ANALYTIC NUMBER THEORY

JULIA BRANDES

To be used with caution – likely to contain misprints!

Part 0. Preliminaries and recapitulation

0.1. Arithmetic functions and Dirichlet series

Let $\mathcal{A} = \{f : \mathbb{N} \to \mathbb{C}\}$ denote the set of arithmetic functions. Examples are

$\mathbb{1}(n) = 1$ for all $n \in \mathbb{N}$	the indicator function on $\mathbb{N}$
$d(n) = \#\{m \in \mathbb{N} : m \mid n\}$	the number of divisors of n,
$\varphi(n) = \#\{m \in [1, n] : (m, n) = 1\}$	the Euler totient function,
$\log n$	
$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, p \text{ prime}, k \in \mathbb{N} \\ 0, & \text{otherwise.} \end{cases}$	the von Mangoldt function.

For $f, g \in \mathcal{A}$ we define the (multiplicative) convolution

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

This convolution characterises the multiplicative structure of $\mathbb{N}$. Examples:

$$d = \mathbb{1} * \mathbb{1}, \qquad \log = \mathbb{1} * \Lambda.$$

One can also show

Lemma 0.1.1. *Together with the convolution and pointwise addition, $\mathcal{A}$ forms a commutative ring. The neutral element with respect to addition is the null function, and the neutral element with respect to multiplication is*

$$\varepsilon(n) = \begin{cases} 1 & n = 1 \\ 0 & \textit{else.} \end{cases}$$

Proof. Check. □

We now introduce an important class of arithmetic functions.

Definition 0.1.2. We say that an arithmetic function $f \neq 0$ is multiplicative if one has $f(mn) = f(m)f(n)$ for all coprime natural numbers m and n. We say that f is strictly multiplicative if the relation $f(mn) = f(m)f(n)$ holds for all pairs $m, n \in \mathbb{N}$. We denote the set of multiplicative functions by $\mathcal{M}$.

Obviously, multiplicative functions are completely determined by their values on prime powers. $\mathbb{1}$, ε, d, φ are multiplicative, whereas log and Λ are not.

Lemma 0.1.3. *(i) For every multiplicative function f we have $f(1) = 1$.*

(ii) The convolution of two multiplicative functions is multiplicative.
(iii) For every $f \in \mathcal{M}$ there exists $g \in \mathcal{M}$ with $f * g = \varepsilon$.
It follows that the multiplicative functions $(\mathcal{M}, *, \mathbb{1})$ form an abelian group.

Proof. (i) For every n we have $(n, 1) = 1$ and therefore $f(n \cdot 1) = f(n)f(1)$.
(ii) Let $f, g \in \mathcal{M}$ and set $h = f * g$. Let $(m, n) = 1$, then we have

$$h(mn) = \sum_{d|mn} f(d)g(mn/d).$$

Since $(m, n) = 1$, for every $d|mn$ there exist unique $a, b \in \mathbb{N}$ such that $ab = d$ and $a|m$, $b|n$ and $(a, b) = 1$. It follows that

$$\sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{a|m}\sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{a|m} f(a)g(m/a)\sum_{b|n} f(b)g(n/b).$$

(iii) Set $g(1) = 1$ and then inductively

$$g(p^k) = -\sum_{i=0}^{k-1} g(p^i)f(p^{k-i}).$$

By construction, this shows $f * g = \varepsilon$ on prime powers. By extending g multiplicatively to the whole of $\mathbb{N}$ we obtain the desired statement.

□

Definition 0.1.4. The inverse of $\mathbb{1}$ is given by the Möbius function μ. We have

$$\mu(p^k) = \begin{cases} -1, & \text{if } k = 1 \\ 0, & \text{if } k \geq 2. \end{cases}$$

Corollary 0.1.5. *We have the Möbius inversion formula: Let $f \in \mathcal{M}$ and write $F(n) = \sum_{d|n} f(n)$, then*

$$f(n) = \sum_{d|n} \mu(d)F(n/d).$$

Proof. $f = \varepsilon * f = (\mu * \mathbb{1}) * f = \mu * (\mathbb{1} * f) = \mu * F$. □

0.2. Dirichlet series: general properties

We now introduce a class of generating series for arithmetic functions.

Definition 0.2.1. Let $f \in \mathcal{A}$ and $s \in \mathbb{C}$, then the formal Dirichlet series $L(f, s)$ is given by

$$L(f, s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

We write $L(\mathbb{1}, s) = \zeta(s)$, the Riemann zeta function.

This choice of generating function respects the convolution.

Lemma 0.2.2. *Let $f, g \in \mathcal{M}$, then we have $L(f * g, s) = L(f, s)L(g, s)$.*

Proof. We have

$$L(f,s)L(g,s) = \sum_{m=1}^{\infty} \frac{f(m)}{m^s} \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)f(n)}{(mn)^s} = \sum_{r=1}^{\infty} \sum_{mn=r} \frac{f(m)f(n)}{r^s}$$
$$= \sum_{r=1}^{\infty} \frac{(f*g)(r)}{r^s} = L(f*g,s).$$

□

Lemma 0.2.3. *If $f \in \mathcal{M}$ and suppose that the series $L(f,s)$ converges absolutely for some $s \in \mathbb{C}$. Then we have*

$$L(f,s) = \prod_p \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}.$$

If f is even completely multiplicative, we have

$$L(f,s) = \prod_p \frac{1}{1 - f(p)p^{-s}}.$$

Proof. By the fundamental theorem of arithmetic we have

$$\prod_{p \le P} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} = \sum_{n : p|n \implies p \le P} \frac{f(n)}{n^s}.$$

For a given $\varepsilon > 0$ let now N be sufficiently large that

$$\sum_{n \ge N} \left| \frac{f(n)}{n^s} \right| < \varepsilon,$$

then

$$\left| L(f,s) - \prod_{p \le N} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \right| \le \sum_{n \ge N} \left| \frac{f(n)}{n^s} \right| < \varepsilon.$$

The second statement follows by the geometric series. □

0.3. Analytic properties of Dirichlet series

Unlike power series, which have a radius of convergence, Dirichlet series have an abscissa of convergence. Before embarking on our proof of this fact, we record here a useful analogue of integration by parts.

Lemma 0.3.1 (Partial Summation)**.** *Let $M \in \mathbb{N}$ and $N \in \mathbb{R}$ with $N > M$. Let further $g : [M,N] \mapsto \mathbb{C}$ be a continously differentiable function. For a complex-valued sequence (a_n) set*

$$A(t) = \sum_{M \le n \le t} a_n.$$

Then we have

$$\sum_{M \le n \le N} a_n g(n) = A(N)g(N) - \int_M^N A(t)g'(t)\mathrm{d}t.$$

Proof. Observe that

$$\begin{aligned} A(N)g(N) - \sum_{M\leq n\leq N} a_n g(n) &= \sum_{M\leq n\leq N} a_n(g(N)-g(n)) \\ &= \sum_{M\leq n\leq N} a_n \int_n^N g'(t)\mathrm{d}t \\ &= \int_M^N g'(t) \sum_{M\leq n\leq t} a_n \mathrm{d}t. \end{aligned}$$

This implies the statement. □

Remark 0.3.2. In the formulation of the Riemann–Stieltjes integral, partial summation can be viewed as integration by parts in the special case where one function is a step function. For two sequences a_n and b_n and integers M and N the formula reads

$$\sum_{n=M}^{N} a_n b_n = A(N)b_N - \sum_{n=M+1}^{N} A(n-1)(b_n - b_{n-1}),$$

and the proof is the same.

Here and for the rest of the lecture we adopt the convention $s = \sigma + it \in \mathbb{C}$.

Lemma 0.3.3. *Let $L(f,s)$ be a Dirichlet series. If $L(f,s)$ converges for some $s \in \mathbb{C}$, then it also converges for all $s' \in \mathbb{C}$ with $\sigma' > \sigma$. If $L(f,s)$ converges absolutely for some $s \in \mathbb{C}$, then it also converges uniformly for all $s' \in \mathbb{C}$ with $\sigma' > \sigma$.*

Proof. For absolute convergence the statement follows at once from $|n^s| = n^\sigma$. We thus focus on the statement for conditional convergence. By summation by parts we have

$$\begin{aligned} \sum_{M\leq n\leq N} \frac{f(n)}{n^s} &= \sum_{M\leq n\leq N} \frac{f(n)}{n^{s_0}} n^{s_0-s} \\ &= N^{s_0-s} \sum_{M\leq n\leq N} \frac{f(n)}{n^{s_0}} - \int_M^N \left(\sum_{M\leq n\leq \xi} \frac{f(n)}{n^{s_0}} \right) (s-s_0)\xi^{s_0-s-1}\mathrm{d}\xi \end{aligned}$$

For $\varepsilon > 0$ we choose M large enough such that by the Cauchy criterion

$$\left| \sum_{M\leq n\leq \xi} \frac{f(n)}{n^{s_0}} \right| < \varepsilon$$

for all $\xi > M$. Thus we have

$$\begin{aligned} \sum_{M\leq n\leq N} \frac{f(n)}{n^s} &\leq \varepsilon \left(N^{s_0-s} + |s-s_0| \int_M^N \xi^{s_0-s-1}\mathrm{d}\xi \right) \\ &\leq \varepsilon \left(N^{s_0-s} + \frac{|s-s_0|}{|\sigma-\sigma_0|}(M^{\sigma_0-\sigma} + M^{\sigma_0-\sigma}) \right) \\ &\leq \varepsilon \left(1 + 2\frac{|s-s_0|}{|\sigma-\sigma_0|} \right). \end{aligned}$$

For any fixed $s \in \mathbb{C}$ with $\sigma > \sigma_0$ we therefore obtain the desired result. Furthermore, in the sector

$$G_H = \{s \in \mathbb{C} : \sigma > \sigma_0, |t - t_0| \leq H|\sigma - \sigma_0|\}$$

we even have uniform convergence, since

$$|s - s_0| \leq |\sigma - \sigma_0| + |t - t_0| \leq (H + 1)|\sigma - \sigma_0|.$$

□

Corollary 0.3.4. *Suppose $L(f, \sigma) = L(g, \sigma)$ for all sufficiently large σ. Then the arithmetic functions f and g agree.*

Proof. Since the Dirichlet series converge uniformly, we can swap the limit and the sum and obtain

$$f(1) = \sum_{n=1}^{\infty} f(n) \lim_{\sigma\to\infty} n^{-\sigma} = \lim_{\sigma\to\infty} L(f, \sigma) = \lim_{\sigma\to\infty} L(g, \sigma) = \sum_{n=1}^{\infty} g(n) \lim_{\sigma\to\infty} n^{-\sigma} = g(1).$$

Suppose we have already shown that $f(i) = g(i)$ for $1 \leq i \leq k - 1$. Then

$$f(k) = \sum_{n=k}^{\infty} f(n) \lim_{\sigma\to\infty} (k/n)^{\sigma} = \sum_{n=k}^{\infty} g(n) \lim_{\sigma\to\infty} (k/n)^{\sigma} = g(k).$$

This shows the statement. □

We write

$$\sigma_0(f) = \inf\{\sigma : L(f, s) \text{ converges}\}$$

for the abscissa of convergence, and

$$\sigma_a(f) = \inf\{\sigma : L(f, s) \text{ converges absolutely}\}$$

for the abscissa of absolute convergence. We will often suppress the dependence on f.

Lemma 0.3.5. *Let $f \in \mathcal{A}$, then we have $\sigma_0(f) \leq \sigma_a(f) \leq \sigma_0(f) + 1$.*

Proof. The first inequality is trivial. For the second one, observe that the convergence of $L(f, \sigma_0 + \varepsilon)$ implies that $|f(n)| \leq n^{\sigma_0+\varepsilon}$ for all large n, and hence

$$\left|\sum_{n\geq n_0} \frac{f(n)}{n^{\sigma_0+1+2\varepsilon}}\right| \leq \sum_{n\geq n_0} \frac{|f(n)|}{n^{\sigma_0+1+2\varepsilon}} \leq \sum_{n\geq n_0} n^{-1-\varepsilon} < \infty.$$

□

For instance, $\sigma_0(\mathbb{1}) = \sigma_a(\mathbb{1}) = 1$. If $a(n) = (-1)^n$, then $\sigma_0(a) = 0$ and $\sigma_a(a) = 1$.

Part I. The prime number theorem

I.1. Perron's formula

Let f be an arithmetic function, and $S_f(x) = \sum_{n\leq x} f(n)$ its summatory function. Then $S_f(x)$ can be connected with the Dirichlet series $L(f, s)$ via a Fourier-type identity.

Theorem I.1.1. *We have*

$$\frac{L(f,s)}{s} = \int_1^\infty \frac{S_f(x)}{x^s}\frac{\mathrm{d}x}{x}$$

for all $s \in \mathbb{C}$ *having* $\sigma > \max\{\sigma_0(f), 0\}$.

Proof. Summation by parts: For large N we have

$$\sum_{n=1}^{N} \frac{f(n)}{n^s} = \frac{S_f(N)}{N^s} + s\int_1^N \frac{S_f(x)}{x^s}\frac{\mathrm{d}x}{x}. \tag{I.1.1}$$

The result follows now on taking $N \to \infty$. If $\sigma_0(f) < 0$, it follows from the definition of the abscissa of convergence that

$$\lim_{x\to\infty} S_f(x) = L(f,0) < \infty,$$

so the first term vanishes in the limit. If $\sigma_0 \geq 0$, then by an argument as in the proof of Lemma 0.3.3 we see

$$S_f(x) = \sum_{n\leq x} \frac{f(n)}{n^\sigma} n^\sigma = x^\sigma \sum_{n\leq x} \frac{f(n)}{n^\sigma} + \sigma\int_1^x \left(\sum_{n\leq t} \frac{f(n)}{n^\sigma}\right) t^{\sigma-1}\mathrm{d}t \ll x^\sigma$$

for any $\sigma > \sigma_0$, so it follows that

$$\sigma_0(f) \geq \limsup \frac{\log S_f(x)}{\log x}, \tag{I.1.2}$$

and by consequence the first term in (I.1.1) vanishes in this case as well. □

As a by-product of this argument we get an easy formula for the abscissa of convergence.

Corollary I.1.2. *When* $\sigma_0 > 0$ *the inequality in* (I.1.2) *is even an equality.*

Proof. Write for simplicity τ for the expression on the right hand side. We have already shown $\sigma_0(f) \leq \tau$. The opposite inequality follows easily from the observation that for any σ satisfying $\tau < \sigma < \sigma_0(f)$ the left hand side of (I.1.1) diverges whereas the right hand side converges, so the interval must be empty. □

It is the converse statement to Theorem I.1.1 which we are mainly interested in. The proof rests on Perron's formula. With future applications in mind, we present a quantitative version.

Theorem I.1.3 (Perron's Formula)**.** *Let* c *and* y *be positive real numbers. We have*

$$\frac{1}{2\pi i}\int_{c+i\mathbb{R}} y^s \frac{\mathrm{d}s}{s} = \begin{cases} 0 & \text{if } y < 1, \\ 1/2 & \text{if } y = 1, \\ 1 & \text{if } y > 1. \end{cases} \tag{I.1.3}$$

More exactly, if the right hand side of (I.1.3) *is denoted by* $\delta(y)$*, we have for every* $T > 0$ *the relation*

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s\frac{\mathrm{d}s}{s} - \delta(y)\right| \ll \begin{cases} cT^{-1} & \text{if } y = 1, \\ \min\left\{y^c, \frac{y^c}{T|\log y|}\right\} & \text{otherwise.} \end{cases}$$

Proof. In the case $y = 1$ we have

$$\frac{1}{2\pi}\int_{-T}^{T}\frac{\mathrm{d}t}{c+it} = \frac{1}{2\pi}\int_{0}^{T}\frac{1}{c+it}+\frac{1}{c-it}\mathrm{d}t = \frac{1}{\pi}\int_{0}^{T}\frac{c}{c^2+t^2}\mathrm{d}t = \frac{1}{2}-\frac{1}{\pi}\int_{T/c}^{\infty}\frac{\mathrm{d}\xi}{1+\xi^2}.$$

This shows the claim in this case.

Consider now the case $y > 1$, and let $r < -1$. We consider the integral

$$\int_W y^s\frac{\mathrm{d}s}{s},$$

where W denotes the boundary of the rectangle with corners $c \pm iT$ and $r \pm iT$. The function y^s/s is meromorphic and has a simple pole at $s = 0$ with residue 1. By Cauchy's integral theorem we find

$$\int_W y^s\frac{\mathrm{d}s}{s} = 1$$

This implies

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s\frac{\mathrm{d}s}{s} = 1 + O\left(\int_{c+iT}^{r+iT} y^s\frac{\mathrm{d}s}{s}+\int_{c-iT}^{r-iT} y^s\frac{\mathrm{d}s}{s}+\int_{r-iT}^{r+iT} y^s\frac{\mathrm{d}s}{s}\right).$$

For $\sigma < -1$ we have $|y^s/s| \le y^\sigma/|\sigma| \le 1/|\sigma|$ since $y > 1$. By taking the limit $r \to \infty$, the last term in the error vanishes. For the other two terms we observe that

$$\left|\int_{c+iT}^{-\infty+iT} y^s\frac{\mathrm{d}s}{s}\right| \ll \int_{-\infty}^{c}\frac{y^\sigma}{T}\mathrm{d}\sigma \ll \frac{y^c}{T\log y}.$$

In order to derive the alternative bound, we consider the circle C centered at the origin and with radius $R = \sqrt{c^2+T^2}$. Denote by C_1 the sector running from $c+iT$ clockwise to $c-iT$, then by Cauchy's integral theorem again we find

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s\frac{\mathrm{d}s}{s} = 1 + O\left(\int_{C_1} y^s\frac{\mathrm{d}s}{s}\right).$$

Since for $s \in C_1$ we have $|y^s/s| \le |y^\sigma|/R \le y^c/R$ and the arc length grows proportionally with R, the result follows.

For $0 < y < 1$ the result is proved in the same way. Here we take $r > 1$ in the rectangle, and use the circle sector $C_2 = C \setminus C_1$. Then there are no poles inside the path of integration, and the estimates work in the same way.

□

We can now establish the inverse transform to Theorem I.1.1.

Theorem I.1.4. *Recall the notation from Theorem I.1.1, and set $S'_f(x) = S_f(x)$ whenever $x \notin \mathbb{N}$, and $S'_f(x) = S_f(x-1) + \frac{1}{2}f(x)$ for integer values x. For every $c > \max\{0, \sigma_a(f)\}$ we have*

$$S'_f(x) = \frac{1}{2\pi i}\int_{(c)} L(f,s)x^s\frac{\mathrm{d}s}{s}.$$

More precisely, we have

$$\left|S'_f(x) - \frac{1}{2\pi i}\int_{c-iT}^{c+iT} L(f,s)x^s\frac{\mathrm{d}s}{s}\right| \ll \frac{x^c}{T}L(f,c) + \left(1+\frac{x\log x}{T}\right)\max_{\substack{x/2<n<2x\\ n\neq x}}|f(n)|.$$

Proof. Since the Dirichlet series converges absolutely at $s = c + it$ for all t, we have

$$\sum_{n=1}^{\infty} f(n) \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^s \frac{\mathrm{d}s}{s} = \int_{c-iT}^{c+iT} x^s \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \frac{\mathrm{d}s}{s} = \int_{c-iT}^{c+iT} L(f,s) x^s \frac{\mathrm{d}s}{s}.$$

On the other hand, Perron's formula implies that on the left hand side of the above equation any value $f(n)$ is counted only if $n < x$, and with half weight when $n = x$. More precisely, we obtain

$$\begin{aligned}\frac{1}{2\pi i} \int_{c-iT}^{c+iT} L(f,s) x^s \frac{\mathrm{d}s}{s} &= \sum_{n=1}^{\infty} \frac{f(n)}{2\pi i} \int_{c-iT}^{c+iT} \left(\frac{x}{n}\right)^s \frac{\mathrm{d}s}{s} \\ &= S_f'(x) + O\left(\frac{1}{T} + \sum_{n=1}^{\infty} |f(n)| \min\left\{(x/n)^c, \frac{(x/n)^c}{T\,|\log x/n|}\right\}\right).\end{aligned}$$

Note that in the limit $T \to \infty$ the error term tends to zero.

The problematic term in the error is $|\log x/n|^{-1}$. For $x/n \notin [1/2, 2]$ this expression is bounded below by an absolute constant, so we have

$$\sum_{n<x/2 \text{ or } n>2x} |f(n)| \min\left\{(x/n)^c, \frac{(x/n)^c}{T\,|\log x/n|}\right\} \ll \frac{x^c}{T} \sum_n \frac{|f(n)|}{n^c}.$$

In order to bound the remaining range, we observe that $n/x = 1 + (n-x)/x$ and that $\log(1+a) \asymp a$ for $-1/2 \le a \le 1$. Thus $|\log x/n|^{-1} \ll \frac{x}{|n-x|}$. It follows that the contribution from these terms is bounded above by

$$\sum_{\substack{x/2<n<2x \\ n\neq x}} |f(n)| \min\{1, \frac{x}{T|n-x|}\}.$$

Bounding the entries of the sequence by their maximum, we can argue further. We have

$$\begin{aligned}\sum_{\substack{x/2<n<2x \\ n\neq x}} \min\{1, \frac{x}{T|n-x|}\} &\ll 2x/T + \sum_{x/2 \le n < x(1-\frac{1}{T})} \frac{x}{T|n-x|} + \sum_{x(1+\frac{1}{T})<n\le 2x} \frac{x}{T|n-x|} \\ &\ll \frac{x \log x}{T}.\end{aligned}$$

Observe also that we can replace $S_f'(x)$ by $S_f(x)$ as the error is $O(1)$ and can be absorbed in the error term. □

I.2. The Mellin transform in context

The theory of arithmetic functions and Dirichlet series, culminating in statements like those of Theorems I.1.1 and I.1.4, have a great similarity to the theory of power series, additive convolution and the Fourier transform and its inversion.

In fact, Dirichlet series and power series can be put into relation as well. For an arithmetic function we have the power series

$$P_f(x) = \sum_{n=1}^{\infty} f(n) x^n,$$

and it is clear that in the region of convergence we have

$$P_f(e^y) = \sum_{n=1}^{\infty} f(n)e^{-yn} = \sum_{n=1}^{\infty} (f \circ \log)(e^n)(e^n)^{-y}.$$

Heuristically, substituting $m = e^n$, this bears some resemblance to the Dirichlet series related to the function $f \circ \log$. This affinity is the underlying reason of why Dirichlet series respect the multiplicative convolution.

Over $\mathbb{Z}$ this analogy reaches only so far, since the change of variables is not an automorphism of $\mathbb{N}$. However, the continuous analogues can be related in this way. Recall the definitions of the Fourier transform

$$\mathcal{F}f(t) = \int_{-\infty}^{\infty} f(x)e^{-2\pi ixt}\mathrm{d}x \qquad \mathcal{F}^{-1}F(x) = \int_{-\infty}^{\infty} F(x)e^{2\pi ixt}\mathrm{d}t$$

and the two-sided Laplace transform

$$\mathcal{L}f(t) = \int_{0}^{\infty} f(x)e^{-xt}\mathrm{d}x \qquad \mathcal{L}^{-1}F(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} F(x)e^{xt}\mathrm{d}t.$$

The formal relation

$$\mathcal{F}f(t) = \mathcal{L}f(2\pi it)$$

is immediate from the definition. For a function f, the Mellin transform (after Hjalmar Mellin, Finland) is defined as

$$\mathcal{M}f(s) = \int_{0}^{\infty} f(x)x^s\frac{\mathrm{d}x}{x},$$

and its inverse is given by

$$\mathcal{M}^{-1}f(x) = \int_{c-i\infty}^{c+i\infty} F(s)x^{-s}\mathrm{d}s,$$

where c lies in the region of convergence. An important example is the Gamma function

$$\Gamma(s) = \int_{0}^{\infty} e^{-x}x^s\frac{\mathrm{d}x}{x},$$

which is by definition the Mellin transform of e^{-x}, and one has the converse transform

$$e^{-y} = \int_{c-i\infty}^{c+i\infty} \Gamma(s)x^{-s}\mathrm{d}s.$$

The Mellin transform can be expressed in terms of the Laplace trancform. In the region of convergence, we have

$$\mathcal{L}(f \circ \exp)(-s) = \int_{-\infty}^{\infty} f(e^x)e^{xs}\mathrm{d}x = \int_{0}^{\infty} f(y)y^s\frac{\mathrm{d}y}{y} = \mathcal{M}f(s).$$

In this language, Theorem I.1.1 asserts that $L(f, s)$ is the Mellin transform of $S_f(1/x)$, and Theorem I.1.4 establishes the inverse statement of this. It follows that at least for real variables these theorems could also have been proved using just the

normal Fourier transform. In fact, taking $g(x) = S_f(e^{2\pi x})e^{-2\pi\sigma s}$ for some suitably large σ Theorem I.1.1 shows that

$$\begin{aligned} G(t) = \widehat{g}(t) &= \int_{\mathbb{R}} S_f(e^{2\pi x})e^{-2\pi\sigma x}e^{-2\pi ixt}\mathrm{d}x \\ &= \int_{\mathbb{R}} S_f(e^{2\pi x})e^{-2\pi sx}\mathrm{d}x = \frac{1}{2\pi}\int_0^\infty S_f(y)y^{-s}\mathrm{d}y = \frac{L(f,\sigma+it)}{2\pi(\sigma+it)}. \end{aligned}$$

We can now compute the Fourier inverse transform. Thus

$$\begin{aligned} \widehat{G}(x) &= \int_{\mathbb{R}} \frac{L(f,\sigma+it)}{2\pi(\sigma+it)}e^{2\pi itx}\mathrm{d}t = \frac{1}{2\pi i}\int_{(\sigma)} \frac{L(f,s)}{s}e^{2\pi(s-\sigma)x}\mathrm{d}s \\ &= e^{-2\pi i\sigma x}\frac{1}{2\pi i}\int_{(\sigma)} \frac{L(f,s)}{s}e^{2\pi sx}\mathrm{d}s. \end{aligned}$$

However, by the Fourier inversion theorem we have $\widehat{G}(x) = g(x)$, so this expression must be equal to $S_f(e^{2\pi x})e^{-2\pi\sigma s}$. It follows that

$$S_f(e^{2\pi x}) = \frac{1}{2\pi i}\int_{(\sigma)} \frac{L(f,s)}{s}e^{2\pi sx}\mathrm{d}s,$$

which after a change of variables recovers the statement of Theorem I.1.4 for non-integral x, and in the integer case the desired result follows after setting the Fourier transform equal to the mean of the upper and lower limits as usual.

I.3. Back to primes

We would like to apply the results of the previous section to the indicator function of the primes. The associated Dirichlet series is given by

$$L(\mathbb{1}_{\text{primes}}, s) = \sum_p \frac{1}{p^s},$$

and this can be related to $\zeta(s)$.

Lemma I.3.1. *For $\sigma > 1$ we have*

$$\log\zeta(s) = \sum_p \frac{1}{p^s} + O(1).$$

Proof. By the Euler product formula (Lemma 0.2.3) we have

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

for $\sigma > 1$, and thus

$$\log\zeta(s) = \sum_p \log\frac{1}{1-p^{-s}} = -\sum_p \log(1-p^{-s}) = \sum_p\sum_{k=1}^\infty \frac{p^{-ks}}{k}. \tag{I.3.1}$$

The contribution from $k = 1$ yields the desired expression, and for larger k we have

$$\sum_{k=2}^\infty \frac{-p^{k\sigma}}{k} \le \frac{1}{p^{2\sigma}}(1 + \frac{1}{p^\sigma} + \frac{1}{p^{2\sigma}} + \dots) = \frac{1}{p^{2\sigma}}\frac{1}{1-p^{-\sigma}} \le \frac{1}{2p^{2\sigma}}.$$

For $\sigma > 1$ this is smaller than $1/2p^2$, so altogether we find

$$\log \zeta(s) = \sum_p \left(\frac{1}{p^s} + O\left(\frac{1}{p^2} \right) \right) = \sum_p \frac{1}{p^s} + O(1).$$

□

Thus, in order to understand the primes, we need to understand the Riemann zeta function better, in particular its singularity at 1. It turns out that $\zeta(s)$ can be extended to the domain $\sigma > 0$. We will use the Gauss bracket $[x]$ to denote the largest integer not exceeding x and write $\{x\} = x - [x]$ for the fractional part of x. The following lemma will be stated in a more general version than what is needed at this point in order to save work later on.

Lemma I.3.2. *Suppose that M is an integer and $\sigma > 1$. Then we have*

$$\sum_{n=M}^{\infty} \frac{1}{n^s} = \frac{s}{s-1} + (1-M)M^{-s} - s\int_M^{\infty} \{x\} x^{-s-1} \mathrm{d}x.$$

Corollary I.3.3. *Suppose that $\sigma > 1$. For any integer $N > M$ we have*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \{x\} x^{-s-1} \mathrm{d}x.$$

In particular, ζ can be meromorphically continued to the entire right half plane. It has a simple pole at 1 with residue 1.

Proof. We apply partial summation. We have

$$\begin{aligned}
\sum_{n=M}^{N} \frac{1}{n^s} &= N^{-s}(N-M+1) + s\int_M^N ([t]-M+1)t^{-s-1}\mathrm{d}t \\
&= N^{-s}(N-M+1) + s\int_M^N t^{-s}\mathrm{d}t - (M-1)s\int_M^N t^{-s-1}\mathrm{d}t - s\int_M^N \{t\}t^{-s-1}\mathrm{d}t \\
&= N^{-s}(N-M+1) + \frac{s}{1-s}(N^{1-s}-M^{1-s}) + (M-1)(N^{-s}-M^{-s}) \\
&\qquad - s\int_M^N \{t\}t^{-s-1}\mathrm{d}t.
\end{aligned}$$

For $\sigma > 1$ we can take the limit $N \to \infty$ and obtain

$$\zeta(s) = \frac{s}{s-1}M^{1-s} + (1-M)M^{-s} - s\int_M^{\infty} \{x\} x^{-s-1}\mathrm{d}x$$

as stated.

The corollary follows on setting $M = 1$ and observing that the last integral converges for all $\sigma > 0$. By the identity theorem of harmonic analysis, it follows that $\zeta(s)$ can be continued to the entire right half plane. □

This result implies that $\log \zeta$ has a logarithmic singularity at 1, which makes it somewhat hard to work with. By differencing $\log \zeta$ with respect to s, these singularities can be converted to 'normal' poles. For $\sigma > 1$ we obtain

$$\frac{\zeta'}{\zeta}(s) = \frac{\mathrm{d}}{\mathrm{d}s}\log\zeta(s) = \frac{\mathrm{d}}{\mathrm{d}s}\sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k} = -\sum_p \sum_{k=1}^{\infty} \frac{\log p}{p^{ks}} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

By Theorem I.1.4 this implies that

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = -\frac{1}{2\pi i} \int_{(c)} \frac{\zeta'}{\zeta}(s) x^s \frac{\mathrm{d}s}{s} \tag{I.3.2}$$

for any $c > 1$. Thus, in order to prove the prime number theorem it suffices to understand the integral on the right hand side of (I.3.2).

In order to deduce a quantitative version of the prime number theorem, we need to employ the quantitative version of Theorem I.1.4. It follows therefore that for arbitrary $c > 1$ and T large we have

$$\begin{aligned}\psi(x) &= -\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\zeta'}{\zeta}(s) x^s \frac{\mathrm{d}s}{s} + O\left(\frac{x^c}{T} L(\Lambda, c) + \left(1 + \frac{x \log x}{T}\right) \max_{\substack{x/2<n<2x \\ n \neq x}} |\Lambda(n)| \right) \\ &= -\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\zeta'}{\zeta}(s) x^s \frac{\mathrm{d}s}{s} + O\left(\frac{x^c}{T} \left| \frac{\zeta'}{\zeta}(c) \right| + \log x + \frac{x (\log x)^2}{T} \right).\end{aligned}$$

We treat the first integral by the residue theorem. Take $0 < c' < 1$ and T such that ζ has no zeros inside the rectangle given by $c \pm iT$ and $c' \pm iT$, and consider the oriented paths

$$\gamma_1 = [c + iT, c' + iT], \qquad \gamma_2 = [c' + iT, c' - iT], \qquad \gamma_3 = [c' - iT, c - iT].$$

We have

$$\operatorname*{res}_{s=1} \frac{\zeta'}{\zeta}(s) \frac{x^s}{s} = -x,$$

and thus

$$-\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\zeta'}{\zeta}(s) x^s \frac{\mathrm{d}s}{s} = 2\pi i x + O(E_1 + E_2 + E_3),$$

where

$$E_i = \int_{\gamma_i} \frac{\zeta'}{\zeta}(s) x^s \frac{\mathrm{d}s}{s}.$$

It follows that

$$\psi(x) = x + O\left(\frac{x^c}{T} \left| \frac{\zeta'}{\zeta}(c) \right| + \log x + \frac{x (\log x)^2}{T} + E_1 + E_2 + E_3 \right).$$

The key to proving the prime number theorem is therefore to obtain good upper bounds for the integrals E_1, E_2 and E_3. In particular, we need to show in some domain to the right of 1 that $\zeta(s)$ is bounded below – in particular, has no zeros – and that $\zeta'(s)$ is bounded above.

I.4. A zero-free region of $\zeta(s)$

In order to achieve this, we will proceed as follows. Suppose that we are able to prove that ζ has no zeros on the line $\sigma = 1$. Then, if the derivative is small in absolute value, ζ cannot decrease too rapidly as σ is moved to the left. We should thus obtain a small zero-free region to the left of the line $\sigma = 0$ that will serve our purposes.

We start by bounding ζ and ζ' above.

Lemma I.4.1. *In the domain $|t| \geq 8$ and $1 - \frac{1}{2\log|t|} \leq \sigma \leq 2$ we have the estimates*

$$\zeta(s) \ll \log|t|, \qquad \zeta'(s) \ll (\log|t|)^2.$$

Furthermore, for $1/2 < \sigma < 2$ we have

$$\zeta(\sigma) \ll (\sigma - 1)^{-1}.$$

Proof. The second estimate follows directly from the identity in Corollary I.3.3.

For all $1 - \frac{1}{\log|t|} \leq \sigma \leq 3$ and all $n \leq t$ we have $n^{-\sigma} \leq en^{-1}$. By Lemma I.3.2 above with $N = [t]$ it follows that

$$\zeta(s) \ll \sum_{n \leq t} \frac{1}{n} + \frac{t^{1-\sigma}}{|s-1|} \ll \log t + t^{-\sigma} \ll \log t.$$

For the second estimate we use Cauchy's integral formula with

$$|\zeta'(s)| = \frac{1}{2\pi i} \int_{|s-w|=r} \frac{\zeta(w)}{(w-s)^2} \mathrm{d}s \ll \log t \int_{|s-w|=r} \frac{\mathrm{d}r}{r^2} \ll \frac{\log t}{r}.$$

This is certainly legitimate for s as in the statement of the lemma and r sufficiently small, and one can check that taking $r = (2\log t)^{-1}$ is an acceptable choice. □

Lemma I.4.2. *We have $\zeta(1 + it) \neq 0$ for all $t \in \mathbb{R}$.*

More precisely, for $|t| \geq 8$ and $1 - \delta(\log|t|)^{-9} < \sigma < 2$ we have

$$\zeta(s) \gg (\log|t|)^{-7}.$$

Proof. From (I.3.1) we have in $\sigma > 1$ the relation

$$\zeta(s) = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k}\right)$$

and thus

$$|\zeta(s)| = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{p^{-k\sigma}}{k} \cos(kt \log p)\right).$$

Observe that

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

for all $\alpha \in \mathbb{R}$. Setting $\alpha_{k,p} = kt \log p$ yields therefore

$$\zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{p^{-k\sigma}}{k} (3 + 4\cos\alpha_{k,p} + \cos 2\alpha_{k,p})\right) \geq 1.$$

In particular, we have

$$\lim_{\sigma \searrow 1} \zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \geq 1. \tag{I.4.1}$$

Now suppose that $\zeta(1 + it_0) = 0$ for some $t_0 \neq 0$. Then we have

$$\lim_{\sigma \searrow 1} \zeta(\sigma)^3 |\zeta(\sigma + it_0)|^4 = 0,$$

so (I.4.1) can only be satisfied if $\zeta(s)$ has a pole at $s = 1 + 2it_0$. However, this contradicts the first statement of Lemma I.4.1.

More precisely, using the bounds of Lemma I.4.1 we see that

$$\left|\frac{1}{\zeta(\sigma+it)}\right| \leq \zeta(\sigma)^{3/4}|\zeta(\sigma+2it)|^{1/4} \leq C_1(\sigma-1)^{-3/4}(\log|t|)^{1/4}$$

for any $1<\sigma<2$ and some suitable constant C_1. On the other hand, for $t\geq 8$ and $0<\eta<\frac{1}{2\log t}$ we have

$$|\zeta(1-\eta+it)-\zeta(1+\eta+it)| \leq \int_{1-\eta}^{1+\eta}|\zeta'(u+it)|\mathrm{d}u \leq C_2\eta(\log|t|)^2$$

for some C_2. Altogether, we find that

$$\begin{aligned}|\zeta(1-\eta+it)| &\geq |\zeta(1+\eta+it)| - C_2\eta(\log|t|)^2\\ &\geq C_1\eta^{3/4}(\log|t|)^{-1/4} - C_2\eta(\log|t|)^2.\end{aligned}$$

We have $\eta^{3/4}(\log|t|)^{-1/4} \asymp \eta(\log|t|)^2$ if $\eta \asymp \log|t|^{-9}$. Thus, if we fix A such that $\delta = A^{3/4}C_1 - AC_2 > 0$ and set $\eta = A(\log|t|)^{-9}$, then the above is bounded below by $\delta(\log|t|)^{-7}$. □

Corollary I.4.3. *In $t\geq 8$ and $1-\delta(\log|t|)^{-9}<\sigma<2$ we have*

$$\frac{\zeta'}{\zeta}(s) \ll (\log|t|)^9.$$

Proof. This follows upon combining Lemmata I.4.1 and I.4.2. □

I.5. Conclusion of the proof

It remains to employ the bounds of the previous section to estimate the contribution from the integrals E_1, E_2 and E_3. Recall that

$$E_1 = \int_{c+iT}^{c'+iT}\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\mathrm{d}s,$$

where $c>1$ is arbitrary and $0<c'<1$ is to be chosen such that the integrand has no zeros inside the rectangle given by the points $c\pm iT$ and $c'\pm iT$. By Corollary I.4.3 we may set $c=1+\eta$ and $c'=1-\eta$, where

$$\eta = \frac{\delta}{2}(\log T)^{-9}$$

for a suitable constant δ. On the path of integration we have $|s|\geq T$ and $|x^s| = x^\sigma \leq x^{1+\eta}$. Furthermore, Corollary I.4.3 shows that $(\zeta'/\zeta)(s)\ll 1/\eta$. We thus obtain

$$\begin{aligned}E_1 &\ll \int_{1-\eta}^{1+\eta}\left|\frac{\zeta'}{\zeta}(\sigma+iT)\right|\frac{x^\sigma}{T}\mathrm{d}\sigma\\ &\ll (2\eta)\frac{1}{\eta}\frac{x^{1+\eta}}{T} \ll \frac{x^{1+\eta}}{T}.\end{aligned}$$

Obviously, the same argument shows $E_3 \ll T^{-1}x^{1+\eta}$ for the integral over the path $[1-\eta-iT, 1+\eta-iT]$.

It remains to understand the integral

$$E_2 = \int_{1-\eta+iT}^{1-\eta-iT}\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\mathrm{d}s.$$

On this path we have $|s| \geq \frac{1}{2}(1+|t|)$, so we obtain

$$E_2 \ll \int_{-T}^{T} \left|\frac{\zeta'}{\zeta}(s)\right| x^{1-\eta} \frac{\mathrm{d}t}{1+|t|}.$$

For $|t| \geq 8$ we have $\left|\frac{\zeta'}{\zeta}(s)\right| \ll (\log T)^9$ by Corollary I.4.3. For the smaller t we recall the bound

$$\zeta(s) = \frac{s}{s-1} + s\int_1^\infty \{x\} x^{-s-1}\mathrm{d}x \gg \frac{1}{|s-1|}$$

coming from Corollary I.3.3 and remark that differentiating yields

$$\zeta'(s) = \frac{1}{s-1^2} + \int_1^\infty \{x\} x^{-s-1}\mathrm{d}x + s\int_1^\infty \{x\} x^{-s-1}\log x \mathrm{d}x,$$

so $\zeta'(s) \ll |s-1|^{-2}$ as $s \to 1$. It follows that $\left|\frac{\zeta'}{\zeta}(s)\right| \ll \frac{1}{|s-1|} \ll \frac{1}{(\log T)^{-9}}$ by recalling the zero-free region of $\zeta(s)$ of Lemma I.4.2. We therefore find

$$E_2 \ll x^{1-\eta}(\log T)^9 \int_{-T}^{T} \frac{\mathrm{d}t}{1+|t|} \ll x^{1-\eta}(\log T)^{10}.$$

Our combined error is now

$$\begin{aligned}\psi(x) - x &\ll \frac{x^{1+\eta}}{T}\left|\frac{\zeta'}{\zeta}(1+\eta)\right| + \log x + \frac{x(\log x)^2}{T} + \frac{x^{1+\eta}}{T} + x^{1-\eta}(\log T)^{10} \\ &\ll \frac{x^{1+\eta}(\log T)^9}{T} + \log x + \frac{x(\log x)^2}{T} + x^{1-\eta}(\log T)^{10}.\end{aligned}$$

We optimise by comparing the first error term with the last one. These two terms are roughly of the same order of magnitude (up to logarithms) if

$$\frac{x^{1+\eta}}{T} = x^{1-\eta},$$

or

$$T = x^{2\eta} = \exp\left(\delta(\log T)^{-9}\log x\right).$$

Taking logarithms, we see that this is satisfied if

$$\log T = (\delta \log x)^{1/10}.$$

This choice of T implies

$$\eta = \frac{\delta}{2}(\delta\log x)^{-9/10}.$$

Hence the last error term is

$$\begin{aligned}x^{1-\eta}(\log T)^{10} &= x\exp(-\eta\log x)(\delta\log x) \\ &\ll x\exp\left(-\frac{\delta}{2}(\delta\log x)^{-9/10}\log x\right)\log x \ll x\exp\left(-c(\log x)^{1/10}\right)\end{aligned}$$

for some $c < (1/2)\delta^{1/10}$. In the last step we used that the exponential grows faster than any power of logarithm.

By construction, the first error term is also of this shape, and it is clear that the other two are smaller. Thus we have proved a quantitative version of the prime number theorem.

Theorem I.5.1 (Prime Number Theorem)**.** *There exists a positive parameter c such that*

$$\Psi(x) = x + O\left(xe^{-c(\log x)^{1/10}}\right),$$

or, equivalently,

$$\pi(x) = \operatorname{li} x + O\left(xe^{-c(\log x)^{1/10}}\right),$$

where

$$\operatorname{li} x = \int_2^x \frac{\mathrm{d}t}{\log t} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \cdots + (k-1)!\frac{x}{(\log x)^k} + O\left(\frac{x}{(\log x)^{k+1}}\right)$$

for any $k \in \mathbb{N}$.

The exponent $1/10$ stems from the size of the zero-free region $\sigma \geq 1 - \delta(\log t)^{1/9}$. This zero-free region has been obtained via the cosine identity, so it is a natural question if a different cosine identity would yield better results. In fact, there is no reason why the identity should be based on a quadratic polynomial, as higher degrees are also thinkable. However, there are a few constraints. It is necessary that the coefficient of the absolute term be larger than that of the linear one, and that all coefficients be positive, for otherwise there would be no contradiction. In §65 of his textbook from 1909, Landau[1] gives a detailed discussion of this issue. He comes to the conclusion that without further ideas this method cannot yield error terms better than $O\left(x\exp(-c(\log x)^{1/7})\right)$, and finds an example with $O\left(x\exp(-c(\log x)^{1/(2+\gamma)})\right)$ where

$$\gamma = 2 + \frac{16\pi}{9\sqrt{3}} \approx 5.2245\ldots.$$

Already in 1899, a mere three years after his proof of the PNT, de la Vallée-Poussin applied more advanced methods to establish a zero-free region of the shape $\sigma \geq 1 - \delta(\log t)^{-1}$, yielding an error of $O\left(x\exp(-c(\log x)^{1/2})\right)$. This is the error recorded in most textbooks. The best zero-free region to date is $1-\sigma \leq \delta(\log t)^{-2/3}(\log\log t)^{1/3}$, which yields the error term $O\left(x\exp(-c(\log x)^{3/5}/(\log\log x)^{1/5})\right)$ with an explicitly computed constant c.

I.6. Sketch of Riemann's ideas

The version of the prime number theorem we proved is a simplified one, and in fact Riemann's original ideas reached significantly further. We will briefly sketch some of his main ideas here.

Recall the Gamma function

$$\Gamma(s) = \int_0^\infty e^{-t}t^s\frac{\mathrm{d}t}{t}.$$

This function is a priori defined in $\sigma > 0$, but can be continued to the entire complex plane by the relation $\Gamma(s+1) = s\Gamma(s)$. We also define the theta series

$$\Theta(x) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}, \qquad \omega(x) = \sum_{n=1}^\infty e^{-\pi n^2 x} = (1/2)(\Theta(x) - 1),$$

[1]Handbuch der Lehre von der Verteilung der Primzahlen. Erster Band, Second Edition. Chelsea Publishing Company, New York, 1953

and state its functional equation

$$\Theta(1/x) = \sqrt{x}\Theta(x) \qquad \omega(1/x) = -1/2 + (1/2)\sqrt{x} + \sqrt{x}\omega(x).$$

Thus with the substitution $t = \pi n^2 y$ we have

$$\Gamma(s/2) = \int_0^\infty e^{-\pi n^2 y}(\pi n^2 y)^{s/2-1}\pi n^2 \mathrm{d}y,$$

and thus

$$\begin{aligned}
\pi^{-s/2}\Gamma(s/2)\zeta(s) &= \pi^{-s/2}\sum_{n=1}^\infty n^{-s}\int_0^\infty e^{-\pi n^2 y}(\pi n^2 y)^{s/2-1}\pi n^2 \mathrm{d}y \\
&= \int_0^\infty \omega(x)x^{s/2-1}\mathrm{d}x \\
&= \int_1^\infty \omega(1/x)x^{-s/2+1}\frac{\mathrm{d}x}{x^2} + \int_1^\infty \omega(x)x^{s/2-1}\mathrm{d}x \\
&= -1/s + 1/(s-1) + \int_1^\infty \omega(x)(x^{s/2-1} + x^{-s/2-1/2})\mathrm{d}x.
\end{aligned}$$

This last expression is symmetric with respect to the transformation $s \leftrightarrow 1-s$. It follows that the zeta function can be continued to the entire complex plane, and we have the functional equation

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

Since Γ has poles at the negative integers, but the product $\Gamma\left(\frac{s}{2}\right)\zeta(s)$ is analytic and non-zero for $\sigma > 1$, it follows that ζ vanishes at all even negative integers. Any additional zeros must lie inside the critical strip with $0 < \sigma < 1$ and are distributed symmetrically. We denote the set of zeros in the critical strip by $\mathcal{N}$.

Now that we understand the zeros of ζ better, we can go back to the proof of the prime number theorem. This time, instead of taking c' so close to 1 that the only singularity the domain of integration is the pole, we aim to let c' tend to $-\infty$. Using that for $\rho \in \mathcal{N}$ or $\rho = -2n$ we have

$$\operatorname*{res}_{s=\rho}\frac{\zeta'}{\zeta}(s)\frac{x^s}{s} = \frac{x^\rho}{\rho},$$

the residue theorem yields

$$\psi'(x) = x - \frac{\zeta'}{\zeta}(0) - \sum_{\substack{\rho\in\mathcal{N}\\ |\Im\rho|<T}}\frac{x^\rho}{\rho} - \sum_{n\le|c'|/2}\frac{x^{-2n}}{-2n} + R(c',T,x). \tag{I.6.1}$$

(Recall the definition of the modified function ψ). One can show that the error vanishes as $c' \to -\infty$ and $T \to \infty$, and further that the sum over the zeros in the critical strip is (conditionally) convergent. Thus we obtain the explicit formula

$$\psi'(x) = x - \frac{\zeta'}{\zeta}(0) - \sum_{\rho\in\mathcal{N}}\frac{x^\rho}{\rho} - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right).$$

As a simple corollary we see that if there is a constant $\alpha < 1$ such that $\Re\rho \le \alpha$ for all $\rho \in \mathbb{N}$, then we would have $\psi(x) = x + O(x^{\alpha+\varepsilon}$.

Conjecture I.6.1 (Riemann Hypothesis)**.** *All $\rho \in \mathcal{N}$ have $\Re\rho = 1/2$.*

Corollary I.6.2. *We have*

$$\psi(x) = x + O(x^{1/2+\varepsilon}).$$

This conjecture is wide open. However, the explicit formula (I.6.1) can be used to show that for some suitable $C > 0$ one has

$$\Re\rho < 1 - C\min\{1, (\log|\Im\rho|)^{-1}\}.$$

Plugged into our analysis of the previous paragraph, this zero-free region delivers the classical error term $O(xe^{-C\sqrt{\log x}})$ for the prime number theorem.

Part II. Primes in arithmetic progressions

II.1. Fundamental properties of Dirichlet characters

A Dirichlet character modulo q is a group homomorphism $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \mapsto S^1$. We extend χ to $\mathbb{Z}$ by setting $\chi(n) = 0$ when $(n, q) > 1$ and $\chi(n + kq) = \chi(n)$ for all $1 \le n \le q$ and $k \in \mathbb{Z}$.

The group $(\mathbb{Z}/q\mathbb{Z})^\times$ is a product of a finite number of cyclic groups and has $\varphi(q)$ elements. Since characters are totally multiplicative, they are uniquely determined by their values on the products of the generators of the cyclic groups. On each generator the number of possible values corresponds to the order of the corresponding cyclic group. It follows that the number of characters modulo q is equal to the order of the group $(\mathbb{Z}/q\mathbb{Z})^\times$ and is given by $\varphi(q)$. Obviously, the values taken are $\varphi(q)$-th roots of unity.

The set of characters modulo q forms a group via pointwise multiplication. The neutral element is given by the principal character χ_0 that takes the value $\chi_0(n) = 1$ for all n coprime to q. We write $\bar\chi$ for the inverse of χ. The following character relations are often useful.

Lemma II.1.1. *Let χ be a character modulo q and $a \in \mathbb{Z}$. Then*

$$\sum_{a \,(\mathrm{mod}\, q)} \chi(a) = \begin{cases} \varphi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{\chi \,(\mathrm{mod}\, q)} \chi(a) = \begin{cases} \varphi(q) & \text{if } a \equiv 1 \,(\mathrm{mod}\, q), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $\chi = \chi_0$ the first statement is trivial. For $\chi \neq \chi_0$ we can pick $b \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $\chi(b) \neq 1$. Then

$$\sum_{a \,(\mathrm{mod}\, q)} \chi(a) = \sum_{a \,(\mathrm{mod}\, q)} \chi(ab) = \chi(b) \sum_{a \,(\mathrm{mod}\, q)} \chi(a),$$

and since $\chi(b) \neq 1$ this implies the desired conclusion. The second statement is similar: If $a = 1$, again this is trivial. In the other case we can fix a character χ' such that $\chi'(a) \neq 1$, and then we find

$$\sum_{\chi \,(\mathrm{mod}\, q)} \chi(a) = \sum_{\chi \,(\mathrm{mod}\, q)} \chi(a)\chi'(a) = \chi'(a) \sum_{\chi \,(\mathrm{mod}\, q)} \chi(a).$$

This shows the statement. □

This lemma is more useful in a slightly reformulated way.

Corollary II.1.2. *Let χ, χ' be characters modulo q and $a, b \in \mathbb{Z}$ with $(a,q) = (b,q) = 1$. Then*

$$\frac{1}{\varphi(q)} \sum_{a \pmod q} \chi(a)\bar{\chi}'(a) = \begin{cases} 1 & \text{if } \chi' = \chi, \\ 0 & \text{otherwise,} \end{cases}$$

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \chi(a)\bar{\chi}(b) = \begin{cases} 1 & \text{if } a \equiv b \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Lemma II.1.1 with $\chi\bar{\chi}'$ resp. ab^{-1}. □

II.2. On the prime number theorem for arithmetic progressions

We now discuss to what an extent the proof of the prime number theorem can be generalised directly to arithmetic progressions. To this end we define the twisted von Mangoldt function

$$\psi(x, \chi) = \sum_{n \le x} \chi(n)\Lambda(n).$$

Then we have

$$\psi(x; q, a) = \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \Lambda(n) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \bar{\chi}(a)\psi(x, \chi),$$

where we used Corollary II.1.2. Observe that

$$|\psi(x, \chi_0) - \psi(x)| \le \sum_{\substack{n \le x \\ (n,q) > 1}} \Lambda(n) \ \le \log x \sum_{p \mid q} \sum_{\substack{k \in \mathbb{N} \\ p^k \le x}} 1.$$

The last term is

$$\sum_{p \mid q} \sum_{\substack{k \in \mathbb{N} \\ p^k \le x}} 1 \le \sum_{p \mid q} \frac{\log x}{\log p} \le \log x \omega(q),$$

where we wrote $\omega(q)$ for the number of distinct prime divisors of q. Trivially, we have $\omega(q) \le \Omega(q)$, where $\Omega(q)$ denotes the total number of prime factors of q, and

$$\Omega(q) = \sum_{p^k \| q} k \le \sum_{p^k \| q} k \log p = \log q. \tag{II.2.1}$$

We therefore have

$$|\psi(x, \chi_0) - \psi(x)| \le (\log x)^2 \log q.$$

The main contribution to the sum above stems therefore from the principal character. Invoking the prime number theorem, we have thus shown that

$$\psi(x; q, a) = \frac{x}{\varphi(x)} + \frac{1}{\varphi(x)} \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} \bar{\chi}(a)\psi(x, \chi) + O\left(\frac{x}{\varphi(q)} e^{-c(\log x)^{1/10}}\right). \tag{II.2.2}$$

The difficulty of the prime number theorem for arithmetic progressions lies therefore in understanding the contribution from the non-principal characters.

Lemma II.2.1. *Let $\chi \neq \chi_0$ be a Dirichlet character modulo q. Then the Dirichlet series $L(\chi, s)$ converges in $\sigma > 0$.*

Proof. This is similar to Lemma I.3.2. Observe that for any non-principal character χ modulo q the character relations of Lemma II.1.1 show that $\sum_{a=1}^{q}\chi(a)=0$ and hence by periodicity

$$\left|\sum_{a=1}^{x}\chi(a)\right|\leq q$$

regardless of the value x.

We now apply partial summation to the sum

$$\sum_{M\leq n\leq N}\frac{\chi(n)}{n^s}=\sum_{n\leq N}\frac{\chi(n)}{n^s}-\sum_{n<M}\frac{\chi(n)}{n^s}$$

and get

$$\begin{aligned}\left|\sum_{M\leq n\leq N}\frac{\chi(n)}{n^s}\right|&\leq q(N^{-\sigma}+M^{-\sigma})+|s|q\int_M^N t^{-\sigma-1}\mathrm{d}t\\&\leq q(1+|s|/\sigma)(N^{-\sigma}+M^{-\sigma})\end{aligned}\tag{II.2.3}$$

For $\sigma>0$ we can let N tend to infinity. Taking $M=1$ then yields the statement. □

It is harder to show that $L(\chi,1)$ does not vanish. We start with a product formula.

Lemma II.2.2. *Let $\sigma>1$, then we have*

$$\prod_{\chi\ (\mathrm{mod}\ q)}L(\chi,\sigma)\geq 1.$$

Proof. Using the Euler product formula of Lemma 0.2.3, we have

$$\log L(\chi,\sigma)=\sum_p\log\frac{1}{1-\frac{\chi(p)}{p^\sigma}}=\sum_p\sum_{k=1}^{\infty}\frac{\chi(p^k)}{k}p^{-k\sigma},$$

and thus we see that

$$\begin{aligned}\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\bar\chi(1)\log L(\chi,\sigma)&=\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\bar\chi(1)\sum_p\sum_{k=1}^{\infty}\frac{\chi(p^k)}{k}p^{-k\sigma}\\&=\sum_{\chi\ (\mathrm{mod}\ q)}\sum_{\substack{p,k\\p^k\equiv 1\ (\mathrm{mod}\ q)}}\frac{p^{-k\sigma}}{k}\geq 0.\end{aligned}$$

Exponentiating yields the result. □

Lemma II.2.3. *Let $\chi\neq\chi_0$ be a Dirichlet character modulo q. Then $L(\chi,1)\neq 0$.*

Proof. We know now that, with the exception of $L(\chi_0,s)$ which has a simple pole at $s=1$, all other Dirichlet series converge for all $\sigma>0$. This implies that there can at most be one character χ with $L(\chi,1)=0$, for otherwise the product of Lemma II.2.2 would have at least a double zero, which is excluded by the lemma. Since further $L(\chi,1)=0$ implies $L(\bar\chi,1)=0$, we are free to assume that $\chi=\bar\chi$, or in other words, that χ takes only real values.

Consider the function $f = \mathbb{1} * \chi$. We have

$$\begin{aligned}\sum_{n\le N^2} f(n)n^{-1/2} &= \sum_{n\le N^2}\sum_{d|n}\chi(d)n^{-1/2}\\ &= \sum_{d\le N}\chi(d)d^{-1/2}\sum_{k\le N^2/d}k^{-1/2} + \sum_{k\le N}k^{-1/2}\sum_{N<d\le N^2/k}\chi(d)d^{-1/2}.\end{aligned}$$

The inner sum of the last term is $O_q(N^{-1/2})$ by (II.2.3). In order to evaluate the inner sum of the first term we use partial summation and obtain

$$\sum_{k\le K}k^{-1/2} = [K]K^{-1/2} + \frac{1}{2}\int_1^K [t]t^{-3/2}\mathrm{d}t = 2K^{1/2} + O(1).$$

Together this shows that

$$\begin{aligned}\sum_{n\le N^2}\frac{f(n)}{n^{1/2}} &= \sum_{d\le N}\frac{\chi(d)}{d^{1/2}}(2Nd^{-1/2}+O(1)) + O_q\left(\sum_{k\le N}k^{-1/2}N^{-1/2}\right)\\ &= 2N\sum_{d\le N}\frac{\chi(d)}{d} + O_q\left(1+\sum_{d\le N}\frac{\chi(d)}{d^{1/2}}\right).\end{aligned}$$

The sum in the error is the truncation of the convergent Dirichlet series $L(\chi,1/2)$ and thus bounded in absolute terms. By (II.2.3) the first term is

$$2N\sum_{d\le N}\frac{\chi(d)}{d} = 2NL(\chi,1) + O(q).$$

It follows that

$$\sum_{n\le N^2}\frac{f(n)}{n^{1/2}} = 2NL(\chi,1) + O_q(1).$$

On the other hand, we can estimate the sum directly. Since f is multiplicative as convolution of multiplicative functions, we have

$$f(p^k) = \sum_{l=0}^{k}\chi(p^l) = \begin{cases}1 & \text{if } p|q,\\ k+1 & \text{if } \chi(p)=1,\\ 1 & \text{if } \chi(p)=-1 \text{ and } k \text{ even},\\ 0 & \text{if } \chi(p)=-1 \text{ and } k \text{ odd}.\end{cases}$$

Thus we have $f(n)\ge 0$ and $f(n^2)\ge 1$ for all $n\in\mathbb{N}$, and therefore

$$\sum_{n\le N^2}\frac{f(n)}{n^{1/2}} \ge \sum_{m\le N}\frac{f(m^2)}{m} \ge \sum_{m\le N}\frac{1}{m} \ge \log N + O(1).$$

Combining both estimates we see that

$$2NL(\chi,1) = \sum_{n\le N^2}\frac{\chi(n)}{n^{1/2}} + O_q(1) \ge \log N + O_q(1),$$

which is possible only if $L(\chi,1)>0$.

□

One can now imitate the proof of the prime number theorem and show that $\frac{L'(\chi,s)}{L(\chi,1)}$ has no poles on the line $\sigma = 1$ and that there is a small zero-free region to the left of the line. This shows

$$\psi(x,\chi) = O_q\left(xe^{-c(\log x)^{1/10}}\right)$$

for some constant $c = c(q)$, and inserting this into (II.2.2) delivers the bound

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O_q\left(xe^{-c(\log x)^{1/10}}\right).$$

Note that both the implied constant and the constant c depend on q.

The great weakness of this result is the fact that the error term is not uniform in q. In fact, since for non-principal characters the pole at $s = 1$ is missing and one has to work with the much weaker statement that $L(\chi,1) > 0$, it is very hard to establish zero-free regions uniformly in q. As we have seen in the proof of Lemma II.2.3, there can be at most one 'bad' character which then has to be real-valued. To this day, the behaviour of zeros of Dirichlet L-functions is quite poorly understood. We summarise the most important facts in a theorem.

Theorem II.2.4 (Theorem on Siegel zeros, without proof)**.**

(1) For any real-valued character $\chi \pmod q$ and for any $\varepsilon > 0$ there is an (ineffective) constant $C(\varepsilon)$ with the property that $L(\chi,1) > C(\varepsilon)q^{-\varepsilon}$.

(2) For any real-valued character $\chi \pmod q$ and for any $\varepsilon > 0$ there is an (ineffective) constant $C'(\varepsilon)$ with the property that if $L(\chi,\rho) = 0$ for some real ρ, then $\rho < 1 - C'(\varepsilon)q^{-\varepsilon}$.

(3) Let c be a sufficiently small constant. If $\chi_1 \neq \chi_0$ is a character modulo q and $L(\chi_1,s)$ has a zero in the region

$$\sigma \geq 1 - c/\log(q(|t|+2)),$$

then χ_1 is real-valued, the zero is on the real axis and there exist no further zeros in this region for any character modulo q.

Using these statements, it is still possible to establish a version of the Prime Number Theorem for arithmetic progressions that shows some uniformity in q.

Theorem II.2.5 (Siegel–Walfisz, without proof)**.** *Let A be arbitrary. There exists a $C = C(A)$ such that for all $q \leq (\log x)^A$ and all $(a,q) = 1$ one has*

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O\left(xe^{-C(\log x)^{1/2}}\right).$$

This theorem, while useful, is somewhat unsatisfactory because the constant C is not effectively computable and because it holds only for a fairly small range of q.

Conjecture II.2.6 (Generalised Riemann hypothesis)**.** *Let χ be any Dirichlet character. Inside the critical strip all zeros of the Dirichlet series $L(\chi,s)$ have real part $1/2$.*

Corollary II.2.7. *Let $(a,q) = 1$. The asymptotic*

$$\psi(x;q,a) = \frac{x}{\varphi(q)} + O(x^{1/2+\varepsilon})$$

holds uniformly in q.

Remark II.2.8. Observe that the conjectural version of the prime number theorem for arithmetic progressions has no $\varphi(q)$ in the error term. However, for most values q the Euler function $\varphi(q)$ is almost of the same magnitude as q. Hence, even if GRH could be proved, the prime number theorem for arithmetic progressions would be useful only for $q \ll x^{1/2}$.

II.3. The Large Sieve inequality

Our main goal for this chapter is to study the error of the prime number theorem for arithmetic progressions in the arithmetic mean. The main tool for this is known as the large sieve inequality, which in its modern formulation is an analytic, Fourier-type inequality relating exponential sums to their coefficients. Let

$$e(x) = e^{2\pi i x},$$

then one is interested in sums of the shape

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha) \tag{II.3.1}$$

with some number-theoretic data $a_n \in \mathbb{C}$. In particular, for a set of pairwise distinct $\alpha_1, \ldots, \alpha_R$ one would like to have a bound

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |a_n|^2$$

where Δ depends only on the length N of the exponential sum and the spacing of the α_r modulo 1. Write $\|x\| = \min_{n\in\mathbb{Z}} |x-n|$ for the distance on $\mathbb{R}/\mathbb{Z}$, and let

$$\delta = \min_{r\neq s} \|\alpha_r - \alpha_s\|. \tag{II.3.2}$$

A typical choice for the α_r might be the fractions a/q with $q \leq Q$; in this case we would have $\delta = 1/(Q(Q-1))$.

Theorem II.3.1 (Large Sieve, analytic version)**.** *Let $S(\alpha)$ and δ be given by* (II.3.1) *and* (II.3.2)*, respectively, where $M \in \mathbb{Z}$ and $N \in \mathbb{N}$. We have*

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq (\pi N + \delta^{-1}) \sum_{n=M+1}^{M+N} |a_n|^2. \tag{II.3.3}$$

We follow a fairly analytic approach to the large sieve, starting with the Sobolev–Gallagher inequality.

Lemma II.3.2. *Let $f \in \mathcal{C}^1[x-\xi, x+\xi]$. Then*

$$|f(x)| \leq (2\xi)^{-1} \int_{x-\xi}^{x+\xi} |f(t)|\mathrm{d}t + \frac{1}{2}\int_{x-\xi}^{x+\xi} |f'(t)|\mathrm{d}t.$$

Proof. Suppose first that $f \in \mathcal{C}^1[0,1]$, and observe that

$$\begin{aligned}
&\int_0^1 f(u)\mathrm{d}u + \int_0^x uf'(u)\mathrm{d}u + \int_x^1 (u-1)f'(u)\mathrm{d}u \\
&= \int_0^1 f(u)\mathrm{d}u + xf(x) - \int_0^x f(u)\mathrm{d}u - (x-1)f(x) - \int_x^1 f(u)\mathrm{d}u \\
&= f(x).
\end{aligned}$$

Taking $x = 1/2$, we see that

$$\begin{aligned}|f(1/2)| &= \left| \int_0^1 f(u)\mathrm{d}u + \int_0^{1/2} uf'(u)\mathrm{d}u + \int_{1/2}^1 (u-1)f'(u)\mathrm{d}u \right| \\ &\leq \int_0^1 |f(u)|\mathrm{d}u + (1/2)\int_0^1 |f'(u)|\mathrm{d}u.\end{aligned}$$

For general x we apply this result to the function $f \circ g$ with $g(u) = x - \xi + 2u\xi$. This yields the desired result. □

Proof of Theorem II.3.1. In order to prove Theorem II.3.1 we take $\xi = \delta/2$. Then the Sobolev–Gallagher inequality applied to the right hand side of (II.3.3) yields

$$\sum_{r=1}^R |S(\alpha)|^2 \leq \sum_{r=1}^R \int_{\alpha_r-\delta/2}^{\alpha_r+\delta/2} \delta^{-1}|S(\alpha)|^2 + |S(\alpha)S'(\alpha)|\mathrm{d}\alpha.$$

The intervals are chosen in such a way that they do not overlap, and the integrand is positive, so we obtain

$$\sum_{r=1}^R |S(\alpha)|^2 \leq \delta^{-1}\int_0^1 |S(\alpha)|^2\mathrm{d}\alpha + \int_0^1 |S(\alpha)S'(\alpha)|\mathrm{d}\alpha.$$

Now recall Parseval's identity

$$\int_0^1 \left| \sum_{n\in\mathbb{Z}} a_n e(\alpha n) \right|^2 \mathrm{d}\alpha = \sum_{n\in\mathbb{Z}} |a_n|^2.$$

Setting $a_n = 0$ for all n not in the interval $[M+1, M+N]$, this takes care of the first term, and for the second term we apply Cauchy's inequality

$$\begin{aligned}\int_0^1 |S(\alpha)S'(\alpha)|\mathrm{d}\alpha &\leq \left(\int_0^1 |S(\alpha)|^2\mathrm{d}\alpha\right)^{1/2}\left(\int_0^1 |S'(\alpha)|^2\mathrm{d}\alpha\right)^{1/2} \\ &= \left(\sum_{n\in\mathbb{Z}} |a_n|^2\right)^{1/2}\left(\sum_{n\in\mathbb{Z}} |2\pi i n a_n|^2\right)^{1/2},\end{aligned}$$

where we used the fact that

$$\frac{\mathrm{d}}{\mathrm{d}\alpha}\sum_{n=M+1}^{M+N} a_n e(n\alpha) = \sum_{n=M+1}^{M+N} 2\pi i n a_n e(n\alpha).$$

Now suppose that $M = -[(N+1)/2]$, so that the interval of summation is $-N/2 \leq n \leq N/2$. Then

$$\sum_{-N/2\leq n\leq N/2} |2\pi i n a_n|^2 \leq (\pi N)^2 \sum_{-N/2\leq n\leq N/2} |a_n|^2,$$

and hence combining our estimates yields

$$\sum_{r=1}^{R}|S(\alpha)|^2 \le \delta^{-1}\sum_{-N/2\le n\le N/2}|a_n|^2 + \left(\sum_{-N/2\le n\le N/2}|a_n|^2\right)^{1/2}\left(\sum_{-N/2\le n\le N/2}|2\pi i n a_n|^2\right)^{1/2}$$
$$\le (\delta^{-1}+\pi N)\sum_{-N/2\le n\le N/2}|a_n|^2.$$

This proves the statement for $M = -[(N+1)/2]$.

For general M it remains to observe that a change of variables yields

$$\sum_{n=M+1}^{M+N} a_n e(n\alpha) = e((K-M)\alpha)\sum_{n=K+1}^{K+N} a_{M-K+n}e(n\alpha).$$

Thus Theorem II.3.1 is proved for all M. □

Remark II.3.3. By stronger methods one can even show

$$\sum_{r=1}^{R}|S(\alpha_r)|^2 \le (N-1+\delta^{-1})\sum_{n=M+1}^{M+N}|a_n|^2.$$

This bound is sharp, as can be seen as follows. Suppose that $R|(N-1)$, and take $\alpha_r = r/R$, so that $\delta = 1/R$. Take further $M = -1$ and $a_n = 1$ if $R|n$ and $a_n = 0$ else. Then

$$\sum_{n=0}^{N-1}|a_n|^2 = \sum_{\substack{n=0\\ R|n}}^{N-1} 1 = 1 + \frac{N-1}{R}.$$

On the other hand, we have

$$\sum_{r=1}^{R}\left|\sum_{n=0}^{N-1}a_n e(nr/R)\right|^2 = \sum_{r=1}^{R}\left|\sum_{m=0}^{(N-1)/R} e(mr)\right|^2 = R\left(1+\frac{N-1}{R}\right)^2$$
$$= (N-1+R)\sum_{n=0}^{N-1}|a_n|^2.$$

II.4. What is a sieve?

In this section we will motivate the nomenclature *large sieve* for the inequality of Theorem II.3.1. Sieve theory stems essentially from the attempt of generalising the sieve of Eratosthenes. The underlying idea is simple: Let $\mathcal{N} \subset \mathbb{N}$ be finite and $\mathcal{P}$ a subset of the primes, and for each $p \in \mathcal{P}$ let Ω_p denote a set of residue classes, then we are interested in the set

$$\mathcal{N}^* = \{n \in \mathcal{N} : n \not\equiv a \pmod p \text{ for all } a \in \Omega_p \text{ for all } p \in \mathcal{P}\}$$

In this notation, the sieve of Eratosthenes has $\mathcal{N} = \{2, 3, \dots, [x]\}$, $\mathcal{P} = \{p : p \le \sqrt{x}\}$ and $\Omega_p = \{0\}$ for each p. If we take $\Omega_p = \{0, 2\}$ instead, then $\mathcal{N}^*$ denotes the set of twin primes up to x. Here, as often, it is hard to derive an explicit expression for the cardinality of $\mathcal{N}^*$, so we are interested in finding an upper bound.

In any applications one would like to set $a_n = 0$ whenever $n \notin \mathcal{N}^*$, so that $|\sum a_n|^2$ gives information about the size of $\mathcal{N}^*$. We set

$$w(p) = \#\{a \pmod p : a_n = 0 \text{ for all } n \equiv a \pmod p\},$$

and define the multiplicative function

$$h(p) = \frac{w(p)}{p - w(p)}, \qquad h(p^k) = 0 \text{ if } k \geq 2.$$

Then we have the following statement.

Lemma II.4.1. *We have*

$$h(q)\left|\sum_n a_n\right|^2 \leq \sum_{\substack{a=1\\(a,q)=1}}^{q} |S(a/q)|^2. \tag{II.4.1}$$

Proof. Suppose first that $q = p$, and write

$$Z(p,a) = \sum_{n \equiv a \pmod p} a_n, \qquad Z = \sum_n a_n = S(0) = S(1).$$

Then

$$\sum_{a=1}^{p} |S(a/p)|^2 = \sum_{a=1}^{p}\sum_{m,n} a_n \bar{a}_m e\left(\frac{(n-m)a}{p}\right) = p \sum_{m \equiv n \pmod p} a_n \bar{a}_m = p\sum_{a=1}^{p} |Z(p,a)|^2,$$

where we used the fact that

$$\sum_{n=1}^{q} e(nx/q) = \begin{cases} q & \text{if } x \equiv 0 \pmod q \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\sum_{a=1}^{p-1} |S(a/p)|^2 = p\sum_{a=1}^{p} |Z(p,a)|^2 - |S(1)|^2 = p\sum_{a=1}^{p} |Z(p,a)|^2 - Z^2.$$

But Cauchy's inequality implies that

$$|Z|^2 = \left|\sum_{a=1}^{p} Z(p,a)\right|^2 \leq \left(\sum_{\substack{a=1\\Z(p,a)\neq 0}}^{p} 1\right)\left(\sum_{a=1}^{p} |Z(p,a)|^2\right),$$

and since the first sum is at most $p - w(p)$, the above becomes

$$\sum_{a=1}^{p-1} |S(a/p)|^2 = p\sum_{a=1}^{p} |Z(p,a)|^2 - |Z|^2 \geq \frac{p}{p-w(p)}|Z|^2 - |Z|^2 = \frac{w(p)}{p-w(p)}|Z|^2.$$

This shows the statement for $q = p$.

For prime powers it is trivial, so the lemma is proven if we can show multiplicativity. Here we observe that replacing a_n by $a_n e(\beta n)$ does not affect the value of $w(p)$, so (II.4.1) is true if and only if

$$h(q)|S(\beta)|^2 = h(q)\left|\sum_n a_n e(n\beta)\right| \leq \sum_{\substack{a=1\\(a,q)=1}}^{q} |S(a/q+\beta)|^2$$

for all β. Now suppose that $q = q_1 q_2$ and $(q_1, q_2) = 1$, then we have

$$\begin{aligned}\sum_{\substack{a=1\\(a,q_1q_2)=1}}^{q} \left|S\left(\frac{a}{q_1q_2}\right)\right|^2 &= \sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} \sum_{\substack{a_2=1\\(a_2,q_2)=1}}^{q_2} \left|S\left(\frac{a_1}{q_1}+\frac{a_2}{q_2}\right)\right|^2 \\ &\geq h(q_2) \sum_{\substack{a_1=1\\(a_1,q_1)=1}}^{q_1} \left|S\left(\frac{a_1}{q_1}\right)\right|^2 \\ &\geq h(q_2)h(q_1)|S(0)|^2.\end{aligned}$$

This completes the proof of the lemma. □

As a corollary to Lemma II.4.1 we obtain an upper bound for $\#\mathcal{N}^*$. Let $\omega(p) = \#\Omega_p$ if $p \in \mathcal{P}$ and $\omega(p) = 0$ else, and define the multiplicative function

$$g(p) = \frac{\omega(p)}{p - \omega(p)}, \qquad g(p^k) = 0 \text{ if } k \geq 2.$$

Then we have the following upper bound for $\mathcal{N}^*$.

Theorem II.4.2 (Large Sieve, arithmetic version)**.** *Let $\mathcal{N} \subseteq [M+1, M+N]$, then in the above notation we have*

$$\mathcal{N}^* \leq (\pi N + Q^2) \left(\sum_{q \leq Q} g(q)\right)^{-1}.$$

Proof. Summing (II.4.1) over $q \leq Q$ and then applying Theorem II.3.1 yields

$$\sum_{q=1}^{Q} h(q) \left|\sum_n a_n\right| \leq \sum_{q=1}^{Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} |S(a/q)|^2 \leq (\pi N + Q^2) \sum_n |a_n|^2.$$

Here we used the fact that

$$\min\left\{\left\|\frac{a}{q} - \frac{a'}{q'}\right\| : \frac{a}{q} \neq \frac{a'}{q'},\, q, q' \leq Q\right\} = \frac{1}{Q(Q-1)}.$$

Now set $a_n = 1$ if $n \in \mathcal{N}^*$ and $a_n = 0$ else, then

$$\sum_n a_n = \sum_n |a_n|^2 = \#\mathcal{N}^*.$$

Furthermore, we have $\omega(p) \leq w(p)$ for all $p \in \mathcal{P}$ and hence $g(q) \leq h(q)$, and the statement follows at once. □

In practice, one will take $Q \asymp \sqrt{N}$, so that the terms of the factor are balanced. Theorem II.4.2 is then useful if $\sum_{q \ll \sqrt{N}} g(q)$ grows as N tends to infinity, and works best if $g(q) \gg 1$. However, this is equivalent to asking $\omega(p) \gg p$. Generally, a sieve is said to be large if $\omega(p) \gg p$, and small if $\omega(p) \ll 1$. In this nomenclature, the sieve of Eratosthenes and the twin prime sieve from above are small sieves, whereas a sieve that sieves e.g. for quadratic residues is a large sieve.

II.5. More on Dirichlet characters

In order to apply the large sieve to prime numbers in arithmetic progressions, we need to formulate it in terms of Dirichlet characters. This requires some further background.

Any Dirichlet character χ modulo q has period q. It is, however, possible that there are shorter periods, in other words, that there exists a $q'|q$ such that $\chi = \chi_0\chi'$, where χ_0 is the principal character modulo q and χ' is a character modulo q'. In such a case we say that χ is induced by χ'.

Lemma II.5.1. *Let χ be a character modulo q. There exists a unique minimal integer $q'|q$ and a unique primitive Dirichlet character χ' modulo q' such that $\chi(n) = \chi'(n)$ for all $(n, q) = 1$.*

Proof. It is clear from the definition of an induced character that q' is unique. It is also clear that $\chi'(n) = \chi(n)$ whenever $(n, q) = 1$, so it remains to show that this completely determines χ'. Suppose that $(n, q) > 1$ and $(n, q') = 1$. Since χ' is periodic modulo q', we need to find some t such that $(n + tq', q) = 1$, and set $\chi'(n) = \chi'(n + t_1q')$. This is then well-defined, because if there are two distinct t_1, t_2 with this property, then it follows from the the q'-periodicity of χ' and the definition of induced characters that

$$\chi(n + t_1q') = \chi'(n + t_1q')\chi_0(n + t_1q') = \chi'(n + t_2q')\chi_0(n + t_2q') = \chi(n + t_2q').$$

We construct such a t by setting

$$t = \prod_{p:p|q,p\nmid q'n} p.$$

Suppose that r is a prime dividing $(n+q't, q)$, then $r|q$ and $r|n+q't$. Suppose $r|t$, then by construction $r \nmid n$ and therefore $r \nmid n + q't$, a contradiction. Suppose therefore that $r \nmid t$, then by construction $r|n$ or $r|q'$. However, if $r|n$ then the assumption $r|n + q't$ implies $r|q'$, so $r|(n, q') = 1$, a contradiction again. Similarly, assuming $r|q'$ leads to the conclusion $r|n$, which produces the same contradiction. □

To a Dirichlet character $\chi \pmod q$ we associate the Gauss sum

$$\tau(\chi) = \sum_{a \pmod q} \chi(a)e(a/q).$$

Since χ respects the multiplicative structure of $(\mathbb{Z}/q\mathbb{Z})^\times$ and $e(a/q)$ is a homomorphism on the additive group $\mathbb{Z}/q\mathbb{Z}$, Gauss sums play a role in relating the additive and multiplicative structure of $\mathbb{Z}/q\mathbb{Z}$. In fact, it can be used to transform a character sum into an exponential sum, which is often easier to handle, and which is required if we want to apply the large sieve of Theorem II.3.1.

Lemma II.5.2. *Let f be an arithmetic function and χ a primitive character modulo q. Then we have*

$$\sum_{n\le x} f(n)\chi(n) = \frac{1}{\tau(\bar\chi)} \sum_{a \pmod q} \bar\chi(a) \sum_{n\le x} f(n)e(an/q).$$

Proof. We show that for primitive $\chi \pmod q$ the relation

$$\chi(n)\tau(\bar\chi) = \sum_{a \pmod q} \bar\chi(a)e(an/q) \tag{II.5.1}$$

holds for any $n \pmod q$. The claim then follows upon multiplying both sides by $f(n)$ and summing.

We start by proving (II.5.1) in the case $(n,q)=1$. In this case the multiplicative inverse $\bar n$ of n is defined and we have

$$\chi(n)\tau(\bar\chi) = \sum_{a \pmod q} \chi(n)\bar\chi(a)e(a/q) = \sum_{a \pmod q} \bar\chi(\bar n a)e(a/q) = \sum_{a \pmod q} \bar\chi(a)e(an/q).$$

Now suppose $(n,q)=d>1$, then the left hand side of (II.5.1) vanishes. In order to understand the right hand side, we write $n=n'd$ and $q=q'd$, and set $a=cq'+b$ with $0\le c<d$ and $0\le b<q'$. Then

$$\sum_{a \pmod q} \bar\chi(a)e(an/q) = \sum_{b \pmod{q'}} \sum_{c \pmod d} \bar\chi(cq'+b)e(bn'/q').$$

It thus suffices to show

$$S_1(b) = \sum_{c \pmod d} \bar\chi(cq'+b) = 0$$

for all $b \pmod{q'}$. Observe that $S_1(b)$ is q'-periodic in b. We fix a number $v \equiv 1 \pmod{q'}$ with the property $\chi(v)\neq 1$. Such a number exists because χ is primitive and therefore cannot have period $q'<q$. We then have

$$\bar\chi(v)S(b) = \sum_{c \pmod d} \bar\chi(vcq'+vb) = \sum_{c \pmod d} \bar\chi(cq'+vb) = S(vb) = S(b).$$

Since we had chosen v such that $\chi(v)\neq 1$, this equality can be satisfied only if $S(b)=0$. □

In order to take full profit of Lemma II.5.2 we need some information on the size of the Gauss sum.

Lemma II.5.3. *Suppose χ is a primitive character modulo q, then we have*

$$|\tau(\chi)|^2 = q.$$

Proof. We square the identity (II.5.1). This yields

$$|\chi(n)|^2|\tau(\bar\chi)|^2 = \left|\sum_{a \pmod q} \bar\chi(a)e(an/q)\right|^2 = \sum_{a \pmod q}\sum_{b \pmod q} \chi(\bar a b)e\left(\frac{(a-b)n}{q}\right).$$

After summing over $n\le q$ we find

$$\varphi(q)|\tau(\bar\chi)|^2 = \sum_{a \pmod q}\sum_{b \pmod q} \chi(\bar a b)\sum_{n=1}^{q} e\left(\frac{(a-b)n}{q}\right) = q\sum_{a \pmod q}|\chi(a)|^2 = q\varphi(q).$$

□

We expect that in sums involving characters other than the principal one some cancellation occurs. With the help of Lemma II.5.2 this can be shown.

Theorem II.5.4 (Pólya–Vinogradov inequality)**.** *Let χ be a non-principal character modulo q. Then*

$$\left|\sum_{n\le N}\chi(n)\right| \le 2\sqrt{q}\log q.$$

Proof. If χ is primitive, Lemma II.5.2 applied to $f = \mathbb{1}$ shows that

$$\sum_{n\le x}\chi(n) = \frac{1}{\tau(\bar\chi)}\sum_{a \pmod q}\bar\chi(a)\sum_{n\le x} e(an/q).$$

The inner sum is a geometric sum and can be evaluated explicitly. We find

$$\begin{aligned}\sum_{n=1}^{x} e(an/q) &= \sum_{n=1}^{x}(e^{2\pi ia/q})^n = e^{2\pi ia/q}\frac{e^{2\pi iax/q}-1}{e^{2\pi ia/q}-1}\\ &= e^{2\pi ia/q}\frac{e^{\pi iax/q}}{e^{\pi ia/q}}\frac{e^{\pi iax/q}-e^{-\pi iax/q}}{e^{\pi ia/q}-e^{-\pi ia/q}} = e\left(\frac{a(x+1)}{2q}\right)\frac{\sin(\pi ax/q)}{\sin(\pi a/q)},\end{aligned}$$

and thus for $a \not\equiv 0 \pmod q$ the useful inequality

$$\left|\sum_{n=1}^{x} e(an/q)\right| = \left|\frac{\sin(\pi ax/q)}{\sin(\pi a/q)}\right| \le \frac{1}{|\sin(\pi a/q)|}.$$

Inserting this above and using Lemma II.5.3 gives

$$\left|\sum_{n\le x}\chi(n)\right| = \frac{1}{\sqrt q}\sum_{a=1}^{q-1}\frac{1}{\sin(\pi a/q)}.$$

We can estimate this sum by comparing it with an integral. For every function f that is convex on an interval I we have $f(x) \le \frac12(f(x+h)+f(x-h))$ for all values x, h satisfying $x \pm h \in I$. Integrating over h yields

$$f(x) \le \frac{1}{2H}\int_0^H \frac12(f(x+h)+f(x-h))\mathrm{d}h = \frac{1}{H}\int_{x-H}^{x+H} f(h)\mathrm{d}h.$$

The function $1/\sin(\pi a/q)$ is convex in the interval $I = [0, q]$. Taking $H = 1/(2q)$, we see that

$$\begin{aligned}\sum_{a=1}^{q-1}\frac{1}{\sin(\pi a/q)} &\le \sum_{a=1}^{q-1} q\int_{a/q-1/(2q)}^{a/q+1/(2q)}\frac{1}{\sin(\pi x)}\mathrm{d}x\\ &= q\int_{1/(2q)}^{1-1/(2q)}\frac{1}{\sin(\pi x)}\mathrm{d}x = 2q\int_{1/(2q)}^{1/2}\frac{1}{\sin(\pi x)}\mathrm{d}x.\end{aligned}$$

For $x \le 1/2$ we have $1/\sin(\pi x) \le 1/2x$, so we obtain

$$2\int_{1/2q}^{1/2}\frac{1}{\sin(\pi x)}\mathrm{d}x \le \int_{1/2q}^{1/2}\frac{\mathrm{d}x}{x} = \log(1/2) - \log(1/2q) = \log q.$$

Altogether we have shown that for primitive characters we have the estimate

$$\left|\sum_{n\le x}\chi(n)\right| = \frac{1}{\sqrt q}\sum_{a \pmod q}\frac{1}{\sin(\pi a/q)} \le 2\sqrt q\int_{1/2q}^{1/2}\frac{1}{\sin(\pi x)}\mathrm{d}x \le \sqrt q\log q.$$

This proves the statement for primitive characters.

It remains to consider the case when χ is not primitive, but induced by a primitive character χ' modulo q'. In this case we have $q = q'r$ and thus

$$\sum_{n\le x}\chi(n) = \sum_{\substack{n\le x\\(n,r)=1}}\chi'(n) = \sum_{n\le x}\sum_{d\mid(n,r)}\mu(d)\chi'(n)$$
$$= \sum_{d\mid r}\mu(d)\sum_{\substack{n\le x\\ d\mid n}}\chi'(n) = \sum_{d\mid r}\mu(d)\chi'(d)\sum_{k\le x/d}\chi'(k).$$

The inner sum involves a primitive character and is thus at most as large as $\sqrt{q'}\log q'$. Since

$$\sum_{d\mid r}|\mu(d)| \le \sum_{d\mid r}1 \le 2\sum_{\substack{d\le\sqrt{r}\\ d\mid r}}1 \le 2\sqrt{r},$$

the theorem follows also for non-primitive characters. □

Unconditinally, our form of the Pólya-Vinogradov inequality is essentially the best known (with more work the factor 2 can be removed). One can prove $\sum_{n\le x}\chi(n) \ll \sqrt{q}\log\log q$ conditionally on GRH, and this is sharp as there are quadratic characters having $\sum_{n\le x}\chi(n) \gg \sqrt{q}\log\log q$.

II.6. The Theorem of Barban–Davenport–Halberstam

We will now show that the prime number theorem for arithmetic progressions holds on average. The first step is to rephrase the large sieve in terms of characters.

Theorem II.6.1. *Let $a_n \in \mathbb{C}$, $M \in \mathbb{Z}$ and $N \in \mathbb{N}$, then*

$$\sum_{1<q\le Q}\frac{q}{\varphi(q)}\sum_{\substack{\chi \pmod q\\ \chi \text{ primitive}}}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2 \le (N+Q^2)\sum_{n=M+1}^{M+N}|a_n|^2$$

Proof. Suppose for a start that χ is primitive. Then we have by Lemma II.5.2 that

$$\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2 = \left|\frac{1}{\tau(\bar\chi)}\sum_{a \pmod q}\bar\chi(a)\sum_{n=M+1}^{M+N}a_n e(an/q)\right|^2$$
$$= \frac{1}{q}\left|\sum_{a \pmod q}\sum_{n=M+1}^{M+N}\bar\chi(a)a_n e(an/q)\right|^2,$$

where we used Lemma II.5.3 for the Gauss sum. We now take the sum over all primitive characters modulo q; note that, since we are summing only positive terms, the right hand side only increases if we extend the sum to include the non-primitive

characters as well. Hence

$$\begin{aligned}
&\sum_{\substack{\chi \pmod q \\ \chi \text{ prim}}} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \\
&\leq \sum_{\chi \pmod q} \frac{1}{q} \left| \sum_{a \pmod q} \sum_{n=M+1}^{M+N} \bar{\chi}(a) a_n e(an/q) \right|^2 \\
&= \sum_{\chi \pmod q} \frac{1}{q} \left(\sum_{a \pmod q} \sum_{n=M+1}^{M+N} \bar{\chi}(a) a_n e(an/q) \right) \left(\sum_{b \pmod q} \sum_{m=M+1}^{M+N} \chi(b) \bar{a}_m e(-bm/q) \right) \\
&= \frac{\varphi(q)}{q} \sum_{\substack{a \pmod q \\ (a,q)=1}} \sum_{m,n=M+1}^{M+N} a_n \bar{a}_m e\left(\frac{a(n-m)}{q} \right)
\end{aligned}$$

by Corollary II.1.2. Setting

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(\alpha n)$$

and summing over $q \leq Q$, we obtain the relation

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \chi \text{ prim}}} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \leq \sum_{q \leq Q} \sum_{\substack{a \pmod q \\ (a,q)=1}} |S(a/q)|^2.$$

We now apply the Large Sieve Inequality. We have

$$\rho = \min \left\{ \frac{a}{q} - \frac{a'}{q'} : \frac{a}{q} \neq \frac{a'}{q'} \text{ and } q, q' \leq Q \right\} = \frac{1}{Q(Q-1)} \geq Q^{-2},$$

so Theorem II.3.1 yields

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \chi \text{ prim}}} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \leq (\pi N + Q^2) \sum_{n=M+1}^{M+N} |a_n|^2,$$

as claimed. □

Corollary II.6.2. *Let $a_n \in \mathbb{C}$, $M \in \mathbb{Z}$ and $N \in \mathbb{N}$, then*

$$\sum_{R < q \leq Q} \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \chi \text{ primitive}}} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2 \ll (\frac{N}{R} + Q) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Proof. Exercise. □

Recall our initial discussion of the prime number theorem for arithmetic progressions. There we had

$$\psi(x; q, a) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \bar{\chi}(a) \psi(x, \chi),$$

and we had noticed that $\psi(x,\chi_0)\sim x$. Denote

$$\psi^*(x,\chi)=\begin{cases}\psi(x,\chi) & \text{if } \chi\neq\chi_0\\ \psi(x,\chi)-x & \text{if } \chi=\chi_0,\end{cases}$$

then we have

$$\psi(x;q,a)-\frac{x}{\varphi(q)}=\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\bar\chi(a)\psi^*(x,\chi).$$

Observe that

$$\begin{aligned}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\sum_{\chi\ (\mathrm{mod}\ q)}\bar\chi(a)\psi^*(x,\chi)\right|^2&=\sum_{\chi,\chi'\ (\mathrm{mod}\ q)}\sum_{\substack{a=1\\(a,q)=1}}^{q}\bar\chi(a)\chi'(a)\psi^*(x,\chi)\bar{\psi}^*(x,\chi')\\&=\varphi(q)\sum_{\chi\ (\mathrm{mod}\ q)}|\psi^*(x,\chi)|^2,\end{aligned}$$

and therefore

$$\begin{aligned}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\psi(x;q,a)-\frac{x}{\varphi(q)}\right|^2&=\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\bar\chi(a)\psi^*(x,\chi)\right|^2\\&=\frac{1}{\varphi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}|\psi^*(x,\chi)|^2.\end{aligned}\tag{II.6.1}$$

Observe further that for primitive characters Corollary II.6.2 implies that

$$\sum_{R<q\le Q}\frac{1}{\varphi(q)}\sum_{\substack{\chi\ (\mathrm{mod}\ q)\\ \chi\ \mathrm{prim}}}|\psi^*(x,\chi)|^2\ll(x/R+Q)\sum_{n\le x}|\Lambda(n)|^2\ll(x/R+Q)x\log x,$$

where in the last step we used

$$\sum_{n\le x}\Lambda(n)^2\le(\log x)^2\left(\sum_{p\le x}1+O\left(\sum_{p^2\le x}1\right)\right)\ll(\log x)^2\left(\frac{x}{\log x}+x^{1/2}\right)\ll x\log x.$$

Hence if we could reduce the character sum in (II.6.1) to a sum over only primitive character, we would be able to obtain an average result on the primes in arithmetic progressions.

If a character $\chi\ (\mathrm{mod}\ q)$ is induced by a character $\chi'\ (\mathrm{mod}\ q')$, then $\chi=\chi'\chi_0$ where χ_0 is the principal character modulo q, and therefore

$$\psi(x,\chi')-\psi(x,\chi)=\sum_{n\le x}(1-\chi_0(n))\chi'(n)\Lambda(n)=\sum_{\substack{p^k\le x\\ p\mid q}}\chi'(p^k)\log(p)\ll\sum_{\substack{p^k\le x\\ p\mid q}}\log(p).$$

Observe that

$$\sum_{\substack{p^k\le x\\ p\mid q}}\log(p)\ll\sum_{p\mid q}\left[\frac{\log x}{\log p}\right]\log p\ll\log x\Omega(q)\ll\log x\log q\ll(\log xq)^2$$

where we used the argument of (II.2.1). Thus, if χ' is used to denote the primitive character that induces χ, this implies

$$\begin{aligned}\sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \,(\mathrm{mod}\ q)}|\psi^*(x,\chi)|^2 &= \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \,(\mathrm{mod}\ q)}\big(|\psi^*(x,\chi')|^2+O((\log xq)^2)\big)\\ &= \sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \,(\mathrm{mod}\ q)}|\psi^*(x,\chi')|^2+O(Q\log(Qx)^2).\end{aligned}$$

Furthermore, every character mod q induces precisely one character for all multiples of q. Hence we find

$$\begin{aligned}\sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \,(\mathrm{mod}\ q)}|\psi^*(x,\chi)|^2 &= \sum_{q\le Q}\sum_{q'\mid q}\sum_{\substack{\chi' \,(\mathrm{mod}\ q')\\ \chi \text{ prim}}}|\psi^*(x,\chi)|^2\sum_{\substack{\chi \,(\mathrm{mod}\ q)\\ \chi \text{ induced by } \chi'}}\frac{1}{\varphi(q)}\\ &= \sum_{q'\le Q}\sum_{\substack{\chi' \,(\mathrm{mod}\ q')\\ \chi \text{ prim}}}|\psi^*(x,\chi)|^2\sum_{1\le k\le Q/q'}\frac{1}{\varphi(kq')}.\end{aligned}$$

Since $\varphi(p^k)=p^k-p^{k-1}=p^k(1-1/p)$, we have $\varphi(n)=n\prod_{p\mid n}(1-1/p)$ and thus $\varphi(kq')\ge\varphi(k)\varphi(q')$. It follows that

$$\sum_{1\le k\le y}\frac{1}{\varphi(kq')}\le\frac{1}{\varphi(q')}\sum_{1\le k\le y}\frac{1}{\varphi(k)}.$$

In order to bound the inner sum we observe that

$$\begin{aligned}\sum_{1\le k\le y}\frac{1}{\varphi(k)} &\le \prod_{p\le y}\sum_{i=0}^{\infty}\frac{1}{\varphi(p^i)}\\ &\le \prod_{p\le y}\left(1+\frac{1}{p-1}+\frac{1}{p(p-1)}+\frac{1}{p^2(p-1)}+\dots\right).\end{aligned}$$

Furthermore, we have

$$\left(1-\frac{1}{p}\right)\left(1+\frac{1}{p-1}+\frac{1}{p(p-1)}+\frac{1}{p^2(p-1)}+\dots\right)=1-\frac{1}{p}+\frac{1}{p-1}=1+\frac{1}{p(p-1)},$$

and therefore

$$\sum_{1\le k\le y}\frac{1}{\varphi(k)}\le\prod_{p\le y}\left(1-\frac{1}{p}\right)^{-1}\left(1+\frac{1}{p(p-1)}\right)\ll\log y. \tag{II.6.2}$$

With this information we find

$$\sum_{q\le Q}\frac{1}{\varphi(q)}\sum_{\chi \,(\mathrm{mod}\ q)}|\psi^*(x,\chi)|^2\ll\sum_{q'\le Q}\frac{\log(Q)}{\varphi(q')}\sum_{\substack{\chi' \,(\mathrm{mod}\ q')\\ \chi' \text{ prim}}}|\psi^*(x,\chi')|^2+O(Q\log(Qx)^2).$$

Now fix a suitable parameter R. The contribution of $q'>R$ is

$$\begin{aligned}\sum_{R\le q'<Q}\frac{\log(Q)}{\varphi(q')}\sum_{\substack{\chi' \,(\mathrm{mod}\ q')\\ \chi' \text{ prim}}}|\psi^*(x,\chi')|^2 &\ll \log(Q)\sum_{R\le q'<Q}\frac{1}{\varphi(q')}\sum_{\substack{\chi' \,(\mathrm{mod}\ q')\\ \chi' \text{ prim}}}|\psi^*(x,\chi')|^2\\ &\ll (x/R+Q)x(\log x)^2.\end{aligned}$$

It remains to bound the contribution arising from small q. Here we use the Theorem of Siegel-Walfisz (Theorem II.2.5). Suppose χ' is a primitive character modulo q' with $q' \ll (\log x)^A$, then we have

$$\begin{aligned}\psi(x,\chi') = \sum_{n\le x}\chi'(n)\Lambda(n) &= \sum_{\substack{b=1\\(b,q')=1}}^{q'}\chi'(b)\sum_{\substack{n\le x\\ n\equiv b \pmod{q'}}}\Lambda(n) = \sum_{\substack{b=1\\(b,q')=1}}^{q'}\chi'(b)\psi(x;b,q')\\ &= \sum_{\substack{b=1\\(b,q')=1}}^{q'}\chi'(b)\frac{x}{\varphi(q')} + O\left(\sum_{\substack{b=1\\(b,q')=1}}^{q'}\chi'(b)xe^{-C\sqrt{\log x}}\right)\\ &\ll \varphi(q')xe^{-C\sqrt{\log x}},\end{aligned}$$

where in the last step we applied the character relations of Corollary II.1.2. (Note that χ' is not principal since it is primitive).

Setting $R = (\log x)^A$ this yields

$$\begin{aligned}\sum_{q'\le R}\frac{\log(Q)}{\varphi(q')}\sum_{\substack{\chi' \pmod{q'}\\ \chi' \text{ prim}}}|\psi^*(x,\chi')|^2 &\ll \sum_{q'\le R}\log(Q)(q'x)^2e^{-2C\sqrt{\log x}}\\ &\ll R^3\log Qx^2e^{-2C\sqrt{\log x}} \ll x^2(\log x)^{-A}.\end{aligned}$$

Altogether this gives the following.

Theorem II.6.3 (Barban–Davenport–Halberstam)**.** *Let A be arbitrary. We have*

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\psi(x;q,a) - \frac{x}{\varphi(q)}\right|^2 \ll x^2(\log x)^{-A} + Qx\log x.$$

In order to get an idea of the strength of the result, assume that we knew the Theorem of Siegel–Walfisz for all $q \le Q$. Then this would yield

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\psi(x;q,a) - \frac{x}{\varphi(q)}\right|^2 \ll \sum_{q\le Q}\varphi(q)x^2e^{-2C\sqrt{\log x}} \ll Q^2x^2e^{-2C\sqrt{\log x}}.$$

This is worse than Barban–Davenport–Halberstam whenever Q is larger than roughly $e^{-C\sqrt{\log x}}$, in particular if Q is comparable to any power of x.

Now assume that we know GRH. In this case, we would find

$$\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\psi(x;q,a) - \frac{x}{\varphi(q)}\right|^2 \ll \sum_{q\le Q}\varphi(q)x(\log x)^4 \ll Q^2x(\log x)^4.$$

Even this is weaker than Barban–Davenport–Halberstam as soon as Q is larger than roughly $\sqrt{x}$.

In fact, the Barban–Davenport–Halberstam theorem implies that

$$\psi(x;q,a) - \frac{x}{\varphi(q)} \ll \left(\frac{x}{\varphi(q)}\right)^{1/2+\varepsilon} \tag{II.6.3}$$

for the vast majority of moduli q. This statement is much stronger than even GRH.

In fact, average results similar to that of Barban–Davenport–Halberstam hold for a much wider class of cunctions.

Theorem II.6.4 (Bombieri–Friedlander–Iwaniec)**.** *Suppose f is an arithmetic function satisfying*

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q\\ (n,l)=1}} f(n) - \frac{1}{\varphi(q)} \sum_{\substack{n\le x\\ (n,ql)=1}} f(n) \ll \frac{\sqrt{x}}{(\log x)^A} \left(\sum_{n\le x} |f(n)|^2\right)^{1/2}$$

for every $A > 0$ and every $q \le x$, $l \le x$ and $(a, q) = 1$. Then the inequality

$$\sum_{q\le Q} \sum_{\substack{a=1\\ (a,q)=1}}^{q} \left| \sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) - \frac{1}{\varphi(q)} \sum_{n\le x} f(n)\right|^2 \ll (Q + x(\log x)^{-B}) \sum_{n\le x} |f(n)|^2$$

holds for every $B > 0$.

The Barban–Davenport–Halberstam theorem is the case $f = \Lambda$. Other functions covered by the theorem of Bombieri–Friedlander–Iwaniec are μ, μ^2 or d.

A result without averages is the theorem of Bombieri and Vinogradov.

Theorem II.6.5 (Bombieri–Vinogradov)**.** *Let A be arbitrary. We have*

$$\sum_{q\le Q} \max_{(a,q)=1} \max_{y\le x} \left|\psi(y; q, a) - \frac{y}{\varphi(q)}\right| \ll x(\log x)^{-A} + Q\sqrt{x}(\log Qx)^6.$$

It is clear that this is most useful for $Q \ll x^{1/2}(\log x)^{-A}$, when the first term dominates. In this range it shows that a statement similar to the Theorem of Siegel–Walfisz holds for all moduli $q \le x^{1/2-\varepsilon}$. In fact, even more is true: An error of the size $x(\log x)^{-A}$ can occur only a finite number of times. Furthermore, inserting GRH shows that

$$\sum_{q\le Q} \max_{(a,q)=1} \max_{y\le x} \left|\psi(y; q, a) - \frac{y}{\varphi(q)}\right| \ll Q\sqrt{x}(\log x)^2 \ll x(\log x)^{-A},$$

so we recover the theorem of Bombieri-Iwaniec. In this sense, Bombieri–Iwaniec is of a strength often comparable to GRH and can in many applications be substituted for it.

A conjectured stronger version of Bombieri–Iwaniec is the conjecture if Elliott and Halberstam.

Conjecture II.6.6 (Elliott–Halberstam)**.** *The inequality*

$$\sum_{q\le x^\theta} \max_{(a,q)=1} \max_{y\le x} \left|\psi(y; q, a) - \frac{y}{\varphi(q)}\right| \ll x(\log x)^{-A}$$

is true for any $\theta < 1$.

The parameter θ is often called the level of distribution. Obviously, Bombieri–Vinogradov proves Elliott–Halberstam for all $\theta < 1/2$. Observe that using GRH trivially only reproduces Bombieri–Vinogradov, so for the Elliott–Halberstam conjecture to be true, the error term should in most cases be closer to (II.6.3). In this sense, Elliott-Halberstam is much stronger than GRH.

In his work on bounded gaps between primes, Zhang managed to establish a modification of Bombieri–Vinogradov that, under some extra conditions, admitted for some values θ slightly larger than $1/2$, and this was the key to his argument. James Maynard found a different argument for which Bombieri–Vinogradov is sufficient.