}^-_{\beta,D}} \mu(d) \cdot \# \{ n \leq x : d \mid \cdots \}$$

$$= x \cdot \sum_{d \in \mathcal{D}^-_{\beta,D}} \mu(d) \cdot a_d + \mathcal{O}\Big(\underbrace{\sum_{d \in \mathcal{D}^-_{\beta,D}} 2^{\nu(d)}}_{\substack{\leq \sum_{d \leq D} 2^{\nu(d)} \\ \asymp D \log D \\ \asymp x^{1/2} \log x}} \Big)$$

Also,

$$\sum_{d \in \mathcal{D}^-_{\beta,D}} \mu(d) \cdot a_d \asymp V(z) \text{ for large } s$$

and appropriate β.

$$\| \qquad \prod_{2<p<z} \left(1 - \frac{2}{p}\right) \asymp (\log z)^{-2} \asymp_s (\log x)^{-2}$$

for fixed s.

$$\Rightarrow N(x) \gg \frac{x}{(\log x)^2} + O(x^{1/2} \log x) \gg \frac{x}{(\log x)^2} .$$

$\square$

~~$\Rightarrow$ For large z,~~

~~$\#\{\dots\} \gg \frac{x}{(\log z)^2} \gg_s \frac{x}{(\log x)^2}$. $\square$~~

Rmk Using more advanced sieves, Chen proved that

~~Every suff. large n,~~

~~every suff. large even n is the sum~~

there are ∞ many primes p such that $p+2$ is prime or the product of two primes.

Rmk Using a very different method (more like Selberg sieves), Zhang showed that there are ∞ many pairs of primes of bounded distance. $(\leq B)$

Better result with simpler proof: Maynard, Small gaps between primes

Idea: Find a sequence $\nu_1, \nu_2, \ldots \geq 0$ such that

$$\sum_{i=0}^{B} \sum_{\substack{\frac{x}{2} < n \leq x \\ n+i \text{ prime}}} \nu_n > \sum_{\frac{x}{2} < n \leq x} \nu_n \quad \text{for all suff. large } x. \quad (I)$$

Then, for some $\frac{x}{2} < n \leq x$, there must be $0 \leq i_1 < i_2 \leq B$ with $n+i_1, n+i_2$ both prime. To ensure (I), one should choose $(\nu_n)_n$ so that ν_n tends to be larger the more of the numbers $n+i$ $(0 \leq i \leq B)$ are prime, but so that we can still bound $\sum_{\substack{n: \\ n+i \text{ prime}}} \nu_n$ from below effectively.

(Essentially, they take $\nu_n = \left(\sum_{\substack{d_0 \mid n \\ d_1 \mid n+1 \\ \vdots \\ d_B \mid n+B}} \mu(d_0) \cdots \mu(d_B)\, f\left(\frac{\log d_0}{\log x}, \dots, \frac{\log d_B}{\log x} \right) \right)^2$

for a suitable smooth compactly supported function $f : \mathbb{R}^{B+1} \longrightarrow \mathbb{R}$.)

11.4. Large sieve

In the previous applications, we've been forbidding only $O(1)$ residue classes mod each prime p. What if we instead forbid a large number of residue classes? (Say $\asymp p$ many.)

Reminder $c : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ any function

$\rightsquigarrow$ Fourier transform $\hat{c} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$

$$\hat{c}(t) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x) e^{2\pi i x t/q}$$

$$q \cdot \sum_{x \in \mathbb{Z}} c(x \bmod q) f(x) = \sum_{t \in \mathbb{Z}} \hat{c}(t \bmod q) \hat{f}\left(\frac{t}{q}\right)$$

Lemma 11.4.1 $\sum_t \hat{c}(t)\overline{\hat{d}(t)} = q \sum_x c(x)\overline{d(x)}$, so in part. $\sum_t |\hat{c}(t)|^2 = q \cdot \sum |c(x)|^2$

Pf HW. □

Lemma 11.4.2 Let p be a prime and $c : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ a function which vanishes on (exactly) $\omega \geq \epsilon p$ of the residue classes mod p.

Then, $$\sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} |\hat{c}(t)|^2 \geq \frac{\omega}{p-\omega} \cdot |\hat{c}(0)|^2.$$

Pf $$\sum_{t \in \mathbb{Z}/p\mathbb{Z}} |\hat{c}(t)|^2 = p \cdot \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |c(x)|^2$$

$$\hat{c}(0) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x).$$

~~Let $d(x) = \begin{cases} 1, & c(x) \neq 0 \\ 0, & c(x) = 0 \end{cases}$.~~

~~$\Rightarrow c(x) = c(x) \cdot d(x)$~~

$$\sum_{t} |\hat{c}(t)|^2 \cdot (p-\omega)$$

$$= p \cdot \sum_{\substack{x: \\ c(x)\neq 0}} |c(x)|^2 \cdot \sum_{\substack{x: \\ c(x)\neq 0}} 1^2$$

$$\underset{\substack{\uparrow \\ \text{Cauchy-} \\ \text{Schwarz}}}{\geq} p \cdot \Big|\sum_{\substack{x: \\ c(x)\neq 0}} c(x)\Big|^2 = p \cdot |\hat{c}(0)|^2.$$

$$\Rightarrow \sum_{t} |\hat{c}(t)|^2 \geq \frac{p}{p-\omega} \cdot |\hat{c}(0)|^2$$

$$\Rightarrow \sum_{t\neq 0} |\hat{c}(t)| \geq \frac{\omega}{p-\omega} \cdot |\hat{c}(0)|^2. \qquad \square$$

Cor 11.4.3 Let $d \geq 1$ be sqfree, $c: \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$, and

assume that for each $p \mid d$, there are $\omega(p)$ residue classes $a \bmod p$ s.t. $c(x) = 0$ whenever $x \equiv a \bmod p$.

Then,
$$\sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} |\hat{c}(t)|^2 \geq \left(\prod_{p \mid d} \frac{\omega(p)}{p-\omega(p)}\right) \cdot |\hat{c}(0)|^2.$$

Pf HW (use the Chin. remainder thm). □

Def The Fourier transform of a fct. $f \in L^1(\mathbb{Z})$ $(f : \mathbb{Z} \to \mathbb{C})$ is the function $\hat{f} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ given by $\hat{f}(t) = \sum_{n \in \mathbb{Z}} f(n) e(nt)$.

Rmk a) If $f \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$, then $\hat{f} \in L^2(\mathbb{R}/\mathbb{Z})$.

b) If $f, g \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$, then

$$\begin{array}{ccc} \langle \hat{f}, \hat{g} \rangle & = & \langle f, g \rangle \\ \| & & \| \\ \int_{\mathbb{R}/\mathbb{Z}} f(t)\overline{g(t)}\,dt & & \sum_{n \in \mathbb{Z}} f(n)\overline{g(n)} \end{array}$$

Lemma 11.4.4 (Analytic large sieve inequality)

Let $M \in \mathbb{R}$, $N \geq 1$, $\delta > 0$.

Let $f : \mathbb{Z} \longrightarrow \mathbb{C}$ with $f(x) = 0$ unless $x \in [M-N, M+N]$.

Let $\alpha_1, \dots, \alpha_k \in \mathbb{R}/\mathbb{Z}$ be δ-separated:

$$\|\alpha_i - \alpha_j\|_{\mathbb{R}/\mathbb{Z}} \geq \delta \quad \forall i \neq j.$$

Then, $\sum_i |\hat{f}(\alpha_i)|^2 \ll \left(N + \frac{1}{\delta}\right) \cdot \underbrace{\sum_{n \in \mathbb{Z}} |f(n)|^2}$.

$$\left(= \int_{\mathbb{R}/\mathbb{Z}} |\hat{f}(t)|^2 \, dt \right)$$

Note $\frac{LHS}{k}$ looks like an approx. for the Riemann integral $\int_{\mathbb{R}/\mathbb{Z}} |\hat{f}(t)|^2 dt$.

Idea $\hat{f}(\alpha_i) = \langle f, g_i \rangle$ for $g_i : \mathbb{Z} \longrightarrow \mathbb{C}$, $g_i(n) = e(-\alpha_i n)$.

$= \langle f, \tilde{g}_i \rangle$ for $\tilde{g}_i = g_i \cdot 1_{[M, M+N]}$.

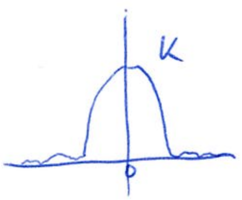
$$\left.\begin{array}{l} \langle \tilde{g}_i, \tilde{g}_i \rangle = \sum_{n \in [M, M+N]} 1 = N+1 \\ \langle \tilde{g}_i, \tilde{g}_j \rangle = \sum_{n \in [M, N+N]} e((\alpha_i - \alpha_j)n) \approx 0 \quad \text{for } i \neq j \end{array}\right\} \Rightarrow \left(\frac{g_i}{\sqrt{N}}\right)_{i=1,\dots,k} \text{ almost orthonormal}$$

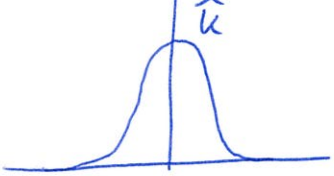
$$\underset{\substack{\uparrow \\ \text{Bythagoras}}}{\overset{\sim}{\Rightarrow}} \sum_i |\langle f, \tilde{g}_i \rangle|^2 \lesssim N \|f\|^2.$$ ~~Bythagoras~~

"$\underset{\sim}{\square}$"

Pf Let g_i as before.

Let $K \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ smooth with



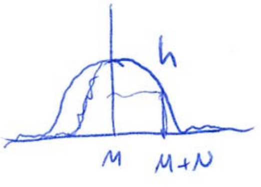


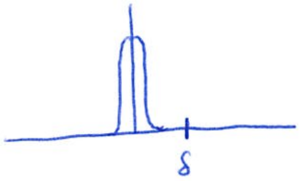
a) $K(x) \geq 0 \quad \forall x \in \mathbb{R}$

b) $\hat{K}(t) \geq 0 \quad \forall t \in \mathbb{R}$

c) $\hat{K}(t) = 0$ if $|t| \geq \frac{1}{2}$.

d) $K(x) \geq 1 \quad \forall x \in (-A, A)$.





$\Rightarrow K(0) = \int \hat{K}(t)\,dt > 0$.

Let $K(x) > 0$ if $0 \leq x \leq A$.

$A > 0$ small enough so

Let $S = \max\left(1, \frac{1}{\delta}, \frac{N}{A}\right)$

and let $h(x) = K\left(\frac{x-M}{S}\right)$. $\Rightarrow h(x) \geq 1 \quad \forall x \in [M-N, M+N]$.

$\Rightarrow \hat{h}(t) = S \cdot \hat{K}(Sx) \cdot e(Mt)$. $\left(\operatorname{supp}(\hat{h}) \subseteq \left(-\frac{1}{2S}, \frac{1}{2S}\right) \subseteq \left(-\frac{\delta}{2}, \frac{\delta}{2}\right)\right)$

Let $\widetilde{g_i} = g_i \cdot h \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$

$$\Rightarrow \langle g_i, g_j \rangle = \sum_{n \in \mathbb{Z}} h(n)^2 \, e((\alpha_i - \alpha_j)n)$$

$$= \sum_{t \in \mathbb{Z}} \widehat{h^2}(t + \alpha_i - \alpha_j)$$

Poisson summation

$$= \sum_{t \in \mathbb{Z}} \underbrace{(\hat{h} * \hat{h})}_{\operatorname{supp}(-) \subseteq \left(-\frac{1}{S}, \frac{1}{S}\right) \subseteq \left(-\frac{\text{[illegible]}}{\delta}, \frac{\text{[illegible]}}{\delta}\right)}(t + \alpha_i - \alpha_j) = \begin{cases} (\hat{h} * \hat{h})(0) = S \cdot (\text{const.}), & i = j, \\ 0, & i \neq j. \end{cases}$$

(because $\|\alpha_i - \alpha_j\|_{\mathbb{R}/\mathbb{Z}} \geq \delta$

Let $\frac{f}{h}(x) = 0$ if $x \notin [M-N, M+N]$.

$$\underset{\uparrow}{\Rightarrow} \sum_i \Big|\big\langle \underset{\shortparallel}{\tfrac{f}{h}}, \tilde{g}_i \big\rangle\Big|^2 \ll S \underbrace{\Big\|\frac{f}{h}\Big\|^2}_{\displaystyle \sum_{n\in\mathbb{Z}} \underbrace{\frac{|f(n)|^2}{|h(n)|^2}}_{\sum_{n\in[M,M+N]} \underset{\uparrow}{\ll} |f(n)|^2}} \ll S \cdot \sum_{n\in\mathbb{Z}} |f(n)|^2$$

Pythagoras $\quad \langle \frac{f}{h}, g_i \cdot h\rangle \underset{\uparrow}{=} \langle f, g_i\rangle = \hat{f}(\alpha_i)$

h is real-valued

h(x) bounded from below for $M \le x \le M+N$

~~$\langle \frac{f}{h}, \tilde{g}_i\rangle = \sum_{n\in\mathbb{Z}} f(n)\,\tilde{g}_i(n)$~~

~~$= \sum_{n\in[M,M+N]} f(n)\, g_i(n)\, h(n)$~~

□

Thm 11.4.5 (Large sieve)

Let ~~$S \subseteq [M, M+$ be a subset~~ $z \geq 1$, $M \in \mathbb{Z}$, $N \geq 1$.

For each $p \leq z$, ~~assume that there are $\omega(p)$ residue~~

let $E_p \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set of size $\omega(p)$.

Then, the set $S := \{M \leq n \leq M+N : \forall p \leq z : n \bmod p \notin E_p\}$

has size $\ll \dfrac{N + z^2}{J}$,

$$\text{where } J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}.$$

Pf Let $f := \mathbb{1}_S \in L^1(\mathbb{Z})$.

The numbers $\frac{t}{d} \in \mathbb{R}/\mathbb{Z}$

with $d \leq z$ are $\frac{1}{z^2}$-separated (as $\frac{t_1}{d_1} - \frac{t_2}{d_2} = \frac{\dots}{d_1 d_2}$).

$$\Rightarrow \sum_{d \leq z} \sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} \left|\hat{f}\left(\tfrac{t}{d}\right)\right|^2 \ll (N + z^2) \cdot \underbrace{\sum_{n \in \mathbb{Z}} |f(n)|^2}_{\#S}. \qquad (I)$$

On the other hand, by Cor 11.4.3, (If $g : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$, $x \mapsto \sum_{n \equiv x \bmod d} f(n)$, then $\hat{f}\left(\frac{t}{d}\right) = \hat{g}(t)$.)

$$\sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} \left|\hat{f}\left(\tfrac{t}{d}\right)\right|^2 \geq \left(\prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}\right) \cdot |\underbrace{\hat{f}(0)}_{\sum_{n \in \mathbb{Z}} f(n) = \#S}|^2 \qquad (II)$$

$$(I), (II) \Rightarrow \#S \ll \frac{N + z^2}{J}.$$

□

Cor 11.4.6 The number of $n \leq N$ which are a quadratic residue modulo each prime $p \leq z$ is $\ll \frac{N}{z} + z$.

Rmk For $z = N^{1/2}$, we get $\ll N^{1/2}$.

Note: Every square $n \leq N$ is a quadr. res. mod every prime p.

Pf of Cor Let $E_p = \{ x \in \mathbb{Z}/p\mathbb{Z}$ quadr. nonres.$\}$.

$$\Rightarrow \omega(p) = \# E_p = \begin{cases} \frac{p-1}{2}, & p > 2, \\ 0, & p = 2. \end{cases}$$

$$\Rightarrow \frac{\omega(p)}{p-\omega(p)} = \begin{cases} \frac{p-1}{p+1}, & p > 2 \\ 0, & p = 2 \end{cases}$$

$$J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)} \asymp z$$ for example by Wiener-Ikehara.

$$\Rightarrow \# \{ n \leq z \text{ quadr. res. mod each } p \leq z \} \ll \frac{N + z^2}{J} \asymp \frac{N}{z} + z \qquad \square$$

An interesting application:

Thm 11.4.17 (Linnik)

For any prime p, let

$$k_p = \min\{ n \geq 1 : (n \bmod p) \notin \mathbb{F}_p^{\times 2} \},$$

(quadr. nonres.)

For any $\varepsilon > 0$, for every $N \geq 1$, there are only $O_\varepsilon(1)$ primes p with $k_p > N^\varepsilon$.

~~For any $\varepsilon > 0$, there are only fin. many p with $k_p > N^\varepsilon$.~~

Rmk The GRH implies that $k_p \ll (\log p)^2$ for all p and even that there is a primite root $n \ll (\log p)^6$ modulo p.

Pf Let $N \geq 1$ be large, $z = N^{1/2}$.

For any p, define $E_p \subseteq \mathbb{Z}/p\mathbb{Z}$ as follows:

$$E_p = \begin{cases} \{a \in \mathbb{Z}/p\mathbb{Z} \text{ quadr. nonresidue}\}, & k_p > N^\varepsilon, \\ \emptyset, & k_p \leq N^\varepsilon \text{ (or } p = 2) \end{cases}$$

Let $S = \{1 \leq n \leq N : \forall p \leq z : (n \bmod p) \notin E_p\}$

$= \{1 \leq n \leq N : \forall p \leq z \text{ with } k_p > N^\varepsilon, \ n \text{ is a quadr. res. mod } p\}.$

Note: $S \supseteq \{1 \leq n \leq N^\varepsilon\}$.

In fact, since any prod. of quadr. res. is a quadr. res., $S \supseteq \{1 \leq n \leq N \mid n = p_1 \cdots p_k \text{ with } p_1, \ldots, p_k \leq N^\varepsilon\}$.

~~W.l.o.g. $\varepsilon = \frac{1}{R}$ with $R \in \mathbb{Z}$~~

~~$\Rightarrow \#\{\geq \frac{1}{R!} \cdot \#\{p \leq N^\varepsilon\}^R \gg_R \left(\frac{N^\varepsilon}{\log(N^\varepsilon)}\right)$~~

$= \{1 \leq n \leq N \mid n \text{ is } \underline{N^\varepsilon\text{-smooth}}\}.$

$\Rightarrow \#S \geq \#\{1 \leq n \leq N \mid n \text{ is } N^\varepsilon\text{-smooth}\} \gg_\varepsilon N.$ (skipped)

On the other hand, the large sieve shows:

$$\underset{\substack{\vee\\\vee\\N}}{\#S} \ll \frac{N+z^2}{J} \asymp \frac{N}{J}.$$

$$\Rightarrow \underset{\rotatebox{90}{$\geq$}}{J} \ll_{\varepsilon} 1$$

$$\sum_{p\le z}\frac{\omega(p)}{p} \underset{\uparrow}{=} \sum_{\substack{p\le z:\\ k_p>N^{\varepsilon}}} \frac{\frac{p-1}{2}}{p} \gg \sum_{\substack{p\le z:\\ k_p>N^{\varepsilon}}} 1 .$$

$$\omega(p) = \#E_p = \begin{cases} \frac{p-1}{2}, & k_p>N^{\varepsilon}, \\ 0, & \text{otherwise.} \end{cases}$$

$\Rightarrow \#\{p\le z : k_p>N^{\varepsilon}\} \ll_{\varepsilon} 1$ is bounded as $N\to\infty$ (and $z\to\infty$). □

~~There's a higher - dim~~

The large sieve can be generalized to higher dimension:

Thm 11.4.8 (Large sieve). Let $m \geq 1$.

Let $z \geq 1$, $N \geq 1$, $B \subset \mathbb{R}^m$ a ball of radius N.

For each p, let $E_p \subseteq (\mathbb{Z}/p\mathbb{Z})^m$ be a set of size $\omega(p)$.

Then,

$$\#\{v \in B \cap \mathbb{Z}^m : \forall p \leq z : (v \bmod p) \in E_p\} \ll_m \frac{(N + z^2)^m}{J},$$

$$\text{where } J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p^m - \omega(p)} \geq \sum_{p \leq z} \frac{\omega(p)}{p^m - \omega(p)} \geq \sum \frac{\omega(p)}{p^m}.$$

Some other consequences:

<u>Thm 11.4.9</u>

Let $V \subset \mathbb{A}^n_{\mathbb{Q}}$ be an irreducible algebraic set of dimension n, not an affine linear subspace.

Then,

$$\#\{(x_1,\dots,x_n) \in V : x_1,\dots,x_n \in \mathbb{Z},\ |x_1|,\dots,|x_n| \le T\}$$

$$\ll T^{n-\frac{1}{2}} \cdot \log T.$$

Pf cf. Thm 13.1.2 in Serre: Lectures on the Mordell-Weil Theorem. □

<u>Rmk</u> If $f \in \mathbb{Q}[X_1,\dots,X_n]$ is a pol. of degree d, how many pts. $(x_1,\dots,x_n) \in \mathbb{Z}^n$ with $|x_1|,\dots,|x_n| \le T$ do we expect?

Naively, $\underset{f}{\asymp} T^{n-d}$ if $d \le n$,

$\underset{f}{\ll} 1$ if $d > n$.

(because $f(x_1,\dots,x_n)$ is a number $\ll T^d$ $\rightsquigarrow$ $=0$ with prob. T^{-d} for random $x_1,\dots,x_n$).

Of course, this is wrong in general.
For example, the result should be the same if we replace f by f^2. Also, $V(f) = \{x \mid f(x)=0\}$ could contain a line. Or $f = gh$. ...

Counterexamples to the naive heuristic

a) $f(X,Y,Z) = X^2+Y^2+Z^2 \rightsquigarrow N(T)=1$

b) $f(X,Y) = 2X+1$

$\rightsquigarrow N(T)=0$

c) $f = gh$

d) ~~$\{P \mid f(P)=0\}$ can contain a line for arbitrarily large d~~

$f(X,Y,Z) = X^d + Y$

$$\rightsquigarrow N(T) \underset{\substack{\uparrow \\ f(0,0,z)=0}}{\gg} T$$

e) $f(X,Y,Z) = XY - Z$

$\rightsquigarrow N(T) \asymp T \log T$

$\vdots$

(See also Manin's conjecture.)

Thm 11.4.10 (Bombieri - Vinogradov)

Let $A > 0$. For large x and for $\frac{x^{1/2}}{(\log x)^A} \le Q \le x^{1/2}$, we have

$$\sum_{q \le Q} \max_{\substack{y \le x \\ a \in (\mathbb{Z}/q\mathbb{Z})^\times}} \left| \sum_{\substack{n \equiv a \bmod q \\ n \le y}} \Lambda(n) - \frac{y}{\varphi(q)} \right| \ll_A Q x^{1/2} (\log x)^5 .$$

Rmk We have

$$\sum_{\substack{n \equiv a \bmod q \\ n \le y}} \Lambda(n) \ll \frac{x \log x}{q} \quad \text{and} \quad \frac{y}{\varphi(q)} \ll \frac{x \log x}{q}, \text{ so}$$

clearly $\mathrm{LHS} \ll x \log x \log Q \le x (\log x)^2$.

Rmk GRH implies

$$\left| \sum \Lambda(n) - \frac{y}{\varphi(q)} \right| \ll y^{1/2} (\log y)^2$$

according to Thm 10.10, which implies

$$\mathrm{LHS} \ll Q x^{1/2} (\log x)^2 .$$

12. The circle method

12.1. Introduction

Dirichlet series $D(a,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ are useful for multiplicative problems.

Power series $F(a,z) = \sum_{n=0}^{\infty} a_n z^n$ are useful for additive problems.

$$F(a,z) \cdot F(b,z) = F(a*b, z)$$

where $a*b$ is (now) the additive convolution:

$$(a*b)_k = \sum_{\substack{n,m \geq 0: \\ k=n+m}} a_n b_m .$$

Ex $F((1,1,\ldots), z) = \sum z^n = \frac{1}{1-z}$

Ex For $d \geq 1$, $a_n = \begin{cases} 1, & d \mid n, \\ 0, & d \nmid n, \end{cases}$

$$F(a,z) = \sum z^{dn} = \frac{1}{1-z^d} .$$

Ex $\frac{1}{1-z} \cdot \frac{1}{1-z^d} = F(a,s)$ for $a_k = \#\{(n,m): k=n+m,\ 2 \mid m\}$.

<u>Exe</u> $\displaystyle\prod_{d=1}^{\infty} \frac{1}{1-z^d} = F(a,z)$

$\uparrow$

formal product

for $a_k = \left\{ (n_1, n_2, \ldots) \;\middle|\; \begin{matrix} a_1, a_2, \ldots \geq 0 \\ d \mid a_d \ \forall d \\ k = a_1 + a_2 + \ldots \end{matrix} \right\}$

$= \left\{ (m_1, m_2, \ldots) \;\middle|\; \begin{matrix} m_1, m_2, \ldots \geq 0 \\ k = \sum_{d=1}^{\infty} d m_d \end{matrix} \right\}$

$=$ # ways to write $k = s_1 + \ldots + s_r$ with $1 \leq s_1 \leq \ldots \leq s_r$, $r \geq 0$.

$=$ # partitions of k.

To study asymptotics of a_n for $n \to \infty$, instead of Perron's formula, use:

<u>Rmk</u> If $F(a,z)$ has radius of convergence R and ℓ is a ccw circle centered at 0 of radius $0<r<R$, then

$$a_n = \frac{1}{2\pi i} \int_{\ell} \frac{F(a,z)}{z^{n+1}} \, dz .$$

<u>Rmk</u> If $a_n = 0$ for all but finitely many n, then $R = \infty$ and we'll take $r = 1$.

$$\Rightarrow a_n = \frac{1}{2\pi i} \int_0^1 \frac{F(a, e(t))}{e(t)^{n+1}} \underbrace{e'(t)}_{2\pi i e(t)} \, dt = \int_0^1 F(a, e(t)) e(-nt) \, dt .$$

Rmk $F(a, e(t)) = \sum a_n e(nt)$ is the Fourier transform

$$\hat{f} : \mathbb{R}/\mathbb{Z} \to \mathbb{C} \text{ of } f : \mathbb{Z} \to \mathbb{C}$$

$$n \mapsto \begin{cases} a_n, & n \geq 0, \\ 0, & n < 0. \end{cases}$$

The prev. remark just describes the inverse Fourier transform.

12.2. Goldbach Conjecture

Conj Every even $n \geq 4$ is the sum of two primes.

Thm (Helfgott; Weak Goldbach Conj)

Every odd $n \geq 7$ is the sum of three primes.

The proof is a book...

We'll only prove:

Thm 12.2.1 (Hardy, Littlewood)

Assume the GRH. Then, every suff. large odd n is the sum of three primes.

Rmk Before Helfgott, Vinogradov removed the GRH assumption.

References: - Chapter 26 in Davenport: Mult. NT

- Chapter 3 in Vaughan: The Hardy - Littlewood Circle Method.

Goal: Let $f(k) = \begin{cases} 1, & k \overset{n}{\leq} \text{prime}, \\ 0, & \text{otherwise.} \end{cases}$

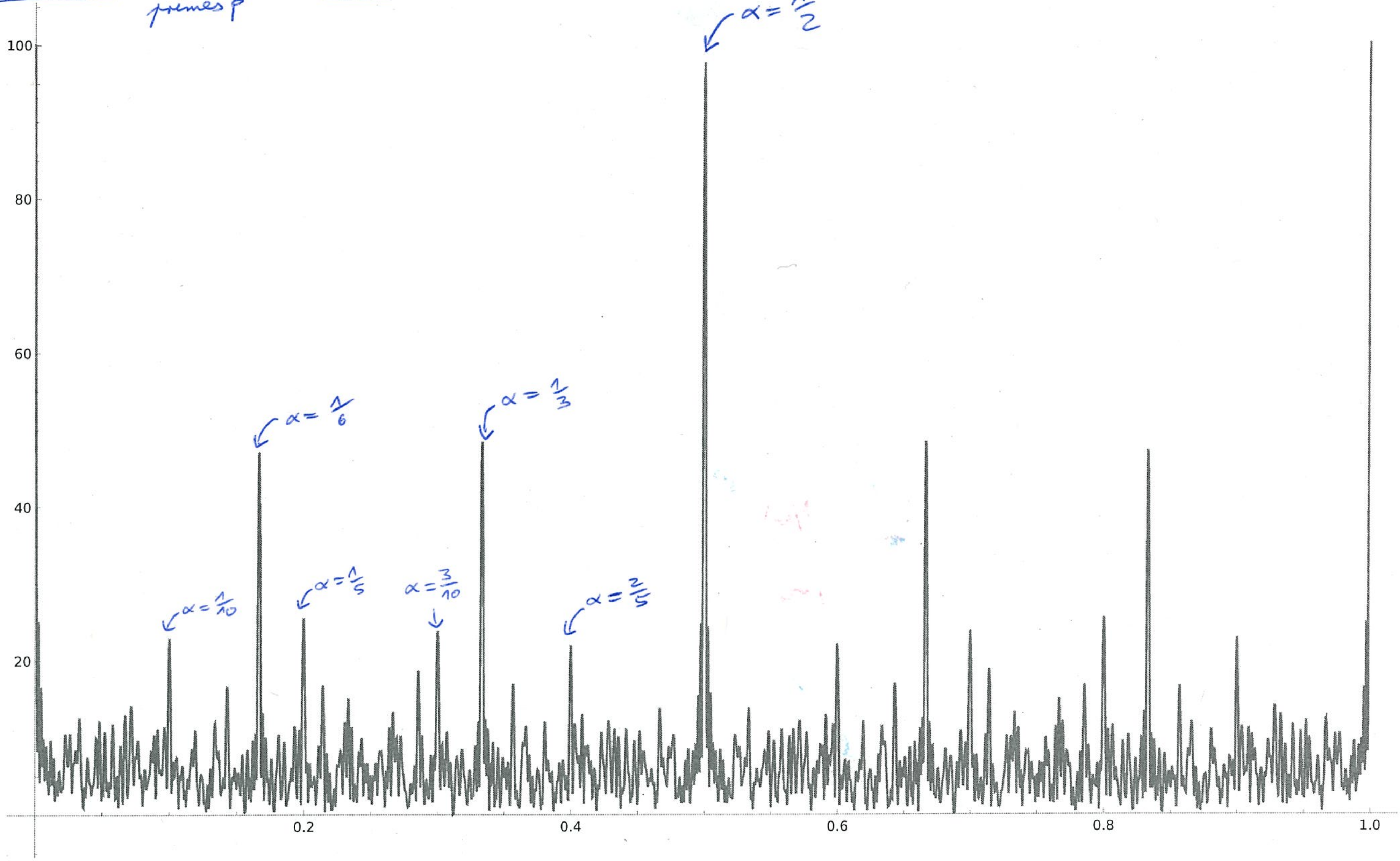
$$\Rightarrow (f * f * f)(n) = \#\{(p_1, p_2, p_3) \text{ prime} : n = p_1 + p_2 + p_3\}.$$

$$\| $$

$$\widehat{f^3}(-n) = \int_{\mathbb{R}/\mathbb{Z}} \hat{f}(t)^3 e(-nt)\, dt$$

Estimate this.

Graph of $\left| \sum_{\substack{\text{first 100} \\ \text{primes } p}} e(pt) \right|$



Observation "$|\hat{f}(t)|$ is largest when t is close to a rational number with small (sqfree) denominator"

$\rightsquigarrow$ The integral $\int_{\mathbb{R}/\mathbb{Z}} \hat{f}(t)^r e(-nt)\,dt$ is (hopefully)

dominated by ~~[illegible]~~ the integral over $t \in \mathbb{R}/\mathbb{Z}$ close to these rat. numbers ~~[illegible]~~, at least for $r \geq 3$."

Terminology Major arcs:

Set of pts $t \in \mathbb{R}/\mathbb{Z}$ close to such a rat. nr.

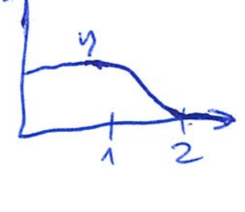
Minor arcs:

Set of other pts.

For simplicity, we'll ~~[illegible]~~ instead work with the function

$$f(k) = \begin{cases} \log k, & k \leq n \text{ prime}, \\ 0, & \text{otherwise}. \end{cases}$$

Rmk It's generally also worth considering a smooth cutoff:
For example, ~~[illegible]~~ fix η as in the picture and let



$$f(k) = \begin{cases} (\log k)\,\eta\left(\frac{k}{n}\right), & k \text{ prime}, \\ 0, & \text{otherwise}. \end{cases}$$

Heuristic

$$\hat{f}\left(\frac{a}{q}\right) = \sum_{p\le n} \log(p)\, e\left(\frac{ap}{q}\right)$$

$$= \sum_{r\in(\mathbb{Z}/q\mathbb{Z})^\times} \sum_{\substack{p\le n\\ p\equiv r \bmod q}} \log(p)\, e\left(\frac{ap}{q}\right)$$

$$\approx \sum_{r} \frac{n}{\varphi(q)}\, e\left(\frac{ar}{q}\right)$$

$$= \frac{n}{\varphi(q)} \sum_{d|q} \mu(d) \underbrace{\sum_{\substack{r\in\mathbb{Z}/q\mathbb{Z}:\\ d|r}} e\left(\frac{r}{q}\right)}_{\substack{1 \text{ if } d=q\\ 0 \text{ if } d\neq q}}$$

$$= \frac{\mu(q)}{\varphi(q)}\cdot n.$$

Lemma 12.2.2 Assume the GRH.

Let $q \geq 1$, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$. Then,

$$\hat{f}\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)} \cdot n + \mathcal{O}\left(q^{1/2} n^{1/2} (\log n)^2\right).$$

Rmk This is useless for $q \geq n$ because obviously $\hat{f}(t) \ll n$ for all t.

Pf $\hat{f}\left(\frac{a}{q}\right) = \sum_{p \leq n} \log(p)\, e\left(\frac{ap}{q}\right) = \sum_{\substack{k \leq n \\ \gcd(k,q)=1}} \Lambda(k)\, e\left(\frac{ak}{q}\right) + \mathcal{O}\left(q^{1/2} n^{1/2} (\log n)^2\right).$

We can write the function

$$c : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$$
$$t \mapsto \begin{cases} e\left(\frac{t}{q}\right), & t \in (\mathbb{Z}/q\mathbb{Z})^\times, \\ 0, & \text{otherwise} \end{cases}$$

as a lin. comb. of the multiplicative characters χ mod q:

$$\frac{1}{\varphi(q)} \sum_{\chi} \overline{\tau(\chi)}\, \chi(-t)$$

$$= \frac{1}{\varphi(q)} \sum_{\chi} \sum_{x} \overline{\chi(x)}\, e\left(-\frac{x}{q}\right) \chi(-t)$$

$$= \frac{1}{\varphi(q)} \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^\times} \underbrace{\sum_{\chi} \chi\left(-\frac{t}{x} \bmod q\right)}_{\substack{\varphi(q) \text{ if } -\frac{t}{x} \equiv 1 \bmod q \\ 0 \text{ otherwise}}} e\left(-\frac{x}{q}\right)$$

$$= \begin{cases} e\left(\frac{t}{q}\right), & t \in (\mathbb{Z}/q\mathbb{Z})^\times \\ 0, & \text{otherwise} \end{cases}$$

$$= c(t).$$

$$\Rightarrow \hat{f}\left(\frac{a}{q}\right) = \sum_{k\le n} \Lambda(k) \frac{1}{\varphi(q)} \sum_{\chi} \overline{\tau(\chi)}\, \chi(-ak) + O(\ldots)$$

$$= \frac{1}{\varphi(q)} \sum_{\chi} \overline{\tau(\chi)} \underbrace{\,}_{\cdot \chi(-a) \cdot} \sum_{k\le n} \Lambda(k)\chi(k) \quad + O(\ldots)$$

The GRH implies that

$$\sum_{k\le n} \Lambda(k)\chi(k) = \begin{cases} n, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0 \end{cases} + O(n^{1/2}(\log n)^2).$$

Furthermore, we've already seen in the heuristic that

$$\tau(\chi_0) = \sum_{x\in(\mathbb{Z}/q\mathbb{Z})^\times} e\left(\frac{x}{q}\right) = \mu(q).$$

Also, one can show that $|\tau(\chi)| \le q^{1/2}$ for all characters χ (not necessarily primitive,).

The claim follows immediately (noting that there are exactly $\varphi(q)$ char. χ). □

<u>Cor 12.2.3</u> Assume the GRH.

Let $q \geq 1$, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, $0 \neq s \in \mathbb{R}$

Then,

$$\hat{f}\left(\frac{a}{q}+s\right) = \frac{\mu(q)}{\varphi(q)} \cdot \underbrace{\frac{e(sn)-1}{2\pi i s}}_{\left(\downarrow^{s\to 0}_{n}\right)} + \mathcal{O}\left(q^{1/2} n^{1/2} (\log n)^2 (1+sn)\right).$$

<u>Pf</u> We "know" $\hat{f}\left(\frac{a}{q}\right) = \sum_{p \leq n} \log(p)\, e\left(\frac{a}{q}\cdot p\right)$ for all n.

We want $\hat{f}\left(\frac{a}{q}+s\right) = \sum_{p \leq n} \log(p)\, e\left(\frac{a}{q}\cdot p\right) \cdot e(s \cdot p)$

$\rightsquigarrow$ Use Abel summation on the functions

$$g(x) := \sum_{p \leq x} \log(p)\, e\left(\frac{a}{q}\cdot p\right) - \frac{\mu(q)}{\varphi(q)} \cdot x$$

and

$$h(x) := e(sx).$$

□

(<u>Rmk</u> If sn is large, ~~integrating~~ differentiating $e(sx)$ in Abel summation might be ill-advised because it oscillates.)

~~Using the fact that $g(x+d)$ $g(x)$~~

Cor 12.2.4 Assume the GRH. Let $q \geq 1$, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, $\delta > 0$.

Then,

$$\int_{\frac{a}{q}-\delta}^{\frac{a}{q}+\delta} \hat{f}(t)^3 \, e(-tn)\, dt$$

$$= \frac{\mu(q)}{\varphi(q)^3} \cdot \left(\frac{n^2}{2} e\left(-\frac{an}{q}\right) + \mathcal{O}\left(\frac{1}{(\delta n)^2}\right)\right) + \mathcal{O}\left(\delta \, \frac{q^{1/2} n^{1/2} (\log n)^2 (1+\delta n)}{\varphi(q)^2} \right.$$

$$\left. + \delta \cdot q^{3/2} n^{3/2} (\log n)^6 (1+\delta n)^3 \right)$$

Pf Just integrate... $\square$

Lemma 12.2.5 Let $t \in \mathbb{R}$, $X \geq 1$. Then, there is a rat. nr. $\frac{a}{q}$ (with $\gcd(a,q)=1$) with $1 \leq q \leq X$ and $\left| t - \frac{a}{q} \right| \leq \frac{1}{qX}$.

Pf $\left| t - \frac{a}{q} \right| \leq \frac{1}{qX} \iff |qt - a| \leq \frac{1}{X}$.

~~$\Rightarrow$ We want to show that one of the numbers $\|qt\|$ with $1 \leq q \leq X$ has distance ≤ 1 from an integer.~~

$\Rightarrow$ We want to show that $\|qt\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{X}$ for some $1 \leq q \leq X$.

But clearly, two of the X elements $\{qt\}$ of $\mathbb{R}/\mathbb{Z}$ have distance $\leq \frac{1}{X}$ in $\mathbb{R}/\mathbb{Z}$. Take their difference. □

We can now prove Thm 12.2.1. More precisely:

Thm 12.2.6 (Assume the GRH.) For $n \to \infty$,

$$\sum_{\substack{p_1,p_2,p_3:\\ n=p_1+p_2+p_3}} \log(p_1)\log(p_2)\log(p_3)$$

$$= \frac{1}{2} n^2 \cdot \prod_{p \nmid n} \left(1+\frac{1}{(p-1)^3}\right) \cdot \prod_{p \mid n} \left(1-\frac{1}{(p-1)^2}\right) + o(n^2).$$

Pf of Thm 12.2.1 (Weak Goldbach)

RHS > 0 for all odd n.

$\Rightarrow$ LHS > 0 for all suff. large odd n. □

Pf of Thm 12.2.6

$$\text{LHS} = \int_{\mathbb{R}/\mathbb{Z}} \hat{f}(t)^3 e(-nt)\,dt.$$

Let $Q = n^{\alpha}$ ~~(in fact, $Q = n^{\alpha}$ for any fixed $0 < \alpha < \frac{1}{2}$ should work).~~ for some sufficiently small $\alpha > 0$.

We let

$$\mathcal{M} = \left\{ t \in \mathbb{R}/\mathbb{Z} : \text{for some } 1 \le q \le Q,\ a \in (\mathbb{Z}/q\mathbb{Z})^{\times},\ \left\| t - \frac{a}{q} \right\|_{\mathbb{R}/\mathbb{Z}} < \frac{1}{2Q^2} \right\}.$$

(points on major arcs).

The difference between any rat. nrs. with denominator $\le Q$ is $\ge \frac{1}{Q^2}$, so for any $t \in \mathcal{M}$, there is exactly one fraction $\frac{a}{q}$ as above. ("The major arcs are disjoint.")

By Cor 12.2.4,

$$\int_{\mathcal{M}} \hat{f}(t)^3 e(-nt)\,dt = \sum_{q=1}^{Q} \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^{\times}} \frac{\mu(q)}{\varphi(q)^3} \cdot \frac{n^2}{2} \cdot e\left(-\frac{an}{q}\right)$$

$$+ O\left(n^{2-\varepsilon}\right)$$

(for some $\varepsilon > 0$).

$$= \sum_{q=1}^{\infty} (\cdots) + O\left(n^{2-\varepsilon}\right)$$

Here, $c_q^{(n)} = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} e\left(-\frac{an}{q}\right) = \sum_{d|q} \mu(d) \sum_{\substack{a \in \mathbb{Z}/q\mathbb{Z}: \\ d|a}} e\left(-\frac{an}{q}\right)$

$$= \sum_{d|q} \mu(d) \underbrace{\sum_{b \in \mathbb{Z}/\frac{q}{d}\mathbb{Z}} e\left(-\frac{bn}{q/d}\right)}_{\substack{\frac{q}{d} \text{ if } \frac{q}{d} | n \\ 0 \text{ otherwise}}}$$

$$\underset{e=\frac{q}{d}}{\overset{\uparrow}{=}} \sum_{\substack{e|q \\ e|n}} e\, \mu\left(\frac{q}{e}\right)$$

is multiplicative in q. If n is divisible by p exactly r times, then

$$\left(\boxed{c_{p^s}^{(n)} = \sum_{0 \le i \le \min(r,s)} p^i \underbrace{\mu(p^{s-i})}_{\substack{1 \text{ if } i=s \\ -1 \text{ if } i=s-1 \\ 0 \text{ if } i \le s-2}} = \begin{cases} p^s - p^{s-1}, & s \le r \\ -p^{s-1}, & s = r+1 \\ 0, & s \ge r+2 \end{cases}} \right)$$

$$c_p(n) = \begin{cases} -1+p, & p | n \\ -1, & p \nmid n \end{cases}$$

$$\Rightarrow \sum_{q=1}^{\infty} \frac{\mu(q)}{\varphi(q)^3} \cdot \frac{n^2}{2} \cdot c_q^{(n)} = \frac{n^2}{2} \cdot \prod_p \left(1 - \frac{c_p(n)}{\varphi(p)^3}\right)$$

$$= \frac{n^2}{2} \cdot \prod_{p \nmid n} \left(1 + \frac{1}{(p-1)^3}\right) \cdot \prod_{p | n} \left(1 - \frac{1}{(p-1)^2}\right)$$

Now, we deal with the minor arcs.

By lemma 12.2.5, for every $t \in \mathbb{R}/\mathbb{Z}$, there is some $\frac{a}{q}$ with $1 \le q \le n^{1-\alpha}$ and $\|t - \frac{a}{q}\| \le \frac{1}{q \cdot n^{1-\alpha}}$.

If $q \le n^{\alpha} = Q$, then $t \in \mathfrak{M}$. Otherwise, $\|t - \frac{a}{q}\| \le \frac{1}{n}$.

This gives an upper bound

$$\hat{f}(t) \ll n^{1-\varepsilon} \quad \text{for some } \varepsilon > 0.$$

This would immediately imply

$$\int_{(\mathbb{R}/\mathbb{Z})\setminus\mathfrak{M}} (\dots) \ll n^{3-\varepsilon} \quad \text{for some } \varepsilon > 0,$$

which is larger than the main term. $\ddot{\frown}$

(for small ε)

Solution: We also know that

$$\int |\hat{f}(t)|^2 \, dt = \sum_{x \in \mathbb{Z}} |f(x)|^2 = \sum_{p \le n} \log p \asymp n.$$

Hence,

$$\int_{(\mathbb{R}/\mathbb{Z})\setminus\mathfrak{M}} (\dots) \ll n \cdot n^{1-\varepsilon} = n^{2-\varepsilon} \quad \text{for some } \varepsilon > 0,$$

which grows more slowly than the main term!

□

Rmk To get rid of the GRH assumption, use the known zero-free region to obtain an estimate on the major arcs.
Unfortunately, it is only useful for $q \ll e^{c\sqrt{\log n}}$, so we take $Q = e^{c\sqrt{\log n}}$.

For the minor arcs, you need a different way of obtaining an upper bound.
This can be done using the following identity by Vaughan, which may remind you of sieve theory:

Vaughan's identity

For a sequence $a = (a_1, a_2, -)$ and any $T \geq 1$, let $a_{\leq T}$, $a_{>T}$ be the sequences with

$$(a_{\leq T})_n = \begin{cases} a_n, & n \leq T \\ 0, & n > T \end{cases} \qquad (a_{>T})_n = \begin{cases} 0, & n \leq T \\ a_n, & n > T \end{cases}.$$

(Clearly, $a = a_{\leq T} + a_{>T}$.)

Then,

$$\Lambda = \Lambda_{\leq V} + \mu_{\leq U} * L - \mu_{\leq U} * \Lambda_{\leq V} * 1 - (\mu_{\leq U} * 1)_{>U} * \Lambda_{>V},$$

where $L_n = \log(n)$.

(See for example Ch. 24 in Davenport or Ch. 3 in Vaughan.)

Thm 12.2.7

Let $f(n) = n \cdot \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{p \mid n} \left(1 + \frac{1}{p-1}\right).$

Then,

$$\sum_{n=1}^{N} \Big(\sum_{\substack{p_1, p_2: \\ n = p_1 + p_2}} \log(p_1) \log(p_2) - f(n) \Big)^2 \ll N^{3-\varepsilon}$$

for some $\varepsilon > 0$.

Note This saves a power of N^{ε} compared to the trivial estimate.

Cor 12.2.8

$$\#\{1 \le n \le N \text{ even not the sum of two primes}\} \ll N^{1-\varepsilon}$$

for some $\varepsilon > 0$.

Pf of Cor

If n is even and not the sum of two primes, then the summand

$\left(\Sigma \cdots - f(n) \right)^2 = f(n)^2$ is $\gg n^2$. $\square$

Pf of Thm (sketch) Take $f(k) = \begin{cases} \log(k), & k \leq N \text{ prime} \\ 0, & \text{otherwise} \end{cases}$

The major arcs work like before.

For the minor arcs:

$$\sum_{n=1}^{N} \left| \int_{(\mathbb{R}/\mathbb{Z}) \setminus \mathfrak{M}} \hat{f}(t)^2 e(-nt) \right|^2$$

$$\leq \sum_{n \in \mathbb{Z}} | \cdots |^2 = \int_{(\mathbb{R}/\mathbb{Z}) \setminus \mathfrak{M}} |\hat{f}(t)|^4 \, dt$$

Fourier transform preserves inner product

This fourth power can be bounded like before.

$\square$

Other applications of the circle method:

1) Asymptotics for the nr. of partitions of an integer n with $n \to \infty$.

2) Other weak forms of Goldbach's conjecture, such as $n = p_1 + p_2 + k^2$, ...
(Reference: Vaughan's book)

3) Number of ways of writing $n = a_1 x_1^2 + \dots + a_k x_k^2$ for fixed $0 < a_1, \dots, a_k \in \mathbb{Z}$, varying $x_1, \dots, x_k \in [-N^{1/2}, N^{1/2}]$, for $n \to \infty$.
(Reference: Heath-Brown: A new form of the circle method, and its applications to quadratic forms.)

4) Waring's problem: Every (suff. large) $n \in \mathbb{Z}$ can be written as a sum of $\boxed{\text{at most } c(k)}$ k-th powers.

What's the smallest such $c(k)$?

(Reference: Vaughan's book)

⋮

13. Equidistribution

References

- Chapter 11 in Murty
- Noam Elkies's lecture notes

Thm/Def 13.1 A sequence $a_1, a_2, \ldots \in \mathbb{R}/\mathbb{Z}$ is equidistributed / uniformly distributed if the following equivalent statements hold:

a) For all (open/closed/arbitrary) intervals $I \subseteq \mathbb{R}/\mathbb{Z}$,

$$\lim_{N\to\infty} \frac{1}{N} \# \{1 \le n \le N : a_n \in I\} = \text{length}(I).$$

b) For every (piecewise) continuous function $f : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ (or $\mathbb{C}$),

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(a_n) = \int_{\mathbb{R}/\mathbb{Z}} f(x)\,dx .$$

a_1
a_5
a_4
a_2
a_3

c) For all $0 \neq t \in \mathbb{Z}$ (or all $0 < t \in \mathbb{Z}$),

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(t a_n) = 0.$$

Rmk There are other notions of equidistribution. E.g.:

A sequence $(S_N)_N$ of (multi-)sets $S_N \subseteq \mathbb{R}/\mathbb{Z}$ is equidistr. if a) $\forall I$:

$$\lim_{N\to\infty} \frac{1}{|S_N|} \sum_{\substack{x\in S_N:\\ x\in I}} (\text{mult. of } x \text{ in } S_N) = \text{length}(I)$$

b) ...

c) ...

A sequence $(\mu_N)_N$ of measures on $\mathbb{R}/\mathbb{Z}$ is equidist. if (weakly conv. to Lebesgue measure)

a) $\forall I$: $\lim\limits_{N\to\infty} \int_{\mathbb{R}/\mathbb{Z}} d\mu_N = \text{length}(I)$

b) —

c) —

Or a sequence could be equidistr. w.r.t. some other (non-Lebesgue) measure on $\mathbb{R}/\mathbb{Z}$.

Pf (sketch) b) $\Rightarrow$ c): clear

b) $\Rightarrow$ a): Approximate 1_I by continuous functions.

a) $\Rightarrow$ b): Approximate f by step functions (= linear combinations of indicator functions 1_I).

c) $\Rightarrow$ b): Approximate f by functions of the form $\sum_{t=-M}^{M} b_t \, e(tx)$.

□

Rmk c) looks like a qualitative version of the kind of estimate we needed for minor arcs in the circle method.

b) ~~[illegible]~~ is also useful. For example, we previously wrote $\sum_{n \le N} d(n) = \sum_{a \le N} \left\lfloor \frac{N}{a} \right\rfloor = \sum_{a \le N} \frac{N}{a} - \sum_{a \le N} \left\{ \frac{N}{a} \right\}$.

~~If the fractional parts $\left\{\frac{N}{a}\right\}$, were equidistributed~~

~~[illegible]~~ Let $S_N = \left\{ \left\{ \frac{N}{a} \right\} : 1 \le a \le N \right\}$.

If ~~the~~ the sequence $(S_N)_N$ were equidistributed, then $\sum_{a \le N} \left\{ \frac{N}{a} \right\} \sim N \cdot \int_0^1 x \, dx = \frac{1}{2} N$.

(But we've previously seen that this is false!)

Ex Let $\lambda \in \mathbb{R}$. Then, $a_n = \{\lambda n\}$ is equidistr. if and only if $\lambda \notin \mathbb{Q}$.

Pf "$\Rightarrow$" via a): If $\lambda \in \mathbb{Q}$, then the sequence only takes finitely many values. $\Rightarrow$ There are gaps.
$\Rightarrow$ not equidistributed.

"$\Rightarrow$" via c): If $t\lambda \in \mathbb{Z}$, then

$$\frac{1}{N}\sum_{n=1}^{N} \underbrace{e(t\lambda n)}_{1} = 1 \overset{N \to \infty}{\not\longrightarrow} 0.$$

"$\Leftarrow$" via c): Since $t\lambda \notin \mathbb{Z}$ and therefore $e(t\lambda) \neq 1$, we have

$$\frac{1}{N}\sum_{n=1}^{N} e(t\lambda n) = \frac{1}{N}\underbrace{e(t\lambda)\cdot \frac{e(t\lambda N)-1}{e(t\lambda)-1}}_{\ll 1} \ll \frac{1}{N} \longrightarrow 0$$

□

Ex The sequence of $S_N = \{ \frac{b}{N} \mid b \in \mathbb{Z}/N\mathbb{Z} \} \subseteq \mathbb{R}/\mathbb{Z}$

is equidistributed:

$$\frac{1}{N} \sum_{b} e\left(t \frac{b}{N}\right) = 0 \quad \text{unless } N \mid t.$$

Ex The sequence of $S_N = \{ \frac{a}{N} \mid a \in (\mathbb{Z}/N\mathbb{Z})^\times \} \subseteq \mathbb{R}/\mathbb{Z}$

is equidistributed:

$$\frac{1}{N} \sum_{b} e\left(t \frac{b}{N}\right) \ll \frac{|t|}{N} \quad \text{(cf. pf. of Thm 12.2.6).}$$

Ex Let $a_1, a_2, \dots$ be the (reduced) fractions $\frac{b}{q} \in [0,1)$ sorted by $q \geq 1$

and in case of ties by b:

$$\frac{0}{1}, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \dots$$

This sequence is equidistributed.

Thm 13.2 (van der Corput; Weyl differencing trick)

If the sequence $(a_{n+d}-a_n)_n$ is equidistributed for all $d \geq 1$, then $(a_n)_n$ is equidistributed.

First attempt of a pf

$$\left|\sum_{n=1}^{N} e(ta_n)\right|^2 = \sum_{n=1}^{N} e(ta_n) \sum_{m=1}^{N} \overline{e(ta_m)}$$

$$= \sum_{n,m} \underbrace{e(t(a_n-a_m))}_{1 \text{ if } n=m}$$

$$= N + \sum_{n \neq m} e(t(a_n-a_m))$$

$$\underset{\substack{\uparrow \\ d=n-m}}{=} N + \sum_{\substack{-N<d<N \\ d\neq 0}} \underbrace{\sum_{\substack{n: \\ 1\le n\le N, \\ 1\le n+d\le N}} e(t(a_{n+d}-a_n))}_{\substack{\text{looks like the sum in} \\ \text{the def. of equidistr. of } (a_{n+d}-a_n)_n}}$$

Problem: We don't know how quickly

$$\frac{1}{N} \sum_{\substack{n: \\ \dots}} e(t(a_{n+d}-a_n)) \text{ goes to } 0 \text{ for } N\to\infty \text{ as } d \text{ varies.}$$

Solution: Only allow bounded differences.

We'll show the following slightly more general lemma:

Lemma 13.3 Let $x_1, \dots, x_N \in \mathbb{C}$, $H \geq 1$. Then,

$$\left|\sum_{n=1}^{N} x_n\right|^2 \leq \frac{H+N}{H+1}\left(\sum_{n=1}^{N} |x_n|^2 + 2\cdot\sum_{d=1}^{H}\left(1-\frac{d}{H+1}\right)\left|\sum_{n=1}^{N-d} x_{n+d}\overline{x_n}\right|\right)$$

Pf Let $x_n = 0$ unless $1 \leq n \leq N$.

$$(H+1)^2\left|\sum_n x_n\right|^2 = \left|\sum_{h=0}^{H}\sum_n x_{n+h}\right|^2 = \left|\sum_{n=-H+1}^{N}\sum_{h=0}^{H} x_{n+h}\right|^2$$

$$\underset{\substack{\uparrow\\ \text{Cauchy-Schwarz}\\ \text{or}\\ \text{AM-QM}}}{\leq} (H+N)\cdot\sum_n\left|\sum_{h=0}^{H} x_{n+h}\right|^2$$

Here, $\displaystyle\sum_n\left|\sum_{h=0}^{H} x_{n+h}\right|^2 = \sum_n \sum_{0\leq h,k\leq H} x_{n+h}\overline{x_{n+k}}$

$$= \sum_n\left\{\sum_h |x_{n+h}|^2 + \sum_n\sum_{\substack{-H\leq d\leq H\\ d\neq 0}}\sum_{\substack{0\leq k\leq H:\\ 0\leq k+d\leq H}} x_{n+k+d}\overline{x_{n+k}}\right\}$$

$$= (H+1)\sum_n |x_n|^2 + 2\,\mathrm{Re}\left(\sum_{d=1}^{H}\sum_{n=1}^{N-d} x_{n+d}\overline{x_n}\right)$$

$$(H+1-d)\cdot$$

$$\leq (H+1)\sum_n |x_n|^2 + 2\sum_{d=1}^{H}(H+1-d)\cdot\left|\sum_{n=1}^{N-d} x_{n+d}\overline{x_n}\right|.$$

$\square$

Pf of Thm

Use the lemma with $x_n = e(ta_n)$.

$$\Rightarrow \left|\frac{1}{N}\sum_{n=1}^{N} e(ta_n)\right|^2$$

$$\leq \frac{\frac{H}{N}+1}{H+1}\left(1+2\cdot\sum_{d=1}^{H}\left(1-\frac{d}{H+1}\right)\underbrace{\left|\frac{1}{N}\sum_{n=1}^{N-d} e(t(a_{n+d}-a_n))\right|}\right)$$

$$\frac{\frac{H}{N}+1}{H+1} \xrightarrow{N\to\infty} \frac{1}{H+1}$$

$$\left|\frac{1}{N}\sum_{n=1}^{N-d} e(t(a_{n+d}-a_n))\right| \xrightarrow{N\to\infty} 0$$ because $(a_{n+d}-a_n)_n$ is equidistributed

$$\Rightarrow \limsup_{N\to\infty} (LHS) \leq \frac{1}{H+1} \text{ for all } H\geq 1.$$

$$\Rightarrow \lim_{N\to\infty} (LHS) = 0$$

$\Rightarrow (a_n)_n$ is equidistributed. $\square$

Cor 13.4 Let $f(X) = b_m X^m + \dots + b_0 \in \mathbb{R}[X]$.

Then, $a_n = \{f(n)\}$ is equidistributed if and only if $b_i \notin \mathbb{Q}$ for some $i \geq 1$.

Pf "$\Longrightarrow$" If $b_i \in \mathbb{Q}$ for all $i \geq 1$, then $\{f(n)\}$ only takes finitely many values.

"$\Longleftarrow$" ~~w.l.o.g. $b_0 = 0$.~~

We prove the statement by induction over m.

w.l.o.g. $b_0 = 0$.

If $b_m \in \mathbb{Q}$, say $b_m = \frac{p}{q}$,

let $g(x) = f(x) - b_m X$.

$\Rightarrow$ $\deg(g) < m$ and g still has an irrational nonconst. coeff.

$$\sum_{n=1}^{N} e(tf(n)) = \sum_{n=1}^{N} e(t \underbrace{b_m}_{\frac{p}{q}} n) e(tg(n))$$

$$= \sum_{r \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{tpr}{q}\right) \underbrace{\sum_{\substack{n=1: \\ n \equiv r \bmod q}}^{N} e(tg(n))}$$

$$= \sum_{0 \leq m \leq \left[\frac{N-r}{q}\right]} e(tg(r+qm)).$$

$n = r + qm$ (where $1 \leq r \leq q$)

The pol. $g(r+qX)$ has an irrational nonconst. coeff., so by induction $\frac{1}{N}\sum_{\underline{m}} e(-\,-) \xrightarrow{N\to\infty} 0$.

$$\Rightarrow \frac{1}{N}\sum_{n=1}^{N} e(t f(n)) \xrightarrow{N\to\infty} 0.$$

<u>If $b_m \notin \mathbb{Q}$</u>: If $m=1$, this is the example $a_n=\{b_1 n\}$, so assume $m \geq 1$.

For any $d \geq 1$, the polynomial $f(x+d)-f(x)$ $= b_m((x+d)^m - x^m) + b_{m-1}((x+d)^{m-1} - x^{m-1}) + \dots$ of degree $m-1$ has the irrational leading coefficient $m d a_m$.

$\Rightarrow$ By induction, the sequence $(f(n+d)-f(n))_n$ is equidistr. for all $d \geq 1$.

$\Rightarrow$ By the Thm, the sequence $(f(n))_n$ is equidistr. □

<u>Rmk</u> One can – and e.g. when applying the circle method to Waring's problem wants to – estimate the rate of convergence ("the speed of equidistribution").

Last time $(a_n)_n$ equidistr.

$$\Updownarrow$$

a) $\lim_{N\to\infty} \frac{1}{N}\#\{1\le n\le N : a_n\in I\} = \text{length}(I) \qquad \forall I$

$$\Updownarrow$$

c) $\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e(ta_n) = 0 \qquad \forall t\neq 0$

Often, c) is easier to show, but we're more interested in a), and in fact in a quantitative version: how fast is the convergence? Given upper bounds on $\left|\frac{1}{N}\sum e(ta_n)\right|$ (for some finite N), can we derive upper bounds on $\left|\frac{1}{N}\#\{1\le n\le N : a_n\in I\} - \text{length}(I)\right|$ (for the same N)?

Def The discrepancy of $a_1,\dots,a_N$ is

$$D_N := D(a_1,\dots,a_N) := \sup_{\substack{I\subseteq\mathbb{R}/\mathbb{Z}\\ \text{interval}}} \left|\frac{1}{N}\#\{1\le n\le N : a_n\in I\} - \text{length}(I)\right|.$$

[If you know $\frac{1}{N}\sum_n e(ta_n)$ exactly for all t, you could recover the values a_n. But that's not so useful. Instead, we want to bound D_N using just the values for $|t|\le T$. This is a little like in sieves, where we only considered small (squarefree) numbers.]

Thm 13.5 (Erdős–Turán inequality)

For any $a_1, \dots, a_N \in \mathbb{R}/\mathbb{Z}$ and any $T \geq 1$,

~~$$D_N = \frac{1}{M+1} + 3 \sum_{m=1}^{M} \frac{1}{Nm} \left| \sum_{n=1}^{N} e(m a_n) \right|$$~~

$$D_N \leq \frac{1}{T+1} + \frac{3}{N} \sum_{t=1}^{T} \frac{1}{t} \left| \sum_{n=1}^{N} e(t a_n) \right|.$$

For example:

Cor 13.6 Let $\lambda \in \mathbb{R}$, $a_n = \{\lambda n\}$, $T \geq 1$. Then,

$$D_N \ll \frac{1}{T} + \frac{1}{N} \sum_{t=1}^{T} \frac{1}{t \cdot \|t\lambda\|_{\mathbb{R}/\mathbb{Z}}}$$

(if $t\lambda \notin \mathbb{Z}$ for all $1 \leq t \leq T$).

"If λ is not close to a rat. nr. with small denominator, D_N is small."

Pf of Cor

$$\sum_{n=1}^{N} e(t\lambda n) = e(t\lambda) \cdot \frac{e(t\lambda N) - 1}{e(t\lambda) - 1} \ll \frac{1}{|e(t\lambda) - 1|} \ll \frac{1}{\|t\lambda\|_{\mathbb{R}/\mathbb{Z}}}. \qquad \square$$

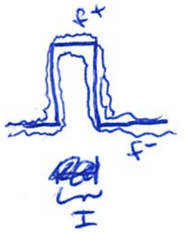
Rmk You can get nice estimates in many other cases. For example, try the sequence $a_n = \{\lambda n^2\}$ or $a_n = \{\lambda p_n\}$ where p_n is the n-th prime number or $a_n = \{\log(n!)\}$ or ...

The theorem follows immediately from the following way of approximating $1_I(x)$ by a sum of the form $\sum_{-T\le t\le T} b_t e(tx)$:

Lemma 13.7 (Selberg) Let $I \subseteq \mathbb{R}/\mathbb{Z}$. There are real-valued functions $f^+, f^- \in L^1(\mathbb{R}/\mathbb{Z})$ such that:

a) $f^-(x) \le 1_I(x) \le f^+(x)$ for all $x \in \mathbb{R}/\mathbb{Z}$

b) $\widehat{f^\pm}(t) = 0$ unless $-T \le t \le T$



c) $\left| \underbrace{\widehat{f^\pm}(0)}_{(=\int f^\pm(x)dx)} - \text{length}(I) \right| = \frac{1}{T+1}$.

d) $|\widehat{f^\pm}(t)| \le \frac{3}{2|t|}$ for $t \ne 0$.

Pf of Thm

$$\frac{1}{N} \sum_{n=1}^{N} 1_I(a_n) \le \frac{1}{N} \sum_n \underbrace{f^+(a_n)}_{\hat{\hat{f}}^+(-a_n)} = \frac{1}{N} \sum_n \sum_t \widehat{f^+}(t) e(-ta_n)$$

$$= \frac{1}{N} \sum_t \widehat{f^+}(t) \underbrace{\sum_{n=1}^{N} e(-ta_n)}_{=N \text{ if } t=0}$$

$$= \widehat{f^+}(0) + \frac{1}{N} \sum_{t\ne 0} \underbrace{\widehat{f^+}(t)}_{=\widehat{f^+}(-t)} \sum_n e(-ta_n)$$

$$\le \text{length}(I) + \frac{1}{T+1} + \frac{\cancel{2}}{N} \sum_{t=1}^{T} \frac{3}{2|t|} \left| \sum_n e(-ta_n) \right|$$

The lower bound works the same way, using f^-. □

~~The lemma allows from Lemma 13.8 There is a~~

Pf of Lemma

~~[illegible]~~

~~Recall that~~ Recall from complex analysis that

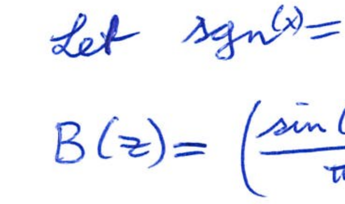
$$\left(\frac{\pi}{\sin(\pi z)}\right)^2 = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2}. \qquad (I)$$

Let $\operatorname{sgn}(x) = \begin{cases} 1 & , \operatorname{Re}(x) \geq 0, \\ -1 & , \operatorname{Re}(x) < 0, \end{cases}$ (!)

$$B(z) = \left(\frac{\sin(\pi z)}{\pi}\right)^2 \left(\sum_{n\in\mathbb{Z}} \frac{\operatorname{sgn}(n)}{(z-n)^2} + \frac{2}{z}\right).$$

This defines an entire function (as $\frac{\sin(\pi z)}{\pi}$ has a zero at $z = n \in \mathbb{Z}$).

$$(I) \Rightarrow B(z) - \operatorname{sgn}(z) = \left(\frac{\sin \pi z}{\pi}\right)^2 \Bigg(\underbrace{\sum_{n\in\mathbb{Z}} \frac{\operatorname{sgn}(n)-\operatorname{sgn}(z)}{(z-n)^2}}_{\substack{\sum_{n=1}^{\infty} \frac{-2}{(z+n)^2} \text{ if } z\geq 0 \\ \sum_{n=0}^{\infty} \frac{2}{(z-n)^2} \text{ if } z<0}} + \frac{2}{z} \Bigg) \geq 0 \quad \forall z \qquad (II)$$



(with equality for $z \in \mathbb{Z}$).

Also,

$$\int_{\mathbb{R}} (B(z)-\operatorname{sgn}(z))\,dz = \lim_{A\to\infty} \int_{-A}^{A} \cdots = \lim_{A\to\infty} \int_{0}^{A} (B(z)+B(-z))\,dz$$

(at least in the principal value)

$$= \int_0^{\infty} \left(\frac{\sin(\pi z)}{\pi}\right)^2 \cdot \frac{2}{z^2}\,dz = \int_{\mathbb{R}} \left(\frac{\sin(\pi z)}{\pi z}\right)^2 dz = 1$$

(III)

Moreover, $B(z) - \operatorname{sgn}(z) \ll \dfrac{e^{2\pi|\operatorname{Im} z|}}{1+|z|^2}$. (IV)

Note: $B \notin L^1(\mathbb{R})$!

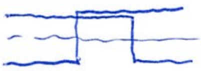
Let $I = [a,b]$, $a<b \in \mathbb{R}$.

Take $F^+(x) = \frac{1}{2}(B(x-a) + B(b-x))$.

$F^-(x) = -\frac{1}{2}(B(a-x) + B(x-b))$.

$$(\text{II}) \Rightarrow F^+(x) \geq \frac{1}{2}(\operatorname{sgn}(x-a) + \operatorname{sgn}(b-x)) = \begin{cases} 0, & b<x, \\ 1, & a\leq x\leq b, \\ 0, & x<a, \end{cases}$$

$$= 1\!\!1_{[a,b]}(x).$$



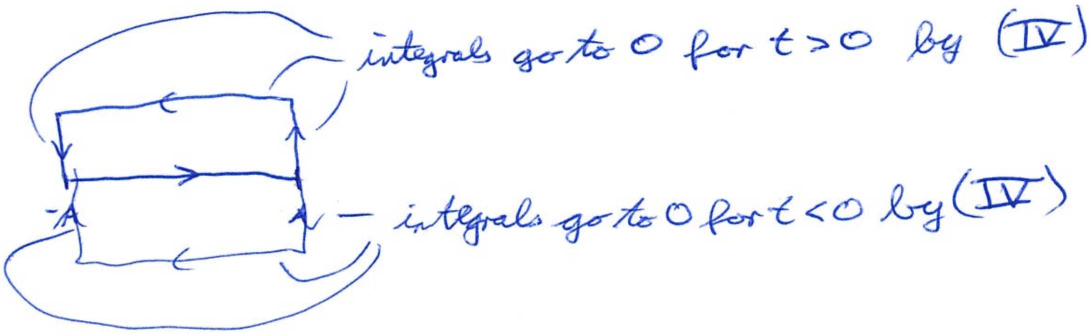
and $F^-(x) \leq \cdots = 1\!\!1_{[a,b]}(x)$.

$$(\text{III}) \Rightarrow \int_{\mathbb{R}} (F^\pm(x) - 1\!\!1_{[a,b]}(x))\,dx = \pm 1$$

Moreover, quite surprisingly,

$$\widehat{F^\pm}(t) = 0 \quad \text{if } |t| \geq 1 :$$

$$\widehat{F^{+}}(t) = \int_{\mathbb{R}} F^{+}(x)\, e(xt)\, dx = \lim_{A\to\infty} \int_{-A}^{A} \cdots \qquad = 0$$


integrals go to 0 for $t>0$ by (IV)
$-A$
A
integrals go to 0 for $t<0$ by (IV)

To finish the proof, rescale and then take

$$f^\pm(x) = \sum_{n\in\mathbb{Z}} F^\pm(x+n)$$

$$\vdots$$

(for details, see Murty/Elkies) □

Outlook:

The Sato-Tate Conjectures:

Ex For any prime p, let

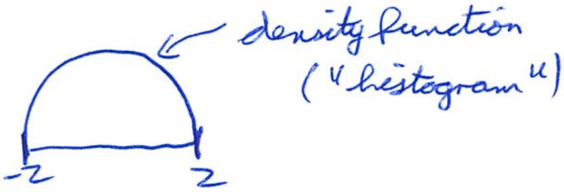
$k_p = \# \{ (x,y) \in \mathbb{F}_p : y^2 = x^3 + x + 1 \}$.

Let $t_p = p - k_p$.

Hasse's thm $\Rightarrow$ $|t_p| \leq 2\sqrt{p}$ for (suff. large) p.

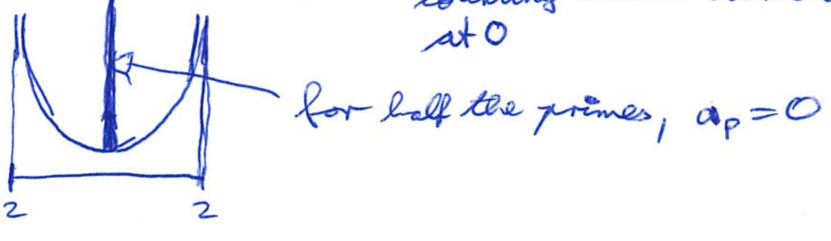
$\rightsquigarrow$ Let $a_p = \frac{t_p}{\sqrt{p}} \in [-2,2]$.

The sequence $(a_p)_p$ is equidistributed w.r.t. the measure $\frac{1}{2\pi}\sqrt{4-x^2}\,dx$.



If you do the same for the equation $y^2 = x^3 + 1$, the sequence is equidistributed w.r.t. the measure

$$\frac{1}{2\pi} \cdot \frac{1}{\sqrt{4-x^2}}\,dx + \underset{\substack{\uparrow \\ \text{counting measure (dirac delta)} \\ \text{at } 0}}{\frac{1}{2}\delta_0(x)\,dx}$$



What's going on?

$a_p = tr(M_p)$ for a particular 2x2-matrix $M_p \in G$,

$$\text{where } G = \begin{cases} SU(2), & y^2 = x^3+x+1 \text{ case} \\ N(U(1)), & y^2 = x^3+1 \text{ case} \end{cases}$$

$$\overset{\shortparallel}{} \left\{ \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix} \middle| u \in \mathbb{C}^\times, |u| = 1 \right\} \cup \left\{ \begin{pmatrix} 0 & u \\ -\bar{u} & 0 \end{pmatrix} \middle| \ldots \right\}$$

"The matrix M_p is equidistr. in G w.r.t. the Haar measure!"