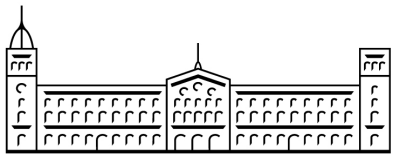

Treball final de màster

MÀSTER DE MATEMÀTICA AVANÇADA

Facultat de Matemàtiques
Universitat de Barcelona

Sieve Theory and Applications

Autor: Mario Sariols Quiles

Director: Dr. Luis Dieulefait
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 06 de setembre de 2017

Contents

Introduction

The object of this Master Thesis is the study of

1) sieve theory

2) a theorem due to J. Chen (1966) stating that every even large enough number is the sum of an odd prime and a product of at most two primes.

The proof of said theorem makes great use of sieving techniques. Thus, this Master Thesis' purpose is to introduce the required sieving methods in order to fully understand their application in said theorem's proof, as well as providing a proof of the theorem.

Section 1 introduces basic notations and methods of sieve theory. An upper bound is found for the prime counting function using elementary sieving methods, which is by no means comparable to the Prime Number Theorem, but is interesting on its own nonetheless. Moreover, a sieve due to Selberg is described and then applied to bounding above the twin prime counting function and the number of representations of any given even number as the sum of two primes. The references for this Section are mainly §7.2 of [1], §1.2 of [4] and §7 of [5].

Section 2 focuses on combinatorial sieves, which are in a sense a generalisation of the sieve shown in Section 1. In particular, it centers on linear sieves, that is, combinatorial sieves of dimension one. Finally, a theorem due to Jurkat and Richert on linear sieves is stated and proved for it will later be used in the proof of Chen's Theorem in Section 4. This section roughy follows §8 of [3] and §9 of [5].

Section 3 briefly presents large sieves due to the fact that a large sieve inequality will be needed in the proof of Chen's Theorem in Section 4. For more details, see §27 of [2] and §8 of [1].

Section 4 is exclusively dedicated to state and prove Chen's Theorem. Said proof is predominantly extracted from §10 of [5] and §11 of [3] to a lesser extent.

Acknowledgements

I would like to thank Professor Dieulefait for his guidance.

Notation

The letters p and q denote prime numbers. Similarly, n, m, d, N, among others, are always used for natural numbers. The set of natural numbers is denoted by

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Given m and n two natural numbers, write (m, n) to denote the greatest common divisor and $[m, n]$ the lowest common multiple of m and n. Moreover, $d^r \parallel n$ means the greatest power of d dividing n, that is, the greatest $r \geq 0$ such that $d^r \mid n$ and $d^{r+1} \nmid n$.
Given two functions f and g, write $f \ll g$ if there exists $A > 0$ such that $|f| \leq Ag$, the same as $f = O(g)$. Similarly, write $f \gg g$ if there exists $B > 0$ such that $|f| \geq Bg$. Finally, $f \ll_C g$ means there exists $A = A(C) > 0$ such that $|f| \leq Ag$.
$\pi(x)$ is the prime counting function:

$$\pi(x) = \sum_{p \leq x} 1$$

$\pi(x, a \bmod n)$ is the number of primes up to x congruent to a modulo n:

$$\pi(x, a \bmod n) = \sum_{\substack{p \leq x \\ p \equiv a (\bmod n)}} 1$$

$\omega(n)$ is the prime divisor function:

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

$\varphi(n)$ is Euler's totient function:

$$\varphi(n) = \sum_{\substack{d \leq n \\ (d,n)=1}} 1$$

γ is Euler's constant, and multiplicative functions are not identically 0.

1 Introduction to Sieve Theory

Given a finite set A of natural numbers, a set of primes $\mathcal{P}$ and a real number $z > 1$, the question is how many elements of A are not divisible by any prime in $\mathcal{P}$ smaller than z. Finding the answer to the previous question is what sieve theory seeks to accomplish.

The set A is referred as the sieving set, and $\mathcal{P}$ and z are often named the sieving range and sieving level, respectively. Together they define the sieving function

$$S(A, \mathcal{P}, z) = \sum_{\substack{a \in A \\ (a, P(z))=1}} 1$$

where

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$$

Thus, sieve theory tries to produce optimal upper and lower bounds for $S(A, \mathcal{P}, z)$.

Perhaps the most famous of sieves is the one due to Eratosthenes, who based the sieving of primes on the following remark:

Every natural number between 2 and N not divisible by any prime smaller or equal than the square root of N is a prime number.

Proof. Let $2 \leq n \leq N$. Write $n = p_1 \dots p_r$ as product of primes, where $r > 0$. If n is not divisible by any prime smaller or equal than $N^{\frac{1}{2}}$, then $p_i > N^{\frac{1}{2}}$, for all i. Hence $n > N^{\frac{r}{2}} \geq n^{\frac{r}{2}}$. Therefore, $1 > \frac{r}{2}$, which implies $r = 1$. □

In the above setting, Eratosthenes' sieve consists in sieving the set

$$A = \{n \in \mathbb{N} \, : \, n \leq N\}$$

with sieving range $\mathcal{P} = \mathbb{P}$ and sieving level $z = [N^{\frac{1}{2}} + 1]$. The value of z cannot simply be set to equal $N^{\frac{1}{2}}$ because of technical reasons with $P(z)$ being the product of primes $p < z$ rather than $p \leq z$. Anyhow

$$\sum_{\substack{N^{\frac{1}{2}} < n \leq N \\ (n, P(z))=1}} 1 = \sum_{N^{\frac{1}{2}} < p \leq N} 1 = \pi(N) - \pi(N^{\frac{1}{2}})$$

and therefore

$$S(A, \mathcal{P}, z) = \sum_{\substack{n \leq N \\ (n, P(z))=1}} 1 = 1 + \sum_{\substack{1 < n \leq N^{\frac{1}{2}} \\ (n, P(z))=1}} 1 + \sum_{\substack{N^{\frac{1}{2}} < n \leq N \\ (n, P(z))=1}} 1 = 1 + \pi(N) - \pi(N^{\frac{1}{2}})$$

since there is no $1 < n \leq N^{\frac{1}{2}}$ coprime with $P(z)$. An upper bound for $S(A, \mathcal{P}, z)$ will be found in order to estimate $\pi(N)$.

In a general setting, a way to find an upper bound for a sieving function, is to make use of the Möbius function (see Appendix B). By Theorem B.1

$$S(A,\mathcal{P},z) = \sum_{\substack{a\in A\\(a,P(z))=1}} 1 = \sum_{a\in A}\sum_{d|(a,P(z))}\mu(d) = \sum_{a\in A}\sum_{\substack{d|a\\d|P(z)}}\mu(d) = \sum_{d|P(z)}\mu(d)\sum_{\substack{a\in A\\d|a}}1$$

Given $d \in \mathbb{N}$ square-free, define

$$A_d = \{a \in A \ : \ d \mid a\}$$

Then

$$S(A,\mathcal{P},z) = \sum_{d|P(z)}\mu(d)|A_d|$$

since $d \mid P(z)$ implies d square-free. The above identity is known as Legendre's identity, and will be used in upcoming sections.
In the particular case of Eratosthenes' sieve

$$|A_d| = \sum_{\substack{n\le N\\d|n}} 1 = \left[\frac{N}{d}\right] = \frac{N}{d} - \left\{\frac{N}{d}\right\}$$

Hence

$$S(A,\mathcal{P},z) = N\sum_{d|P(z)}\frac{\mu(d)}{d} - \sum_{d|P(z)}\mu(d)\left\{\frac{N}{d}\right\}$$

By Theorem B.1 with $f(n) = \frac{1}{n}$, rewrite the first sum as

$$\sum_{d|P(z)}\frac{\mu(d)}{d} = \prod_{p|P(z)}\left(1-\frac{1}{p}\right)$$

Therefore

$$S(A,\mathcal{P},z) = N\prod_{p|P(z)}\left(1-\frac{1}{p}\right) + R$$

where

$$R = -\sum_{d|P(z)}\mu(d)\left\{\frac{N}{d}\right\} = \sum_{d|P(z)}O(1) = O\left(2^{\pi(z)}\right)$$

since the number of divisors of $P(z)$ is exatcly $2^{\omega(P(z))} = 2^{\pi(z)}$. The problem is that the error term R is too big for the chosen value of z (which is of order $N^{\frac{1}{2}}$) and thus very little can be said of $S(A,\mathcal{P},z)$. A solution appears itself by reducing the size of z. Set $z = \log N$. In this case

$$R = O\left(2^{\pi(\log N)}\right) = O(N^{\log 2})$$

since $2^{\pi(\log N)} \le 2^{\log N} = e^{\log N \log 2} = N^{\log 2}$. Moreover

$$S(A,\mathcal{P},z) \ge 1 + \pi(N) - \pi(z) \ge \pi(N) - z$$

since $S(A, \mathcal{P}, z)$ certainly counts the number one and every prime between z and N. Then

$$\pi(N) \leq z + S(A, \mathcal{P}, z) = \log N + N \prod_{p|P(z)} \left(1 - \frac{1}{p}\right) + R = N \prod_{p|P(z)} \left(1 - \frac{1}{p}\right) + O\left(N^{\log 2}\right)$$

where

$$\prod_{p|P(z)} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p<z} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p<z} \sum_{m \geq 0} \frac{1}{p^m} > \sum_{n<z} \frac{1}{n} > \int_1^z \frac{dx}{x} = \log z$$

Hence

$$\prod_{p|P(z)} \left(1 - \frac{1}{p}\right) < \frac{1}{\log z} = \frac{1}{\log \log N}$$

and therefore

$$\pi(N) \ll \frac{N}{\log \log N}$$

This result is much weaker than the Prime Number Theorem. Nonetheless it serves the purpose of showing how sieve theory can be applied.

1.1 Selberg's Sieve

In Selberg's sieve one replaces the Möbius function in

$$S(A, \mathcal{P}, z) = \sum_{\substack{a \in A \\ (a, P(z))=1}} 1 = \sum_{a \in A} \sum_{d|(a, P(z))} \mu(d)$$

with a sequence of real numbers $\{\lambda_d\}$, where d is square-free and $\lambda_1 = 1$, carefully chosen to minimise the final estimates. The reason being that

$$\sum_{d|(a, P(z))} \mu(d) \leq \left(\sum_{d|(a, P(z))} \lambda_d \right)^2$$

for any arbitrary sequence of numbers $\{\lambda_d\}$, with $\lambda_1 = 1$. The choice of $\lambda_d = 0$ for every $d \neq 1$ produces the trivial and useless bound

$$S(A, \mathcal{P}, z) \leq \sum_{a \in A} 1 = |A|$$

Theorem 1.1 (Selberg Sieve)**.** *Let A be a sieving set, $\mathcal{P}$ a sieving range and z a sieving level. Let*

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p<z}} p$$

and consider the sieving function

$$S(A, \mathcal{P}, z) = \sum_{\substack{a \in A \\ (a, P(z))=1}} 1$$

Let $A_d = \{a \in A \,:\, d \mid a\}$, for any $d \in \mathbb{N}$ square-free and f a multiplicative function such that $0 < f(p) < 1$, for every $p \in \mathcal{P}$. Define

$$r(d) = |A_d| - |A| f(d)$$

Let g be the completely multiplicative function defined by $g(p) = f(p)$ for every $p \in \mathcal{P}$ and

$$G(z) = \sum_{\substack{n<z \\ p|n \Rightarrow p \in \mathcal{P}}} g(n)$$

Then

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} |r(d)|$$

Proof. For every divisor d of $P(z)$, define $\lambda_1 = 1$ and $\lambda_d = 0$, for every $d \geq z$. Then, by Lemma A.5

$$\begin{aligned} S(A, \mathcal{P}, z) = \sum_{\substack{a \in A \\ (a, P(z))=1}} 1 &\leq \sum_{a \in A} \left(\sum_{d|(a,P(z))} \lambda_d \right)^2 = \sum_{a \in A} \sum_{\substack{d_1|a \\ d_1|P(z)}} \sum_{\substack{d_2|a \\ d_2|P(z)}} \lambda_{d_1} \lambda_{d_2} \\ &= \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{a \in A \\ [d_1,d_2]|a}} 1 = \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} |A_{[d_1,d_2]}| \\ &= |A| \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} f([d_1, d_2]) + \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} r([d_1, d_2]) \\ &= |A| \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} \frac{f(d_1) f(d_2)}{f((d_1, d_2))} + R = |A| T + R \end{aligned}$$

where

$$T = \sum_{\substack{d_1, d_2 < z \\ d_1, d_2 | P(z)}} \lambda_{d_1} \lambda_{d_2} \frac{f(d_1) f(d_2)}{f((d_1, d_2))}$$

is to be minimised by choosing appropriate values for λ_d, and

$$R = \sum_{\substack{d_1, d_2 < z \\ d_1, d_2 | P(z)}} \lambda_{d_1} \lambda_{d_2} r([d_1, d_2])$$

is the error term.
Let

$$F(n) = (\tfrac{1}{f} * \mu)(n) = \sum_{d|n} \frac{\mu(d)}{f\left(\frac{n}{d}\right)}$$

Then F is multiplicative, since both $\frac{1}{f}$ and μ are multiplicative functions and the Dirichlet convolution preserves multiplicativity. By Möbius inversion formula (Theorem B.2)

$$\frac{1}{f(n)} = \sum_{d|n} F(d)$$

Therefore

$$T = \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \lambda_{d_1}\lambda_{d_2}\frac{f(d_1)f(d_2)}{f((d_1,d_2))} = \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \lambda_{d_1}\lambda_{d_2}f(d_1)f(d_2)\sum_{d|(d_1,d_2)} F(d)$$

$$= \sum_{\substack{d<z \\ d|P(z)}} F(d) \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z) \\ d|(d_1,d_2)}} \lambda_{d_1}\lambda_{d_2}f(d_1)f(d_2) = \sum_{\substack{d<z \\ d|P(z)}} F(d)\left(\sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \lambda_\delta f(\delta)\right)^2$$

Let

$$w_d = \sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \lambda_\delta f(\delta)$$

By the dual Möbius inversion formula (Theorem B.3)

$$\lambda_d f(d) = \sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \mu\left(\frac{\delta}{d}\right) w_\delta$$

since w_d and $\lambda_d f(d)$ are defined in the divisor-closed set $\{\delta < z \,:\, \delta \mid P(z)\}$. In particular, for $d = 1$

$$1 = \lambda_1 f(1) = \sum_{\substack{\delta<z \\ \delta|P(z)}} \mu(\delta) w_\delta$$

Let $d \mid P(z)$. Then d is the product of distinct primes. This implies that $F(d) > 0$, since

$$F(p) = \frac{\mu(1)}{f(p)} + \frac{\mu(p)}{f(1)} = \frac{1}{f(p)} - 1 > 0$$

for all primes in $\mathcal{P}$, and F is multiplicative. Moreover, $\mu^2(d) = 1$. Let

$$V(z) = \sum_{\substack{d<z \\ d|P(z)}} \frac{1}{F(d)}$$

Then

$$T = \sum_{\substack{d<z \\ d|P(z)}} F(d) w_d^2 = \sum_{\substack{d<z \\ d|P(z)}} F(d)\left(w_d - \frac{\mu(d)}{F(d)V(z)}\right)^2 + \frac{1}{V(z)}$$

since

$$\sum_{\substack{d<z \\ d|P(z)}} F(d)\left(w_d - \frac{\mu(d)}{F(d)V(z)}\right)^2 = T + \sum_{\substack{d<z \\ d|P(z)}} \frac{\mu^2(d)}{F(d)V^2(z)} - 2\sum_{\substack{d<z \\ d|P(z)}} \frac{\mu(d)w_d}{V(z)}$$

$$= T + \frac{1}{V^2(z)}\sum_{\substack{d<z \\ d|P(z)}} \frac{1}{F(d)} - \frac{2}{V(z)}\sum_{\substack{d<z \\ d|P(z)}} \mu(d)w_d = T + \frac{1}{V(z)} - \frac{2}{V(z)} = T - \frac{1}{V(z)}$$

It is therefore manifest that the minimum value of T is

$$\frac{1}{V(z)}$$

attained at

$$w_d = \frac{\mu(d)}{F(d)V(z)}$$

since $F(d) > 0$. Substitute these values of w_d in the expression previously found for λ_d, to obtain

$$\lambda_d = \frac{1}{f(d)} \sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \mu\left(\frac{\delta}{d}\right) \frac{\mu(\delta)}{F(\delta)V(z)} = \frac{\mu(d)}{f(d)V(z)} \sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \frac{1}{F(\delta)}$$

since

$$\mu\left(\frac{\delta}{d}\right)\mu(\delta) = \frac{\mu^2(\delta)}{\mu(d)} = \frac{1}{\mu(d)} = \mu(d)$$

for every $\delta \mid P(z)$ such that $d \mid \delta$, for in this case, δ and d are both products of distinct primes. Moreover

$$\sum_{\substack{\delta<z \\ \delta|P(z) \\ d|\delta}} \frac{1}{F(\delta)} = \sum_{\substack{d\ell<z \\ d\ell|P(z)}} \frac{1}{F(d\ell)} = \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(d\ell)} = \frac{1}{F(d)} \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)}$$

Hence

$$\begin{aligned}\lambda_d &= \frac{\mu(d)}{f(d)F(d)V(z)} \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)} = \frac{\mu(d)}{V(z)} \prod_{p|d} \frac{1}{f(p)F(p)} \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)} \\ &= \frac{\mu(d)}{V(z)} \prod_{p|d} \frac{F(1)+F(p)}{F(p)} \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)} = \frac{\mu(d)}{V(z)} \prod_{p|d} \left(1+\frac{1}{F(p)}\right) \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)}\end{aligned}$$

since d is product of distinct primes, and therefore, $f(d)$ and $F(d)$ are completely multiplicative. By Theorem B.1

$$\begin{aligned}|\lambda_d| &= \frac{1}{V(z)} \left|\sum_{h|d} \frac{\mu(h)}{F(h)}\right| \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)} \leq \frac{1}{V(z)} \sum_{h|d} \frac{1}{F(h)} \sum_{\substack{d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(\ell)} \\ &= \frac{1}{V(z)} \sum_{\substack{h,\ell \\ h|d \\ d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(h)F(\ell)} = \frac{1}{V(z)} \sum_{\substack{h,\ell \\ h|d \\ d\ell<z \\ d\ell|P(z) \\ (d,\ell)=1}} \frac{1}{F(h\ell)} \leq \frac{1}{V(z)} \sum_{\substack{h\ell<z \\ h\ell|P(z)}} \frac{1}{F(h\ell)} = 1\end{aligned}$$

Thus

$$|R| \leq \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} |r([d_1,d_2])| = \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \sum_{[d_1,d_2]=d} |r(d)| \leq \sum_{\substack{d<z^2 \\ d|P(z)}} |r(d)| \sum_{\substack{d_1,d_2 \\ [d_1,d_2]=d}} 1$$
$$= \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|$$

since the amount of ordered pairs (d_1,d_2) such that $[d_1,d_2]=d$, where d is the product of distinct primes, say $d=p_1\dots p_r$, is exactly 3^r, because of the fact that $d_1=\prod_{i=1}^r p_i^{\alpha_i}$ and $d_2=\prod_{i=1}^r p_i^{\beta_i}$ where α_i,β_i are nonnegative integers, and

$$p_1\dots p_r = d = [d_1,d_2] = \prod_{i=1}^r p_i^{\max(\alpha_i,\beta_i)}$$

which implies that the amount of ordered pairs (d_1,d_2) such that $[d_1,d_2]=d$ is equal to the amount of ordered pairs (α_i,β_i) such that $\max(\alpha_i,\beta_i)=1$, which is 3 for every i, corresponding to the pairs $(1,0)$, $(0,1)$ and $(1,1)$.
Hence

$$S(A,\mathcal{P},z) \leq \frac{|A|}{V(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|$$

To conclude, it is enough to prove that $V(z)\geq G(z)$. Let $d \mid P(z)$. Then, d is the product of distinct primes. Thus, $(h,\frac{d}{h})=1$, for every $h \mid d$. Hence $f(d)=f(h\frac{d}{h})=f(h)f(\frac{d}{h})$. Therefore

$$F(d) = \sum_{h|d} \frac{\mu(h)}{f\left(\frac{d}{h}\right)} = \frac{1}{f(d)} \sum_{h|d} \mu(h)f(h) = \frac{1}{f(d)} \prod_{p|d}(1-f(p))$$

by Theorem B.1. Then

$$V(z) = \sum_{\substack{d<z \\ d|P(z)}} \frac{1}{F(d)} = \sum_{\substack{d<z \\ d|P(z)}} f(d) \prod_{p|d} \frac{1}{1-f(p)} = \sum_{\substack{d<z \\ d|P(z)}} g(d) \prod_{p|d} \frac{1}{1-g(p)}$$
$$= \sum_{\substack{d<z \\ d|P(z)}} g(d) \prod_{p|d} \sum_{n\geq 0} g(p)^n = \sum_{\substack{d<z \\ d|P(z)}} g(d) \prod_{p|d} \sum_{n\geq 0} g(p^n)$$
$$= \sum_{\substack{d<z \\ d|P(z)}} g(d) \sum_{\substack{m\geq 1 \\ p|m\Rightarrow p|d}} g(m) = \sum_{\substack{d<z \\ d|P(z)}} \sum_{\substack{m\geq 1 \\ p|m\Rightarrow p|d}} g(dm) = \sum_{\substack{d<z \\ d|P(z)}} \sum_{\substack{k\geq 1 \\ d|k \\ p|\frac{k}{d}\Rightarrow p|d}} g(k)$$
$$= \sum_{\substack{k<z \\ p|k\Rightarrow p\in\mathcal{P}}} g(k) \sum_{\substack{d<z \\ d|P(z) \\ d|k \\ p|\frac{k}{d}\Rightarrow p|d}} 1 \geq \sum_{\substack{k<z \\ p|k\Rightarrow p\in\mathcal{P}}} g(k) = G(z)$$

where the last inequality follows from the fact that

$$\sum_{\substack{d<z \\ d|P(z) \\ d|k \\ p|\frac{k}{d}\Rightarrow p|d}} 1 \geq 1$$

since the sum certainly includes d equal the product of all distinct primes that divide k. Thus

$$S(A,\mathcal{P},z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)|$$

□

1.2 Twin Primes and Sums of Two Primes

Selberg's sieve can be applied to provide an upper bound for the number of twin primes up to a given number and for the number of representations of an even number as the sum of two primes.

The twin prime conjecture states that there exist infinitely many primes p such that $p+2$ is prime. Let $\pi_2(x)$ be the number of twin primes up to x. Then, the twin prime conjecture is equivalent to $\lim_{x\to+\infty}\pi_2(x) = +\infty$. Selberg's sieve will provide the following upper bound for $\pi_2(x)$:

$$\pi_2(x) \ll \frac{x}{\log^2 x}$$

Goldbach's conjecture states that every even natural number greater than 2 can be written as the sum of two primes. Equivalently, $\mathfrak{R}(N) \geq 1$, for every even $N > 2$, where $\mathfrak{R}(N)$ is the number of representations of N as the sum of two primes. Using Selberg's sieve, one can find the following upper bound for $\mathfrak{R}(N)$:

$$\mathfrak{R}(N) \ll \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{N}{\log^2 N}$$

Before proving either of the above, a lemma.

Lemma 1.2. *Let N be an even natural number and f the completely multiplicative function defined by*

$$f(p) = \begin{cases} \frac{1}{p} & \text{if } p \mid N \\ \frac{2}{p} & \text{otherwise} \end{cases}$$

Let $G(z) = \sum_{n<z} f(n)$. Then

$$\frac{1}{G(z)} \ll \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{1}{\log^2 z}$$

Proof. Let $n < z$. Write

$$n = \prod_{i=1}^{\omega(N)} p_i^{\alpha_i} \prod_{j=1}^{k} q_j^{\beta_j}$$

where $p_1, \ldots, p_{\omega(N)}$ are the distinct primes that divide N, and $q_1, \ldots, q_k$ are distinct primes not dividing N, with k, α_i and β_j nonnegative integers. Then

$$f(n) = \prod_{i=1}^{\omega(N)} f(p_i)^{\alpha_i} \prod_{j=1}^{k} f(q_j)^{\beta_j} = \prod_{i=1}^{\omega(N)} \frac{1}{p_i^{\alpha_i}} \prod_{j=1}^{k} \frac{2^{\beta_j}}{q_j^{\beta_j}} = \frac{2^{\beta_1+\ldots+\beta_k}}{n}$$

Let $d(s) = \sum_{d|s} 1$ be the divisor function and

$$d(s, N) = \sum_{\substack{d|s \\ (d,N)=1}} 1$$

Then

$$d(n, N) = d\left(\prod_{j=1}^{k} q_j^{\beta_j}\right) = \prod_{j=1}^{k}(1+\beta_j) \leq \prod_{j=1}^{k} 2^{\beta_j} = 2^{\beta_1+\ldots+\beta_k}$$

since $d \mid \prod_{j=1}^{k} q_j^{\beta_j}$ if and only if

$$d = \prod_{j=1}^{k} q_j^{\gamma_j}$$

where $0 \leq \gamma_j \leq \beta_j$, for every j, that is, $1 + \beta_j$ possible different values for γ_j, for every j. Hence

$$G(z) = \sum_{n<z} f(n) \geq \sum_{n<z} \frac{d(n, N)}{n}$$

Rewrite

$$\prod_{p|N}\left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|N} \sum_{m\geq 0} \frac{1}{p^m} = \sum_{\substack{r\geq 1 \\ p|r \Rightarrow p|N}} \frac{1}{r}$$

to get

$$\begin{aligned} G(z) \prod_{p|N}\left(1 - \frac{1}{p}\right)^{-1} &\geq \sum_{n<z} \frac{d(n, N)}{n} \sum_{\substack{r\geq 1 \\ p|r\Rightarrow p|N}} \frac{1}{r} = \sum_{n<z} d(n, N) \sum_{\substack{r\geq 1 \\ p|r\Rightarrow p|N}} \frac{1}{nr} \\ &= \sum_{n<z} d(n, N) \sum_{\substack{s\geq 1 \\ n|s \\ p|\frac{s}{n}\Rightarrow p|N}} \frac{1}{s} = \sum_{s\geq 1} \frac{1}{s} \sum_{\substack{n<z \\ n|s \\ p|\frac{s}{n}\Rightarrow p|N}} d(n, N) \\ &\geq \sum_{s<z} \frac{1}{s} \sum_{\substack{n|s \\ p|\frac{s}{n}\Rightarrow p|N}} d(n, N) \end{aligned}$$

Let $s < z$ and n be such that $n \mid s$ and $p \mid N$ for every $p \mid \frac{s}{n}$. Write

$$s = \prod_{i=1}^{\omega(N)} p_i^{a_i} \prod_{j=1}^{k} q_j^{b_j}$$

and

$$n = \prod_{i=1}^{\omega(N)} p_i^{c_i} \prod_{j=1}^{k} q_j^{d_j}$$

where $p_1, \ldots, p_{\omega(N)}$ are the distinct primes that divide N, and $q_1, \ldots, q_k$ are distinct primes not dividing N, with k, a_i, b_j, c_i and d_j nonnegative integers. Then

$$\frac{s}{n} = \prod_{i=1}^{\omega(N)} p_i^{a_i - c_i} \prod_{j=1}^{k} q_j^{b_j - d_j}$$

where $a_i - c_i \geq 0$ and $b_j - d_j \geq 0$, since $n \mid s$. In fact, $b_j = d_j$, since $p \mid N$ for every $p \mid \frac{s}{n}$. In particular

$$d(n, N) = \prod_{j=1}^{k} (1 + d_j) = \prod_{j=1}^{k} (1 + b_j)$$

Furthermore, the number of divisors n of s such that $p \mid N$ for every $p \mid \frac{s}{n}$ is exactly

$$\prod_{i=1}^{\omega(N)} (1 + a_i)$$

since the exponents d_j are completely determined by s and there are as much as $1 + a_i$ possible different values for c_i, for every i, because $0 \leq c_i \leq a_i$, for every i. Thus

$$\sum_{\substack{n \mid s \\ p \mid \frac{s}{n} \Rightarrow p \mid N}} d(n, N) = \prod_{j=1}^{k} (1 + b_j) \sum_{\substack{n \mid s \\ p \mid \frac{s}{n} \Rightarrow p \mid N}} 1 = \prod_{j=1}^{k} (1 + b_j) \prod_{i=1}^{\omega(N)} (1 + a_i) = d(s)$$

Finally, by Lemma A.2

$$G(z) \prod_{p \mid N} \left(1 - \frac{1}{p}\right)^{-1} \geq \sum_{s < z} \frac{d(s)}{s} \gg \log^2 z$$

which implies

$$\begin{aligned} \frac{1}{G(z)} &\ll \frac{1}{\log^2 z} \prod_{p \mid N} \frac{p}{p-1} = \frac{1}{\log^2 z} \prod_{p \mid N} \frac{p(p+1)}{p^2 - 1} = \frac{1}{\log^2 z} \prod_{p \mid N} \frac{p^2}{p^2 - 1} \prod_{p \mid N} \frac{p+1}{p} \\ &= \frac{1}{\log^2 z} \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \ll \frac{1}{\log^2 z} \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \end{aligned}$$

where, in the last inequality, one uses that fact that

$$\prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)^{-1} \leq \prod_{p} \left(1 - \frac{1}{p^2}\right)^{-1} = \zeta(2) < +\infty$$

□

After the lemma, both previously stated results can be proved.

Theorem 1.3. *Let $x \geq 1$ be a real number and $\pi_2(x)$ the number of twin primes up to x. Then*

$$\pi_2(x) \ll \frac{x}{\log^2 x}$$

Proof. Consider the sieving set

$$A = \{n(n+2) \ : \ n \leq x\}$$

of $[x]$ elements. Let $\mathcal{P} = \mathbb{P}$ be the sieving range and $z = x^{\frac{1}{8}}$ the sieving level. Then

$$S(A, \mathbb{P}, z) = \sum_{\substack{n \leq x \\ (n(n+2), P(z))=1}} 1$$

Let $z < n \leq x$. Assume that $p \mid n(n+2)$, for some $p < z$. Then, $p \mid n$ or $p \mid (n+2)$, which implies, $n \notin \mathbb{P}$ or $n+2 \notin \mathbb{P}$, since $n+2 > n > z > p$. This means that $(n(n+2), P(z)) = 1$ if both $n \in \mathbb{P}$ and $n+2 \in \mathbb{P}$, with $z < n \leq x$. Therefore

$$\pi_2(x) = \sum_{\substack{p \leq x \\ p+2 \in \mathbb{P}}} 1 = \pi_2(z) + \sum_{\substack{z < p \leq x \\ p+2 \in \mathbb{P}}} 1 \leq \pi_2(z) + S(A, \mathbb{P}, z) \leq z + S(A, \mathbb{P}, z)$$

In order to apply Selberg's sieve, consider the sets $A_d = \{a \in A \ : \ d \mid a\}$, for all $d \in \mathbb{N}$ square-free. Let f the completely multiplicative function defined by

$$f(p) = \begin{cases} \frac{1}{p} & \text{if } p \mid N \\ \frac{2}{p} & \text{otherwise} \end{cases}$$

Define

$$r(d) = |A_d| - [x]f(d)$$

and

$$G(z) = \sum_{n<z} f(n)$$

Then, by Selberg's sieve (Theorem 1.1)

$$S(A, \mathbb{P}, z) \leq \frac{[x]}{G(z)} + \sum_{\substack{d < z^2 \\ d \mid P(z)}} 3^{\omega(d)} |r(d)|$$

and by Lemma 1.2 with $N = 2$

$$\frac{1}{G(z)} \ll \prod_{p \mid 2} \left(1 + \frac{1}{p}\right) \frac{1}{\log^2 z} = \left(1 + \frac{1}{2}\right) \frac{64}{\log^2 x} \ll \frac{1}{\log^2 x}$$

To find an upper bound for the error term, let $d \mid P(z)$. Write d as $d = p_1 \dots p_r$ or $d = 2p_1 \dots p_r$, with $2 < p_i < z$ distinct primes and $r \geq 0$, and consider

$$|A_d| = \sum_{\substack{n \leq x \\ d \mid n(n+2)}} 1$$

which equals the number of solutions to the congruence $n(n+2) \equiv 0 \pmod{d}$, for $n \leq x$. It is enough to solve this congruence for primes only and then apply the Chinese Remainder Theorem, since d is product of distinct primes. Let $p = 2$. Then $n(n+2) \equiv 0 \pmod{2}$ if and only if $n \equiv 0 \pmod{2}$, which corresponds to only 1 residue class modulo 2. Let $p > 2$. Then $n(n+2) \equiv 0 \pmod{p}$ if and only if $n \equiv 0 \pmod{p}$ or $n+2 \equiv 0 \pmod{p}$, which corresponds to 2 different residue classes modulo p. Hence, by the Chinese Remainder Theorem, $n(n+2) \equiv 0 \pmod{d}$ if and only if n lies on any of some 2^r different residue classes modulo d. Therefore

$$|A_d| = \sum_{i=1}^{2^r} \sum_{\substack{n \leq x \\ n \equiv \alpha_i \pmod{d}}} 1 = \sum_{i=1}^{2^r} \left[\frac{x}{d}\right] = 2^r \left[\frac{x}{d}\right]$$

where α_i are the said 2^r different residue classes modulo d. Thus

$$|A_d| = 2^r \left(\frac{[x]}{d} + O(1)\right) = [x] f(d) + O(2^r)$$

since $f(d) = \frac{2^r}{d}$, whence

$$r(d) = O(2^r) = O(2^{\omega(d)})$$

since $\omega(d)$ equals either r or $r+1$ (depending whether d is odd or even). This bound for $r(d)$ allows the proof to be concluded, because

$$\begin{aligned}\sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)| \ll \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}2^{\omega(d)} = \sum_{\substack{d<z^2 \\ d|P(z)}} 6^{\omega(d)} \leq \sum_{d<z^2} 6^{\omega(d)} < \sum_{d<z^2} z^{2\frac{\log 6}{\log 2}} < z^{2+2\frac{\log 6}{\log 2}} \\ < z^{7.2} = x^{\frac{7.2}{8}} = x^{\frac{9}{10}}\end{aligned}$$

since

$$6^{\omega(d)} = 2^{\frac{\log 6}{\log 2}\omega(d)} = (2^{\omega(d)})^{\frac{\log 6}{\log 2}} \leq d^{\frac{\log 6}{\log 2}} < z^{2\frac{\log 6}{\log 2}}$$

for any $d < z^2$, and therefore

$$\pi_2(x) \leq x^{\frac{1}{8}} + S(A, \mathbb{P}, z) \ll x^{\frac{1}{8}} + \frac{x}{\log^2 x} + x^{\frac{9}{10}} \ll \frac{x}{\log^2 x}$$

□

Corollary 1.4. *The sum of reciprocals of twin primes converges.*

Proof. Let p_n be the n-th twin prime. Then, by Theorem 1.3

$$n = \pi_2(p_n) \ll \frac{p_n}{\log^2 p_n} \leq \frac{p_n}{\log^2 n}$$

for every $n > 1$. Hence

$$\sum_{\substack{p \\ p+2 \in \mathbb{P}}} \frac{1}{p} = \sum_{n \geq 1} \frac{1}{p_n} \leq \frac{1}{3} + \sum_{n \geq 2} \frac{1}{n \log^2 n} < +\infty$$

since $p_1 = 3$. □

Finally, the second application of Selberg's sieve, whose proof is very similar to that of Theorem 1.3.

Theorem 1.5. *Let $N > 2$ be an even natural number and $\mathfrak{R}(N)$ denote the number of representations of N as the sum of two primes. Then*

$$\mathfrak{R}(N) \ll \prod_{p|N} \left(1 + \frac{1}{p}\right) \frac{N}{\log^2 N}$$

It has to be made clear that the number of representations of N as the sum of two primes is to be understood as the number of ordered pairs of primes whose sum is N. Hence $12 = 5 + 7 = 7 + 5$ are considered different representations of 12 as sum of two primes. This can be adjusted by a factor of 2.

Proof. Consider the sieving set

$$A = \{n(N-n) \ : \ n \leq N\}$$

of N elements. Let $\mathcal{P} = \mathbb{P}$ be the sieving range and $z = N^{\frac{1}{8}}$ the sieving level. In particular

$$S(A, \mathbb{P}, z) = \sum_{\substack{n \leq N \\ (n(N-n), P(z))=1}} 1$$

Let $z < n < N - z$. Assume that $p \mid n(N-n)$, for some $p < z$. Then, $p \mid n$ or $p \mid (N-n)$, which implies, $n \notin \mathbb{P}$ or $N - n \notin \mathbb{P}$, since $n > z > p$ and $N - n > z > p$. This means that $(n(N-n), P(z)) = 1$ if both $n \in \mathbb{P}$ and $N - n \in \mathbb{P}$, with $z < n < N - z$. Therefore

$$\mathfrak{R}(N) = \sum_{\substack{p \leq z \\ N-p \in \mathbb{P}}} 1 + \sum_{\substack{z < p < N-z \\ N-p \in \mathbb{P}}} 1 + \sum_{\substack{p \geq N-z \\ N-p \in \mathbb{P}}} 1 \leq z + S(A, \mathbb{P}, z) + z = 2z + S(A, \mathbb{P}, z)$$

Similarly to the proof of Theorem 1.3, consider the sets $A_d = \{a \in A \ : \ d \mid a\}$, for all $d \in \mathbb{N}$ square-free, and f the completely multiplicative function defined by

$$f(p) = \begin{cases} \frac{1}{p} & \text{if } p \mid N \\ \frac{2}{p} & \text{otherwise} \end{cases}$$

Let

$$r(d) = |A_d| - Nf(d)$$

and

$$G(z) = \sum_{n<z} f(n)$$

By Selberg's sieve (Theorem 1.1)

$$S(A, \mathbb{P}, z) \leq \frac{N}{G(z)} + \sum_{\substack{d < z^2 \\ d | P(z)}} 3^{\omega(d)} |r(d)|$$

and by Lemma 1.2

$$\frac{1}{G(z)} \ll \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{1}{\log^2 z} = \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{64}{\log^2 N} \ll \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{1}{\log^2 N}$$

The same bound for the error term will be found as in Theorem 1.3. Write $d \mid P(z)$ as $d = q_1 \dots q_k p_1 \dots p_r$, with $q_j \mid N$ and $p_i \nmid N$ all distinct primes and $k, r \geq 0$. Now

$$|A_d| = \sum_{\substack{n \leq N \\ d \mid n(N-n)}} 1$$

which equals the number of solutions to the congruence $n(N-n) \equiv 0 \pmod d$, for $n \leq x$. It is enough to solve this congruence for primes only and then apply the Chinese Remainder Theorem, since d is product of distinct primes. Let $q \mid N$. Then $n(N-n) \equiv 0 \pmod q$ if and only if $n \equiv 0 \pmod q$, which corresponds to only 1 residue class modulo q. Let $p \nmid N$. Then $n(N-n) \equiv 0 \pmod p$ if and only if $n \equiv 0 \pmod p$ or $N - n \equiv 0 \pmod p$, which corresponds to 2 different residue classes modulo p. Hence, by the Chinese Remainder Theorem, $n(N-n) \equiv 0 \pmod d$ if and only if n lies on any of some $1^k 2^r = 2^r$ different residue classes modulo d. Therefore

$$|A_d| = \sum_{i=1}^{2^r} \sum_{\substack{n \leq N \\ n \equiv \alpha_i \pmod d}} 1 = \sum_{i=1}^{2^r} \left[\frac{N}{d}\right] = 2^r \left[\frac{N}{d}\right]$$

where α_i are the said 2^r different residue classes modulo d. Thus

$$|A_d| = 2^r \left(\frac{N}{d} + O(1)\right) = Nf(d) + O(2^r)$$

since $f(d) = \frac{2^r}{d}$, whence

$$r(d) = O(2^r) = O(2^{\omega(d)})$$

since $r \leq \omega(d)$. Finally

$$\sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}|r(d)| \ll \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}2^{\omega(d)} = \sum_{\substack{d<z^2 \\ d|P(z)}} 6^{\omega(d)} \leq \sum_{d<z^2} 6^{\omega(d)} < \sum_{d<z^2} z^{2\frac{\log 6}{\log 2}} < z^{2+2\frac{\log 6}{\log 2}}$$
$$< z^{7.2} = N^{\frac{7.2}{8}} = N^{\frac{9}{10}}$$

since

$$6^{\omega(d)} = 2^{\frac{\log 6}{\log 2}\omega(d)} = (2^{\omega(d)})^{\frac{\log 6}{\log 2}} \leq d^{\frac{\log 6}{\log 2}} < z^{2\frac{\log 6}{\log 2}}$$

for any $d < z^2$, and therefore

$$\mathfrak{R}(N) \leq 2N^{\frac{1}{8}} + S(A, \mathbb{P}, z) \ll 2N^{\frac{1}{8}} + \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{N}{\log^2 N} + N^{\frac{9}{10}} \ll \prod_{p|N}\left(1+\frac{1}{p}\right)\frac{N}{\log^2 N}$$

□

2 Linear Sieve

Given a sieving set A, a sieving range $\mathcal{P}$ and a sieving level z, the sieving function

$$S(A, \mathcal{P}, z) = \sum_{\substack{a \in A \\ (a, P(z))=1}} 1$$

where

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$$

can be rewritten as

$$S(A, \mathcal{P}, z) = \sum_{d | P(z)} \mu(d) |A_d|$$

as seen in Section 1, known as Legendre's identity, where

$$A_d = \{a \in A \ : \ d \mid a\}$$

for any square-free $d \in \mathbb{N}$. Let f be a multiplicative function such that

$$0 < f(p) < 1$$

for every $p \in \mathcal{P}$. Define

$$r(d) = |A_d| - |A| f(d)$$

Then, by Theorem B.1

$$\begin{aligned} S(A, \mathcal{P}, z) &= |A| \sum_{d | P(z)} \mu(d) f(d) + \sum_{d | P(z)} \mu(d) r(d) = |A| \prod_{p | P(z)} (1 - f(p)) + \sum_{d | P(z)} \mu(d) r(d) \\ &= |A| V(z) + R(z) \end{aligned}$$

where

$$V(z) = \prod_{p | P(z)} (1 - f(p))$$

and

$$R(z) = \sum_{d | P(z)} \mu(d) r(d)$$

The sum that defines the error term $R(z)$ has as much as $2^{\omega(P(z))} = 2^{\pi(z)}$ addends, which makes it bigger than the non-error terms in many occasions.

In a combinatorial sieve, the Möbius function is replaced by two arithmetic functions with similar properties to those of μ with the objective of reducing the size of $R(z)$. Two functions λ^+ and λ^- are respectively called upper and lower bound sieves if

$$\lambda^-(1) = 1 = \lambda^+(1)$$

and

$$\sum_{d | n} \lambda^-(d) \leq 0 \leq \sum_{d | n} \lambda^+(d)$$

for every $n > 1$.

Moreover, assume there exists $D > 0$ and a set of primes $\mathcal{P}_0$, such that

$$\lambda^-(d) = 0 = \lambda^+(d)$$

for all $d \geq D$ and for all $d \mid p$ with $p \notin \mathcal{P}_0$. Then $\lambda^\pm$ are said to have support level D and sieving range $\mathcal{P}_0$.

A combinatorial sieve is said to have dimension $n > 0$ if

$$\prod_{\substack{p \in \mathcal{P} \\ u \leq p < z}} \frac{1}{1 - f(p)} \leq C \left(\frac{\log z}{\log u} \right)^n$$

for some $C > 1$ and for all $1 < u < z$. The case $n = 1$ is called linear sieve.

The Jurkat-Richert Theorem is a result on linear sieves that provides upper and lower bounds for sieving functions. This theorem makes use of a general combinatorial sieve and a particular upper and lower bound sieves, which are to be studied in Section 2.1, and some bounds for

$$\sum_{p \mid P(z)} \lambda^\pm(d) f(d)$$

involving two functions Φ and ϕ defined in Section 2.2.

2.1 Combinatorial Sieve

Theorem 2.1. *Let A be a sieveing set, $\mathcal{P}$ a sieving range and z a sieving level. Let $\mathcal{P}_0$ be a subset of $\mathcal{P}$ such that $\mathcal{Q} = \mathcal{P} \setminus \mathcal{P}_0$ is finite. Let $\lambda^\pm$ be upper and lower bound sieves with support level D and sieving range $\mathcal{P}_0$, such that $|\lambda^\pm(d)| \leq 1$, for all d. Let $P(z) = \prod_{\mathcal{P} \ni p < z} p$, $P_0(z) = \prod_{\mathcal{P}_0 \ni p < z} p$, $Q(z) = \prod_{\mathcal{Q} \ni p < z} p$ and $Q = \prod_{p \in \mathcal{Q}} p$. Let f be a multiplicative function such that $0 < f(p) < 1$, for every $p \in \mathcal{P}$. For every square-free d, define*

$$r(d) = |A_d| - |A| f(d)$$

where $A_d = \{a \in A \,:\, d \mid a\}$. Finally, let

$$F(z, \lambda^\pm) = \sum_{d \mid P_0(z)} \lambda^\pm(d) f(d)$$

Then

$$S(A, \mathcal{P}, z) \leq |A| F(z, \lambda^+) \prod_{p \mid Q(z)} (1 - f(p)) + R$$

and

$$S(A, \mathcal{P}, z) \geq |A| F(z, \lambda^-) \prod_{p \mid Q(z)} (1 - f(p)) - R$$

where

$$R = \sum_{\substack{d < DQ \\ d \mid P(z)}} |r(d)|$$

Proof. Let $d \in \mathbb{N}$ be square-free. There exist unique d_1 and d_2 such that $d = d_1 d_2$ with $(d_1, Q) = 1$ and d_2 is divisible only by primes in $\mathcal{Q}$. Define

$$\Lambda^{\pm}(d) = \lambda^{\pm}(d_1)\mu(d_2)$$

Then $\Lambda^{-}(1) = 1 = \Lambda^{+}(1)$, since $\lambda^{-}(1) = 1 = \lambda^{+}(1)$. Moreover, for every $n \in \mathbb{N}$, there exist unique n_1 and n_2 such that $n = n_1 n_2$ with $(n_1, Q) = 1$ and n_2 is divisible only by primes in $\mathcal{Q}$. Hence

$$\sum_{d|n} \Lambda^{\pm}(d) = \sum_{d_1 d_2 | n_1 n_2} \lambda^{\pm}(d_1)\mu(d_2) = \sum_{d_1|n_1} \lambda^{\pm}(d_1) \sum_{d_2|n_2} \mu(d_2)$$

By Theorem B.1

$$\sum_{d|n} \Lambda^{-}(d) \leq 0 \leq \sum_{d|n} \Lambda^{+}(d)$$

for every $n > 1$, since $\lambda^{\pm}$ are upper and lower bound sieves. Thus, $\Lambda^{\pm}$ are upper and lower bound sieves.
Let $p \mid d$ where $p \notin \mathcal{P}$. Then, $p \notin \mathcal{P}_0$ and $p \notin \mathcal{Q}$. Write $d = d_1 d_2$, for some unique d_1 and d_2 with $(d_1, Q) = 1$ and d_2 divisible only by primes in $\mathcal{Q}$. It follows that $p \mid d_1$, since $(p, d_2) = 1$. Let $d_1 = pd_3$. Then $d = pd_3 d_2$, where $(pd_3, Q) = 1$ and d_2 is divisible only by primes in $\mathcal{Q}$. Therefore

$$\Lambda^{\pm}(d) = \lambda^{\pm}(pd_3)\mu(d_2) = 0$$

since $\lambda^{\pm}(pd_3) = 0$, because $\lambda^{\pm}$ are upper and lower bound sieves with sieving range $\mathcal{P}_0$ and $p \notin \mathcal{P}_0$. This implies that $\Lambda^{\pm}$ have sieving range $\mathcal{P}$.
Let $d \geq DQ$. Write $d = d_1 d_2$, for some unique d_1 and d_2 with $(d_1, Q) = 1$ and d_2 divisible only by primes in $\mathcal{Q}$. Then, either $d_2 \leq Q$, which implies $d_1 \geq D$ and in particular, $\lambda^{\pm}(d_1) = 0$, since $\lambda^{\pm}$ have support level D; or $d_2 > Q$, which implies d_2 is not square-free, and hence, $\mu(d_2) = 0$. In either case, $\Lambda^{\pm}(d) = 0$. Therefore, $\Lambda^{\pm}$ have support level DQ.
Finally

$$\begin{aligned}\sum_{a\in A} \sum_{d|(a,P(z))} \Lambda^{\pm}(d) &= \sum_{d|P(z)} \Lambda^{\pm}(d) \sum_{\substack{a\in A \\ d|a}} 1 = \sum_{d|P(z)} \Lambda^{\pm}(d)|A_d| \\ &= \sum_{d|P(z)} \Lambda^{\pm}(d)|A|f(d) + \sum_{d|P(z)} \Lambda^{\pm}(d)r(d) = |A| \sum_{d|P(z)} \Lambda^{\pm}(d)f(d) + \sum_{\substack{d<DQ \\ d|P(z)}} \Lambda^{\pm}(d)r(d)\end{aligned}$$

where

$$\sum_{d|P(z)} \Lambda^{\pm}(d)f(d) = \sum_{d_1|P_0(z)} \sum_{d_2|Q(z)} \Lambda^{\pm}(d_1 d_2)f(d_1 d_2) = \sum_{d_1|P_0(z)} \lambda^{\pm}(d_1)f(d_1) \sum_{d_2|Q(z)} \mu(d_2)f(d_2)$$

since $P(z) = P_0(z)Q(z)$ and $(P_0(z), Q(z)) = 1$, because $\mathcal{P}_0$ and $\mathcal{Q}$ are disjoint, and $f(d_1 d_2) = f(d_1)f(d_2)$ by multilicativity of f. By Theorem B.1

$$\sum_{a\in A} \sum_{d|(a,P(z))} \Lambda^{\pm}(d) = |A|F(z, \lambda^{\pm}) \prod_{p|Q(z)} (1 - f(p)) + \sum_{\substack{d<DQ \\ d|P(z)}} \Lambda^{\pm}(d)r(d)$$

Use the fact that $-1 \leq \Lambda^{\pm}(d) \leq 1$ to obtain

$$S(A,\mathcal{P},z) = \sum_{\substack{a\in A\\(a,P(z))=1}} 1 \leq \sum_{a\in A}\sum_{d|(a,P(z))} \Lambda^{+}(d) \leq |A|F(z,\lambda^{+}) \prod_{p|Q(z)}(1-f(p)) + \sum_{\substack{d<DQ\\d|P(z)}} r(d)$$

and

$$S(A,\mathcal{P},z) = \sum_{\substack{a\in A\\(a,P(z))=1}} 1 \geq \sum_{a\in A}\sum_{d|(a,P(z))} \Lambda^{-}(d) \geq |A|F(z,\lambda^{-}) \prod_{p|Q(z)}(1-f(p)) - \sum_{\substack{d<DQ\\d|P(z)}} r(d)$$

□

Next, two functions will be defined and proved to be upper and lower bound sieves with both support level and sieving range at choice, and such that they are always bounded by 1 in absolute value.

Lemma 2.2. *Let $D > 0$ and $\mathcal{P}$ be a set of primes. Let*

$$P(D) = \prod_{\substack{p\in\mathcal{P}\\p<D}} p$$

Define the sets

$$\mathcal{D}^{+} = \{p_1 \dots p_j \ : \ j \geq 0,\ p_j < \dots < p_1 < D,\ p_1 \dots p_{i-1}p_i^3 < D,\ \forall i \text{ odd}\}$$

and

$$\mathcal{D}^{-} = \{p_1 \dots p_j \ : \ j \geq 0,\ p_j < \dots < p_1 < D,\ p_1 \dots p_{i-1}p_i^3 < D,\ \forall i \text{ even}\}$$

Then, the functions $\lambda^{+}_{D,\mathcal{P}}$ and $\lambda^{-}_{D,\mathcal{P}}$ defined by

$$\lambda^{\pm}_{D,\mathcal{P}}(d) = \begin{cases} \mu(d) & \text{if } d \in \mathcal{D}^{\pm} \text{ and } d \mid P(D) \\ 0 & \text{otherwise} \end{cases}$$

are upper and lower bound sieves, respectively, with support level D and sieving range $\mathcal{P}$. In particular, $|\lambda^{\pm}_{D,\mathcal{P}}(d)| \leq 1$, for all d.

Proof. Both $\mathcal{D}^{\pm}$ are finite sets of square-free natural numbers smaller than D. Moreover, $1 \in \mathcal{D}^{\pm}$.
Let $d \in \mathcal{D}^{+}$. Write $d = p_1 \dots p_{\omega(d)}$ with $p_{\omega(d)} < \dots < p_1$. If $\omega(d)$ happens to be odd, then $d < p_1 \dots p^3_{\omega(d)} < D$. If $\omega(d)$ is even, then $d < p_1 \dots p^2_{\omega(d)-1} < p_1 \dots p^3_{\omega(d)-1} < D$. In either case, $d < D$, for every $d \in \mathcal{D}^{+}$. Analogously, $d < D$, for every $d \in \mathcal{D}^{-}$.
It it therefore enough to prove that $\lambda^{\pm}_{D,\mathcal{P}}$ are upper bound sieves, for it is plain to see that their support level is D and sieving range $\mathcal{P}$, by construction.
First

$$\lambda^{\pm}_{D,\mathcal{P}}(1) = \mu(1) = 1$$

since $1 \in \mathcal{D}^{\pm}$. It remains to be proved that

$$\sum_{d|n} \lambda^{-}_{D,\mathcal{P}}(d) \leq 0 \leq \sum_{d|n} \lambda^{+}_{D,\mathcal{P}}(d)$$

for every $n > 1$. Without loss of generality, assume $n \mid P(D)$, since $\lambda^{\pm}_{D,\mathcal{P}}(d) = 0$, for all $d \nmid P(D)$.
Let $n \mid P(D)$. Then, n is the product of distinct $\omega(n)$ primes in $\mathcal{P}$ and smaller than D. The proof goes by induction on $\omega(n)$.
Let $\omega(n) = 1$. Then $n = p$, with $D > p \in \mathcal{P}$. In particular, $n \in \mathcal{D}^-$. Hence

$$\sum_{d|n} \lambda^-_{D,\mathcal{P}}(d) = \mu(1) + \mu(p) = 1 - 1 = 0$$

and

$$\sum_{d|n} \lambda^+_{D,\mathcal{P}}(d) = \mu(1) + \lambda^+_{D,\mathcal{P}}(p) \geq 1 - 1 = 0$$

which proves the case $\omega(n) = 1$.
Assume the result holds for every n with $\omega(n) = r > 1$. Let n be such that $\omega(n) = r + 1$. Write

$$n = q_0 q_1 \dots q_r$$

with $q_r < \dots < q_0 < D$ and $q_i \in \mathcal{P}$, for every i. Let

$$N = \frac{n}{q_0} = q_1 \dots q_r$$

Then $N \mid P(D)$ and $\omega(N) = r$. By induction hypothesis

$$\sum_{d|N} \lambda^-_{D,\mathcal{P}}(d) \leq 0 \leq \sum_{d|N} \lambda^+_{D,\mathcal{P}}(d)$$

Every divisor of n is either of the form d or $q_0 d$, where $d \mid N$. Thus

$$\sum_{d|n} \lambda^+_{D,\mathcal{P}}(d) = \sum_{d|N} \lambda^+_{D,\mathcal{P}}(d) + \sum_{d|N} \lambda^+_{D,\mathcal{P}}(q_0 d) \geq \sum_{d|N} \lambda^+_{D,\mathcal{P}}(q_0 d) = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^+}} \mu(q_0 d)$$

$$= - \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^+}} \mu(d)$$

and likewise

$$\sum_{d|n} \lambda^-_{D,\mathcal{P}}(d) = \sum_{d|N} \lambda^-_{D,\mathcal{P}}(d) + \sum_{d|N} \lambda^-_{D,\mathcal{P}}(q_0 d) \leq \sum_{d|N} \lambda^-_{D,\mathcal{P}}(q_0 d) = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^-}} \mu(q_0 d)$$

$$= - \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^-}} \mu(d)$$

Let $d \mid N$. Write $d = p_1 \dots p_s$, with $p_s < \dots < p_1 \leq q_1 < q_0 < D$ and $p_i \in \mathcal{P}$, for every i. Let

$$E = \frac{D}{q_0}$$

Consider the sets $\mathcal{E}^{\pm}$ be the sets $\mathcal{D}^{\pm}$ with E instead of D, respectively. Then $q_0 d \in \mathcal{D}^+$ if and only if $q_0^3 < D$ and $p_1 \dots p_i^3 < E$ for every even i. Hence, assuming $q_0^3 < D$, the

condition $q_0 d \in \mathcal{D}^+$ is equivalent to $d \in \mathcal{E}^-$. Similarly, $q_0 d \in \mathcal{D}^-$ if and only if $d \in \mathcal{E}^+$, provided that $q_0^3 < D$. Moreover

$$0 = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^- \\ q_0^3 \geq D}} \mu(d) = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^+ \\ q_0^3 \geq D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^- \\ q_0^3 \geq D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^+ \\ q_0^3 \geq D}} \mu(d)$$

since all the above sums are empty. Therefore

$$\sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^+}} \mu(d) = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^+ \\ q_0^3 < D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^- \\ q_0^3 < D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^-}} \mu(d) \leq 0$$

where the inequality hold by induction hypothesis. Hence

$$\sum_{d|n} \lambda^+_{D,\mathcal{P}}(d) \geq 0$$

Analogously

$$\sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^-}} \mu(d) = \sum_{\substack{d|N \\ q_0 d \in \mathcal{D}^- \\ q_0^3 < D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^+ \\ q_0^3 < D}} \mu(d) = \sum_{\substack{d|N \\ d \in \mathcal{E}^+}} \mu(d) \geq 0$$

whence

$$\sum_{d|n} \lambda^-_{D,\mathcal{P}}(d) \leq 0$$

□

The objective is to bound $\sum_{d|P(z)} \lambda^{\pm}_{D,\mathcal{P}}(d) f(d)$, where f is a multiplicative function. The following lemma, expresses this sum in terms of a sum of some other functions T_n, and in the next subsection, a bound for T_n will be found.

Lemma 2.3. *Let $2 \leq z < D$ and $\mathcal{P}$ be a set of primes. Let*

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$$

and f be a multiplicative function such that $0 < f(p) < 1$, for every $p \in \mathcal{P}$. Let

$$F(z, \lambda^{\pm}_{D,\mathcal{P}}) = \sum_{d|P(z)} \lambda^{\pm}_{D,\mathcal{P}}(d) f(d)$$

where $\lambda^{\pm}_{D,\mathcal{P}}$ are the upper and lower bound sieves with support level D and sieving range $\mathcal{P}$, defined in Lemma 2.2. Then

$$F(z, \lambda^+_{D,\mathcal{P}}) = V(z) + \sum_{n \ odd} T_n(D, z)$$

and

$$F(z, \lambda^-_{D,\mathcal{P}}) = V(z) - \sum_{n \text{ even}} T_n(D, z)$$

where

$$V(z) = \prod_{p|P(z)} (1 - f(p))$$

and

$$T_n(D, z) = \sum_{\substack{p_1,\dots,p_n \in \mathcal{P} \\ w_n \le p_n < \dots < p_1 < z \\ p_m < w_m, \forall m < n, m \text{ odd}}} f(p_1 \dots p_n) V(p_n)$$

where w_n, which depend on D and $p_1, \dots, p_n$, are defined by

$$p_1 \dots p_n w_n^2 = D$$

Proof. By definition of the sets $\mathcal{D}^\pm$

$$F(z, \lambda^\pm_{D,\mathcal{P}}) = \sum_{d|P(z)} \lambda^\pm_{D,\mathcal{P}}(d) f(d) = \sum_{\substack{d|P(z) \\ d \in \mathcal{D}^+}} \mu(d) f(d)$$

Let $d \mid P(z)$ such that $d \in \mathcal{D}^+$. Then d is product of distinct primes in $\mathcal{P}$ smaller than $z \le D$ such that $p_1 \dots p_i^3 < D$ for every odd i, which is equivalent to $p_i^2 \frac{D}{w_i^2} < D$, that is, $p_i < w_i$. Therefore

$$F(z, \lambda^+_{D,\mathcal{P}}) = \sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z \\ p_m < w_m, \forall m \text{ odd}}} (-1)^j f(p_1 \dots p_j)$$

By Theorem B.1

$$V(z) = \sum_{d|P(z)} \mu(d) f(d) = \sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z}} (-1)^j f(p_1 \dots p_j)$$

Hence

$$\begin{aligned} V(z) &= \sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z \\ p_m < w_m, \forall m \text{ odd}}} (-1)^j f(p_1 \dots p_j) + \sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z \\ \exists m \text{ odd} : p_m \ge w_m}} (-1)^j f(p_1 \dots p_j) \\ &= F(z, \lambda^+_{D,\mathcal{P}}) + \sum_{n \text{ odd}} \sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z \\ p_m < w_m, \forall m < n, m \text{ odd} \\ p_n \ge w_n}} (-1)^j f(p_1 \dots p_j) \end{aligned}$$

The inner sum

$$\sum_{\substack{p_1,\dots,p_j \in \mathcal{P} \\ p_j < \dots < p_1 < z \\ p_m < w_m, \forall m < n, m \text{ odd} \\ p_n \ge w_n}} (-1)^j f(p_1 \dots p_j)$$

equals, for any fixed n

$$\sum_{\substack{p_1,\dots,p_n\in\mathcal{P}\\ w_n\le p_n<\dots<p_1<z\\ p_m<w_m\\ \forall m<n, m \text{ odd}}} (-1)^n f(p_1\dots p_n) \sum_{\substack{p_{n+1},\dots,p_j\in\mathcal{P}\\ p_j<\dots<p_{n+1}<p_n}} (-1)^{j-n} f(p_{n+1}\dots p_j)$$

which in turn, the above inner sum can be rewritten as

$$\sum_{\substack{p_{n+1},\dots,p_j\in\mathcal{P}\\ p_j<\dots<p_{n+1}<p_n}} (-1)^{j-n} f(p_{n+1}\dots p_j) = \sum_{\substack{p_{n+1},\dots,p_j\in\mathcal{P}\\ p_j<\dots<p_{n+1}<p_n}} \mu(p_{n+1}\dots p_j) f(p_{n+1}\dots p_j) = V(p_n)$$

Hence

$$V(z) = F(z,\lambda^+_{D,\mathcal{P}}) - \sum_{n \text{ odd}} \sum_{\substack{p_1,\dots,p_n\in\mathcal{P}\\ w_n\le p_n<\dots<p_1<z\\ p_m<w_m\\ \forall m<n, m \text{ odd}}} f(p_1\dots p_n)V(p_n) = F(z,\lambda^+_{D,\mathcal{P}}) - \sum_{n \text{ odd}} T_n(D,z)$$

By an analogous argument

$$V(z) = F(z,\lambda^-_{D,\mathcal{P}}) + \sum_{n \text{ even}} T_n(D,z)$$

□

2.2 The Functions Φ and φ

Lemma 2.3 characterizes the functions $F(z,\lambda^\pm_{D,\mathcal{P}})$ used to bound the sieving function in a combinatorial sieve (Theorem 2.1) in terms of a sum of functions $T_n(D,z)$. Two functions Φ and ϕ are to be introduced, to further bound T_n.

Let

$$\Phi(x) = e^\gamma\left(u(x) + \frac{v(x)}{x}\right)$$

and

$$\phi(x) = e^\gamma\left(u(x) - \frac{v(x)}{x}\right)$$

for $x > 0$, where γ is Euler's constant and $u(x) = \frac{1}{x}$ and $v(x) = 1$ for $0 < x \le 2$ and

$$(xu(x))' = u(x-1), \qquad v'(x) = -\frac{v(x-1)}{x-1}$$

for $x \ge 2$. From this definition, it follows that $\Phi(x) = \frac{2e^\gamma}{x}$ and $\phi(x) = 0$ for $0 < x \le 2$. Moreover, for $x \ge 2$

$$x(\Phi(x) + \phi(x)) = 2e^\gamma x u(x)$$

and

$$x(\Phi(x) - \phi(x)) = 2e^\gamma v(x)$$

Whence

$$(x\Phi(x))' + (x\phi(x))' = 2e^{\gamma}(xu(x))' = 2e^{\gamma}u(x-1)$$

and

$$(x\Phi(x))' - (x\phi(x))' = 2e^{\gamma}v'(x) = -2e^{\gamma}\frac{v(x-1)}{x-1}$$

for $x \geq 2$. Therefore

$$(x\Phi(x))' = \phi(x-1), \qquad (x\phi(x))' = \Phi(x-1)$$

for $x \geq 2$. Hence

$$\int_2^x \phi(s-1)\,ds = x\Phi(x) - 2\Phi(2) = x\Phi(x) - 2e^{\gamma}$$

for all $x \geq 2$. Then, $\Phi(x) = \frac{2e^{\gamma}}{x}$, for $2 \leq x \leq 3$, since $\int_2^x \phi(s-1)\,ds = 0$, because $\phi(s-1) = 0$ when $s - 1 \leq 2$. Hence

Lemma 2.4. *Let $0 < x \leq 3$. Then*

$$\Phi(x) = \frac{2e^{\gamma}}{x}$$

Similarly

$$\int_2^x \Phi(s-1)\,ds = x\phi(x) - 2\phi(2) = x\phi(x)$$

for all $x \geq 2$, since $\phi(2) = 0$. Then, for $2 \leq x \leq 4$, by Lemma 2.4

$$\phi(x) = \frac{1}{x}\int_2^x \Phi(s-1)\,ds = \frac{2e^{\gamma}}{x}\int_2^x \frac{1}{s-1}\,ds = \frac{2e^{\gamma}\log(x-1)}{x}$$

Thus

Lemma 2.5. *Let $2 < x \leq 4$. Then*

$$\phi(x) = 2e^{\gamma}\frac{\log(x-1)}{x}$$

Lastly, Φ and ϕ are expressed as sums of the functions f_n defined in pages 245−246 of [5], in the following way:

$$\Phi(s) = 1 + \sum_{n \text{ odd}} f_n(s)$$

$$\phi(s) = 1 - \sum_{n \text{ even}} f_n(s)$$

The functions f_n are used to bound the functions T_n defined in Lemma 2.3, whenever the sieve is linear, as follows:

Lemma 2.6. *Let $z \geq 2$ and $\mathcal{P}$ be a set of primes. Let f be a multiplicative function such that $0 < f(p) < 1$, for every $p \in \mathcal{P}$, and such that*

$$\prod_{\substack{p \in \mathcal{P} \\ u \leq p < z}} \frac{1}{1 - f(p)} \leq (1+\varepsilon)\frac{\log z}{\log u}$$

for some $0 < \varepsilon < \frac{1}{200}$ *and for all* $1 < u < z$. *Then,*

$$T_n(D,z) < V(z)\left(f_n(\tfrac{\log D}{\log z}) + \varepsilon 0.99^n e^{10-\frac{\log D}{\log z}}\right)$$

for every odd n *and* $D \geq z$, *and for every even* n *and* $D \geq z^2$, *where*

$$V(z) = \prod_{p|P(z)} (1 - f(p))$$

A detailed proof of the above can be found in pages 253−256 of [5].

2.3 The Jurkat-Richert Theorem

The Jurkat-Richert Theorem provides both an upper and lower bound for sieving functions when the sieve is linear. The bounds depend on the functions Φ and ϕ, previously detailed.

Theorem 2.7 (Jurkat-Richert)**.** *Let* A *be a sieveing set,* $\mathcal{P}$ *a sieving range and* $z \geq 2$ *a sieving level. Let*

$$P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$$

and f *a multiplicative function such that* $0 < f(p) < 1$, *for every* $p \in \mathcal{P}$. *For every square-free* d, *define*

$$r(d) = |A_d| - |A| f(d)$$

where $A_d = \{a \in A \,:\, d \mid a\}$. *Let* $\mathcal{Q}$ *be a finite subset of* $\mathcal{P}$, *with* $Q = \prod_{p \in \mathcal{Q}} p$, *such that*

$$\prod_{\substack{p \in \mathcal{P} \setminus \mathcal{Q} \\ u \leq p < z}} \frac{1}{1 - f(p)} \leq (1 + \varepsilon) \frac{\log z}{\log u}$$

for some $0 < \varepsilon < \frac{1}{200}$ *and for all* $1 < u < z$. *Then, for any* $D \geq z$

$$S(A, \mathcal{P}, z) < \left(\Phi(\tfrac{\log D}{\log z}) + \varepsilon e^{14-\frac{\log D}{\log z}}\right) |A| V(z) + R$$

and for any $D \geq z^2$

$$S(A, \mathcal{P}, z) > \left(\phi(\tfrac{\log D}{\log z}) - \varepsilon e^{14-\frac{\log D}{\log z}}\right) |A| V(z) - R$$

where the functions Φ *and* ϕ *are the ones defined in Section 2.2,*

$$V(z) = \prod_{p|P(z)} (1 - f(p))$$

and

$$R = \sum_{\substack{d < DQ \\ d | P(z)}} |r(d)|$$

Proof. Let $\mathcal{P}_0 = \mathcal{P} \setminus \mathcal{Q}$. By Lemma 2.2, the functions $\lambda^{\pm}_{D,\mathcal{P}_0}$ there defined, are upper and lower bound sieves with support level D and sieving range $\mathcal{P}_0$ and such that $|\lambda^{\pm}_{D,\mathcal{P}}(d)| \le 1$, for every d. Let

$$P_0(z) = \prod_{\substack{p \in \mathcal{P}_0 \\ p < z}} p$$

and

$$Q(z) = \prod_{\substack{p \in \mathcal{Q} \\ p < z}} p$$

Define

$$F(z, \lambda^{\pm}_{D,\mathcal{P}_0}) = \sum_{p | P_0(z)} \lambda^{\pm}_{D,\mathcal{P}_0}(d) f(d)$$

and

$$V_0(z) = \prod_{p | P_0(z)} (1 - f(p))$$

By Lemma 2.3 and Lemma 2.6

$$\begin{aligned} F(z, \lambda^{+}_{D,\mathcal{P}}) = V_0(z) + \sum_{n \text{ odd}} T_n(D, z) &< V_0(z) \left(1 + \sum_{n \text{ odd}} f_n\big(\tfrac{\log D}{\log z}\big) + \varepsilon e^{10 - \frac{\log D}{\log z}} \sum_{n \text{ odd}} 0.99^n \right) \\ &< V_0(z) \left(\Phi\big(\tfrac{\log D}{\log z}\big) + \varepsilon e^{14 - \frac{\log D}{\log z}} \right) \end{aligned}$$

for any $D \ge z$, since $\sum_{n \text{ odd}} 0.99^n = \frac{9900}{199} < e^4$. Again, by Lemma 2.3 and Lemma 2.6

$$\begin{aligned} F(z, \lambda^{-}_{D,\mathcal{P}}) = V_0(z) - \sum_{n \text{ even}} T_n(D, z) &> V_0(z) \left(1 - \sum_{n \text{ even}} f_n\big(\tfrac{\log D}{\log z}\big) - \varepsilon e^{10 - \frac{\log D}{\log z}} \sum_{n \text{ even}} 0.99^n \right) \\ &> V_0(z) \left(\phi\big(\tfrac{\log D}{\log z}\big) - \varepsilon e^{14 - \frac{\log D}{\log z}} \right) \end{aligned}$$

for any $D \ge z$, since $\sum_{n \text{ even}} 0.99^n = \frac{9801}{199} < e^4$. Hence, by Theorem 2.1

$$\begin{aligned} S(A, \mathcal{P}, z) &\le |A| F(z, \lambda^{+}_{D,\mathcal{P}}) \prod_{p | Q(z)} (1 - f(p)) + R \\ &< |A| \left(\Phi\big(\tfrac{\log D}{\log z}\big) + \varepsilon e^{14 - \frac{\log D}{\log z}} \right) \prod_{p | P_0(z)} (1 - f(p)) \prod_{p | Q(z)} (1 - f(p)) + R \\ &= \left(\Phi\big(\tfrac{\log D}{\log z}\big) + \varepsilon e^{14 - \frac{\log D}{\log z}} \right) |A| V(z) + R \end{aligned}$$

for any $D \ge z$, and similarly

$$\begin{aligned} S(A, \mathcal{P}, z) &\ge |A| F(z, \lambda^{-}_{D,\mathcal{P}}) \prod_{p | Q(z)} (1 - f(p)) - R \\ &> |A| \left(\phi\big(\tfrac{\log D}{\log z}\big) - \varepsilon e^{14 - \frac{\log D}{\log z}} \right) \prod_{p | P_0(z)} (1 - f(p)) \prod_{p | Q(z)} (1 - f(p)) - R \\ &= \left(\phi\big(\tfrac{\log D}{\log z}\big) - \varepsilon e^{14 - \frac{\log D}{\log z}} \right) |A| V(z) - R \end{aligned}$$

for any $D \ge z^2$. □

A relevant remark on Theorem 2.7 is that the hypothesis

$$\prod_{\substack{p\in\mathcal{P}\setminus\mathcal{Q}\\ u\le p<z}}\frac{1}{1-f(p)}\le(1+\varepsilon)\frac{\log z}{\log u}$$

for all $1<u<z$, implies the linearity of the sieve, since

$$\prod_{\substack{p\in\mathcal{Q}\\ u\le p<z}}\frac{1}{1-f(p)}\le\prod_{\substack{p\in Q\\ p<z}}\frac{1}{1-f(p)}\ll 1$$

for all $1<u<z$, because $\mathcal{Q}$ is finite, and hence

$$\prod_{\substack{p\in\mathcal{P}\\ u\le p<z}}\frac{1}{1-f(p)}=\prod_{\substack{p\in\mathcal{P}\setminus\mathcal{Q}\\ u\le p<z}}\frac{1}{1-f(p)}\prod_{\substack{p\in\mathcal{Q}\\ u\le p<z}}\frac{1}{1-f(p)}\ll\frac{\log z}{\log u}$$

for all $1<u<z$, which means the sieve is linear. In particular

$$\frac{1}{V(z)}=\prod_{\substack{p\in\mathcal{P}\\ p<z}}\frac{1}{1-f(p)}\ll\log z$$

by setting $u=2$ whenever $z>2$.

3 Large Sieve

All previous sieves rely on the Möbius function. In this brief section, however, a completely different type of sieve is introduced. Given a sequence $(a_n)_n$ of complex numbers, a sequence $(b_r)_r$ of rational numbers and $R, x \geq 1$, a large sieve is an inequality of the form

$$\sum_{r \leq R} \left| \sum_{n \leq x} a_n e^{2\pi i n b_r} \right|^2 \leq C \sum_{n \leq x} |a_n|^2$$

where C is to depend on R and x only and hence not on b_r nor a_n.

One of the most advanced applications of large sieves is the Bombieri-Vinogradov Theorem. This is a result on the average distribution of primes in congruence classes of large moduli. To be precise, on the error term in approximating the number of primes up to x of any single class modulo d by $\frac{\pi(x)}{\varphi(d)}$, on average, where φ is Euler's totient function. Under a generalised Riemann hypothesis, the error term of the above approximation is $O(\sqrt{x} \log x)$, before averaging, which is exactly the same bound Bombieri-Vinogradov's Theorem provides, after averaging, that is.

Theorem 3.1 (Bombieri-Vinogradov)**.** *Let $x \geq 1$, $n \in \mathbb{N}$ and $A > 0$. Then, there exists $\beta(A) > 0$ such that*

$$\sum_{d < \sqrt{x} \, (\log x)^{-\beta(A)}} \max_{(d,n)=1} \left| \pi(x, n \bmod d) - \frac{\pi(x)}{\varphi(d)} \right| \ll_A \frac{x}{\log^A x}$$

where $\pi(x, n \bmod d)$ is the number of primes up to x congruent to n modulo d.

Proofs of the above theorem can be found in section 9.2 of [1] or in section 28 of [2] for a slightly different version. Two main ingredients are needed to prove Theorem 3.1. The first are advanced large sieving techniques nowhere to be found in this Thesis whatsoever. The second is the Siegel-Walfisz Theorem:

Theorem 3.2 (Siegel-Walfisz)**.** *Let $x \geq 1$, $n \in \mathbb{N}$ and $A > 0$. Then*

$$\left| \pi(x, n \bmod d) - \frac{\pi(x)}{\varphi(d)} \right| \ll_A \frac{x}{\log^A x}$$

where $\pi(x, n \bmod d)$ is the number of primes up to x congruent to n modulo d.

3.1 A Large Sieve Inequality

Back to large sieve for beginners, consider a differentiable function $f : [0, 1] \longrightarrow \mathbb{C}$ with continuous derivative and extended by periodicity to all $\mathbb{R}$ (with period one). Let $R \geq 1$ and $u \in [0, 1]$. For every natural numbers $r \leq R$ and $h \leq r$ with $(h, r) = 1$, one has

$$-f(\tfrac{h}{r}) = -f(u) + \int_{\frac{h}{r}}^{u} f'(t) \, dt$$

by the Fundamental Theorem of Calculus. Take absolute values on either side of the above to obtain

$$|f(\tfrac{h}{r})| \leq |f(u)| + \int_{\frac{h}{r}}^{u} |f'(t)| \, dt$$

Consider now the family of intervals $(\frac{h}{r}-\frac{1}{2R^2},\frac{h}{r}+\frac{1}{2R^2})$ where h and r are natural numbers with $h\leq r\leq R$ and $(h,r)=1$. Then, the union of them all is contained in $[0,1]$, since $\frac{h}{r}-\frac{1}{2R^2}>\frac{1}{R}-\frac{1}{2R^2}>0$ and $\frac{h}{r}+\frac{1}{2R^2}\leq\frac{r-1}{r}+\frac{1}{2R^2}<1-\frac{1}{R}+\frac{1}{2R^2}<1$, since $R\geq 1$. Moreover, said intervals are nonoverlapping, since given $x\in(\frac{h}{r}-\frac{1}{2R^2},\frac{h}{r}+\frac{1}{2R^2})\cap(\frac{h'}{r'}-\frac{1}{2R^2},\frac{h'}{r'}+\frac{1}{2R^2})$ with $\frac{h}{r}\neq\frac{h'}{r'}$, then $|x-\frac{h}{r}|<\frac{1}{2R^2}$ and $|x-\frac{h'}{r'}|<\frac{1}{2R^2}$. On the one hand, by the triangular inequality

$$\left|\frac{h}{r}-\frac{h'}{r'}\right|\leq\left|x-\frac{h}{r}\right|+\left|x-\frac{h'}{r'}\right|<\frac{1}{2R^2}+\frac{1}{2R^2}=\frac{1}{R^2}$$

On the other hand, $hr'-h'r\neq 0$ since $0\neq\frac{h}{r}-\frac{h'}{r'}=\frac{hr'-h'r}{rr'}$. Hence $|hr'-h'r|\geq 1$, since h,h',r,r' are natural numbers. Therefore

$$\left|\frac{h}{r}-\frac{h'}{r'}\right|=\frac{|hr'-h'r|}{rr'}\geq\frac{1}{rr'}\geq\frac{1}{R^2}$$

which is a contradiction. Before integrating the previous inequality over the interval $(\frac{h}{r}-\frac{1}{2R^2},\frac{h}{r}+\frac{1}{2R^2})$ with respect to u and adding over all such intervals, take into account that

$$\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}\int_{\frac{h}{r}}^{u}|f'(t)|\,dt\,du\leq\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f'(t)|\,dt\,du=\frac{1}{R^2}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f'(t)|\,dt$$

Hence, integrating and adding all intervals, one obtains

$$\begin{aligned}\frac{1}{R^2}\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}|f(\tfrac{h}{r})|&=\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f(\tfrac{h}{r})|\,du\\&\leq\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f(u)|\,du+\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}\int_{\frac{h}{r}}^{u}|f'(t)|\,dt\,du\\&\leq\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f(u)|\,du+\frac{1}{R^2}\sum_{r\leq R}\sum_{\substack{h\leq r\\(h,r)=1}}\int_{\frac{h}{r}-\frac{1}{2R^2}}^{\frac{h}{r}+\frac{1}{2R^2}}|f'(t)|\,dt\\&\leq\int_0^1|f(u)|\,du+\frac{1}{R^2}\int_0^1|f'(t)|\,dt=\int_0^1|f(u)|\,du+\frac{1}{R^2}\int_0^1|f'(u)|\,du\end{aligned}$$

Given $x\geq 1$ and a sequence $(a_n)_n$ of complex numbers, let

$$f(u)=S(u)^2$$

where

$$S(u)=\sum_{n\leq x}a_ne^{2\pi inu}$$

Then f clearly is a differentiable function $f:\mathbb{R}\longrightarrow\mathbb{C}$ with continuous derivative and $f(u+1)=f(u)$, for every $u\in[0,1]$. Moreover

$$f'(u)=2S(u)S'(u)$$

Therefore, by the above reasoning

$$\frac{1}{R^2}\sum_{r\le R}\sum_{\substack{h\le r\\(h,r)=1}}\left|S(\tfrac{h}{r})\right|^2 \le \int_0^1 |S(u)|^2\,du + \frac{2}{R^2}\int_0^1 |S(u)||S'(u)|\,du$$

First

$$\begin{aligned}\int_0^1 |S(u)|^2\,du &= \int_0^1 \left(\sum_{n\le x} a_n e^{2\pi i n u}\right)\left(\sum_{m\le x}\overline{a_m}e^{-2\pi i m u}\right)\,du\\ &= \sum_{n\le x}\sum_{m\le x} a_n\overline{a_m}\int_0^1 e^{2\pi i(n-m)u}\,du = \sum_{n\le x} a_n\overline{a_n} = \sum_{n\le x}|a_n|^2\end{aligned}$$

And second, by the Cauchy-Schwarz inequality

$$\int_0^1 |S(u)||S'(u)|\,du \le \left(\int_0^1 |S(u)|^2\,du\right)^{\frac{1}{2}}\left(\int_0^1 |S'(u)|^2\,du\right)^{\frac{1}{2}}$$

where the squared of the first factor has just been dealt with above, and the squared of the second similarly equals

$$\begin{aligned}\int_0^1 |S'(u)|^2\,du &= \int_0^1 \left(\sum_{n\le x} 2\pi i n a_n e^{2\pi i n u}\right)\left(\sum_{m\le x} 2\pi\bar{i} m\overline{a_m}e^{-2\pi i m u}\right)\,du\\ &= 4\pi^2\sum_{n\le x}\sum_{m\le x} nm a_n\overline{a_m}\int_0^1 e^{2\pi i(n-m)u}\,du = 4\pi^2\sum_{n\le x} n^2 a_n\overline{a_n} \le 4\pi^2x^2\sum_{n\le x}|a_n|^2\end{aligned}$$

Whence

$$\begin{aligned}\frac{1}{R^2}\sum_{r\le R}\sum_{\substack{h\le r\\(h,r)=1}}\left|S(\tfrac{h}{r})\right|^2 &\le \sum_{n\le x}|a_n|^2 + \frac{2}{R^2}\left(\sum_{n\le x}|a_n|^2\right)^{\frac{1}{2}}\left(4\pi^2x^2\sum_{n\le x}|a_n|^2\right)^{\frac{1}{2}}\\ &= \left(1+\frac{4\pi x}{R^2}\right)\sum_{n\le x}|a_n|^2\end{aligned}$$

Multiplying by R^2

Theorem 3.3. *Let $(a_n)_n$ be a sequence of complex numbers and $R, x \ge 1$. Then*

$$\sum_{r\le R}\sum_{\substack{h\le r\\(h,r)=1}}\left|\sum_{n\le x} a_n e^{2\pi i n\frac{h}{r}}\right|^2 \le (R^2+4\pi x)\sum_{n\le x}|a_n|^2$$

The next step is to improve the above result by introducing Dirichlet characters (see Appendix C).

Theorem 3.4. *Let $(a_n)_n$ be a sequence of complex numbers and $R, x \geq 1$. Then*

$$\sum_{r \leq R} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{n \leq x} a_n \chi(n) \right|^2 \leq (R^2 + 4\pi x) \sum_{n \leq x} |a_n|^2$$

where $\sum^*_{\chi \bmod r}$ denotes the sum over primitive characters χ modulo r.

Proof. Let $r \leq R$ and $(n, r) = 1$. Let χ be a primitive character modulo r. Then, by Lemma C.2

$$\chi(n) = \frac{1}{\tau(\bar{\chi})} \sum_{h \leq r} \bar{\chi}(h) e^{2\pi i n \frac{h}{r}}$$

Multiply by a_n, sum over $n \leq x$, apply modulus and square it all out to obtain

$$\left| \sum_{n \leq x} a_n \chi(n) \right|^2 = \frac{1}{|\tau(\bar{\chi})|^2} \left| \sum_{n \leq x} a_n \sum_{h \leq r} \bar{\chi}(h) e^{2\pi i n \frac{h}{r}} \right|^2 = \frac{1}{r} \left| \sum_{h \leq r} \bar{\chi}(h) \sum_{n \leq x} a_n e^{2\pi i n \frac{h}{r}} \right|^2$$

by Lemma C.3. Sum over all primitive characters modulo r

$$\begin{aligned}
\sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{n \leq x} a_n \chi(n) \right|^2 &= \frac{1}{r} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{h \leq r} \bar{\chi}(h) \sum_{n \leq x} a_n e^{2\pi i n \frac{h}{r}} \right|^2 \\
&\leq \frac{1}{r} \sum_{\chi \bmod r} \left| \sum_{h \leq r} \bar{\chi}(h) \sum_{n \leq x} a_n e^{2\pi i n \frac{h}{r}} \right|^2 \\
&= \frac{1}{r} \sum_{\chi \bmod r} \left(\sum_{h_1 \leq r} \bar{\chi}(h_1) \sum_{n \leq x} a_n e^{2\pi i n \frac{h_1}{r}} \right) \left(\sum_{h_2 \leq r} \chi(h_2) \sum_{n \leq x} \overline{a_n} e^{-2\pi i n \frac{h_2}{r}} \right) \\
&= \frac{1}{r} \sum_{h_1 \leq r} \sum_{h_2 \leq r} \left(\sum_{n \leq x} a_n e^{2\pi i n \frac{h_1}{r}} \right) \left(\sum_{n \leq x} \overline{a_n} e^{-2\pi i n \frac{h_2}{r}} \right) \sum_{\chi \bmod r} \bar{\chi}(h_1) \chi(h_2) \\
&= \frac{\varphi(r)}{r} \sum_{\substack{h_1 \leq r \\ (h_1, r) = 1}} \left(\sum_{n \leq x} a_n e^{2\pi i n \frac{h_1}{r}} \right) \left(\sum_{n \leq x} \overline{a_n} e^{-2\pi i n \frac{h_1}{r}} \right) = \frac{\varphi(r)}{r} \sum_{\substack{h \leq r \\ (h, r) = 1}} \left| \sum_{n \leq x} a_n e^{2\pi i n \frac{h}{r}} \right|^2
\end{aligned}$$

since, by Lemma C.1

$$\sum_{\chi \bmod r} \bar{\chi}(h_1) \chi(h_2) = \sum_{\chi \bmod r} \chi(h_1^{-1} h_2) = \begin{cases} \varphi(r) & \text{if } h_1 = h_2 \text{ and } (h_1, r) = 1 \\ 0 & \text{otherwise} \end{cases}$$

for all $h_1, h_2 \leq r$. Hence

$$\frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{n \leq x} a_n \chi(n) \right|^2 \leq \sum_{\substack{h \leq r \\ (h, r) = 1}} \left| \sum_{n \leq x} a_n e^{2\pi i n \frac{h}{r}} \right|^2$$

Sum over $r \leq R$ and apply Theorem 3.3

$$\sum_{r\leq R} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left|\sum_{n\leq x} a_n \chi(n)\right|^2 \leq \sum_{r\leq R} \sum_{\substack{h\leq r \\ (h,r)=1}} \left|\sum_{n\leq x} a_n e^{2\pi i n \frac{h}{r}}\right|^2 \leq (R^2 + 4\pi x) \sum_{n\leq x} |a_n|^2$$

□

In the following Section, a particular inequality will have to be used at one point in the proof of Chen's Theorem. The above result is used to prove said inequality, presented in the following Theorem.

Theorem 3.5. *Let $(a_n)_n$ be a sequence of complex numbers such that $|a_n| \leq 1$, for all $n \in \mathbb{N}$. Let $A, X, Y, Z \geq 1$ such that $X > (\log Y)^{2A}$. Set*

$$S = \frac{(XY)^{\frac{1}{2}}}{\log^A Y}$$

Then

$$\sum_{d<S} \max_{(h,d)=1} \left| \sum_{n<X} \sum_{\substack{Z\leq p<Y \\ pn\equiv h (\bmod d)}} a_n - \frac{1}{\varphi(d)} \sum_{n<X} \sum_{\substack{Z\leq p<Y \\ (pn,d)=1}} a_n \right| \ll_A \frac{XY(\log XY)^2}{\log^A Y}$$

Proof. Let $(h,d) = 1$, p a prime and $n \in \mathbb{N}$. By Lemma C.1

$$\sum_{\chi \bmod d} \bar{\chi}(h)\chi(pn) = \sum_{\chi \bmod d} \chi(h^{-1}pn) = \begin{cases} \varphi(d) & \text{if } pn \equiv h \ (\bmod d) \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\begin{aligned} \sum_{n<X} \sum_{\substack{Z\leq p<Y \\ pn\equiv h (\bmod d)}} a_n &= \sum_{n<X} \sum_{Z\leq p<Y} \frac{a_n}{\varphi(d)} \sum_{\chi \bmod d} \bar{\chi}(h)\chi(pn) \\ &= \frac{1}{\varphi(d)} \sum_{\chi \bmod d} \bar{\chi}(h) \sum_{n<X} a_n \chi(n) \sum_{Z\leq p<Y} \chi(p) \end{aligned}$$

where the principal character χ_0 modulo d contributes in the above sum in

$$\frac{1}{\varphi(d)} \bar{\chi}_0(h) \sum_{n<X} \sum_{Z\leq p<Y} a_n \chi_0(pn) = \frac{1}{\varphi(d)} \sum_{n<X} \sum_{\substack{Z\leq p<Y \\ (pn,d)=1}} a_n$$

Hence

$$\sum_{d<S} \max_{(h,d)=1} \left| \sum_{n<X} \sum_{\substack{Z\le p<Y \\ pn\equiv h (\mathrm{mod}\, d)}} a_n - \frac{1}{\varphi(d)} \sum_{n<X} \sum_{\substack{Z\le p<Y \\ (pn,d)=1}} a_n \right|$$

$$\le \sum_{d<S} \frac{1}{\varphi(d)} \sum_{\substack{\chi \bmod d \\ \chi\neq\chi_0}} |\bar{\chi}(h)| \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z\le p<Y} \chi(p) \right|$$

$$\le \sum_{d<S} \frac{1}{\varphi(d)} \sum_{\chi \bmod d} \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z\le p<Y} \chi(p) \right|$$

Every Dirichlet character χ modulo d factors into a product of a primitive Dirichlet character modulo a divisor r of d and the principal Dirichlet character modulo $s = \frac{d}{r}$, meaning

$$\chi = \chi' \cdot \chi_0''$$

where χ' is a primitive Dirichlet character modulo r and χ_0'' is the principal Dirichlet character modulo s. Therefore

$$\sum_{d<S} \frac{1}{\varphi(d)} \sum_{\chi \bmod d} \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z\le p<Y} \chi(p) \right|$$

$$= \sum_{rs<S} \frac{1}{\varphi(rs)} \sideset{}{^*}\sum_{\chi' \bmod r} \left| \sum_{n<X} a_n \chi'(n)\chi_0''(n) \right| \left| \sum_{Z\le p<Y} \chi'(p)\chi_0''(p) \right|$$

$$= \sum_{rs<S} \frac{1}{\varphi(rs)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z\le p<Y \\ (p,s)=1}} \chi(p) \right|$$

where $\sum_{\chi \bmod r}^*$ means the sum over primitive Dirichlet characters modulo r. Moreover, $\varphi(rs) \ge \varphi(r)\varphi(s)$. Hence

$$\sum_{d<S} \frac{1}{\varphi(d)} \sum_{\chi \bmod d} \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z\le p<Y} \chi(p) \right|$$

$$\le \sum_{s<S} \frac{1}{\varphi(s)} \sum_{r<S} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z\le p<Y \\ (p,s)=1}} \chi(p) \right|$$

On the one hand, by the Siegel-Walfisz Theorem (Theorem 3.2)

$$\sum_{p<Y} \chi(p) = \sum_{a \ (\mathrm{mod}\, r)} \chi(a) \sum_{\substack{p<Y \\ p\equiv a (\mathrm{mod}\, r)}} 1 = \sum_{a \ (\mathrm{mod}\, r)} \chi(a)\pi(Y, a \bmod r)$$

$$= \sum_{a \ (\mathrm{mod}\, r)} \chi(a) \left(\frac{\pi(Y)}{\varphi(r)} + O\left(\frac{Y}{(\log Y)^{4A}} \right) \right) \ll \frac{rY}{(\log Y)^{4A}}$$

since

$$\left| \sum_{a \pmod r} \chi(a) \frac{\pi(Y)}{\varphi(r)} \right| = \frac{\pi(Y)}{\varphi(r)} \left| \sum_{a \pmod r} \chi(a) \right| = 0$$

due to

$$\sum_{a \pmod r} \chi(a) = 0$$

which follows from the fact that there exists a natural number b coprime with r and such that $\chi(b) \neq 1$, for which

$$\chi(b) \sum_{a \pmod r} \chi(a) = \sum_{a \pmod r} \chi(ab) = \sum_{a \pmod r} \chi(a)$$

Analogously

$$\left| \sum_{p<Z} \chi(p) \right| \ll \frac{rZ}{(\log Z)^{4A}} \ll \frac{rY}{(\log Y)^{4A}}$$

By the triangular inequality

$$\left| \sum_{Z \leq p<Y} \chi(p) \right| = \left| \sum_{p<Y} \chi(p) - \sum_{p<Z} \chi(p) \right| \leq \left| \sum_{p<Y} \chi(p) \right| + \left| \sum_{p<Z} \chi(p) \right| \ll \frac{rY}{(\log Y)^{4A}}$$

The number of terms removed in the above sum by adding the condition $(p, s) = 1$ is less than or equal to $\omega(s)$, which by Lemma A.4 is bounded above by $2 \log s \ll \log S$, since $s < S$. Hence

$$\left| \sum_{\substack{Z \leq p<Y \\ (p,s)=1}} \chi(p) \right| \ll \frac{rY}{(\log Y)^{4A}} + \log S$$

On the other hand

$$\left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \leq \sum_{\substack{n<X \\ (n,s)=1}} |a_n||\chi(n)| \leq \sum_{\substack{n<X \\ (n,s)=1}} 1 \leq X$$

Now, the sum

$$\sum_{r<S} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \leq p<Y \\ (p,s)=1}} \chi(p) \right|$$

will be counted dividing the range $r < S$ into $r < S_0 = \log^A Y$ and a second range $S_0 \leq r < S$ which is to be partitioned into pairwise disjoint subintervals $S_j \leq r < 2S_j$,

where $S_j = 2^j S_0$ and $0 \le j \ll \log S$ (since $2^{\log S} S_0 = e^{\log S \log 2} S_0 = S^{\log 2} S_0 > S$). Thus

$$\begin{aligned}\sum_{r<S_0} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| &\ll \sum_{r<S_0} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} X \left(\frac{rY}{(\log Y)^{4A}} + \log S \right) \\ &\le \sum_{r<S_0} \frac{X}{\varphi(r)} \left(\frac{rY}{(\log Y)^{4A}} + \log S \right) \sum_{\chi \bmod r} 1 = \sum_{r<S_0} X \left(\frac{rY}{(\log Y)^{4A}} + \log S \right) \\ &\ll X \frac{S_0 Y \log S}{(\log Y)^{4A}} \sum_{r<S_0} 1 < \frac{S_0 XY \log S}{(\log Y)^{4A}} S_0^2 = \frac{(\log Y)^{3A} XY \log S}{(\log Y)^{4A}} = \frac{XY \log S}{\log^A Y}\end{aligned}$$

and

$$\begin{aligned}&\sum_{\substack{S_j \le r < 2S_j \\ r<S}} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \\ &= \sum_{\substack{S_j \le r < 2S_j \\ r<S}} \frac{1}{r} \sideset{}{^*}\sum_{\chi \bmod r} \left(\left(\frac{r}{\varphi(r)} \right)^{\frac{1}{2}} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \right) \left(\left(\frac{r}{\varphi(r)} \right)^{\frac{1}{2}} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \right) \\ &\le \frac{1}{S_j} \sum_{\substack{r<2S_j \\ \chi \bmod r \\ \chi \text{ primitive}}} \left(\left(\frac{r}{\varphi(r)} \right)^{\frac{1}{2}} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \right) \left(\left(\frac{r}{\varphi(r)} \right)^{\frac{1}{2}} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \right) \\ &\le \frac{1}{S_j} \left(\sum_{\substack{r<2S_j \\ \chi \bmod r \\ \chi \text{ primitive}}} \frac{r}{\varphi(r)} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right|^2 \right)^{\frac{1}{2}} \left(\sum_{\substack{r<2S_j \\ \chi \bmod r \\ \chi \text{ primitive}}} \frac{r}{\varphi(r)} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right|^2 \right)^{\frac{1}{2}} \\ &= \frac{1}{S_j} \left(\sum_{r<2S_j} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right|^2 \right)^{\frac{1}{2}} \left(\sum_{r<2S_j} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right|^2 \right)^{\frac{1}{2}}\end{aligned}$$

by Cauchy-Schwarz's inequality. Both the first and second factors are to be bounded applying Theorem 3.4. When it comes to the first factor, use Theorem 3.4 with $R = 2S_j$, $x = X$ and the sequence of numbers equal to a_n when $(n, s) = 1$ and 0 otherwise, to obtain

$$\begin{aligned}\sum_{r<2S_j} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right|^2 &\le (4S_j^2 + 4\pi X) \sum_{\substack{n<X \\ (n,s)=1}} |a_n|^2 \le (4S_j^2 + 4\pi X) \sum_{\substack{n<X \\ (n,s)=1}} 1 \\ &\le (4S_j^2 + 4\pi X) X\end{aligned}$$

since $|a_n| \leq 1$. As for the second factor, apply Theorem 3.4 this time with $R = 2S_j$, $x = Y$ and the sequence of numbers equal to 1 when n is a prime, $n \geq Z$ and $(n, s) = 1$, and 0 otherwise, to obtain

$$\sum_{r<2S_j} \frac{r}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{Z\leq p<Y \\ (p,s)=1}} \chi(p) \right|^2 \leq (4S_j^2 + 4\pi Y) \sum_{\substack{Z\leq p<Y \\ (p,s)=1}} 1^2 \leq (4S_j^2 + 4\pi Y)Y$$

Therefore

$$\begin{aligned}
&\sum_{\substack{S_j\leq r<2S_j \\ r<S}} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n\chi(n) \right| \left| \sum_{\substack{Z\leq p<Y \\ (p,s)=1}} \chi(p) \right| \leq \frac{1}{S_j} \big((4S_j^2 + 4\pi X)X\big)^{\frac{1}{2}} \big((4S_j^2 + 4\pi Y)Y\big)^{\frac{1}{2}} \\
&= \frac{4}{S_j} \big((S_j^4 + \pi S_j^2(X+Y) + \pi^2 XY)XY\big)^{\frac{1}{2}} = 4\left(\left(S_j^2 + \pi(X+Y) + \pi^2 \frac{XY}{S_j^2}\right)XY\right)^{\frac{1}{2}} \\
&\ll \left(\left(S_j^2 + X + Y + \frac{XY}{S_j^2}\right)XY\right)^{\frac{1}{2}} \leq \left(S_j + X^{\frac{1}{2}} + Y^{\frac{1}{2}} + \frac{(XY)^{\frac{1}{2}}}{S_j}\right)(XY)^{\frac{1}{2}} \\
&\leq \left(S + X^{\frac{1}{2}} + Y^{\frac{1}{2}} + \frac{(XY)^{\frac{1}{2}}}{S_0}\right)(XY)^{\frac{1}{2}} = \left(\frac{S}{(XY)^{\frac{1}{2}}} + \frac{1}{Y^{\frac{1}{2}}} + \frac{1}{X^{\frac{1}{2}}} + \frac{1}{S_0}\right)XY \\
&= \left(\frac{2}{\log^A Y} + \frac{1}{Y^{\frac{1}{2}}} + \frac{1}{X^{\frac{1}{2}}}\right)XY \ll \frac{XY}{\log^A Y}
\end{aligned}$$

since the square root of a sum is less than or equal to the sum of square roots, and using that $Y^{\frac{1}{2}} \gg \log^A Y$ and $X^{\frac{1}{2}} > \log^A Y$, by hypothesis. Whence

$$\sum_j \sum_{\substack{S_j\leq r<2S_j \\ r<S}} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n\chi(n) \right| \left| \sum_{\substack{Z\leq p<Y \\ (p,s)=1}} \chi(p) \right| \ll \frac{XY}{\log^A Y} \sum_j 1 \ll \frac{XY \log S}{\log^A Y}$$

The contribution of the sum in the range $r < S_0$ and $S_0 \leq r < S$ are both bounded by a certain constant times $\frac{XY \log S}{\log^A Y}$. Hence their sum is too, which means

$$\sum_{r<S} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n\chi(n) \right| \left| \sum_{\substack{Z\leq p<Y \\ (p,s)=1}} \chi(p) \right| \ll \frac{XY \log S}{\log^A Y}$$

By Lemma B.4

$$\begin{aligned}
&\sum_{d<S} \frac{1}{\varphi(d)} \sum_{\chi \bmod d} \left| \sum_{n<X} a_n \chi(n) \right| \left| \sum_{Z \le p < Y} \chi(p) \right| \\
&\qquad \le \sum_{s<S} \frac{1}{\varphi(s)} \sum_{r<S} \frac{1}{\varphi(r)} \sideset{}{^*}\sum_{\chi \bmod r} \left| \sum_{\substack{n<X \\ (n,s)=1}} a_n \chi(n) \right| \left| \sum_{\substack{Z \le p < Y \\ (p,s)=1}} \chi(p) \right| \\
&\qquad \ll \frac{XY \log S}{\log^A Y} \sum_{s<S} \frac{1}{\varphi(s)} \ll \frac{XY \log^2 S}{\log^A Y} \le \frac{XY (\log XY)^2}{\log^A Y}
\end{aligned}$$

since $S \le XY$. □

4 Chen's Theorem

The chinese mathematician Jingrun Chen proved in 1966 (although did not publish his result until 1973 due to political turmoil in China) that there is a lower bound on the number of representations of even numbers as sums of an odd prime and a product of at most two primes.

Theorem 4.1 (Chen, 1966)**.** *Let N be an even large enough natural number and $\mathfrak{R}(N)$ denote the number of representations of N as the sum of an odd prime and a product of at most two primes. Then*

$$\mathfrak{R}(N) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

where

$$\mathfrak{S}(N) = 2\prod_{\substack{p>2\\ p|N}}\frac{p-1}{p-2}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)$$

In particular, every even large enough natural number is the sum of a prime and a product of at most two primes, since $\mathfrak{S}(N) \gg 1$ in view of the fact that

$$2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = O(1)$$

and

$$\prod_{\substack{p>2\\ p|N}}\frac{p-1}{p-2} > \prod_{\substack{p>2\\ p|N}} 1 = 1$$

A couple of remarks ought to be made before starting with the proof.

First, representations are to be understood as ordered pairs, meaning that $a+b$ and $b+a$ are considered different respresenations of a number as the sum of two other. This affects $\mathfrak{R}(N)$ only by a factor of at most 2.

The second remark to make is the fact that 1 is considered a product of at most two primes (for it is the product of no primes at all). This consideration does not alter the result, since $\mathfrak{R}(N)$ is increased by 2 when $N-1$ is prime and left unaffected otherwise.

Finally, the result has been deliberately stated in a simple form. One can be more precise in the prime decomposition of the product of at most two primes that occurs in the statement. In fact, said product is either 1 or a prime greater than $N^{\frac{1}{8}}$ or a semiprime product of a prime greater than $N^{\frac{1}{8}}$ and another prime greater than $N^{\frac{1}{3}}$. Moreover, representations of the form $N = p + (N-p)$, where p divides N are not counted. This implies that the representation $3+3$ for 6 or $24 = 2+22 = 3+21$, for instance, are excluded.

To motivate Chen's strategy for the proof of the theorem, consider first the following elementary remark:

Every natural number between 2 and $N-1$ not divisible by any prime strictly smaller than the k-th root of N is the product of at most $k-1$ primes.

Proof. Let $2 \leq n < N$. Write $n = p_1 \dots p_r$ as product of primes, where $r > 0$. If n is not divisible by any prime strictly smaller than $N^{\frac{1}{k}}$, then $p_i \geq N^{\frac{1}{k}}$, for all i. Hence $n \geq N^{\frac{r}{k}} > n^{\frac{r}{k}}$. Therefore, $1 > \frac{r}{k}$, which implies $k < r$. □

Initially, one may consider sieving the set

$$\{N - p \in \mathbb{N} \ : \ p < N\}$$

with sieving range $\mathbb{P}$ and sieving level $z = N^{\frac{1}{3}}$ to count how many $N - p$ in said set are product of at most two primes. The reason for it being that said amount equals the number of representations of N as the sum of a prime and a product of at most two primes, since $N = p + (N - p)$.

However, it will be made clear in the upcoming proof that in this case, lower bounds for the sieving function when applying Jurkat-Richert's Theorem turn out to be negative, and thus useless.

Hence, the strategy is to consider a larger initial set, and sieve out all numbers which are product of three or more primes. The way of doing this is by assigning weights to the elements of the set in a way that these are positive when such elements are at most product of two primes.

Finally, three main ingredients are to be used in the proof: the Jurkat-Richert Theorem (Theorem 2.7) to find upper and lower bounds for sieving functions and either the large sieve inequality in Theorem 3.5 or the Bombieri-Vinogradov Theorem (Theorem 3.1) to bound the error term the linear sieve produces.

4.1 Three Sieving Functions

Let N be an even integer. Consider the sieving set

$$A = \{N - p \ : \ p < N, \ (p, N) = 1\}$$

the sieving range

$$\mathcal{P} = \{p \in \mathbb{P} \ : \ (p, N) = 1\}$$

and the sieving level

$$z = N^{\frac{1}{k}}$$

where $k > 3$ is to be later established. Let

$$P(z) = \prod_{\substack{p < z \\ (p,N)=1}} p$$

Therefore the sieving function

$$S(A, \mathcal{P}, z) = \sum_{\substack{p < N \\ (p,N)=1 \\ (N-p,P(z))=1}} 1$$

counts all primes less than N that do not divide N and such that $N - p$ is not divisible by any prime smaller than z that does not divide N. Let $n \in A$. Then $n = N - p$ where

$p < N$ and $(p, N) = 1$. Let $d = (n, N)$. Then, $d \mid (N - p)$ and $d \mid N$. Hence, $d \mid p$, which implies $d = 1$ or $d = p$. The latter is impossible since $(p, N) = 1$. Hence the former must hold. Thus, any $n \in A$ such that $(n, P(z)) = 1$ can be written as

$$n = p_1 \dots p_r p_{r+1} \dots p_{r+s}$$

where

$$z = N^{\frac{1}{k}} \leq p_1 \leq \dots \leq p_r < N^{\frac{1}{3}} \leq p_{r+1} \leq \dots \leq p_{r+s}$$

since $n < N$, $(n, N) = 1$ and $(n, P(z)) = 1$. In particular

$$N^{\frac{s}{3}} \leq p_{r+1} \dots p_{r+s} \leq n < N$$

whence $\frac{s}{3} < 1$, which implies $s \in \{0, 1, 2\}$. Let

$$y = N^{\frac{1}{3}}$$

The way to proceed is to assign to any $n = N - p \in A$ with $(n, P(z)) = 1$ a positive weight if and only if either:

(*i*) $N - p = 1$, or

(*ii*) $N - p$ is a prime greater or equal than z, or

(*iii*) $N - p$ is the product of exactly two primes, both greater or equal than y, or

(*iv*) $N - p$ is the product of exactly two primes, one of them greater or equal than z and smaller than y, and the other greater or equal than y

Let

$$\alpha_n = 1 - \frac{1}{2} \sum_{\substack{z \leq q < y \\ q^j \| n}} j - \frac{1}{2} \sum_{\substack{n = p_1 p_2 p_3 \\ z \leq p_1 < y \leq p_2 \leq p_3}} 1$$

be the weight assigned to $n \in A$ such that $(n, P(z)) = 1$. The only positive values taken by α_n are 1 and $\frac{1}{2}$. By the factorization of n above, the first sum equals

$$\sum_{\substack{z \leq q < y \\ q^j \| n}} j = r$$

Moreover, the second sum

$$\sum_{\substack{n = p_1 p_2 p_3 \\ z \leq p_1 < y \leq p_2 \leq p_3}} 1$$

only takes the values 0 or 1.

Hence $\alpha_n > 0$ if and only if $r = 0$, or $r = 1$ and the second sum equals 0. Assume $r = 1$. Then the second sum equals 0 if and only if $s = \{0, 1\}$. Therefore $\alpha_n > 0$ if and only if $r = 0$ and $s \in \{0, 1, 2\}$, or $r = 1$ and $s = \{0, 1\}$. The case $r = s = 0$ corresponds to (*i*). The case $r + s = 1$ (meaning $r = 0$ and $s = 1$ and vice versa) refers to (*ii*). The case $r = 0$ and $s = 2$ is exactly (*iii*). Finally, $r = s = 1$ corresponds to (*iv*).

In any of the above cases, $r + s \leq 2$. With all these considerations, a lower bound for $\mathfrak{R}(N)$ can be found as follows

$$\begin{aligned}\mathfrak{R}(N) &= \sum_{\substack{N=p+n \\ n\in\{1,p_1,p_1p_2\}}} 1 \geq \sum_{\substack{n=N-p \\ p<N \\ (p,N)=1 \\ n\in\{1,p_1,p_1p_2\}}} 1 = \sum_{\substack{n\in A \\ n\in\{1,p_1,p_1p_2\}}} 1 \geq \sum_{\substack{n\in A \\ n\in\{1,p_1,p_1p_2\,:\,p_1,p_2\geq z\}}} 1 \\ &= \sum_{\substack{n\in A \\ (n,P(z))=1 \\ n\in\{1,p_1,p_1p_2\,:\,p_1,p_2\geq z\}}} 1 \geq \sum_{\substack{n\in A \\ (n,P(z))=1 \\ n\in\{1,p_1,p_1p_2\,:\,p_1,p_2\geq z\}}} \alpha_n\end{aligned}$$

where the last inequality trivially holds, since $\alpha_n \leq 1$. Therefore

$$\begin{aligned}\mathfrak{R}(N) &\geq \sum_{\substack{n\in A \\ (n,P(z))=1 \\ n\in\{1,p_1,p_1p_2\,:\,p_1,p_2\geq z\}}} \alpha_n \geq \sum_{\substack{n\in A \\ (n,P(z))=1}} \alpha_n \\ &= \left(\sum_{\substack{n\in A \\ (n,P(z))=1}} 1\right) - \frac{1}{2}\left(\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{z\leq q<y \\ q^j \| n}} j\right) - \frac{1}{2}\left(\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{n=p_1p_2p_3 \\ z\leq p_1<y\leq p_2\leq p_3}} 1\right)\end{aligned}$$

since $n \in A$ with $(n, P(z)) = 1$ such that $n \notin \{1, p_1, p_1p_2 \ : \ p_1, p_2 \geq z\}$ means $r + s > 2$, which implies $\alpha_n \leq 0$, by the above considerations.

Now the first sum is exactly the sieving function

$$\sum_{\substack{n\in A \\ (n,P(z))=1}} 1 = S(A, \mathcal{P}, z)$$

The second sum equals

$$\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{z\leq q<y \\ q^j \| n}} j = \left(\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{z\leq q<y \\ q \mid n}} 1\right) + \left(\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{z\leq q<y \\ q^j \| n}} (j-1)\right)$$

where in turn, the first sum equals

$$\sum_{\substack{n\in A \\ (n,P(z))=1}} \sum_{\substack{z\leq q<y \\ q \mid n}} 1 = \sum_{z\leq q<y} \sum_{\substack{n\in A \\ (n,P(z))=1 \\ q \mid n}} 1 = \sum_{z\leq q<y} S(A_q, \mathcal{P}, z)$$

where A_d is the usual

$$A_d = \{n \in A \ : \ d \mid n\}$$

and the second sum turns out to be

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le q<y\\q^j\|n}}(j-1)=\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le q<y\\q^j\|n\\j>1}}(j-1)=\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{j>1}(j-1)\sum_{\substack{z\le q<y\\q^j\|n}}1$$

$$=\sum_{z\le q<y}\sum_{j>1}(j-1)\sum_{\substack{n\in A\\(n,P(z))=1\\q^j\|n}}1\le\sum_{z\le q<y}\sum_{j>1}(j-1)\sum_{\substack{n<N\\q^j|n}}1\le N\sum_{z\le q<y}\sum_{j>1}\frac{j-1}{q^j}$$

since the amount of $n<N$ divisible by q^j adds up to $\left[\frac{N}{q^j}\right]\le\frac{N}{q^j}$. For any $|x|<1$

$$\frac{1}{(1-x)^2}=\sum_{j>0}jx^{j-1}=\sum_{j>1}(j-1)x^{j-2}$$

Therefore

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le q<y\\q^j\|n}}(j-1)\le N\sum_{z\le q<y}\sum_{j>1}\frac{j-1}{q^j}=N\sum_{z\le q<y}\frac{1}{q^2}\sum_{j>1}\frac{j-1}{q^{j-2}}=N\sum_{z\le q<y}\frac{1}{q^2(1-\frac{1}{q})^2}$$

$$=N\sum_{z\le q<y}\frac{1}{(q-1)^2}<N\sum_{q\ge z}\frac{1}{(q-1)^2}=N\sum_{q\ge z-1}\frac{1}{q^2}<N\int_{z-2}^{\infty}\frac{dx}{x^2}=\frac{N}{z-2}$$

$$=\frac{N}{N^{\frac{1}{k}}-2}\le\frac{2N}{N^{\frac{1}{k}}}=2N^{1-\frac{1}{k}}$$

since $N^{\frac{1}{k}}-2\ge\frac{1}{2}N^{\frac{1}{k}}$, for big enough values of N. Hence

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{z\le q<y\\q^j\|n}}j<\sum_{z\le q<y}S(A_q,\mathcal{P},z)+2N^{1-\frac{1}{k}}$$

Finally, for the third sum

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{n=p_1p_2p_3\\z\le p_1<y\le p_2\le p_3}}1$$

consider the set

$$B=\{N-p_1p_2p_3\ :\ p_1p_2p_3<N,\ z\le p_1<y\le p_2\le p_3,\ (p_1p_2p_3,N)=1\}$$

Let $N-p_1p_2p_3\in B\cap\mathbb{P}$. Then, $p=N-p_1p_2p_3\in B$. Hence, $p_1p_2p_3=N-p\in A$, since $p<N$ and $(p,N)=1$. Let now $p_1p_2p_3\in A$ with $z\le p_1<y\le p_2\le p_3$. Then, $N-p_1p_2p_3$ is prime, and in particular, $p_1p_2p_3<N$. Moreover, $(p_1p_2p_3,N)=1$, since otherwise $p_1p_2p_3\notin A$. Therefore, $N-p_1p_2p_3\in B\cap\mathbb{P}$ if and only if $p_1p_2p_3\in A$ and $z\le p_1<y\le p_2\le p_3$. Thus

$$\sum_{\substack{n\in A\\(n,P(z))=1}}\sum_{\substack{n=p_1p_2p_3\\z\le p_1<y\le p_2\le p_3}}1=\sum_{\substack{p_1p_2p_3\in A\\z\le p_1<y\le p_2\le p_3\\(p_1p_2p_3,P(z))=1}}1=\sum_{\substack{p_1p_2p_3\in A\\z\le p_1<y\le p_2\le p_3}}1=\sum_{n\in B\cap\mathbb{P}}1=\sum_{p\in B}1$$

$$=\sum_{\substack{p\in B\\p<y}}1+\sum_{\substack{p\in B\\p\ge y}}1<y+\sum_{\substack{p\in B\\p\ge y}}1\le y+\sum_{\substack{p\in B\\(p,P(y))=1}}1\le y+\sum_{\substack{n\in B\\(n,P(y))=1}}1=N^{\frac{1}{3}}+S(B,\mathcal{P},y)$$

Therefore, putting all the above together

Theorem 4.2.

$$\mathfrak{R}(N) > S(A,\mathcal{P},z) - \frac{1}{2}\sum_{z\le q<y} S(A_q,\mathcal{P},z) - \frac{1}{2}S(B,\mathcal{P},y) - N^{1-\frac{1}{k}} - \frac{1}{2}N^{\frac{1}{3}}$$

4.2 Linearity of the Sieves

The following step is to apply the Jurkat-Richert Theorem for each of the above three sieving functions. To do so, one must choose a suitable multiplicative function. For all the sieves to come, let

$$f(d) = \frac{1}{\varphi(d)}$$

where $\varphi(d)$ is Euler's totient function. Then, clearly $0 < f(p) < 1$, for all $p \in \mathcal{P}$, since $\varphi(p) = p-1$ and $2 \notin \mathcal{P}$ because N is even. The linearity of a sieve does not depend on the sieving set, but rather on the multiplicative function, the sieving range (which is $\mathcal{P}$ in all three cases) and the sieving level (either z or y).

Consider both cases z and y simultaneously, since both are of the form $w = N^{\frac{1}{K}}$ with $K \ge 3$. The only thing yet to be defined is the finite subset $\mathcal{Q}$ of $\mathcal{P}$ in such a way that

$$\prod_{\substack{p\in\mathcal{P}\setminus\mathcal{Q}\\ u\le p<w}} \frac{1}{1-\frac{1}{\varphi(p)}} \le (1+\varepsilon)\frac{\log w}{\log u}$$

holds for some $0 < \varepsilon < \frac{1}{200}$ and for all $1 < u < w$. By Lemma A.7, for any $\varepsilon > 0$, there exists $n_1(\varepsilon)$, such that

$$\prod_{u\le p<w} \frac{p}{p-1} = \prod_{u\le p<w} \left(1-\frac{1}{p}\right)^{-1} < (1+\tfrac{\varepsilon}{3})\frac{\log w}{\log u}$$

for every $n_1(\varepsilon) \le u < w$, independently of $w = N^{\frac{1}{K}}$. Moreover, there exists $n_2(\varepsilon)$, such that

$$\prod_{p\ge n_2(\varepsilon)} \frac{(p-1)^2}{p(p-2)} < 1+\tfrac{\varepsilon}{3}$$

since the product $\prod_p \frac{(p-1)^2}{p(p-1)} = \prod_p (1+\frac{1}{p(p-2)})$ converges. Let $n_3(\varepsilon) = \max\{n_1(\varepsilon), n_2(\varepsilon)\}$. Then, for any $u \ge n_3(\varepsilon)$

$$\begin{aligned}\prod_{u\le p<w} \frac{1}{1-\frac{1}{\varphi(p)}} = \prod_{u\le p<w} \frac{1}{1-\frac{1}{p-1}} = \prod_{u\le p<w} \frac{p-1}{p-2} = \prod_{u\le p<w} \frac{(p-1)^2}{p(p-2)} \prod_{u\le p<w} \frac{p}{p-1}\\ < (1+\tfrac{\varepsilon}{3})^2 \frac{\log w}{\log u} < (1+\varepsilon)\frac{\log w}{\log u}\end{aligned}$$

for any $0 < \varepsilon < 3$, and in particular, for any $0 < \varepsilon < \frac{1}{200}$. Let $\mathcal{Q}_\varepsilon$ be the set of primes not exceeding $n_3(\varepsilon)$. Define the finite subset $\mathcal{Q} = \mathcal{P} \cap \mathcal{Q}_\varepsilon$ of $\mathcal{P}$. Then

$$\prod_{\substack{p \in \mathcal{P} \setminus \mathcal{Q} \\ u \leq p < w}} \frac{1}{1 - \frac{1}{\varphi(p)}} \leq (1 + \varepsilon) \frac{\log w}{\log u}$$

holds for $0 < \varepsilon < \frac{1}{200}$ and for all $1 < u < N^{\frac{1}{K}}$, for all w. Hence, all hypothesis of Jurkat-Richert's Theorem (Theorem 2.7) are verified, since moreover $w = N^{\frac{1}{K}} \geq 2$ because N is big enough. By the remarks after said theorem, one concludes that the three sieves are linear and $V(w) \ll \frac{1}{\log N}$, where

$$V(w) = \prod_{p | P(w)} \left(1 - \frac{1}{\varphi(p)}\right) = \prod_{\substack{2 < p < w \\ (p,N)=1}} \left(1 - \frac{1}{p-1}\right)$$

Let $Q_\varepsilon = \prod_{p \in \mathcal{Q}_\varepsilon} p$ and $Q = \prod_{p \in \mathcal{Q}} p$. Then

$$Q \leq Q_\varepsilon < \log N$$

for sufficiently large N, since Q_ε does not depend on N. Finally

Theorem 4.3. *Let $w = N^{\frac{1}{K}}$, with $K \geq 3$. Then*

$$V(w) = \frac{K e^{-\gamma} \mathfrak{S}(N)}{\log N} \left(1 + O\left(\frac{1}{\log N}\right)\right)$$

for large enough N.

Proof. Let $N \geq 4^K$. Then $w = N^{\frac{1}{K}} \geq 4$. First, compute

$$\begin{aligned} V(w) \prod_{2 < p < w} \left(1 - \frac{1}{p-1}\right)^{-1} &= \prod_{\substack{2 < p < w \\ (p,N)=1}} \left(1 - \frac{1}{p-1}\right) \prod_{2 < p < w} \left(1 - \frac{1}{p-1}\right)^{-1} \\ &= \prod_{\substack{2 < p < w \\ p | N}} \left(1 - \frac{1}{p-1}\right)^{-1} = \prod_{\substack{p > 2 \\ p | N}} \left(1 - \frac{1}{p-1}\right)^{-1} \prod_{\substack{p \geq w \\ p | N}} \left(1 - \frac{1}{p-1}\right) \end{aligned}$$

Secondly, $0 < \frac{1}{p-1} \leq \frac{1}{w-1} < \frac{1}{3}$, for all $p \geq w$. Use the fact that $1 - x > e^{-2x}$, certainly for $0 < x < \frac{1}{3}$, and that $e^{-x} > 1 - x$, for all real x, to obtain

$$\begin{aligned} \prod_{\substack{p \geq w \\ p | N}} \left(1 - \frac{1}{p-1}\right) &> \prod_{\substack{p \geq w \\ p | N}} \exp\left(\frac{-2}{p-1}\right) = \exp\left(\sum_{\substack{p \geq w \\ p | N}} \frac{-2}{p-1}\right) \geq \exp\left(\sum_{\substack{p \geq w \\ p | N}} \frac{-2}{w-1}\right) \\ &\geq \exp\left(\frac{-2}{w-1} \sum_{p | N} 1\right) = \exp\left(\frac{-2\omega(N)}{w-1}\right) > \exp\left(\frac{-4 \log N}{w-1}\right) \\ &> \exp\left(\frac{-8 \log N}{w}\right) > 1 - 8 \frac{\log N}{w} = 1 - 8 \frac{\log N}{N^{\frac{1}{K}}} \end{aligned}$$

since $\omega(N) \leq 2\log N$, by Lemma A.4. Whence

$$V(w)\prod_{2<p<w}\left(1-\frac{1}{p-1}\right)^{-1} = \prod_{\substack{p>2\\ p|N}}\left(1-\frac{1}{p-1}\right)^{-1}\left(1+O\left(\frac{\log N}{N^{\frac{1}{K}}}\right)\right)$$
$$= \prod_{\substack{p>2\\ p|N}}\frac{p-2}{p-1}\ \left(1+O\left(\frac{1}{\log N}\right)\right)$$

Next

$$\sum_{n\geq w}\frac{1}{n(n-2)} < \int_{w-1}^{\infty}\frac{dx}{x(x-2)} = \frac{1}{2}\int_{w-1}^{\infty}\frac{dx}{x-2} - \frac{1}{2}\int_{w-1}^{\infty}\frac{dx}{x}$$
$$= -\frac{1}{2}\log(w-3) + \frac{1}{2}\log(w-1) = \frac{1}{2}\log\frac{w-1}{w-3}$$

Hence

$$\prod_{p\geq w}\left(1+\frac{1}{p(p-2)}\right) < \prod_{p\geq w}\exp\left(\frac{1}{p(p-2)}\right) = \exp\left(\sum_{p\geq w}\frac{1}{p(p-2)}\right) < \exp\left(\frac{1}{2}\log\frac{w-1}{w-3}\right)$$
$$= \left(\frac{w-1}{w-3}\right)^{\frac{1}{2}} = \left(1+\frac{2}{w-3}\right)^{\frac{1}{2}} < 1+\frac{2}{w-3} = 1+O\left(\frac{1}{w}\right)$$

since $1+x<e^x$ for all $x>0$. Therefore

$$\prod_{2<p<w}\left(1-\frac{1}{p-1}\right)\prod_{p<w}\left(1-\frac{1}{p}\right)^{-1} = 2\prod_{2<p<w}\left(1-\frac{1}{p-1}\right)\left(1-\frac{1}{p}\right)^{-1} = 2\prod_{2<p<w}\frac{p(p-2)}{(p-1)^2}$$
$$= 2\prod_{p>2}\frac{p(p-2)}{(p-1)^2}\prod_{p\geq w}\frac{(p-1)^2}{p(p-2)} = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\geq w}\left(1+\frac{1}{p(p-2)}\right)$$
$$= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{w}\right)\right)$$

Thus, by Theorem A.6

$$\prod_{2<p<w}\left(1-\frac{1}{p-1}\right) = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{w}\right)\right)\prod_{p<w}\left(1-\frac{1}{p}\right)$$
$$= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{w}\right)\right)\frac{e^{-\gamma}}{\log w}\left(1+O\left(\frac{1}{\log w}\right)\right)$$
$$= \frac{2e^{-\gamma}}{\log w}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\left(1+O\left(\frac{1}{\log N}\right)\right)$$

which finally implies

$$\begin{aligned} V(w) &= V(w) \prod_{2<p<w} \left(1 - \frac{1}{p-1}\right)^{-1} \prod_{2<p<w} \left(1 - \frac{1}{p-1}\right) \\ &= \prod_{\substack{p>2 \\ p|N}} \frac{p-2}{p-1} \left(1 + O\left(\frac{1}{\log N}\right)\right) \frac{2e^{-\gamma}}{\log w} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \left(1 + O\left(\frac{1}{\log N}\right)\right) \\ &= \frac{2e^{-\gamma}}{\log w} \prod_{\substack{p>2 \\ p|N}} \frac{p-2}{p-1} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \left(1 + O\left(\frac{1}{\log N}\right)\right) \\ &= \frac{e^{-\gamma}\mathfrak{S}(N)}{\log w} \left(1 + O\left(\frac{1}{\log N}\right)\right) = \frac{Ke^{-\gamma}\mathfrak{S}(N)}{\log N} \left(1 + O\left(\frac{1}{\log N}\right)\right) \end{aligned}$$

□

As a side note, recall that $V(w) \ll \frac{1}{\log N}$. Then, by Theorem 4.3, not only is $\mathfrak{S}(N) \gg 1$ as evidenced when first introducing $\mathfrak{S}(N)$, but also $\mathfrak{S}(N) \ll 1$.

With that, all is set to be begin sieving.

4.3 The Sieve of $S(A, \mathcal{P}, z)$

Jurkat-Richert's Theorem (Theorem 2.7) provides the following lower bound for $S(A, \mathcal{P}, z)$

$$S(A, \mathcal{P}, z) > \left(\phi\left(\tfrac{\log D}{\log z}\right) + O(\varepsilon)\right) |A| V(z) - R$$

for any $D \geq z^2 = N^{\frac{2}{k}}$, where ϕ is the function defined in Section 2.2, and

$$R = \sum_{\substack{d<DQ \\ d|P(z)}} |r(d)|$$

where

$$r(d) = |A_d| - \frac{|A|}{\varphi(d)}$$

The size of A and a bound for R are to be found and a value of D is to be fixed. First

$$|A| = \sum_{\substack{p<N \\ (p,N)=1}} 1 = \sum_{\substack{p\leq N \\ (p,N)=1}} 1 = \pi(N) - \omega(N)$$

since $p < N$ is equivalent to $p \leq N$, because N is even (and $p \neq 2$), and where $\omega(N)$ is the number of distinct prime divisors of N. By Lemma A.4

$$\omega(N) = O(\log N)$$

Hence, by the Prime Number Theorem

$$|A| = \frac{N}{\log N}\left(1 + O\left(\frac{1}{\log N}\right)\right) + O(\log N) = \frac{N}{\log N}\left(1 + O\left(\frac{1}{\log N}\right)\right) = \frac{N}{\log N}(1 + O(\varepsilon))$$

Secondly

$$|A_d| = \sum_{\substack{N-p\in A \\ d|(N-p)}} 1 = \sum_{\substack{p\leq N \\ (p,N)=1 \\ p\equiv N \bmod d}} 1 = \pi(N, N \bmod d) + O(\omega(N)) = \pi(N, N \bmod d) + O(\log N)$$

Then

$$\begin{aligned} r(d) = |A_d| - \frac{|A|}{\varphi(d)} &= \pi(N, N \bmod d) + O(\log N) - \frac{\pi(N)}{\varphi(d)} + \frac{\omega(N)}{\varphi(d)} \\ &= \pi(N, N \bmod d) - \frac{\pi(N)}{\varphi(d)} + O(\log N) \end{aligned}$$

Bombieri-Vinogradov (Theorem 3.1) is to be applied to bound

$$\begin{aligned} R = \sum_{\substack{d<DQ \\ d|P(z)}} |r(d)| &= \sum_{\substack{d<DQ \\ d|P(z)}} \left|\pi(N, N \bmod d) - \frac{\pi(N)}{\varphi(d)}\right| + \sum_{\substack{d<DQ \\ d|P(z)}} O(\log N) \\ &\leq \sum_{\substack{d<DQ \\ (d,N)=1}} \left|\pi(N, N \bmod d) - \frac{\pi(N)}{\varphi(d)}\right| + DQ\, O(\log N) \end{aligned}$$

The bound of R to seek is $O\big(\frac{N}{\log^3 N}\big)$. Hence, apply Theorem 3.1 with $N = x = n$ and $A = 3$. Choose

$$D = \frac{N^{\frac{1}{2}}}{(\log N)^{1+\beta(3)}}$$

for, by doing so, $D \geq z^2 = N^{\frac{2}{k}}$, provided that $k > 4$, for N big enough. Moreover

$$DQ < \frac{N^{\frac{1}{2}}}{(\log N)^{\beta(3)}}$$

since $Q < \log N$ for N big enough. Then, by Theorem 3.1

$$R \ll \frac{N}{\log^3 N}$$

since

$$DQ \log N < \frac{N^{\frac{1}{2}}}{(\log N)^{\beta(3)-1}} \ll \frac{N}{\log^3 N}$$

Finally

$$\frac{\log D}{\log z} = \frac{\frac{1}{2}\log N - (1+\beta(3))\log\log N}{\frac{1}{k}\log N} = \frac{k}{2} - k(1+\beta(3))\frac{\log\log N}{\log N}$$

Hence, if $4 < k \leq 8$

$$2 < \frac{\log D}{\log z} < \frac{k}{2} \leq 4$$

for big enough values of N. By Lemma 2.5

$$\begin{aligned}\phi\big(\tfrac{\log D}{\log z}\big) &= \frac{2e^\gamma \log z}{\log D}\log\big(\tfrac{\log D}{\log z}-1\big) = \frac{4e^\gamma \log\big(\frac{k}{2}-1\big)}{k} + O\left(\frac{\log\log N}{\log N}\right)\\ &= \frac{4e^\gamma \log\frac{k-2}{2}}{k} + O(\varepsilon)\end{aligned}$$

Hence

$$S(A,\mathcal{P},z) > \left(\frac{4e^\gamma \log\frac{k-2}{2}}{k} + O(\varepsilon)\right)\frac{N}{\log N}(1+O(\varepsilon))V(z) + O\left(\frac{N}{\log^3 N}\right)$$

Therefore

Theorem 4.4. *Let $4 < k \leq 8$. Then*

$$S(A,\mathcal{P},z) > \left(\frac{4e^\gamma \log\frac{k-2}{2}}{k} + O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\log^3 N}\right)$$

for large enough N.

An intermediate result can be obtained at this point by setting $k = 5$ momentarily. The number of representations of N as the sum of an odd prime and a product of at most four primes is bounded below by $S(A, \mathcal{P}, N^{\frac{1}{5}})$. In other words:

Corollary 4.5. *Let N be an even large enough natural number and $\mathfrak{R}_4(N)$ denote the number of representations of N as the sum of an odd prime and a product of at most four primes. Then*

$$\mathfrak{R}_4(N) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

Proof. By Theorem 4.4 with $k = 5$

$$\begin{aligned}\mathfrak{R}_4(N) > S(A,\mathcal{P},N^{\frac{1}{5}}) &> \left(\frac{4e^\gamma \log\frac{3}{2}}{5} + O(\varepsilon)\right)\frac{N}{\log N}V(N^{\frac{1}{5}}) + O\left(\frac{N}{\log^3 N}\right)\\ &= (4\log\tfrac{3}{2} + O(\varepsilon))\frac{e^\gamma}{5}\frac{N}{\log N}V(N^{\frac{1}{5}}) + O\left(\frac{N}{\log^3 N}\right)\end{aligned}$$

Choose $0 < \varepsilon < \frac{1}{200}$ small enough such that

$$4\log\tfrac{3}{2} + O(\varepsilon) = 1.6218... + O(\varepsilon) > 1$$

Then, by Theorem 4.3

$$\mathfrak{R}_4(N) > \mathfrak{S}(N)\frac{N}{\log^2 N}\left(1 + O\left(\frac{1}{\log N}\right)\right) + O\left(\frac{N}{\log^3 N}\right) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

□

4.4 The Sieve of $\sum_{z\leq q<y} S(A_q,\mathcal{P},z)$

Let q be a prime such that $z \leq q < y$. Jurkat-Richert's Theorem (Theorem 2.7) provides the following upper bound for $S(A_q,\mathcal{P},z)$

$$S(A_q,\mathcal{P},z) < \left(\Phi\left(\tfrac{\log D_q}{\log z}\right) + O(\varepsilon)\right)|A_q|V(z) + R_q$$

for any $D_q \geq z = N^{\frac{1}{k}}$, where Φ is the function defined in Section 2.2, and

$$R_q = \sum_{\substack{d<D_qQ\\ d|P(z)}} |r_q(d)|$$

where

$$r_q(d) = |(A_q)_d| - \frac{|A_q|}{\varphi(d)}$$

First, assume $q \mid N$. If $q \mid (N-p)$, where $N-p \in A$, then $q \mid p$, which implies $q = p$ and contradicts the fact that $N-p \in A$, since $(p,N)=1$. Thus, $|A_q| = 0$ for every $q \mid N$. From now on, assume $q \nmid N$, that is, $(q,N)=1$. In other words

$$\sum_{z\leq q<y} S(A_q,\mathcal{P},z) = \sum_{\substack{z\leq q<y\\ (q,N)=1}} S(A_q,\mathcal{P},z)$$

Let $d \mid P(z)$. Then $(q,d)=1$, since $q \geq z$. Then

$$|(A_q)_d| = \sum_{\substack{n\in A_q\\ d|n}} 1 = \sum_{\substack{n\in A\\ q|n\\ d|n}} 1 = \sum_{\substack{n\in A\\ qd|n}} 1 = |A_{qd}|$$

Therefore

$$\begin{aligned} r_q(d) &= |A_{qd}| - \frac{|A_q|}{\varphi(d)} = |A_{qd}| - \frac{|A|}{\varphi(qd)} - \frac{|A_q|}{\varphi(d)} + \frac{|A|}{\varphi(qd)} = r(qd) - \frac{1}{\varphi(d)}\left(|A_q| - \frac{|A|}{\varphi(q)}\right) \\ &= r(qd) - \frac{r(q)}{\varphi(d)} \end{aligned}$$

since $\varphi(qd) = \varphi(q)\varphi(d)$. Hence

$$R_q = \sum_{\substack{d<D_qQ\\ d|P(z)}} |r_q(d)| \leq \sum_{\substack{d<D_qQ\\ d|P(z)}} |r(qd)| + |r(q)| \sum_{\substack{d<D_qQ\\ d|P(z)}} \frac{1}{\varphi(d)}$$

For any $z \leq q < y$, let

$$D_q = \frac{N^{\frac{1}{2}}}{q(\log N)^{1+\beta(4)}}$$

which is greater than $z = N^{\frac{1}{k}}$, provided that $k > 6$, for in this case

$$D_q > \frac{N^{\frac{1}{2}}}{y(\log N)^{1+\beta(4)}} = \frac{N^{\frac{1}{6}}}{(\log N)^{1+\beta(4)}} > N^{\frac{1}{k}} = z$$

for N big enough. Instead of estimating R_q alone, a bound for

$$\begin{aligned}\sum_{\substack{z\le q<y\\(q,N)=1}} R_q &\le \sum_{\substack{z\le q<y\\(q,N)=1}}\sum_{\substack{d<D_qQ\\d|P(z)}}|r(qd)| + \sum_{\substack{z\le q<y\\(q,N)=1}}|r(q)|\sum_{\substack{d<D_qQ\\d|P(z)}}\frac{1}{\varphi(d)}\\ &\le \sum_{\substack{s<qD_qQ\\(s,N)=1}}|r(s)| + \sum_{\substack{z\le q<y\\(q,N)=1}}|r(q)|\sum_{d<N}\frac{1}{\varphi(d)}\end{aligned}$$

is found using Bombieri-Vinogradov (Theorem 3.1) once again. As a matter of fact, apply Theorem 3.1 with $N=x=n$ and $A=4$, to obtain

$$\begin{aligned}\sum_{\substack{s<qD_qQ\\(s,N)=1}}|r(s)| &= \sum_{\substack{s<qD_qQ\\(s,N)=1}}\left|\pi(N,N \bmod s)-\frac{\pi(N)}{\varphi(s)}\right| + \sum_{\substack{s<qD_qQ\\(s,N)=1}}O(\log N)\\ &\le \sum_{\substack{s<qD_qQ\\(s,N)=1}}\left|\pi(N,N \bmod s)-\frac{\pi(N)}{\varphi(s)}\right| + qD_qQ\,O(\log N) \ll \frac{N}{\log^4 N}\end{aligned}$$

since

$$qD_qQ < \frac{N^{\frac12}}{(\log N)^{\beta(4)}}$$

because $Q<\log N$ for N big enough. In particular

$$\sum_{\substack{z\le q<y\\(q,N)=1}}|r(q)| \le \sum_{\substack{q<y\\(q,N)=1}}|r(q)| \le \sum_{\substack{s<qD_qQ\\(q,N)=1}}|r(s)| \ll \frac{N}{\log^4 N}$$

since $y<qD_q<qD_qQ$. Moreover, by Lemma B.4

$$\sum_{d<N}\frac{1}{\varphi(d)} \ll \log N$$

Then

$$\sum_{\substack{z\le q<y\\(q,N)=1}} R_q \ll \frac{N}{\log^4 N} + \frac{N}{\log^4 N}\log N \ll \frac{N}{\log^3 N}$$

On the one hand

$$\frac{\log D_q}{\log z} = \frac{\frac12\log N - \log q - (1+\beta(4))\log\log N}{\frac1k\log N} = \frac{k}{2} - k\frac{\log q}{\log N} - k(1+\beta(4))\frac{\log\log N}{\log N}$$

where, if $6<k\le 8$

$$1 < \frac{k}{6} < \frac{k}{2} - k\frac{\log q}{\log N} < \frac{k}{2} - 1 \le 3$$

since $\frac1k\log N \le \log q < \frac13\log N$. Hence $1<\frac{\log D_q}{\log z}<3$, for N big enough. By Lemma 2.4

$$\Phi\big(\tfrac{\log D_q}{\log z}\big) = \frac{2e^\gamma}{\frac{k}{2} - k\frac{\log q}{\log N}} + O\left(\frac{\log\log N}{\log N}\right) = \frac{2e^\gamma}{k(\frac12 - \frac{\log q}{\log N})} + O(\varepsilon)$$

On the other hand, by the Prime Number Theorem

$$\begin{aligned}|A_q| &= \pi(N, N \bmod q) + O(\log N) = \frac{\pi(N)}{\varphi(q)} + \pi(N, N \bmod q) - \frac{\pi(N)}{\varphi(q)} + O(\log N) \\ &= \frac{N}{\varphi(q)\log N}\left(1 + O\left(\frac{1}{\log N}\right)\right) + \pi(N, N \bmod q) - \frac{\pi(N)}{\varphi(q)}\end{aligned}$$

Therefore

$$\begin{aligned}\sum_{\substack{z\le q<y\\(q,N)=1}} \left(\Phi\left(\tfrac{\log D_q}{\log z}\right) + O(\varepsilon)\right)|A_q| = &\sum_{\substack{z\le q<y\\(q,N)=1}} \left(\frac{2e^\gamma}{k(\frac{1}{2} - \frac{\log q}{\log N})} + O(\varepsilon)\right) \frac{N\left(1 + O\left(\frac{1}{\log N}\right)\right)}{\varphi(q)\log N} \\ &+ \sum_{\substack{z\le q<y\\(q,N)=1}} \left(\frac{2e^\gamma}{k(\frac{1}{2} - \frac{\log q}{\log N})} + O(\varepsilon)\right)\left(\pi(N, N \bmod q) - \frac{\pi(N)}{\varphi(q)}\right)\end{aligned}$$

The factor

$$\frac{2e^\gamma}{k(\frac{1}{2} - \frac{\log q}{\log N})} + O(\varepsilon) \le \frac{2e^\gamma}{k(\frac{1}{2} - \frac{1}{3})} + O(\varepsilon) = O(1)$$

since $\varepsilon < \frac{1}{200} = O(1)$. Hence the second sum is

$$O\left(\sum_{\substack{q<y\\(q,N)=1}} \left|\pi(N, N \bmod q) - \frac{\pi(N)}{\varphi(q)}\right|\right) = O\left(\frac{N}{\log^2 N}\right) = O(\varepsilon)\frac{N}{\log N}$$

after applying Bombieri-Vinogradov (Theorem 3.1) with $N = x = n$ and $A = 2$, since $y = N^{\frac{1}{3}} < \frac{N^{\frac{1}{2}}}{(\log N)^{\beta(2)}}$ for big enough values of N. The first sum is equal to

$$\frac{2e^\gamma N}{k}\left(1 + O\left(\frac{1}{\log N}\right)\right)\sum_{\substack{z\le q<y\\(q,N)=1}} \frac{1}{\varphi(q)(\frac{1}{2}\log N - \log q)} + O(\varepsilon)\frac{N}{\log N}\sum_{\substack{z\le q<y\\(q,N)=1}} \frac{1}{\varphi(q)}$$

By Lemma A.3

$$\begin{aligned}\sum_{\substack{z\le q<y\\(q,N)=1}} \frac{1}{\varphi(q)} = \sum_{\substack{z\le q<y\\(q,N)=1}} \frac{1}{q-1} &\le \sum_{z\le q<y} \frac{1}{q-1} \ll \sum_{z\le q<y} \frac{1}{q} = \log\log y - \log\log z + O(1) \\ &= \log(\tfrac{1}{3}\log N) - \log(\tfrac{1}{k}\log N) + O(1) = \log\tfrac{k}{3} + O(1) = O(1)\end{aligned}$$

Hence

$$O(\varepsilon)\frac{N}{\log N}\sum_{\substack{z\le q<y\\(q,N)=1}} \frac{1}{\varphi(q)} = O(\varepsilon)\frac{N}{\log N}$$

and

$$\frac{N}{\log N}\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)(\frac{1}{2}\log N-\log q)}=\frac{kN}{\log^2 N}\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)(\frac{k}{2}-k\frac{\log q}{\log N})}$$
$$\ll\frac{N}{\log^2 N}\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)}\ll\frac{N}{\log^2 N}=O(\varepsilon)\frac{N}{\log N}$$

since $1<\frac{k}{2}-k\frac{\log q}{\log N}<3$. This means, by all the above, that

$$\sum_{\substack{z\le q<y\\(q,N)=1}}\Big(\Phi\big(\tfrac{\log D_q}{\log z}\big)+O(\varepsilon)\Big)\,|A_q|<\frac{2e^{\gamma}N}{k}\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)(\frac{1}{2}\log N-\log q)}+O(\varepsilon)\frac{N}{\log N}$$

To bound the above sum, write

$$\frac{1}{\varphi(q)}=\frac{1}{q-1}\le\frac{1}{q}+\frac{2}{q^2}$$

Then

$$\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)(\frac{1}{2}\log N-\log q)}\le\sum_{z\le q<y}\frac{1}{q(\frac{1}{2}\log N-\log q)}+\sum_{z\le q<y}\frac{2}{q^2(\frac{1}{2}\log N-\log q)}$$

where

$$\sum_{z\le q<y}\frac{2}{q^2(\frac{1}{2}\log N-\log q)}\le\sum_{z\le q<y}\frac{2}{q^2(\frac{1}{2}\log N-\log y)}=\sum_{z\le q<y}\frac{2}{q^2(\frac{1}{2}-\frac{1}{3})\log N}$$
$$=\frac{12}{\log N}\sum_{z\le q<y}\frac{1}{q^2}<\frac{12}{\log N}\int_{z-1}^{\infty}\frac{dx}{x^2}=\frac{12}{\log N}\frac{1}{z-1}\ll\frac{1}{z\log N}=O\left(\frac{1}{\log^2 N}\right)$$

Consider next the continuous, positive and increasing function

$$f(x)=\frac{1}{\frac{1}{2}\log N-\log x}$$

defined for $z\le x\le y$. Then, by twice integrating by parts and using Lemma A.3 in the form

$$\sum_{p<x}\frac{1}{p}=\log\log x+a+O\left(\frac{1}{\log x}\right)$$

for some constant $a>0$

$$\begin{aligned}\sum_{z\le q<y}\frac{1}{q(\frac12\log N-\log q)}&=\sum_{z\le q<y}\frac{f(q)}{q}=\int_z^y f(x)\,d\left(\sum_{q<x}\frac1q\right)\\&=f(y)\sum_{q<y}\frac1q-f(z)\sum_{q<z}\frac1q-\int_z^y\sum_{q<x}\frac1q\,df(x)\\&=f(y)(\log\log y+a)-f(z)(\log\log z+a)-\int_z^y(\log\log x+a)\,df(x)+\\&\qquad+O\left(\frac{f(y)}{\log y}\right)+O\left(\frac{f(z)}{\log z}\right)+\int_z^y O\left(\frac{1}{\log x}\right)df(x)\\&=\int_z^y f(x)\,d(\log\log x+a)+O\left(\frac{f(y)}{\log y}\right)+O\left(\frac{f(z)}{\log z}\right)+O\left(\int_z^y\frac{df(x)}{\log x}\right)\end{aligned}$$

First

$$O\left(\frac{f(y)}{\log y}\right)+O\left(\frac{f(z)}{\log z}\right)=O\left(\frac{f(y)}{\log z}\right)=O\left(\frac{1}{\log^2 N}\right)$$

since f is increasing and

$$\frac{f(y)}{\log z}=\frac{1}{\frac1k\log N(\frac12\log N-\frac13\log N)}=\frac{6k}{\log^2 N}$$

Second

$$\begin{aligned}\int_z^y\frac{df(x)}{\log x}&=\int_z^y\frac{dx}{x\log x(\frac12\log N-\log x)^2}<\int_z^y\frac{dx}{x\log z(\frac12\log N-\log y)^2}\\&=\frac{1}{\frac1k\log N(\frac12\log N-\frac13\log N)^2}\int_z^y\frac{dx}{x}=\frac{\frac13\log N-\frac1k\log N}{\frac{1}{36k}\log^3 N}=O\left(\frac{1}{\log^2 N}\right)\end{aligned}$$

Third, using the change of variables $x=N^u$

$$\begin{aligned}\int_z^y f(x)\,d\log\log x=\int_z^y\frac{dx}{x\log x(\frac12\log N-\log x)}&=\int_{\frac1k}^{\frac13}\frac{N^u\log N\,du}{N^u u\log N(\frac12\log N-u\log N)}\\&=\frac{1}{\log N}\int_{\frac1k}^{\frac13}\frac{du}{u(\frac12-u)}=\frac{2}{\log N}\int_{\frac1k}^{\frac13}\left(\frac{du}{u}+\frac{du}{\frac12-u}\right)\\&=\frac{2}{\log N}\big(\log\tfrac13-\log\tfrac1k-\log\tfrac16+\log(\tfrac12-\tfrac1k)\big)=\frac{2\log(k-2)}{\log N}\end{aligned}$$

Whence

$$\sum_{\substack{z\le q<y\\(q,N)=1}}\frac{1}{\varphi(q)(\frac12\log N-\log q)}\le\frac{2\log(k-2)}{\log N}+O\left(\frac{1}{\log^2 N}\right)$$

Finally

$$\begin{aligned}\sum_{\substack{z\le q<y\\(q,N)=1}}\Big(\Phi\big(\tfrac{\log D_q}{\log z}\big)+O(\varepsilon)\Big)|A_q|&<\frac{2e^\gamma N}{k}\frac{2\log(k-2)}{\log N}+\frac{2e^\gamma N}{k}O\left(\frac{1}{\log^2 N}\right)+O(\varepsilon)\frac{N}{\log N}\\&=\frac{4e^\gamma N\log(k-2)}{k\log N}+O(\varepsilon)\frac{N}{\log N}\end{aligned}$$

Thus

$$\sum_{z\le q<y} S(A_q,\mathcal{P},z) = \sum_{\substack{z\le q<y\\(q,N)=1}} S(A_q,\mathcal{P},z) < \sum_{\substack{z\le q<y\\(q,N)=1}} \left(\Phi\left(\tfrac{\log D_q}{\log z}\right)+O(\varepsilon)\right)|A_q|V(z) + \sum_{\substack{z\le q<y\\(q,N)=1}} R_q$$
$$< \frac{4e^\gamma \log(k-2)}{k}\frac{N}{\log N}V(z) + O(\varepsilon)\frac{N}{\log N}V(z) + O\left(\frac{N}{\log^3 N}\right)$$

Therefore

Theorem 4.6. *Let $6 < k \le 8$. Then*

$$\sum_{z\le q<y} S(A_q,\mathcal{P},z) < \left(\frac{4e^\gamma\log(k-2)}{k}+O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\log^3 N}\right)$$

for large enough N.

Another intermediate result can be obtained at this point. Having studied the two first terms of the weight α_n allows one to produce an upper bound for the number of representations of N as the sum of an odd prime and a product of at most three primes, say $\mathfrak{R}_3(N)$, which is obtained by assigning the weights

$$\widetilde{\alpha}_n = 1 - \frac{1}{2}\sum_{\substack{z\le q<y\\ q^j\|n}} j$$

to $n \in A$ such that $(n, P(z)) = 1$ instead of

$$\alpha_n = \widetilde{\alpha}_n - \frac{1}{2}\sum_{\substack{n=p_1p_2p_3\\ z\le p_1<y\le p_2\le p_3}} 1$$

This implies, that $\widetilde{\alpha}_n > 0$ if and only if n is such that $\alpha_n > 0$, or $\alpha_n = 0$ and the above sum equals 1. Now, if said sum is 1 exactly, then $\alpha_n = 0$. Hence, $\widetilde{\alpha}_n > 0$ if and only if n is of the case (i), (ii), (iii), (iv), or the product of three primes, $n = p_1p_2p_3$, with $z \le p_1 < y \le p_2 \le p_3$. Thus

$$\mathfrak{R}_3(N) > S(A,\mathcal{P},z) - \frac{1}{2}\sum_{z\le q<y} S(A_q,\mathcal{P},z) - N^{1-\frac{1}{k}}$$

and by Theorem 4.4 and Theorem 4.6, with $k = 7$ (or similarly with $k = 8$)

$$S(A,\mathcal{P},z) - \frac{1}{2}\sum_{z\le q<y} S(A_q,\mathcal{P},z) - N^{\frac{6}{7}}$$
$$> \left(\frac{4e^\gamma\log\frac{5}{2}}{7} - \frac{1}{2}\frac{4e^\gamma\log 5}{7} + O(\varepsilon)\right)\frac{N}{\log N}V(N^{\frac{1}{7}}) + O\left(\frac{N}{\log^3 N}\right)$$

Whence

Corollary 4.7. *Let N be an even large enough natural number and $\mathfrak{R}_3(N)$ denote the number of representations of N as the sum of an odd prime and a product of at most three primes. Then*

$$\mathfrak{R}_3(N) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

Proof. By Theorem 4.4 and Theorem 4.6 with $k = 7$

$$\mathfrak{R}_3(N) > (2\log\tfrac{5}{2} - \log 5 + O(\varepsilon))\frac{2e^\gamma}{7}\frac{N}{\log N}V(N^{\frac{1}{7}}) + O\left(\frac{N}{\log^3 N}\right)$$

Choose $0 < \varepsilon < \frac{1}{200}$ small enough such that

$$2\log\tfrac{5}{2} - \log 5 + O(\varepsilon) = \log\tfrac{5}{4} + O(\varepsilon) = 0.2231... + O(\varepsilon) > \frac{1}{5}$$

Then, by Theorem 4.3

$$\mathfrak{R}_3(N) > \frac{2}{5}\mathfrak{S}(N)\frac{N}{\log^2 N}\left(1 + O\left(\frac{1}{\log N}\right)\right) + O\left(\frac{N}{\log^3 N}\right) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

□

4.5 The Sieve of $S(B, \mathcal{P}, y)$

Bombieri-Vinogradov will no longer be of any use when bounding the error term. Instead, this is accomplished by large sieving techniques and particularly Theorem 3.5.

The set

$$B = \{N - p_1p_2p_3 \ : \ p_1p_2p_3 < N,\ z \le p_1 < y \le p_2 \le p_3,\ (p_1p_2p_3, N) = 1\}$$

is far too restrictive. Instead, a new set B' is defined containing B. Divide the interval $z \le x < y$ into pairwise disjoint subintervals $x_j \le x < (1+\varepsilon)x_j$, where

$$x_j = (1+\varepsilon)^j z$$

and $0 \le j \le \frac{\log y - \log z}{\log(1+\varepsilon)}$, since $x_0 = z$ and

$$(1+\varepsilon)^{\frac{\log y - \log z}{\log(1+\varepsilon)}} z = e^{\frac{\log y}{\log(1+\varepsilon)}\log(1+\varepsilon)}e^{\log z} = e^{\log y} = y$$

This implies that for every $z \le p_1 < y$, there exists a unique j, such that $x_j \le p_1 < (1+\varepsilon)x_j$. Define the sets B^j by

$$\{N - p_1p_2p_3 \ : \ z \le p_1 < y \le p_2 \le p_3,\ x_j \le p_1 < (1+\varepsilon)x_j,\ x_jp_2p_3 < N,\ (p_2p_3, N) = 1\}$$

The number of sets B^j is bounded above by

$$\frac{\log y - \log z}{\log(1+\varepsilon)} + 1 = \frac{(\frac{1}{3} - \frac{1}{k})\log N}{\log(1+\varepsilon)} + 1 \ll \frac{\log N}{\log(1+\varepsilon)} \ll \frac{\log N}{\varepsilon}$$

since $k > 3$ and $0 < \varepsilon < \frac{1}{200}$. Define

$$B' = \bigcup_j B^j$$

Then

$$|B'| = \sum_j |B^j|$$

since B^j are pairwise disjoint. Furthermore

$$B \subseteq B'$$

Hence

$$S(B, \mathcal{P}, y) \leq S(B', \mathcal{P}, y) = \sum_{\substack{b \in B' \\ (b, P(y))=1}} 1 = \sum_j \sum_{\substack{b \in B^j \\ (b, P(y))=1}} 1 = \sum_j S(B^j, \mathcal{P}, y)$$

The estimate of $S(B^j, \mathcal{P}, y)$ is once again provided by Jurkat-Richert's Theorem (Theorem 2.7), by means of

$$S(B^j, \mathcal{P}, y) < \left(\Phi\left(\tfrac{\log D}{\log y}\right) + O(\varepsilon)\right) |B^j| V(y) + R_j$$

for any $D \geq y = N^{\frac{1}{3}}$, where Φ is the function defined in Section 2.2, and

$$R_j = \sum_{\substack{d < DQ \\ d | P(y)}} |r_j(d)|$$

where

$$r_j(d) = |B_d^j| - \frac{|B^j|}{\varphi(d)}$$

and $B_d^j = \{b \in B^j \ : \ d \mid b\}$, for all $d \mid P(y)$. Then, for any j and any $d \mid P(y)$

$$r_j(d) = \sum_{\substack{b \in B^j \\ d | b}} 1 - \frac{1}{\varphi(d)} \sum_{b \in B^j} 1 = \sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1 \\ p_1 p_2 p_3 \equiv N \pmod d}} 1 - \frac{1}{\varphi(d)} \sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1}} 1$$

A prime p_1 either divides d or is coprime with d. Hence, the second sum can be written as

$$\sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1}} 1 = \sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1 \\ (p_1, d) = 1}} 1 + \sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1 \\ p_1 | d}} 1$$

where

$$\sum_{\substack{z \leq p_1 < y \leq p_2 \leq p_3 \\ x_j \leq p_1 < (1+\varepsilon) x_j \\ x_j p_2 p_3 < N, \, (p_2 p_3, N) = 1 \\ p_1 | d}} 1 \leq \sum_{\substack{p_1 \geq z \\ p_1 p_2 p_3 < (1+\varepsilon) N \\ p_1 | d}} 1 = \sum_{\substack{p_1 \geq z \\ p_1 | d}} \sum_{p_2 p_3 < (1+\varepsilon) \frac{N}{p_1}} 1 \leq (1+\varepsilon) N \sum_{\substack{p_1 \geq z \\ p_1 | d}} \frac{1}{p_1}$$

$$\leq \frac{2N}{z} \sum_{\substack{p_1 \geq z \\ p_1 | d}} 1 \leq 2 N^{1 - \frac{1}{k}} \omega(d) = O\left(N^{1 - \frac{1}{k}} \log d\right)$$

by Lemma A.4. For any d dividing $P(y)$, the condition $(p_1, d) = 1$ is equivalent to $(p_1p_2p_3, d) = 1$, since $(p_2p_3, d) = 1$ is already implied by $d \mid P(y)$, since both p_2 and p_3 are greater or equal than y. Therefore

$$r_j(d) = \sum_{\substack{z \le p_1 < y \le p_2 \le p_3 \\ x_j \le p_1 < (1+\varepsilon)x_j \\ x_j p_2 p_3 < N,\ (p_2p_3, N) = 1 \\ p_1p_2p_3 \equiv N \pmod d}} 1 - \frac{1}{\varphi(d)} \sum_{\substack{z \le p_1 < y \le p_2 \le p_3 \\ x_j \le p_1 < (1+\varepsilon)x_j \\ x_j p_2 p_3 < N,\ (p_2p_3, N) = 1 \\ (p_1p_2p_3, d) = 1}} 1 + O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)}\right)$$

Let $(a_n)_n$ be the sequence defined by

$$a_n = \begin{cases} 1 & \text{if } n = p_2p_3,\ \ y \le p_2 \le p_3,\ \ (p_2p_3, N) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then

$$r_j(d) = \sum_{\substack{z \le p_1 < y \\ x_j \le p_1 < (1+\varepsilon)x_j \\ x_j n < N \\ p_1 n \equiv N \pmod d}} a_n - \frac{1}{\varphi(d)} \sum_{\substack{z \le p_1 < y \\ x_j \le p_1 < (1+\varepsilon)x_j \\ x_j n < N \\ (p_1 n, d) = 1}} a_n + O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)}\right)$$

Let

$$X_j = \frac{N}{x_j}, \qquad Y_j = \min(y, (1+\varepsilon)x_j), \qquad Z_j = \max(z, x_j) = x_j$$

Then

$$\begin{aligned} r_j(d) &= \sum_{n < \frac{N}{x_j}} \sum_{\substack{z \le p_1 < y \\ x_j \le p_1 < (1+\varepsilon)x_j \\ p_1 n \equiv N \pmod d}} a_n - \frac{1}{\varphi(d)} \sum_{n < \frac{N}{x_j}} \sum_{\substack{z \le p_1 < y \\ x_j \le p_1 < (1+\varepsilon)x_j \\ (p_1 n, d) = 1}} a_n + O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)}\right) \\ &= \sum_{n < X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ p_1 n \equiv N \pmod d}} a_n - \frac{1}{\varphi(d)} \sum_{n < X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ (p_1 n, d) = 1}} a_n + O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)}\right) \end{aligned}$$

Let

$$D = \frac{N^{\frac{1}{2}}}{\log^7 N}$$

which is greater than $y = N^{\frac{1}{3}}$. Then

$$DQ < \frac{N^{\frac{1}{2}}}{\log^6 N} < \frac{N^{\frac{1}{2}}}{\log^6 y} \left(\min\left(\frac{y}{x_j}, 1+\varepsilon\right)\right)^{\frac{1}{2}} = \frac{N^{\frac{1}{2}}}{\log^6 y} \left(\frac{Y_j}{x_j}\right)^{\frac{1}{2}} = \frac{(X_jY_j)^{\frac{1}{2}}}{\log^6 y} \le \frac{(X_jY_j)^{\frac{1}{2}}}{\log^6 Y_j}$$

since $Q < \log N$ for N big enough and both $\frac{y}{x_j}$ and $1+\varepsilon$ are greater than 1. By Theorem 3.5,

with $X = X_j$, $Y = Y_j$, $Z = Z_j$, $h = N$ and $A = 6$

$$R_j = \sum_{\substack{d<DQ \\ d|P(y)}} |r_j(d)| =$$

$$= \sum_{\substack{d<DQ \\ d|P(y)}} \left| \sum_{n<X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ p_1 n \equiv N (\mathrm{mod}\, d)}} a_n - \frac{1}{\varphi(d)} \sum_{n<X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ (p_1 n, d)=1}} a_n \right| + \sum_{\substack{d<DQ \\ d|P(y)}} O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)} \right)$$

$$\le \sum_{\substack{d<\frac{\sqrt{X_j Y_j}}{\log^6 Y_j} \\ d|P(y)}} \left| \sum_{n<X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ p_1 n \equiv N (\mathrm{mod}\, d)}} a_n - \frac{1}{\varphi(d)} \sum_{n<X_j} \sum_{\substack{Z_j \le p_1 < Y_j \\ (p_1 n, d)=1}} a_n \right| + \sum_{\substack{d<\frac{\sqrt{X_j Y_j}}{\log^6 Y_j} \\ d|P(y)}} O\left(\frac{N^{1-\frac{1}{k}} \log d}{\varphi(d)} \right)$$

$$\ll \frac{X_j Y_j (\log X_j Y_j)^2}{\log^6 Y_j} + N^{1-\frac{1}{k}} \log \frac{(X_j Y_j)^{\frac{1}{2}}}{\log^6 Y_j} \sum_{\substack{d<\frac{\sqrt{X_j Y_j}}{\log^6 Y_j} \\ d|P(y)}} \frac{1}{\varphi(d)}$$

since $d \mid P(y)$ implies $(d, N) = 1$. Theorem 3.5 can be applied since

$$\log^{12} Y_j \le \log^{12} y < \log^{12} N < N^{\frac{2}{3}} = \frac{N}{y} \le \frac{N}{x_j} = X_j$$

In addition

$$X_j Y_j = \frac{N}{x_j} \min(y, (1+\varepsilon) x_j) \le \frac{N}{x_j} (1+\varepsilon) x_j = N(1+\varepsilon) \le 2N \ll N$$

and

$$\log Y_j \gg \log N$$

since clearly $\log y = \frac{1}{3} \log N \gg \log N$ and $\log((1+\varepsilon)x_j) > \log x_j \ge \log x_0 = \log z = \frac{1}{k} \log N \gg \log N$. Moreover, by Lemma B.4

$$\sum_{\substack{d<\frac{\sqrt{X_j Y_j}}{\log^6 Y_j} \\ d|P(y)}} \frac{1}{\varphi(d)} \le \sum_{d<\frac{\sqrt{X_j Y_j}}{\log^6 Y_j}} \frac{1}{\varphi(d)} \ll \log \frac{(X_j Y_j)^{\frac{1}{2}}}{\log^6 Y_j} \ll \log \frac{N^{\frac{1}{2}}}{\log^6 N}$$

Therefore

$$R_j \ll \frac{N \log^2 N}{\log^6 N} + N^{1-\frac{1}{k}} \log^2 \frac{N^{\frac{1}{2}}}{\log^6 N} \ll \frac{N}{\log^4 N}$$

Hence

$$S(B^j, \mathcal{P}, y) < \left(\Phi\left(\tfrac{\log D}{\log y}\right) + O(\varepsilon) \right) |B^j| V(y) + O\left(\frac{N}{\log^4 N} \right)$$

where

$$\frac{\log D}{\log y} = \frac{\frac{1}{2} \log N - 7 \log \log N}{\frac{1}{3} \log N} = \frac{3}{2} - 21 \frac{\log \log N}{\log N}$$

By Lemma 2.4

$$\Phi\big(\tfrac{\log D}{\log y}\big) = \frac{2e^{\gamma}}{\frac{3}{2} - 21\frac{\log\log N}{\log N}} = \frac{4e^{\gamma}}{3} + O\left(\frac{\log\log N}{\log N}\right) = \frac{4e^{\gamma}}{3} + O(\varepsilon)$$

Next, by Theorem 4.3

$$\frac{V(y)}{V(z)} = \frac{\frac{3e^{-\gamma}\mathfrak{S}(N)}{\log N}}{\frac{ke^{-\gamma}\mathfrak{S}(N)}{\log N}}\left(1+O\left(\frac{1}{\log N}\right)\right)\left(1+O\left(\frac{1}{\log N}\right)\right) = \frac{3}{k}\left(1+O(\varepsilon)\right) = \frac{3}{k} + O(\varepsilon)$$

whence

$$\begin{aligned} S(B^j,\mathcal{P},y) &< \left(\frac{4e^{\gamma}}{3}+O(\varepsilon)\right)|B^j|\left(\frac{3}{k}+O(\varepsilon)\right)V(z) + O\left(\frac{N}{\log^4 N}\right) \\ &= \left(\frac{4e^{\gamma}}{k}+O(\varepsilon)\right)|B^j|V(z) + O\left(\frac{N}{\log^4 N}\right) \end{aligned}$$

Recall that the amount of sets B^j is $O\big(\frac{\log N}{\varepsilon}\big)$. Thus

$$\begin{aligned} S(B,\mathcal{P},y) \le \sum_j S(B^j,\mathcal{P},y) &< \left(\frac{4e^{\gamma}}{k}+O(\varepsilon)\right)\sum_j |B^j|V(z) + \sum_j O\left(\frac{N}{\log^4 N}\right) \\ &= \left(\frac{4e^{\gamma}}{k}+O(\varepsilon)\right)|B'|V(z) + O\left(\frac{N}{\varepsilon\log^3 N}\right) \end{aligned}$$

Finally, $|B'|$ is to be estimated. From the definition of B' it follows that

$$B' \subseteq \{N - p_1p_2p_3 \,:\, z \le p_1 < y \le p_2 \le p_3,\ p_1p_2p_3 < (1+\varepsilon)N\}$$

since, given $N - p_1p_2p_3 \in B^j$, for any j

$$p_1p_2p_3 < (1+\varepsilon)x_jp_2p_3 < (1+\varepsilon)N$$

Then

$$|B'| \le \sum_{\substack{z\le p_1<y\le p_2\le p_3\\ p_1p_2p_3<(1+\varepsilon)N}} 1$$

Let $p_1 < y \le p_2 \le p_3$ such that $p_1p_2p_3 < (1+\varepsilon)N$. Then, $p_1p_2^2 < (1+\varepsilon)N$ and

$$p_3 < \frac{(1+\varepsilon)N}{p_1p_2}$$

which implies $\pi\big(\frac{(1+\varepsilon)N}{p_1p_2}\big) \ge \pi(p_3) \ge 1$. By the Prime Number Theorem

$$\pi\left(\frac{(1+\varepsilon)N}{p_1p_2}\right) = \frac{(1+\varepsilon)N}{p_1p_2\log\frac{(1+\varepsilon)N}{p_1p_2}}\left(1+O\left(\frac{1}{\log\frac{(1+\varepsilon)N}{p_1p_2}}\right)\right) < \frac{(1+\varepsilon)N}{p_1p_2\log\frac{N}{p_1p_2}}\left(1+O\left(\frac{1}{\log N}\right)\right)$$

where the error term was bounded as follows

$$\frac{1}{\log\frac{(1+\varepsilon)N}{p_1p_2}} < \frac{1}{\log\frac{N}{p_1p_2}} < \frac{1}{\log N^{1-\frac{2}{3}}} = \frac{1}{\frac{1}{3}\log N}$$

since $p_1p_2 < \frac{N}{p_3} \leq \frac{N}{y} = N^{\frac{2}{3}}$. There exists $N(\varepsilon) > 0$ such that the error term $1+O\big(\frac{1}{\log N}\big) < 1+\varepsilon$, for $N \geq N(\varepsilon)$, in which case

$$(1+\varepsilon)\left(1+O\left(\frac{1}{\log N}\right)\right) < (1+\varepsilon)^2 = 1+2\varepsilon+\varepsilon^2 < 1+3\varepsilon$$

Thus

$$\pi\left(\frac{(1+\varepsilon)N}{p_1p_2}\right) < \frac{(1+3\varepsilon)N}{p_1p_2\log\frac{N}{p_1p_2}}$$

for N big enough. Therefore

$$\begin{aligned}|B'| &\leq \sum_{\substack{z\leq p_1<y\leq p_2\leq p_3\\ p_1p_2p_3<(1+\varepsilon)N}} 1 \leq \sum_{\substack{z\leq p_1<y\leq p_2\\ p_1p_2^2<(1+\varepsilon)N}} 1 \leq \sum_{\substack{z\leq p_1<y\leq p_2\\ p_1p_2^2<(1+\varepsilon)N}} \pi\left(\frac{(1+\varepsilon)N}{p_1p_2}\right)\\ &< (1+3\varepsilon)N \sum_{\substack{z\leq p_1<y\leq p_2\\ p_1p_2^2<(1+\varepsilon)N}} \frac{1}{p_1p_2\log\frac{N}{p_1p_2}} = (1+3\varepsilon)N \sum_{z\leq p_1<y}\frac{1}{p_1}\sum_{y\leq p_2<w}\frac{1}{p_2\log\frac{N}{p_1p_2}}\end{aligned}$$

where $w = ((1+\varepsilon)Np_1^{-1})^{\frac{1}{2}}$ for convenience purposes only. In a similar way as in the the bound of $\sum_{z\leq q<y} S(A_q, \mathcal{P}, z)$, consider the continuous, positive and increasing function

$$f(x) = \frac{1}{\log\frac{N}{p_1x}}$$

defined for $0 < x < \frac{N}{p_1}$. Then, by twice integrating by parts and using Lemma A.3 in the form

$$\sum_{p<x}\frac{1}{p} = \log\log x + a + O\left(\frac{1}{\log x}\right)$$

for some constant $a > 0$

$$\begin{aligned}\sum_{y\leq p_2<w}\frac{1}{p_2\log\frac{N}{p_1p_2}} &= \sum_{y\leq p_2<w}\frac{f(p_2)}{p_2} = \int_y^w f(x)\,d\left(\sum_{p<x}\frac{1}{p}\right)\\ &= f(w)\sum_{p<w}\frac{1}{p} - f(y)\sum_{p<y}\frac{1}{p} - \int_y^w \sum_{p<x}\frac{1}{p}\,df(x)\\ &= f(w)(\log\log w + a) - f(y)(\log\log y + a) - \int_y^w (\log\log x + a)\,df(x) +\\ &\qquad + O\left(\frac{f(w)}{\log w}\right) + O\left(\frac{f(y)}{\log y}\right) + \int_y^w O\left(\frac{1}{\log x}\right)df(x)\\ &= \int_y^w f(x)\,d(\log\log x + a) + O\left(\frac{f(w)}{\log w}\right) + O\left(\frac{f(y)}{\log y}\right) + O\left(\int_y^w \frac{df(x)}{\log x}\right)\end{aligned}$$

First

$$O\left(\frac{f(w)}{\log w}\right) + O\left(\frac{f(y)}{\log y}\right) = O\left(\frac{f(w)}{\log y}\right) = O\left(\frac{1}{\log^2 N}\right)$$

since f is increasing and

$$\frac{f(w)}{\log y}=\frac{1}{\log y\log\frac{N}{p_1w}}=\frac{1}{\log y\frac{1}{2}\log\frac{N}{(1+\varepsilon)p_1}}\ll\frac{1}{\log y\log\frac{N}{y}}=\frac{1}{\frac{1}{3}\log N\frac{2}{3}\log N}\ll\frac{1}{\log^2 N}$$

Second

$$\begin{aligned}\int_y^w\frac{df(x)}{\log x}&=\int_y^w\frac{dx}{x\log x\log^2\frac{N}{p_1x}}\le\int_y^w\frac{dx}{x\log y\log^2\frac{N}{p_1w}}=\frac{1}{\frac{1}{3}\log N(\frac{1}{2}\log\frac{N}{(1+\varepsilon)p_1})^2}\int_y^w\frac{dx}{x}\\&=\frac{12(\log w-\log y)}{\log N\log^2\frac{N}{(1+\varepsilon)p_1}}\le\frac{12(\frac{1}{2}\log N-\frac{1}{3}\log N)}{\log N\log^2\frac{N}{(1+\varepsilon)p_1}}\ll\frac{\log N}{\log N\log^2\frac{N}{y}}=\frac{1}{(\frac{2}{3}\log N)^2}\\&=O\left(\frac{1}{\log^2 N}\right)\end{aligned}$$

Third

$$\int_y^w f(x)\,d(\log\log x+a)=\int_y^{(\frac{N}{p_1})^{\frac{1}{2}}}f(x)\,d\log\log x+\int_{(\frac{N}{p_1})^{\frac{1}{2}}}^w f(x)\,d\log\log x$$

where, using the change of variables $x=(\frac{N}{p_1})^{\frac{1}{2}}u$

$$\begin{aligned}\int_{(\frac{N}{p_1})^{\frac{1}{2}}}^w f(x)\,d\log\log x&=\int_{(\frac{N}{p_1})^{\frac{1}{2}}}^w\frac{dx}{x\log x\log\frac{N}{p_1x}}=\int_1^{\sqrt{1+\varepsilon}}\frac{\sqrt{\frac{N}{p_1}}du}{\sqrt{\frac{N}{p_1}}u\log\left(\sqrt{\frac{N}{p_1}}u\right)\log\frac{N}{p_1\sqrt{\frac{N}{p_1}}u}}\\&=\int_1^{\sqrt{1+\varepsilon}}\frac{du}{u\left(\frac{1}{2}\log\frac{N}{p_1}+\log u\right)\left(\frac{1}{2}\log\frac{N}{p_1}-\log u\right)}\\&=\int_1^{\sqrt{1+\varepsilon}}\frac{du}{u\left(\frac{1}{4}\log^2\frac{N}{p_1}-\log^2 u\right)}\ll\frac{1}{\log^2 N}\int_1^{\sqrt{1+\varepsilon}}\frac{du}{u}\\&=\frac{\frac{1}{2}\log(1+\varepsilon)}{\log^2 N}<\frac{\frac{1}{2}\log 2}{\log^2 N}\ll\frac{1}{\log^2 N}\end{aligned}$$

since

$$\left(\frac{1}{4}\log^2\frac{N}{p_1}-\log^2 u\right)>\left(\frac{1}{4}\log^2\frac{N}{y}-\log^2\sqrt{1+\varepsilon}\right)=\left(\frac{1}{4}\left(\frac{2}{3}\log N\right)^2-\log^2 2\right)\gg\log^2 N$$

Whence

$$\sum_{y\le p_2<w}\frac{1}{p_2\log\frac{N}{p_1p_2}}=\int_y^{(\frac{N}{p_1})^{\frac{1}{2}}}f(x)\,d\log\log x+O\left(\frac{1}{\log^2 N}\right)$$

Therefore

$$\begin{aligned}|B'|&<(1+3\varepsilon)N\sum_{z\le p_1<y}\int_y^{(\frac{N}{p_1})^{\frac{1}{2}}}\frac{f(x)\,d\log\log x}{p_1}+O\left(\frac{(1+3\varepsilon)N}{\log^2 N}\right)\sum_{z\le p_1<y}\frac{1}{p_1}\\&=(1+3\varepsilon)N\sum_{z\le p_1<y}\int_y^{(\frac{N}{p_1})^{\frac{1}{2}}}\frac{d\log\log x}{p_1\log\frac{N}{p_1x}}+O\left(\frac{N}{\log^2 N}\right)\end{aligned}$$

since, by Lemma A.3

$$\sum_{z\le p_1<y}\frac{1}{p_1}=\log(\tfrac{1}{3}\log N)-\log(\tfrac{1}{k}\log N)+O(1)=\log\tfrac{k}{3}+O(1)=O(1)$$

Finally, consider the function

$$g(t)=\int_y^{(\frac{N}{t})^{\frac12}}\frac{d\log\log x}{\log\frac{N}{tx}}$$

defined for $z\le t\le y$. Then, once again, by twice integrating by parts and Lemma A.3

$$\begin{aligned}\sum_{z\le p_1<y}\int_y^{(\frac{N}{p_1})^{\frac12}}\frac{d\log\log x}{p_1\log\frac{N}{p_1x}}&=\sum_{z\le p_1<y}\frac{g(p_1)}{p_1}=\int_z^y g(t)\,d\left(\sum_{p<t}\frac1p\right)\\&=g(y)\sum_{p<y}\frac1p-g(z)\sum_{p<z}\frac1p-\int_z^y\sum_{p<t}\frac1p\,dg(t)\\&=g(y)(\log\log y+a)-g(z)(\log\log z+a)-\int_z^y(\log\log t+a)\,dg(t)+\\&\qquad+O\left(\frac{g(y)}{\log y}\right)+O\left(\frac{g(z)}{\log z}\right)+\int_z^y O\left(\frac{1}{\log t}\right)dg(t)\\&=\int_z^y g(t)\,d(\log\log t+a)+O\left(\frac{g(y)}{\log y}\right)+O\left(\frac{g(z)}{\log z}\right)+O\left(\int_z^y\frac{dg(t)}{\log t}\right)\end{aligned}$$

First

$$g(y)=\int_y^{(\frac{N}{y})^{\frac12}}\frac{d\log\log x}{\log\frac{N}{yx}}=\int_y^y\frac{d\log\log x}{\log\frac{N}{yx}}=0$$

and, by the change of variable $x=N^u$

$$\begin{aligned}\frac{g(z)}{\log z}&=\frac{1}{\log z}\int_y^{(\frac{N}{z})^{\frac12}}\frac{d\log\log x}{\log\frac{N}{zx}}=\frac{1}{\log z}\int_y^{N^{\frac{k-1}{2k}}}\frac{d\log\log x}{\log\frac{N^{1-\frac1k}}{x}}=\frac{1}{\log z}\int_{\frac13}^{\frac{k-1}{2k}}\frac{du}{u(1-\frac1k-u)\log N}\\&=\frac{1}{\log z\log N}\int_{\frac13}^{\frac{k-1}{2k}}\frac{du}{u(1-\frac1k-u)}\ll\frac{1}{\log z\log N}\ll\frac{1}{\log^2 N}\end{aligned}$$

Second, by the chain rule

$$g'(t)=\frac{1}{\sqrt{\frac{N}{t}}\log\sqrt{\frac{N}{t}}\log\frac{N}{t\sqrt{\frac{N}{t}}}}\,\frac{-\frac{N}{t^2}}{2\sqrt{\frac{N}{t}}}=\frac{-2}{t\log^2\frac{N}{t}}$$

and therefore

$$\begin{aligned}\left|\int_z^y\frac{dg(t)}{\log t}\right|&=\int_z^y\frac{2dt}{t\log t\log^2\frac{N}{t}}\le\int_z^y\frac{2dt}{t\log z\log^2\frac{N}{y}}=\frac{2}{\frac1k\log N(\frac23\log N)^2}\int_z^y\frac{dt}{t}\\&=\frac{9k(\frac13\log N-\frac1k\log N)}{2\log^3 N}\ll\frac{1}{\log^2 N}\end{aligned}$$

Last but not least, by the changes of variables $x = N^u$ and $t = N^w$

$$\begin{aligned}\int_z^y g(t)\, d(\log\log t + a) &= \int_z^y \int_y^{(\frac{N}{t})^{\frac{1}{2}}} \frac{d\log\log x}{\log\frac{N}{tx}}\, d\log\log t \\ &= \int_{\frac{1}{k}}^{\frac{1}{3}} \int_{\frac{1}{3}}^{\frac{1-w}{2}} \frac{du\, dw}{uw(1-w-u)\log N} = \frac{1}{\log N}\int_{\frac{1}{k}}^{\frac{1}{3}} \frac{1}{w}\int_{\frac{1}{3}}^{\frac{1-w}{2}} \frac{du}{u(1-w-u)}dw\end{aligned}$$

where

$$\begin{aligned}\int_{\frac{1}{3}}^{\frac{1-w}{2}} \frac{du}{u(1-w-u)} &= \frac{1}{1-w}\int_{\frac{1}{3}}^{\frac{1-w}{2}} \left(\frac{1}{u} + \frac{1}{1-w-u}\right) du \\ &= \frac{\log\frac{1-w}{2} - \log\frac{1}{3} - \log(1-w-\frac{1-w}{2}) + \log(1-w-\frac{1}{3})}{1-w} \\ &= \frac{\log\frac{1-w}{2} + \log 3 - \log\frac{1-w}{2} + \log(\frac{2}{3}-w)}{1-w} = \frac{\log(2-3w)}{1-w}\end{aligned}$$

whence

$$\int_z^y g(t)\, d(\log\log t + a) = \frac{1}{\log N}\int_{\frac{1}{k}}^{\frac{1}{3}} \frac{\log(2-3w)}{w(1-w)}dw$$

Let

$$I_k = \int_{\frac{1}{k}}^{\frac{1}{3}} \frac{\log(2-3w)}{w(1-w)}dw$$

Then

$$\sum_{z\le p_1<y} \int_y^{(\frac{N}{p_1})^{\frac{1}{2}}} \frac{d\log\log x}{p_1\log\frac{N}{p_1 x}} = \frac{I_k}{\log N} + O\left(\frac{1}{\log^2 N}\right)$$

Therefore

$$\begin{aligned}|B'| &< (1+3\varepsilon)N\frac{I_k}{\log N} + O\left(\frac{N}{\log^2 N}\right) = \left(I_k + O(\varepsilon) + O\left(\frac{1}{\log N}\right)\right)\frac{N}{\log N} \\ &= (I_k + O(\varepsilon))\frac{N}{\log N}\end{aligned}$$

to finally deduce

$$S(B, \mathcal{P}, y) < \left(\frac{4e^\gamma}{k} + O(\varepsilon)\right)(I_k + O(\varepsilon))\frac{N}{\log N}V(z) + O\left(\frac{N}{\varepsilon\log^3 N}\right)$$

Whence

Theorem 4.8. *Let $k > 3$. Then*

$$S(B, \mathcal{P}, y) < \left(\frac{4e^\gamma I_k}{k} + O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\varepsilon\log^3 N}\right)$$

for large enough N.

4.6 Completion of the Proof

Let N be big enough and $6 < k \leq 8$. Recall Theorem 4.4, Theorem 4.6 and Theorem 4.8

$$S(A, \mathcal{P}, z) > \left(\frac{4e^{\gamma}\log\frac{k-2}{2}}{k} + O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\log^3 N}\right)$$

$$\sum_{z\leq q<y} S(A_q, \mathcal{P}, z) < \left(\frac{4e^{\gamma}\log(k-2)}{k} + O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\log^3 N}\right)$$

$$S(B, \mathcal{P}, y) < \left(\frac{4e^{\gamma}I_k}{k} + O(\varepsilon)\right)\frac{N}{\log N}V(z) + O\left(\frac{N}{\varepsilon\log^3 N}\right)$$

Thus, by Theorem 4.2 and Theorem 4.3

$$\begin{aligned}
\mathfrak{R}(N) &> S(A, \mathcal{P}, z) - \frac{1}{2}\sum_{z\leq q<y} S(A_q, \mathcal{P}, z) - \frac{1}{2}S(B, \mathcal{P}, y) - N^{1-\frac{1}{k}} - \frac{1}{2}N^{\frac{1}{3}} \\
&> \left(2\log\tfrac{k-2}{2} - \log(k-2) - I_k + O(\varepsilon)\right)\frac{2e^{\gamma}}{k}\frac{N}{\log N}V(z) + O\left(\frac{N}{\varepsilon\log^3 N}\right) \\
&= \left(\log\tfrac{k-2}{4} - I_k + O(\varepsilon)\right)\mathfrak{S}(N)\frac{2N}{\log^2 N}\left(1 + O\left(\frac{1}{\log N}\right)\right) + O\left(\frac{N}{\varepsilon\log^3 N}\right)
\end{aligned}$$

since

$$O\left(\frac{N}{\log^3 N}\right) - N^{1-\frac{1}{k}} - \frac{1}{2}N^{\frac{1}{3}} = O\left(\frac{N}{\varepsilon\log^3 N}\right)$$

The above bound becomes of any use when

$$\mathfrak{I}(k) = \log\tfrac{k-2}{4} - I_k = \log\tfrac{k-2}{4} - \int_{\frac{1}{k}}^{\frac{1}{3}} \frac{\log(2-3x)}{x(1-x)}dx > 0$$

Set $k = 8$. Then

$$\mathfrak{I}(8) = \log\frac{3}{2} - \int_{\frac{1}{8}}^{\frac{1}{3}} \frac{\log(2-3x)}{x(1-x)}dx = 0.04238... > 0$$

Pick a small enough value of $0 < \varepsilon < \frac{1}{200}$ in a way that

$$\mathfrak{I}(8) + O(\varepsilon) > 0.04$$

For said fixed value of ε

$$O\left(\frac{N}{\varepsilon\log^3 N}\right) = O\left(\frac{N}{\log^3 N}\right) = O\left(\frac{\mathfrak{S}(N)N}{\log^3 N}\right) = \mathfrak{S}(N)\frac{N}{\log^2 N}O\left(\frac{1}{\log N}\right)$$

since $\mathfrak{S}(N) \gg 1$. Therefore

$$\mathfrak{R}(N) > 0.08\ \mathfrak{S}(N)\frac{N}{\log^2 N}\left(1 + O\left(\frac{1}{\log N}\right)\right)$$

Thus, for big enough N

$$\mathfrak{R}(N) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

which completes the proof of Theorem 4.1. □

Nevertheless, $k = 8$ is not the best choice for k. Of course, the statement of Theorem 4.1 cares not about its specific value. However, it has been made clear throughout the proof that the closer $z = N^{\frac{1}{k}}$ is to $y = N^{\frac{1}{3}}$, the more information it is given about the range where the prime p and the prime factors of $N - p$ lie.

This now turns out to be a problem of finding a zero of $\mathfrak{I}(k)$ as a function of k. Its derivative is positive whenever $6 < k \leq 8$, meaning $\mathfrak{I}(k)$ is increasing with k. Moreover

$$\mathfrak{I}(7) = -0.06761... < 0$$

This is the reason why $k = 8$ is finally used to conclude Theorem 4.1, since it is the only possible integer value of k. The ideal value for k lies between 7.585 and 7.586. Take

$$k = 7.586$$

Then

$$\mathfrak{I}(7.586) = 1.0126...\cdot 10^{-4} > 0$$

and

$$N^{\frac{1}{7.586}} = N^{0.1318...}$$

Thus, the complete and unabbreviated statement of Theorem 4.1 ought to be:

Let N be an even large enough natural number and $\mathfrak{R}(N)$ denote the number of representations of N as $N = p + (N - p)$, where $p < N$ is a prime not dividing N and

(*i*) $N - p = 1$, or

(*ii*) $N - p$ is a prime greater or equal than $N^{0.1319}$, or

(*iii*) $N - p$ is the product of exactly two primes, both greater or equal than $N^{\frac{1}{3}}$, or

(*iv*) $N - p$ is the product of exactly two primes, one of them greater or equal than $N^{0.1319}$ and smaller than $N^{\frac{1}{3}}$, and the other greater or equal than $N^{\frac{1}{3}}$

Then

$$\mathfrak{R}(N) > 2.025\cdot 10^{-4}\ \mathfrak{S}(N)\frac{N}{\log^2 N}\left(1 + O\left(\frac{1}{\log N}\right)\right)$$

In particular

$$\mathfrak{R}(N) \gg \mathfrak{S}(N)\frac{N}{\log^2 N}$$

Appendices

A Arithmetic Functions

Lemma A.1 (Abel's Summation Formula)**.** *Let $\{a_n\}_{n\geq 1}$ be a sequence of real numbers, $A(x) = \sum_{n\leq x} a_n$, and f a function with continuous derivative on $[1,\infty)$. Then*

$$\sum_{n\leq x} a_n f(n) = A(x)f(x) - \int_1^x A(u)f'(u)\,du$$

for any $x \geq 1$.

Proof. Let $x \geq 1$ and set $k = [x]$ and $a_0 = 0$. Then

$$\begin{aligned}
\sum_{n\leq x} a_n(f(x) - f(n)) &= \sum_{n\leq k}(A(n) - A(n-1))(f(x) - f(n)) \\
&= \sum_{n\leq k} A(n)(f(x) - f(n)) - \sum_{n\leq k-1} A(n)(f(x) - f(n+1)) \\
&= \sum_{n\leq k-1} A(n)(f(n+1) - f(n)) + A(k)(f(x) - f(k)) \\
&= \sum_{n\leq k-1} A(n)\int_n^{n+1} f'(u)\,du + A(k)\int_k^x f'(u)\,du \\
&= \sum_{n\leq k-1}\int_n^{n+1} A(u)f'(u)\,du + \int_k^x A(u)f'(u)\,du = \int_1^x A(u)f'(u)\,du
\end{aligned}$$

□

Lemma A.2. *Let $d(n) = \sum_{d|n} 1$ be the divisor function. Then*

$$\sum_{n\leq x} \frac{d(n)}{n} \gg \log^2 x$$

Proof. Let

$$A(x) = \sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{d|n} 1 = \sum_{d\leq x}\sum_{\substack{n\leq x \\ d|n}} 1 = \sum_{d\leq x}\left[\frac{x}{d}\right] = x\sum_{d\leq x}\frac{1}{d} + O(x)$$

where

$$\sum_{d\leq x}\frac{1}{d} = 1 + \sum_{2\leq d\leq x}\frac{1}{d} < 1 + \int_1^x \frac{du}{u} = 1 + \log x$$

which implies

$$\sum_{d\leq x}\frac{1}{d} = \log x + O(1)$$

Then

$$A(x) = x\log x + O(x)$$

By Lemma A.1 with $a_n = d(n)$ and $f(x) = \frac{1}{x}$

$$\sum_{n\leq x} \frac{d(n)}{n} = \frac{A(x)}{x} + \int_1^x \frac{A(u)}{u^2}\,du = \log x + O(1) + \int_1^x \frac{\log u}{u}\,du + O\left(\int_1^x \frac{du}{u}\right)$$
$$= \log x + O(1) + \frac{\log^2 x}{2} + O(\log x) \gg \log^2 x$$

□

Lemma A.3. *Let $x \geq 1$. Then*

$$\sum_{p<x} \frac{1}{p} = \log\log x + O(1)$$

In fact

$$\sum_{p<x} \frac{1}{p} = \log\log x + a + O\left(\frac{1}{\log x}\right)$$

for some constant $a > 0$.

Proof. Let $\pi(x)$ be the prime counting function. By the Prime Number Theorem

$$\pi(x) = \frac{x}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right)$$

Then

$$\sum_{p<x} \frac{1}{p} = \sum_{n<x} \frac{\pi(n) - \pi(n-1)}{n} = \sum_{n<x} \frac{\pi(n)}{n} - \sum_{n<x-1} \frac{\pi(n)}{n+1}$$
$$= \sum_{2<n<x-1} \left(\frac{\pi(n)}{n} - \frac{\pi(n)}{n+1}\right) + O(1) = \sum_{2<n<x-1} \frac{\pi(n)}{n(n+1)} + O(1)$$
$$= \sum_{2<n<x-1} \frac{\pi(n)}{n^2} + O(1) = \sum_{2<n<x-1} \frac{1}{n\log n}\left(1 + \frac{1}{\log n}\right) + O(1)$$
$$= \sum_{2<n<x-1} \frac{1}{n\log n} + O(1) = \log\log x + O(1)$$

since

$$\sum_{2<n<x-1} \frac{1}{n\log^2 n} < \int_2^\infty \frac{du}{u\log^2 u} = \frac{1}{\log 2}$$

and

$$\sum_{2<n<x-1} \frac{1}{n\log n} < \int_2^x \frac{du}{u\log u} = \log\log x - \log\log 2$$

□

Lemma A.4. *Let $\omega(n) = \sum_{p|n} 1$ be the prime divisor function. Then*

$$\omega(n) \leq 2\log n$$

for all $n \in \mathbb{N}$.

Proof. Assume there exists n with $\omega(n) > 2\log n$. Then

$$n \geq \prod_{p|n} p \geq \prod_{p|n} 2 = 2^{\omega(n)} > 2^{2\log n} = e^{2\log n \log 2} > e^{\log n} = n$$

which is a contradiction. Thus, no such n can exist. □

Lemma A.5. *Let f be a multiplicative function. Then*

$$f([m,n])f((m,n)) = f(m)f(n)$$

for every $m, n \in \mathbb{N}$.

Proof. Let $p_1, \ldots, p_r$ be the primes dividing m or n. Then, write $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $n = \prod_{i=1}^{r} p_i^{\beta_i}$, where α_i, β_i are nonnegative integers. Then

$$[m,n] = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$$

and

$$(m,n) = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$$

If $\max(\alpha_i, \beta_i) = \alpha_i$, then $\min(\alpha_i, \beta_i) = \beta_i$, and vice versa. Therefore

$$\begin{aligned} f([m,n])f((m,n)) &= \prod_{i=1}^{r} f\left(p_i^{\max(\alpha_i,\beta_i)}\right) \prod_{i=1}^{r} f\left(p_i^{\min(\alpha_i,\beta_i)}\right) = \prod_{i=1}^{r} f(p_i^{\alpha_i}) \prod_{i=1}^{r} f(p_i^{\beta_i}) \\ &= f(m)f(n) \end{aligned}$$

□

For brevity's sake, the following result will not be proved. For a detailed proof see pages 165-166 of [5] and pages 65-67 of [1], for instance.

Theorem A.6 (Mertens' formula)**.** *Let $x \geq 2$. Then*

$$\prod_{p<x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right)$$

In particular

$$\prod_{p<x} \left(1 - \frac{1}{p}\right) = O\left(\frac{1}{\log x}\right)$$

And

$$\prod_{p<x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x \left(1 + O\left(\frac{1}{\log x}\right)\right) = e^{\gamma} \log x + O(1)$$

Lemma A.7. *Let $x \geq 2$ and $\varepsilon > 0$. Then, there exists $n_1(\varepsilon)$ such that*

$$\prod_{u \leq p < x} \left(1 - \frac{1}{p}\right)^{-1} < (1+\varepsilon)\frac{\log x}{\log u}$$

for every $n_1(\varepsilon) \leq u < x$.

Proof. Let $s = \frac{e^\gamma \varepsilon}{2+\varepsilon}$. Then

$$\frac{e^\gamma + s}{e^\gamma - s} = \frac{(2+\varepsilon)e^\gamma + e^\gamma\varepsilon}{(2+\varepsilon)e^\gamma - e^\gamma\varepsilon} = \frac{2+2\varepsilon}{2} = 1+\varepsilon$$

By Mertens' formula (Theorem A.6), there exists $n_1(s) = n_1(\varepsilon)$ such that

$$(e^\gamma - s)\log x < \prod_{p<x}\left(1-\frac{1}{p}\right)^{-1} < (e^\gamma + s)\log x$$

for all $x \geq n_1(\varepsilon)$. Let $x > u \geq n_1(\varepsilon)$. Then

$$\prod_{u\leq p<x}\left(1-\frac{1}{p}\right)^{-1} = \frac{\prod_{p<x}\left(1-\frac{1}{p}\right)^{-1}}{\prod_{p<u}\left(1-\frac{1}{p}\right)^{-1}} < \frac{(e^\gamma+s)\log x}{(e^\gamma - s)\log u} = (1+\varepsilon)\frac{\log x}{\log u}$$

□

B The Möbius and Euler's Totient Functions

The Möbius function, defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^{\omega(d)} & \text{if } d > 1 \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$$

is a multiplicative function with many interesting and useful properties is number theory.

Theorem B.1. *Let f be a multiplicative function with $f(1) = 1$. Then*

$$\sum_{d|n}\mu(d)f(d) = \prod_{p|n}(1-f(p))$$

for every $n \in \mathbb{N}$. In particular

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{otherwise} \end{cases}$$

Proof. The result trivially holds for $n = 1$. Assume $n > 1$. Let $n = p_1^{n_1}\dots p_r^{n_r}$, where $p_1, \dots, p_r$ are distinct primes, $n_i > 0$ and $r = \omega(n) > 0$. Let $N = p_1 \dots p_r$. Then

$$\begin{aligned}\sum_{d|n}\mu(d)f(d) &= \sum_{d|N}\mu(d)f(d) = f(1) - \sum_{p_i} f(p_i) + \sum_{p_i<p_j} f(p_ip_j) - \sum_{p_i<p_j<p_k} f(p_ip_jp_k) + \dots \\ &= 1 - \sum_{p_i} f(p_i) + \sum_{p_i<p_j} f(p_i)f(p_j) - \sum_{p_i<p_j<p_k} f(p_i)f(p_j)f(p_k) + \dots = \prod_{p|n}(1-f(p))\end{aligned}$$

In the particular case that f is identically 1, then $\sum_{d|n}\mu(d) = 0$ for $n > 1$, and clearly $\sum_{d|1}\mu(d) = \mu(1) = 1$. □

The Dirichlet convolution of two arithmetic functions f and g is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{d|n} f\left(\frac{n}{d}\right)g(d)$$

Therefore $f * g = g * f$. Moreover, the Dirichlet convolution is associative, meaning $f*(g*h) = (f*g)*h$, for all arithmetic functions f, g and h, and preserves multiplicativity, that is, $f * g$ is multiplicative if both f and g are multiplicative. Let

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then, for every arithmetic function f

$$(f * \delta)(n) = \sum_{d|n} f(d)\delta\left(\frac{n}{d}\right) = f(n)$$

Finally, let $1(n) = 1$. Then, Theorem B.1 can be stated as follows

$$\mu * 1 = \delta$$

Theorem B.2 (Möbius inversion)**.** *Let $\mathcal{D}$ be a divisor-closed set of natural numbers and f and g two arithmetic functions defined on $\mathcal{D}$. Then*

$$f(n) = (g * \mu)(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right)$$

if and only if

$$g(n) = (f * 1)(n) = \sum_{d|n} f(d)$$

Proof. Assume first $f = g * \mu$. Then

$$f * 1 = (g * \mu) * 1 = g * (\mu * 1) = g * \delta = g$$

Assume now that $g = f * 1$. Then

$$g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * \delta = f$$

□

Theorem B.3 (Dual Möbius inversion)**.** *Let $\mathcal{D}$ be a divisor-closed set of natural numbers and f an arithmetic function defined on $\mathcal{D}$. Let*

$$g(n) = \sum_{\substack{d \in \mathcal{D} \\ n|d}} f(d)$$

for all $n \in \mathcal{D}$. Then

$$f(n) = \sum_{\substack{d \in \mathcal{D} \\ n|d}} \mu\left(\frac{d}{n}\right)g(d)$$

Proof. Let $n \in \mathcal{D}$. Then

$$\begin{aligned}\sum_{\substack{d\in\mathcal{D}\\ n|d}}\mu\left(\frac{d}{n}\right)g(d) &= \sum_{\substack{d\in\mathcal{D}\\ n|d}}\mu\left(\frac{d}{n}\right)\sum_{\substack{m\in\mathcal{D}\\ d|m}}f(m) = \sum_{nr\in\mathcal{D}}\mu(r)\sum_{\substack{m\in\mathcal{D}\\ nr|m}}f(m)\\ &= \sum_{nr\in\mathcal{D}}\mu(r)\sum_{nrs\in\mathcal{D}}f(nrs) = \sum_{na\in\mathcal{D}}f(na)\sum_{\substack{r\in\mathcal{D}\\ r|a}}\mu(r) = \sum_{na\in\mathcal{D}}f(na)\sum_{r|a}\mu(r) = f(n)\end{aligned}$$

by Theorem B.1. □

Euler's totient function is a multiplicative function defined by

$$\varphi(n) = \sum_{\substack{d\le n\\ (d,n)=1}} 1 = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

and hence $\varphi(p) = p(1-\frac{1}{p}) = p-1$. Moreover

Lemma B.4. *Let $x > 1$. Then*

$$\sum_{n<x}\frac{1}{\varphi(n)} \ll \log x$$

Proof. Given any $r \in \mathbb{N}$, let

$$R = \prod_{p|r} p$$

Then

$$\begin{aligned}\sum_{n<x}\frac{1}{\varphi(n)} &= \sum_{n<x}\frac{1}{n}\prod_{p|n}\frac{1}{1-\frac{1}{p}} = \sum_{n<x}\frac{1}{n}\sum_{\substack{r\ge1\\ R|n}}\frac{1}{r} = \sum_{r\ge1}\frac{1}{r}\sum_{\substack{n<x\\ R|n}}\frac{1}{n} = \sum_{r\ge1}\frac{1}{r}\sum_{h<\frac{x}{R}}\frac{1}{hR}\\ &= \sum_{r\ge1}\frac{1}{rR}\sum_{h<\frac{x}{R}}\frac{1}{h} \ll \log x\sum_{r\ge1}\frac{1}{rR}\end{aligned}$$

since

$$\sum_{h<\frac{x}{R}}\frac{1}{h} < 1 + \sum_{2\le h<x}\frac{1}{h} < 1 + \int_1^x\frac{du}{u} = 1+\log x \ll \log x$$

Finally

$$\begin{aligned}\sum_{r\ge1}\frac{1}{rR} &= \sum_{\substack{m\ge1\\ p^2|m,\forall p|m}}\frac{1}{m} = \prod_p\left(1+\frac{1}{p^2}+\frac{1}{p^3}+\dots\right) = \prod_p\left(1+\frac{1}{p^2}\left(1+\frac{1}{p}+\dots\right)\right)\\ &= \prod_p\left(1+\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}\right) = \prod_p\left(1+\frac{1}{p(p-1)}\right) < +\infty\end{aligned}$$

□

C Dirichlet Characters

A Dirichlet character modulo $d \in \mathbb{N}$ is a completely multiplicative function $\chi : \mathbb{N} \longrightarrow \mathbb{C}$ such that $\chi(n+d) = \chi(n)$, for all $n \in \mathbb{N}$ and it is supported on coprimes of d only, meaning $\chi(n) \neq 0$ if and only if $(n, d) = 1$.

This implies that $\chi(1) = 1$, since $\chi(1) = \chi(1)\chi(1) = \chi(1)^2$ and $\chi(1) \neq 0$ because $(1, d) = 1$. Moreover, $\chi(n_1) = \chi(n_2)$, for every $n_1 \equiv n_2 \pmod d$. In particular, given n such that $(n, d) = 1$

$$\chi(n)^{\varphi(d)} = \chi(n^{\varphi(d)}) = \chi(1) = 1$$

since $n^{\varphi(d)} \equiv 1 \pmod d$ by Euler's Theorem. Hence, $\chi(n)$ is either a $\varphi(d)$-th root of unity when $(n, d) = 1$, or 0 otherwise. In particular, $|\chi(n)| = 1$, for every $(n, d) = 1$.

The principal character modulo d is denoted by χ_0 and defined by

$$\chi_0 = \begin{cases} 1 & \text{if } (n, d) = 1 \\ 0 & \text{otherwise} \end{cases}$$

The total number of different characters modulo d is $\varphi(d)$, since χ are completely determined by the value at a single n such that $(n, d) = 1$ (for which there are $\varphi(d)$ possible values), because of complete multiplicativity.

Lemma C.1.

$$\sum_{\chi \bmod d} \chi(n) = \begin{cases} \varphi(d) & \textit{if } n \equiv 1 \pmod d \\ 0 & \textit{otherwise} \end{cases}$$

Proof. Let m be such that $(m, d) = 1$. Then

$$\sum_{\chi \bmod d} \chi(n) = \sum_{\chi \bmod d} \chi(nm) = \chi(m) \sum_{\chi \bmod d} \chi(n)$$

Assume $\sum_{\chi \bmod d} \chi(n) \neq 0$. Then, $\chi(m) = 1$, for all $(m, d) = 1$, which implies $\chi = \chi_0$, and in this case $\sum_{\chi \bmod d} \chi(n) = \sum_{\chi \bmod d} 1 = \varphi(d)$. □

Let n be such that $(n, d) = 1$. Then $\chi(n) = e^{\frac{\pi i r}{\varphi(d)}}$, for some r, since $\chi(n)$ is some $\varphi(d)$-th root of unity. Then

$$\bar{\chi}(n) = \overline{\chi(n)} = e^{-\frac{\pi i r}{\varphi(d)}} = \chi(n)^{-1} = \chi(n^{-1})$$

where $\chi(n^{-1})$ is to be understood as $\chi(a)$, where $n^{-1} \equiv a \pmod d$.

Dirichlet characters modulo d are not defined to be d-periodic, but rather that the value at any n and $n + d$ coincide. A Dirichlet characters modulo d is said to be primitive when it is in fact d-periodic, restricted to coprimality with d. Otherwise, the character is said to be imprimitive, meaning it has period strictly less than d.

Define the Gauss sum associated to a Dirichlet character χ modulo d by

$$\tau(\chi) = \sum_{h \leq d} \chi(h) e^{2\pi i \frac{h}{d}}$$

Lemma C.2. *Let χ be a primitive Dirichlet charatcer modulo d. Then*

$$\chi(n) = \frac{1}{\tau(\bar{\chi})} \sum_{h \leq d} \bar{\chi}(h) e^{2\pi i n \frac{h}{d}}$$

for all $n \in \mathbb{N}$.

Proof. Assume first $(n,d)=1$. Then

$$\chi(n)\tau(\bar{\chi}) = \sum_{h\leq d} \chi(n)\bar{\chi}(h)e^{2\pi i\frac{h}{d}} = \sum_{h\leq d} \bar{\chi}(n^{-1}h)e^{2\pi i\frac{h}{d}}$$

Let $a \equiv n^{-1}h \pmod d$. Then $\chi(n^{-1}h) = \chi(a)$ and $e^{2\pi i\frac{h}{d}} = e^{2\pi in\frac{a}{d}}$. Therefore

$$\chi(n)\tau(\bar{\chi}) = \sum_{a\leq d} \bar{\chi}(a)e^{2\pi in\frac{a}{d}}$$

where the condition χ primitive is left unused.
Assume now $(n,d)>1$ and χ primitive. Then $\chi(n)=0$. It is therefore needed to be proved that

$$\sum_{h\leq d} \bar{\chi}(h)e^{2\pi in\frac{h}{d}} = 0$$

Write the fraction $\frac{n}{d}$ as an irreducible fraction $\frac{n_0}{d_0}$. Then, $(n_0,d_0)=1$ and d_0 divides d. Moreover $d_0<d$, since $(n,d)>1$. If $d_0=1$, then n is a multiple of d and the result trivially holds since both $\chi(n)$ and $e^{2\pi in\frac{h}{d}}$ are zero. Assume then $d_0>1$. Let $d'=\frac{d}{d_0}$ and write $h=sd_0+r$, where $0\leq s<d'$ and $1\leq r\leq d_0$. Then, if h runs from 1 to d, then s and r range from $0\leq s<d'$ and $1\leq r\leq d_0$, respectively. Hence

$$\begin{aligned}\sum_{h\leq d} \bar{\chi}(h)e^{2\pi in\frac{h}{d}} &= \sum_{h\leq d} \bar{\chi}(h)e^{2\pi in_0\frac{h}{d_0}} = \sum_{s=0}^{d'-1}\sum_{r=1}^{d_0} \bar{\chi}(sd_0+r)e^{2\pi in_0 s}e^{2\pi in_0\frac{r}{d_0}} \\ &= \sum_{r=1}^{d_0} e^{2\pi in_0\frac{r}{d_0}} \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r)\end{aligned}$$

It is therefore enough to prove that the inner sum, say $f(r)$, is zero. That is

$$f(r) = \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r) = 0$$

for every $1\leq r\leq d_0$. Note that

$$\begin{aligned}f(r+d_0) &= \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r+d_0) = \sum_{s=0}^{d'-1} \bar{\chi}((s+1)d_0+r) = \sum_{s=1}^{d'} \bar{\chi}(sd_0+r) \\ &= \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r) = f(r)\end{aligned}$$

since $\chi(d'd_0+r) = \chi(d+r) = \chi(r)$. However, χ is primitive. Thus, χ is d-periodic. In particular, χ is not d_0-periodic. Hence, there exist m_1 and m_2 such that $(m_1,d) = (m_2,d) = 1$ and $m_1 \equiv m_2 \pmod{d_0}$, such that $\chi(m_1)\neq\chi(m_2)$; since otherwise, χ would be d_0-periodic. Let $m \equiv m_1m_2^{-1} \equiv 1 \pmod{d_0}$. In particular $(m,d)=1$ and $m=1+kd_0$. Then

$$\bar{\chi}(m)f(r) = \sum_{s=0}^{d'-1} \bar{\chi}(smd_0+rm) = \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r+(sd_0+r)kd_0) = \sum_{s=0}^{d'-1} \bar{\chi}(sd_0+r) = f(r)$$

whence $f(r) = 0$, since $\bar{\chi}(m) \neq 1$.

□

Lemma C.3. *Let χ be a primitive Dirichlet charatcer modulo d. Then*

$$|\tau(\chi)|^2 = d$$

Proof. If χ is primitive, then so is $\bar{\chi}$. By Lemma C.2

$$\chi(n)\tau(\chi) = \sum_{h \leq d} \chi(h) e^{2\pi i n \frac{h}{d}}$$

for all $n \in \mathbb{N}$. Hence

$$\begin{aligned}
|\tau(\chi)|^2 \varphi(d) &= |\tau(\chi)|^2 \sum_{\substack{1 \leq n \leq d \\ (n,d)=1}} 1 = |\tau(\chi)|^2 \sum_{n \leq d} |\chi(n)|^2 = \sum_{n \leq d} |\chi(n)|^2 |\tau(\chi)|^2 \\
&= \sum_{n \leq d} \sum_{h_1 \leq d} \sum_{h_2 \leq d} \chi(h_1)\bar{\chi}(h_2) e^{2\pi i n \frac{h_1}{d}} e^{-2\pi i n \frac{h_2}{d}} = \sum_{h_1 \leq d} \sum_{h_2 \leq d} \chi(h_1)\bar{\chi}(h_2) \sum_{n \leq d} e^{2\pi i n \frac{h_1 - h_2}{d}} \\
&= \sum_{h_1 \leq d} \chi(h_1)\bar{\chi}(h_1) \sum_{n \leq d} 1 = d \sum_{h \leq d} |\chi(h)|^2 = d \sum_{\substack{1 \leq h \leq d \\ (h,d)=1}} 1 = d\varphi(d)
\end{aligned}$$

□

References

[1] Cojocaru, A.C. and Murty, M.R., *An Introduction to Sieve Methods and their Applications*. London Mathematical Society 66. Cambridge University Press, 2006.

[2] Davenport H., *Multiplicative Number Theory*. Graduate Texts in Mathematics 74, second edition. Springer-Verlag, 1980.

[3] Halberstam H. and Richert H.E., *Sieve Methods*. London Mathematical Society. Academic Press, 1974.

[4] Hooley C., *Applications of sieve methods to the theory of numbers*. Cambridge Tracts in Mathematics 70. Cambridge University Press, 1976.

[5] Nathanson M. B., *Additive Number Theory. The Classical Bases*. Graduate Texts in Mathematics 164. Springer-Verlag, 1996.