Chapter I.4

Sieve methods

4.1. The sieve of Eratosthenes

The inclusion–exclusion principle or the Möbius inversion formula can in theory be used to calculate $\pi(x)$. For sufficiently large x, let us write

$$P = \prod_{p \leqslant \sqrt{x}} p\,;$$

then an integer n, $\sqrt{x} < n \leqslant x$, is a prime number if, and only if, $(n, P) = 1$. Thus we may write

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{n \leqslant x} \delta((n, P)) = \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor . \tag{4.1}$$

At this stage, if we content ourselves with estimating $\lfloor x/d \rfloor$ using $x/d + O(1)$, we obtain

$$\pi(x) - \pi(\sqrt{x}) + 1 = x \prod_{p \leqslant \sqrt{x}} \Big(1 - \frac{1}{p}\Big) + O\Big(2^{\pi(\sqrt{x})}\Big).$$

By Mertens' formula, the main term in this estimate equals

$$\{2\mathrm{e}^{-\gamma} + o(1)\} x / \ln x,$$

but Chebyshev's estimates show that the error term is larger than any power of x.

This calls for two comments. On the one hand, the exact formula (4.1)—called the sieve formula of Eratosthenes—involves far too many terms for any reasonable practical validity. On the other hand, the estimate for the main term shows *a posteriori*, taking into account the prime number theorem, that the "error terms" created by replacing $\lfloor x/d \rfloor$ by x/d contribute globally

at the same order as the "main terms". This suggests that, even suitably adapted, this method will never allow us to prove the prime number theorem. However, we shall see that it can provide Chebyshev-type estimates in a very general context.

In order to obtain a non-trivial result starting from formula (4.1), it is necessary to introduce a parameter y, $1 \leqslant y \leqslant x$, and to bound $\pi(x)-\pi(y)+1$ from above by the number of integers n not exceeding x and having no prime factor $\leqslant y$. With the same calculations, we obtain

$$\pi(x) \leqslant x \prod_{p \leqslant y} \Big(1 - \frac{1}{p}\Big) + O(2^y) = x \frac{\mathrm{e}^{-\gamma} + o(1)}{\ln y} + O(2^y) \leqslant \{\mathrm{e}^{-\gamma} + o(1)\} \frac{x}{\ln_2 x}$$

for the essentially optimal choice $y = \ln x$.

It was with the aim of improving the efficiency of this method that the Norwegian mathematician Viggo Brun invented the theory of the combinatorial sieve between 1917 and 1924.

4.2. Brun's combinatorial sieve

The sieve of Eratosthenes is based on the identity

$$\mu * \mathbf{1} = \delta.$$

Brun's idea consists in introducing two auxiliary functions μ_1, μ_2, satisfying

$$\mu_1 * \mathbf{1} \leqslant \delta \leqslant \mu_2 * \mathbf{1}, \tag{4.2}$$

and vanishing sufficiently often so that the number of terms in the resulting formula analogous to (4.1) is not prohibitive.

Brun's initial choice, leading to what is customarily referred to in the literature as *Brun's pure sieve*, is the following.

Theorem 4.1 (Brun)**.** *Denote by χ_t the characteristic function of the set of integers n such that $\omega(n) \leqslant t$. Then, for any integer $h \geqslant 0$, the functions defined by*

$$\mu_i(n) := \mu(n)\chi_{2h+2-i}(n) \qquad (i = 1, 2) \tag{4.3}$$

satisfy the inequalities (4.2)*.*

Proof. Since $\mu_i * \mathbf{1}(n)$ only depends on the squarefree kernel of n, it is enough to consider the case when $\mu(n)^2 = 1$. If $\omega(n) = k$, then, for each r, $0 \leqslant r \leqslant k$, it is clear that n has exactly $\binom{k}{r}$ divisors d such that $\omega(d) = r$. We can thus write, for any given $t \geqslant 0$,

$$\mu\chi_t * \mathbf{1}(n) = \sum_{d|n,\, \omega(d) \leqslant t} \mu(d) = \sum_{r \leqslant t} (-1)^r \binom{k}{r} = (-1)^t \binom{k-1}{t},$$

where the last equality is easily obtained by induction on t. □

Corollary 4.2. *Let $\mathcal{A}$ be a finite set of integers, and $\mathcal{P}$ be a set of prime numbers. Write*

$$A_d := \operatorname{card}\{a \in \mathcal{A} : a \equiv 0 \,(\mathrm{mod}\, d)\},$$
$$P(y) := \prod_{p \in \mathcal{P},\, p \leqslant y} p,$$
$$S(\mathcal{A}, \mathcal{P}; y) := \operatorname{card}\{a \in \mathcal{A} : (a, P(y)) = 1\}.$$

Then, for each integer $h \geqslant 0$, we have

$$\sum_{d \mid P(y),\, \omega(d) \leqslant 2h+1} \mu(d) A_d \leqslant S(\mathcal{A}, \mathcal{P}; y) \leqslant \sum_{d \mid P(y),\, \omega(d) \leqslant 2h} \mu(d) A_d. \tag{4.4}$$

Let us see how this result allows us to improve considerably the upper bound for $\pi(x)$ provided by the sieve of Eratosthenes.

We select, in the above corollary, $\mathcal{A} = \{n : n \leqslant x\}$ and $\mathcal{P} = \mathbb{P}$, the set of all prime numbers. Whence

$$\begin{aligned} \pi(x) &\leqslant \sum_{\substack{d \mid P(y) \\ \omega(d) \leqslant 2h}} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor + y = x \sum_{\substack{d \mid P(y) \\ \omega(d) \leqslant 2h}} \frac{\mu(d)}{d} + O\Big(y + \sum_{\substack{d \mid P(y) \\ \omega(d) \leqslant 2h}} 1 \Big) \\ &= x \prod_{p \leqslant y} \Big(1 - \frac{1}{p}\Big) + O\Big(y + \sum_{\substack{d \mid P(y) \\ \omega(d) \leqslant 2h}} 1 + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{1}{d} \Big). \end{aligned} \tag{4.5}$$

The second of the three error terms does not exceed y^{2h} since this is an upper bound for all integers d such that $d \mid P(y)$, $\omega(d) \leqslant 2h$. The d-sum arising in the third remainder term is bounded from above, for each value of the parameter $u \geqslant 1$, by

$$\sum_{d \mid P(y)} \frac{u^{\omega(d)-2h}}{d} = u^{-2h} \prod_{p \leqslant y} \Big(1 + \frac{u}{p}\Big) \leqslant \exp\Big\{ -2h \ln u + u \sum_{p \leqslant y} \frac{1}{p} \Big\}.$$

For the optimal choice $u = 2h \Big/ \sum_{p \leqslant y} p^{-1}$, we obtain that this quantity is

$$\ll_u (\ln y)^{-v}$$

where $v = u \ln u - u$: this follows from Theorem 1.10. When $u > 5$, we have $v > 3$. It is easy to see that, for y large enough, there is some $u = u(y)$, $5 < u < 6$, such that

$$h := \tfrac{1}{2} u \sum_{p \leqslant y} \frac{1}{p}$$

is an integer. With these choices of the parameters, we have, for sufficiently large x,

$$y^{2h} \leqslant y^{6 \ln_2 y + O(1)} < x^{2/3}$$

whenever

$$y \leqslant x^{1/(10\ln_2 x)} =: Y(x). \tag{4.6}$$

Collecting all previous estimates, and selecting $y = Y(x)$, we obtain

$$\pi(x) \ll \frac{x \ln_2 x}{\ln x}.$$

Even though inferior to Chebyshev's, this result is remarkable because of the great generality of the argument. The corresponding lower bound for $S(\mathcal{A}, \mathcal{P}; y)$ can be established in the same way. This quantity actually is of intrinsic arithmetic interest: it is equal to the number of integers not exceeding x all of whose prime factors are larger than y. We can thus formulate the following result. Recall that, for each integer $n \geqslant 1$, we denote by $P^-(n)$ the smallest prime factor of n, with the convention $P^-(1) = +\infty$, and we define

$$\Phi(x, y) := \operatorname{card}\{n \leqslant x : P^-(n) > y\}. \tag{4.7}$$

Theorem 4.3. *Under condition* (4.6), *we have*

$$\Phi(x, y) = x \prod_{p \leqslant y} \Big(1 - \frac{1}{p}\Big) \Big\{1 + O\Big(\frac{1}{(\ln y)^2}\Big)\Big\}. \tag{4.8}$$

The choice of the functions μ_1, μ_2 defined by (4.3) is certainly not optimal. At the cost of technical complications, the method can be refined by introducing a partition of $]1, y]$ into subintervals $]y_j, y_{j+1}]$, $0 \leqslant j \leqslant k$, and selecting for $i = 1, 2$,

$$\mu_i(d) = \mu(d)\chi_i^*(d)$$

where χ_i^* is the characteristic function of the set of those integers d having at most $2h_j + 2 - i$ distinct prime factors in $\mathcal{P} \cap]y_j, y]$ for each j, $0 \leqslant j \leqslant k$—see Exercise 86. There are thus two families of parameters to optimize, the y_j and the h_j.

It would take too long to develop here the full theory of the combinatorial sieve, which is still evolving at the present moment. The interested reader will find a pedagogical exposition of the subject in the book by Halberstam & Richert, *Sieve Methods* (1974)—see also the Notes for this chapter.

We confine ourselves to quoting the basic result of the theory, which was obtained with the choice of the $\mu_i(d)$ indicated above. It is this very theorem which is intended when "Brun's method" is invoked in the literature without further qualification.

Theorem 4.4 (Fundamental lemma of the combinatorial sieve)**.** *With the notation of Corollary* 4.2*, assume there exists a multiplicative function* $w \geqslant 0$*, a real number* X*, and positive constants* κ, A*, such that*

$$\text{(a)} \quad A_d =: Xw(d)/d + R_d \qquad (d \mid P(y))$$

$$\text{(b)} \quad \prod_{\eta \leqslant p \leqslant \xi} \Big(1 - \frac{w(p)}{p}\Big)^{-1} < \Big(\frac{\ln \xi}{\ln \eta}\Big)^{\kappa} \Big(1 + \frac{A}{\ln \eta}\Big) \qquad (2 \leqslant \eta \leqslant \xi).$$

Then, uniformly in $\mathcal{A}$*,* X*,* y *and* $u \geqslant 1$*, we have*

(4.9)
$$S(\mathcal{A}, \mathcal{P}; y) = X \prod_{p \leqslant y,\, p \in \mathcal{P}} \Big(1 - \frac{w(p)}{p}\Big)\big\{1 + O\big(u^{-u/2}\big)\big\} + O\Big(\sum_{d \leqslant y^u,\, d \mid P(y)} |R_d|\Big).$$

From this result a Chebyshev-type upper bound for $\pi(x)$ may easily deduced, as well as an evaluation of the order of magnitude of $\Phi(x, y)$ for $y \leqslant x^{\delta}$, where δ is some fixed positive real number. We leave the details to the reader.

The best sieve results currently obtained by combinatorial techniques are due to Iwaniec (1980a,b).

4.3. Application to twin primes

Here we illustrate the results of the previous paragraph with Brun's theorem on twin primes.

It is obvious that the difference between two consecutive odd primes must be at least 2. When it is exactly 2, we say that these primes are *twins*, such as $\{3, 5\}, \{5, 7\}, \{11, 13\}, \{17, 19\}, \{29, 31\}$, etc. A famous conjecture asserts the existence of infinitely many twin primes.

Let us write

$$\mathcal{J} := \{p : p + 2 \text{ is prime}\} \qquad \text{and} \qquad J(x) := \big|\mathcal{J} \cap [1, x]\big|.$$

On the basis of an analytic approach, and in agreement with a heuristic probabilistic calculation, Hardy & Littlewood (1922) conjectured that

$$J(x) \sim 2 \prod_{p > 2} \Big(1 - \frac{1}{(p-1)^2}\Big) \frac{x}{(\ln x)^2} \quad (x \to \infty). \tag{4.10}$$

By Brun's pure method, we establish the following result.

Theorem 4.5 (Brun)**.** *As* x *tends to infinity, we have*

$$J(x) \ll x \Big(\frac{\ln_2 x}{\ln x}\Big)^2. \tag{4.11}$$

Corollary 4.6. *We have*

$$\sum_{p\in\mathcal{J}} \frac{1}{p} < \infty. \tag{4.12}$$

Proof. Apply Corollary 4.2 with

$$\mathcal{A} = \{m(m+2) : m \leqslant x\},$$

choosing for $\mathcal{P}$ the set of all prime numbers. For all y, $1 \leqslant y \leqslant x$, we have

$$J(x) \leqslant S(\mathcal{A}, \mathcal{P}; y) + y \leqslant \sum_{d|P(y),\, \omega(d)\leqslant 2h} \mu(d) A_d + y, \tag{4.13}$$

where A_d is the number of integral solutions $m \leqslant x$ to the congruence

$$m(m+2) \equiv 0 \,(\mathrm{mod}\, d). \tag{4.14}$$

This relation is equivalent to

$$m \equiv 0 \,(\mathrm{mod}\, 2^\nu), \quad m \equiv 0 \text{ or } -2 \,\big(\mathrm{mod}\, p\big) \quad (p|d,\, p \neq 2), \tag{4.15}$$

where ν is 1 or 0 according to whether d is even or odd. By the Chinese remainder theorem, there are thus $\varrho(d)$ solutions modulo d, where ϱ is the strongly multiplicative function defined by

$$\varrho(2) = 1, \quad \varrho(p) = 2 \qquad (p \geqslant 3). \tag{4.16}$$

Each interval of length d contains $\varrho(d)$ integers m counted in A_d. Therefore we can write

$$A_d = x\frac{\varrho(d)}{d} + O(\varrho(d)) \qquad (\mu(d)^2 = 1). \tag{4.17}$$

Inserting this back into (4.13) and performing a calculation parallel to (4.5), it follows that

$$J(x) \leqslant x \sum_{d|P(y)} \frac{\mu(d)\varrho(d)}{d} + O\Bigg(y + \sum_{\substack{d|P(y)\\ \omega(d)\leqslant 2h}} \varrho(d) + x \sum_{\substack{d|P(y)\\ \omega(d)>2h}} \frac{\varrho(d)}{d}\Bigg). \tag{4.18}$$

The main term equals

$$\tfrac{1}{2}x \prod_{2<p\leqslant y} \Big(1 - \frac{2}{p}\Big) \leqslant 2x \prod_{p\leqslant y} \Big(1 - \frac{1}{p}\Big)^2 \sim 2\mathrm{e}^{-2\gamma} x (\ln y)^{-2}.$$

Selecting, as in the application described in § 4.2, $h = c\ln_2 y + O(1)$ for a suitable constant c, and

$$\ln y \sim c' \ln x / \ln_2 x$$

with c' sufficiently small, we check that the error term is of smaller order than $x/(\ln y)^2$. This implies (4.11) and thereby completes the proof of the theorem. The corollary follows at once by Abel summation. □

4.4. The large sieve—analytic form

The large sieve is one of the most powerful tools in analytic number theory. Invented by Linnik in 1941, it has been systematically developed since then, as much from the point of view of its fundamental principle as for its arithmetic applications.

The reader will find complete expositions and an exhaustive bibliography in Bombieri's monograph (1974) and Montgomery's survey (1978a). We will be content here with indicating that the crucial steps in the development of the current theory of the large sieve are due to Rényi (1950), Roth (1965) and Bombieri (1965). The optimal version was obtained by Montgomery & Vaughan (1973, 1974).

It was Davenport & Halberstam (1966) who were the first to isolate the analytic foundations of the large sieve. Let $\{a_n\}_{n=0}^{\infty}$ be a sequence of complex numbers, and for given arbitrary integers $M, N \geqslant 0$, let

$$S(\alpha) := \sum_{M<n\leqslant M+N} a_n \mathrm{e}(\alpha n) \tag{4.19}$$

be a trigonometric polynomial, where we have written $\mathrm{e}(u) := \exp\{2\pi i u\}$ $(u \in \mathbb{R})$. The analytic form of the large sieve is an inequality of the type

$$\sum_{1\leqslant i\leqslant R} |S(\alpha_i)|^2 \leqslant \Delta(N,\delta) \sum_{M<n\leqslant M+N} |a_n|^2 \tag{4.20}$$

which holds for all R-tuples $\{\alpha_1, \dots, \alpha_R\}$ of real numbers which are δ-*well spaced* in the sense that

$$\min_{1\leqslant i<j\leqslant R} \|\alpha_j - \alpha_i\| \geqslant \delta > 0, \tag{4.21}$$

where $\|u\|$ denotes the distance from the real number u to the set of integers. The aim of this section is to prove the following optimal result.

Theorem 4.7 (Montgomery & Vaughan; Selberg)**.** *Under the above conditions, the large sieve inequality* (4.20) *holds with the choice*

$$\Delta(N,\delta) = N + \delta^{-1} - 1. \tag{4.22}$$

The proof we give here, due to Selberg, is presented in the article of Montgomery (1978a). The value of $\Delta(N,\delta)$ obtained by Montgomery & Vaughan in 1974 was only slightly weaker: $\Delta = N + 1/\delta$. Selberg's improvement is unimportant for applications—where an upper bound of the type $\Delta \ll N + 1/\delta$ is usually sufficient—and it is mainly the nature of the argument which motivated our choice.

Let us observe, meanwhile, that the value given in equation (4.22) is attained for certain values of α_i, N and δ. Indeed, for each integer $R \geqslant 1$,

set $\alpha_j = j/R$ $(1 \leqslant j \leqslant R)$, so that $\delta = 1/R$, and let us consider for $N \equiv 1 \,(\mathrm{mod}\, R)$ the case $a_n := \mathbf{1}_{\mathbb{N}}(n/R)$ $(0 \leqslant n < N)$. Then we have

$$\sum_{1\leqslant j\leqslant R} |S(\alpha_j)|^2 = \sum_{1\leqslant j\leqslant R} \Big| \sum_{\substack{0\leqslant n\leqslant N-1\\ n\equiv 0\,(\mathrm{mod}\, R)}} 1\Big|^2 = R\Big(\frac{N-1}{R}+1\Big)^2$$
$$= (N-1+R)\Big(1+\frac{N-1}{R}\Big) = \Big(N-1+\frac{1}{\delta}\Big)\sum_{0\leqslant n<N}|a_n|^2.$$

The proof of Theorem 4.7 rests on a general duality principle asserting the equality of the norms of a Banach space operator and its adjoint. We only use this in the case of endomorphisms of $\ell^2(\mathbb{C})$. The duality principle then takes the following simple form.

Lemma 4.8. *Let (c_{nr}) be an $N \times R$ matrix with complex coefficients. The three following assertions concerning the real number D are equivalent:*

$$\text{(i)} \quad \sum_r \Big|\sum_n c_{nr}x_n\Big|^2 \leqslant D\sum_n |x_n|^2 \qquad (\forall x_n \in \mathbb{C}),$$

$$\text{(ii)} \quad \Big|\sum_{n,r} c_{nr}y_r x_n\Big|^2 \leqslant D\sum_n |x_n|^2 \sum_r |y_r|^2 \qquad (\forall x_n, y_r \in \mathbb{C}),$$

$$\text{(iii)} \quad \sum_n \Big|\sum_r c_{nr}y_r\Big|^2 \leqslant D\sum_r |y_r|^2 \qquad (\forall y_r \in \mathbb{C}).$$

Proof. Let us show the equivalence of (i) and (ii). That of (ii) and (iii) follows from this by interchanging the roles of the indices r and n.

(i) $\Rightarrow$ (ii). We have

$$\Big|\sum_{n,r} c_{nr}y_r x_n\Big|^2 = \Big|\sum_r y_r \sum_n c_{nr}x_n\Big|^2$$
$$\leqslant \sum_r |y_r|^2 \sum_r \Big|\sum_n c_{nr}x_n\Big|^2 \leqslant D\sum_n |x_n|^2 \sum_r |y_r|^2$$

where the first upper bound comes from the Cauchy–Schwarz inequality.

(ii) $\Rightarrow$ (i). For each r, define $L_r := \sum_n c_{nr}x_n$ and apply (ii) with $y_r = \overline{L_r}$. We get

$$\Big(\sum_r |L_r|^2\Big)^2 \leqslant D\sum_n |x_n|^2 \sum_r |L_r|^2,$$

that is we have (i). □

In the sequel, we will systematically use notation (4.19). The following statement results immediately from Lemma 4.8.

Lemma 4.9. *Let α_r $(1 \leqslant r \leqslant R)$ be fixed real numbers. The two following assertions, concerning the sequence of real numbers $b_n \geqslant 0$ $(n \in \mathbb{Z})$ such that $b_n > 0$ $(M < n \leqslant M+N)$ and the positive real number B, are equivalent:*

$$\text{(i)} \quad \sum_{1\leqslant r\leqslant R} |S(\alpha_r)|^2 \leqslant B \sum_{M<n\leqslant M+N} |a_n|^2/b_n \qquad (\forall a_n \in \mathbb{C})$$

$$\text{(ii)} \quad \sum_{M<n\leqslant M+N} b_n \Big| \sum_{1\leqslant r\leqslant R} y_r\, \mathrm{e}(n\alpha_r)\Big|^2 \leqslant B \sum_{1\leqslant r\leqslant R} |y_r|^2 \qquad (\forall y_r \in \mathbb{C}).$$

Proof. We use Lemma 4.8 with $c_{nr} = \mathrm{e}(n\alpha_r)\sqrt{b_n}$. Up to replacing a_n by $a_n\sqrt{b_n}$, assertion (i) is equivalent to

$$\sum_{1\leqslant r\leqslant R} \Big| \sum_{M<n\leqslant M+N} a_n\sqrt{b_n}\,\mathrm{e}(\alpha_r n)\Big|^2 \leqslant B \sum_{M<n\leqslant M+N} |a_n|^2 \quad (\forall a_n \in \mathbb{C}).$$

Using the equivalence of (i) and (iii) in Lemma 4.8, we obtain that the above condition can also be written

$$\sum_{M<n\leqslant M+N} \Big| \sum_{1\leqslant r\leqslant R} y_r \mathrm{e}(n\alpha_r)\sqrt{b_n}\Big|^2 \leqslant B \sum_{1\leqslant r\leqslant R} |y_r|^2 \quad (\forall y_r \in \mathbb{C}),$$

which is the required inequality. □

Corollary 4.10. *Let $B(\alpha) := \sum_{n\in\mathbb{Z}} b_n\,\mathrm{e}(n\alpha)$ be a convergent Fourier series such that $b_n \geqslant 0$ $(n \in \mathbb{Z}), b_n > 0$ $(M < n \leqslant M+N)$. Then, for any positive real number B, the inequality*

$$\text{(i)} \quad \sum_{1\leqslant r\leqslant R} |S(\alpha_r)|^2 \leqslant B \sum_{M<n\leqslant M+N} |a_n|^2/b_n \qquad (\forall a_n \in \mathbb{C})$$

is satisfied provided that

$$\text{(ii)} \quad \sum_{1\leqslant r,s\leqslant R} y_r\overline{y_s}\, B(\alpha_r - \alpha_s) \leqslant B \sum_{1\leqslant r\leqslant R} |y_r|^2 \qquad (\forall y_r \in \mathbb{C}).$$

Proof. Expanding $B(\alpha_r - \alpha_s)$ as a series and interchanging summations, we see that (ii) is equivalent to the second inequality of Lemma 4.9 in which the sum over n is extended to $\mathbb{Z}$. Since $b_n \geqslant 0$ for all n, the conclusion is immediate. □

An obvious way to construct functions satisfying the conditions of Corollary 4.10 consists in insisting that

(a) $b_n \geqslant 0$ $(n \in \mathbb{Z})$, $\quad b_n \geqslant 1$ $(M < n \leqslant M+N)$,

(b) $B(\alpha) = 0$ $\quad (\|\alpha\| \geqslant \delta)$,

where δ is defined by (4.21). It is convenient to suppose here that $0 < \delta < \frac{1}{2}$, the case $\delta = \frac{1}{2}$ (which is possible only if $R = 2$) then following by a straightforward limit procedure. When (a) and (b) are realized,

assertion (i) of Corollary 4.10 implies that the large sieve inequality (4.20) holds with

$$\Delta(N,\delta) = B(0). \tag{4.23}$$

The remainder of this section is devoted to making explicit a suitable choice for the sequence $\{b_n\}_{n\in\mathbb{Z}}$ of Fourier coefficients of $B(\alpha)$.

It is natural to try and write b_n as the value at n of a function $b \in L^1(\mathbb{R})$ whose Fourier transform

$$\widehat{b}(\vartheta) := \int_{-\infty}^{+\infty} b(t)\mathrm{e}(-\vartheta t)\,\mathrm{d}t$$

has a support contained in $[-\delta,\delta]$. The Poisson summation formula

$$B(\alpha) := \sum_{n\in\mathbb{Z}} b(n)\mathrm{e}(\alpha n) = \sum_{k\in\mathbb{Z}} \widehat{b}(k-\alpha) \tag{4.24}$$

then guarantees the validity of condition (b).

To verify that the summation formula (4.24) is effectively applicable in this context, we first observe that $\widehat{b} \in L^1(\mathbb{R})$, from which we deduce (cf., for example, Katznelson (1968), p. 126) the integral representation

$$b(t) = \int_{-\delta}^{\delta} \widehat{b}(\vartheta)\mathrm{e}(\vartheta t)\,\mathrm{d}\vartheta. \tag{4.25}$$

In particular, $b(n)$ is the Fourier coefficient of the periodic continuous function $\beta(\alpha) := \sum_{k\in\mathbb{Z}} \widehat{b}(k-\alpha)$. Now, for $N \geqslant 1$, $|\alpha| \leqslant \frac{1}{2}$, we have by (4.25),

$$\begin{aligned}\sum_{|n|\leqslant N} b(n)\mathrm{e}(\alpha n) - \int_{-N-\frac{1}{2}}^{N+\frac{1}{2}} b(t)\mathrm{e}(\alpha t)\,\mathrm{d}t \\ = \int_{-\delta+\alpha}^{\delta+\alpha} \lambda_\alpha(\vartheta)\sin\{(2N+1)\pi\vartheta\}\,\mathrm{d}\vartheta,\end{aligned} \tag{4.26}$$

with

$$\lambda_\alpha(\vartheta) := \widehat{b}(\vartheta-\alpha)\Big\{\frac{1}{\sin(\pi\vartheta)} - \frac{1}{\pi\vartheta}\Big\}.$$

Since $|\pm\delta+\alpha| < 1$ (it is here we use the assumption $\delta < \frac{1}{2}$), we have $\lambda_\alpha \in L^1[-\delta+\alpha,\, \delta+\alpha]$. The Riemann–Lebesgue lemma allows us to conclude that the last ϑ-integral tends to 0 as $N\to\infty$. Since $b \in L^1(\mathbb{R})$, this implies the (symmetric) convergence of the series

$$\sum_{n\in\mathbb{Z}} b(n)\mathrm{e}(\alpha n)$$

to $\widehat{b}(-\alpha) = \beta(\alpha)$. That establishes (4.24) when $|\alpha| \leqslant \frac{1}{2}$, and hence for all α, by periodicity.

We are thus led to investigate an integrable function b such that the quantity

$$B(0) = \widehat{b}(0) = \int_{-\infty}^{+\infty} b(t)\,\mathrm{d}t \tag{4.27}$$

is as small as possible within the constraints

$$\begin{cases} b(t) \geqslant 0 & (t \in \mathbb{R}), \\ b(t) \geqslant 1 & (M+1 \leqslant t \leqslant M+N), \\ \widehat{b}(\vartheta) = 0 & (|\vartheta| \geqslant \delta). \end{cases} \tag{4.28}$$

The Fejér kernel provides an easy way to exhibit an initial possibility. For

$$b(t) := C \sum_{\delta(M+1)\leqslant n\leqslant \delta(M+N)} \left(\frac{\sin\left(\frac{1}{2}\pi(n-\delta t)\right)}{\frac{1}{2}\pi(n-\delta t)} \right)^2$$

we have

$$\widehat{b}(\vartheta) = \frac{2C}{\delta}(1-|\vartheta/\delta|)^+ \sum_{\delta(M+1)\leqslant n\leqslant \delta(M+N)} \mathrm{e}(-n\vartheta/\delta)$$

so that the conditions (4.28) are certainly satisfied with $C = \frac{1}{4}\pi^2$. This gives the inequality

$$\widehat{b}(0) \leqslant \tfrac{1}{2}\pi^2(N - 1 + 1/\delta)$$

which suffices for most applications. Selberg remarked that the following lemma provides an even better choice for $b(t)$.

Lemma 4.11. *Let*

$$F(z) := \Big(\frac{\sin \pi z}{\pi}\Big)^2 \Big\{ \sum_{n\geqslant 0} \frac{1}{(z-n)^2} - \sum_{n\geqslant 1} \frac{1}{(z+n)^2} + \frac{2}{z} \Big\}.$$

Then F defines an entire function of z, such that

$$F(z) \ll \mathrm{e}^{2\pi|\Im m\, z|}, \qquad F(x) \geqslant \operatorname{sgn}(x) \quad (x \in \mathbb{R}), \qquad F(0) = 1,$$

and

$$\int_{-\infty}^{+\infty} \big\{F(x) - \operatorname{sgn}(x)\big\}\,\mathrm{d}x = 1. \tag{4.29}$$

Remark. It plainly follows from (4.29) that $F \notin L^1(\mathbb{R})$. However, we can interpret the upper bound on $F(z)$ as meaning that, in a certain sense, $\widehat{F}(\vartheta) = 0$ for $|\vartheta| \geqslant 1$. Consider for example, for $T > 0$, the function

$F_T(x) := \frac{1}{2}\{F(T+x)+F(T-x)\}$. Then $F_T \in L^1(\mathbb{R})$ for all $T>0$ and, as shown by Vaaler (1985), we have

$$\widehat{F}_T(\vartheta) = \begin{cases} \dfrac{\sin(2\pi T|\vartheta|)}{\pi} + (1-|\vartheta|)\dfrac{\sin\{\pi\vartheta(2T+1)\}}{\sin(\pi\vartheta)} & \text{if } |\vartheta|\leqslant 1,\\ 0 & \text{if } |\vartheta|>1. \end{cases}$$

where the Fourier transform is defined by $\widehat{F}_T(\vartheta) := \int_{\mathbb{R}} F_T(x)\mathrm{e}(\vartheta x)\,\mathrm{d}x$.

Proof. The first two assertions are clear: writing $z=x+iy$, then, assuming for instance that $|y|\geqslant 1$, we have $|z\pm n|^2 \geqslant 1+(|x|-n)^2$ $(n\geqslant 0)$. To establish the third assertion, we first recall Euler's formula

$$\Big(\frac{\sin\pi z}{\pi}\Big)^2 \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2} = 1 \qquad (z\in\mathbb{C})$$

and notice that for $x>0$

$$\sum_{n\geqslant 1}\frac{1}{(x+n)^2} \leqslant \sum_{n\geqslant 1}\int_{x+n-1}^{x+n}\frac{\mathrm{d}u}{u^2} = \frac{1}{x} = \sum_{n\geqslant 0}\int_{x+n}^{x+n+1}\frac{\mathrm{d}u}{u^2} \leqslant \sum_{n\geqslant 0}\frac{1}{(x+n)^2}.$$

This implies, still for $x>0$,

$$F(x) = \Big(\frac{\sin\pi x}{\pi}\Big)^2\Big\{\sum_{n\in\mathbb{Z}}\frac{1}{(x-n)^2} - 2\sum_{n\geqslant 1}\frac{1}{(x+n)^2} + \frac{2}{x}\Big\} \geqslant 1,$$

and for $x<0$, with $y=-x$,

$$F(x) = \Big(\frac{\sin\pi x}{\pi}\Big)^2\Big\{-\sum_{n\in\mathbb{Z}}\frac{1}{(x-n)^2} + 2\sum_{n\geqslant 0}\frac{1}{(y+n)^2} - \frac{2}{y}\Big\} \geqslant -1.$$

Finally

$$F(0) = \lim_{z\to 0}\Big(\frac{\sin\pi z}{\pi z}\Big)^2 = 1 \geqslant 0 = \operatorname{sgn}(0).$$

Let us prove (4.29). We have

$$\begin{aligned}\int_{-\infty}^{+\infty}\big\{F(x)-\operatorname{sgn}(x)\big\}\,\mathrm{d}x &= \int_0^\infty\big\{F(x)-1\big\}\,\mathrm{d}x + \int_0^\infty\big\{F(-y)+1\big\}\,\mathrm{d}y\\ &= \int_0^\infty\big\{F(x)+F(-x)\big\}\,\mathrm{d}x = 2\int_0^\infty\Big(\frac{\sin\pi x}{\pi x}\Big)^2\,\mathrm{d}x = 1.\end{aligned}$$

□

Conclusion of the proof of Theorem 4.7. Define

$$b(t) := \tfrac{1}{2}\big\{F\big(\delta(t-M-1)\big) + F\big(\delta(M+N-t)\big)\big\}. \tag{4.30}$$

Then $b(t)$ satisfies the first of conditions (4.28) and relation (4.29) shows that b is integrable on $\mathbb{R}$, together with

$$\int_{-\infty}^{+\infty} b(t)\,\mathrm{d}t = N-1+\frac{1}{\delta}. \tag{4.31}$$

This results immediately from the identity

$$b(t) = \mathbf{1}_{[M+1,M+N]}(t) + \tfrac{1}{2}\big\{F\big(\delta(t-M-1)\big) - \operatorname{sgn}\big(\delta(t-M-1)\big)\big\} + \tfrac{1}{2}\big\{F\big(\delta(M+N-t)\big) - \operatorname{sgn}\big(\delta(M+N-t)\big)\big\},$$

valid for $t \neq M+1, M+N$. In addition, we then have from Lemma 4.11

$$b(z) \ll \mathrm{e}^{2\pi\delta|\Im m\, z|} \qquad (z \in \mathbb{C}). \tag{4.32}$$

In particular, b is bounded on $\mathbb{R}$. Since $b \in L^1(\mathbb{R})$, we hence also have $b \in L^2(\mathbb{R})$. The estimate (4.32) then implies, by the Paley–Wiener theorem,[1] that

$$\widehat{b}(\vartheta) = 0 \qquad (|\vartheta| \geqslant \delta).$$

This completes the proof of Theorem 4.7. □

4.5. The large sieve—arithmetic form

Let $\{a_n\}_{n=M+1}^{M+N}$ be a finite sequence of complex numbers, and set

$$S(\alpha) := \sum_{M<n\leqslant M+N} a_n \mathrm{e}(n\alpha).$$

Apply Theorem 4.7 to the case where the α_r are all rational numbers of the form $\alpha_r = a/q, (a,q) = 1, q \leqslant Q$. For $r \neq s$, we clearly have

$$\|\alpha_r - \alpha_s\| = \|a/q - a'/q'\| = \|(aq' - a'q)/qq'\| \geqslant 1/Q^2,$$

which shows that the α_r are $1/Q^2$-well spaced. We may thus write

$$\sum_{q\leqslant Q} \sum_{1\leqslant a\leqslant q,\,(a,q)=1} |S(a/q)|^2 \leqslant (N-1+Q^2) \sum_{M<n\leqslant M+N} |a_n|^2. \tag{4.33}$$

The usefulness of this inequality lies in the observation that one may bound the inner sum from below by an explicit function of q related to the numbers, $w(p)$, of classes modulo p, $p|q$, which contain no integer n such that $a_n \neq 0$. More precisely, write, for each prime p,

$$w(p) := \operatorname{card}\{h : 0 \leqslant h < p,\, n \equiv h \,(\mathrm{mod}\, p) \Rightarrow a_n = 0\}, \tag{4.34}$$

and

$$g(q) := \mu(q)^2 \prod_{p|q} \frac{w(p)}{p - w(p)} \tag{4.35}$$

(We may assume that $w(p) < p$ for all p since otherwise $a_n \equiv 0$.) The basis for the arithmetic form of the large sieve is set out in the following result.

[1] See, for example, Katznelson (1968), th. 7.4, p. 176.

Theorem 4.12. *With the previous notation, we have, for all $q \geqslant 1$,*

$$\Big|\sum_{M<n\leqslant M+N} a_n\Big|^2 g(q) \leqslant \sum_{\substack{1\leqslant a\leqslant q\\(a,q)=1}} |S(a/q)|^2. \tag{4.36}$$

Corollary 4.13 (Arithmetic large sieve)**.** *For any finite sequence of complex numbers $\{a_n\}_{M+1}^{M+N}$ and any integer $Q \geqslant 1$, we have*

$$\Big|\sum_{M<n\leqslant M+N} a_n\Big|^2 \leqslant \frac{N-1+Q^2}{L} \sum_{M<n\leqslant M+N} |a_n|^2 \tag{4.37}$$

with

$$L := \sum_{q\leqslant Q} g(q), \tag{4.38}$$

where $g(q)$ is defined by (4.34) *and* (4.35)*.*

Proof of Theorem 4.12. We have to show that, for any sequence $\{a_n\}$, we have

$$|S(0)|^2 g(q) \leqslant \sum_{1\leqslant a\leqslant q,\,(a,q)=1} |S(a/q)|^2. \tag{4.39}$$

Since the definition of the $w(p)$ is unchanged when one replaces a_n by $a_n \mathrm{e}(n\beta)$, relation (4.39) is equivalent to

$$|S(\beta)|^2 g(q) \leqslant \sum_{1\leqslant a\leqslant q,\,(a,q)=1} |S(a/q+\beta)|^2 \quad (\beta\in\mathbb{R}). \tag{4.40}$$

Let us assume (4.40) is satisfied for q and q' with $(q,q')=1$. By the Chinese remainder theorem we may then write

$$\begin{aligned}\sum_{\substack{1\leqslant c\leqslant qq'\\(c,qq')=1}} |S(c/qq')|^2 &= \sum_{\substack{1\leqslant a\leqslant q\\(a,q)=1}} \sum_{\substack{1\leqslant b\leqslant q'\\(b,q')=1}} |S(a/q+b/q')|^2\\ &\geqslant \sum_{1\leqslant a\leqslant q,\,(a,q)=1} |S(a/q)|^2 g(q') \geqslant |S(0)|^2 g(q)g(q').\end{aligned}$$

Since g is multiplicative, it ensues that (4.39) (and consequently (4.40)) holds for qq'. Since $g(q)=0$ when q is not squarefree, we can confine ourselves to establishing (4.39) when q is prime.

For any prime number p, we have

$$|S(0)|^2 + \sum_{1\leqslant a<p} |S(a/p)|^2 = \sum_{0\leqslant a,a'<p} \frac{S(a/p)\overline{S(a'/p)}}{p} \sum_{0\leqslant h<p} \mathrm{e}\big((a-a')h/p\big)$$

$$= \frac{1}{p} \sum_{0\leqslant h<p} \Big| \sum_{0\leqslant a<p} \mathrm{e}\big(-ah/p\big) S(a/p)\Big|^2$$

$$= \frac{1}{p} \sum_{0\leqslant h<p} \Big|\sum_n a_n \sum_{0\leqslant a<p} \mathrm{e}\big(a(n-h)/p\big)\Big|^2 = p \sum_{0\leqslant h<p} |S(p,h)|^2, \text{ say,} \tag{4.41}$$

where we have set

$$S(p,h) := \sum_{\substack{M<n\leqslant M+N\\ n\equiv h \,(\mathrm{mod}\, p)}} a_n.$$

Note that, by assumption, $S(p,h)$ vanishes for at least $w(p)$ values of h modulo p. By the Cauchy–Schwarz inequality, we therefore have

$$|S(0)|^2 = \Big| \sum_{0\leqslant h<p} S(p,h)\Big|^2 \leqslant \{p-w(p)\} \sum_{0\leqslant h<p} |S(p,h)|^2$$

from which it follows by (4.41) that

$$\sum_{1\leqslant a<p} \big|S(a/p)\big|^2 = p \sum_{0\leqslant h<p} |S(p,h)|^2 - |S(0)|^2$$

$$\geqslant \left(\frac{p}{p-w(p)} - 1\right) |S(0)|^2 = g(p)|S(0)|^2.$$

This establishes (4.39) for $q = p$, and thereby completes the proof. □

In view of the identity $S(0) = \sum_{0\leqslant h<p} S(p,h)$, we obtain

$$p \sum_{0\leqslant h<p} \Big|S(p,h) - \frac{1}{p}S(0)\Big|^2 = p \sum_{0\leqslant h<p} |S(p,h)|^2 - |S(0)|^2$$

from which, using (4.41), it follows that

$$p \sum_{0\leqslant h<p} \Big|S(p,h) - \frac{1}{p}S(0)\Big|^2 = \sum_{0\leqslant a<p} |S(a/p)|^2.$$

By (4.33) we hence obtain the following result.

Theorem 4.14. *With the previous notation, we have*

$$\sum_{p\leqslant Q} p \sum_{0\leqslant h<p} \Big|S(p,h) - \frac{1}{p}S(0)\Big|^2 \leqslant (N-1+Q^2) \sum_{M<n\leqslant M+N} |a_n|^2. \tag{4.42}$$

Relation (4.42) is a weakened form of the large sieve inequality (4.33), since only the contribution of the numbers q which are prime is estimated. Nonetheless it is a very useful result in applications—cf., Notes. Moreover, it may be extended to congruence classes for composite moduli. Montgomery (1968) showed that, for any squarefree integer q, we have

$$q \sum_{0 \leqslant h < q} \Big| \sum_{d \mid q} \frac{\mu(d)}{d} S(q/d, h) \Big|^2 = \sum_{\substack{1 \leqslant a \leqslant q \\ (a,q)=1}} \big| S(a/q) \big|^2.$$

Inserting this in (4.33), we thus obtain that $S(q/d, h)$ is, on average over d dividing q and h in $[0, q-1]$, close to $(d/q)S(0)$.

4.6. Applications of the large sieve

By comparison with Brun's method, the large sieve delivers a remarkably effective upper bound on the number $J(x)$ of prime twins not exceeding x.

Theorem 4.15. *As x tends to infinity, we have*

$$J(x) \leqslant \{8C + o(1)\} x/(\ln x)^2 \tag{4.43}$$

with

$$C := 2 \prod_{p \geqslant 3} \Big(1 - \frac{1}{(p-1)^2} \Big). \tag{4.44}$$

This upper bound is thus asymptotically equal to eight times the value conjectured for $J(x)$—cf., the Notes for references to improvements.

Proof. Let $\varepsilon > 0$. We employ (4.37) with $N = \lfloor x \rfloor$, $Q = x^{1/2-\varepsilon}$, $M = 0$, and $a_n := 1$ if $P^-\big(n(n+2)\big) > Q$, $a_n := 0$ otherwise. We get

$$J(x) - J(\sqrt{x}) \leqslant \{1 + o(1)\} x/L \tag{4.45}$$

where L is defined by (4.38) with $w(2) = 1$, $w(p) = 2$ $(p \geqslant 3)$. We have $g(q) = 2^\omega * h(q)/q$ where h is the multiplicative function defined by

$$h(2) = 0, \quad h(2^\nu) = 2(-1)^{\nu-1} \qquad (\nu \geqslant 2)$$

$$h(p) = \frac{4}{p-2} \quad (p > 2), \quad h(p^\nu) = \frac{2(-1)^{\nu-1}(p+2)}{p-2} \qquad (p > 2,\ \nu \geqslant 2).$$

It is easily checked that the series $\sum_{d \geqslant 1} h(d)/d^\sigma$ converges absolutely for $\sigma > \frac{1}{2}$, whence

$$\sum_{q \leqslant y} g(q) = \sum_{md \leqslant y} \frac{h(d)}{d} \frac{2^{\omega(m)}}{m} \sim \frac{3}{\pi^2} (\ln y)^2 \sum_{d \geqslant 1} \frac{h(d)}{d} \qquad (y \to \infty)$$

where the sum over m is evaluated by partial summation starting with the estimate

$$\sum_{m\leqslant y} 2^{\omega(m)} = \sum_{m\leqslant y} \mathbf{1} * \mu^2(m) \sim \frac{6}{\pi^2} y \ln y.$$

We therefore deduce from (4.45) that we have

$$J(x) \leqslant \frac{\{2C + o(1)\}x}{\big(\ln\sqrt{x}\big)^2}$$

with

$$\begin{aligned} C &= \frac{\pi^2}{6}\Big(\sum_{d\geqslant 1}\frac{h(d)}{d}\Big)^{-1} \\ &= \prod_p (1-p^{-2})^{-1}\,\tfrac{3}{2}\prod_{p\geqslant 3}\Big(1+\frac{4}{p(p-2)}-\frac{2(p+2)}{p^2(p-2)(1+p^{-1})}\Big)^{-1} \\ &= 2\prod_{p\geqslant 3}\Big(1-\frac{1}{(p-1)^2}\Big), \end{aligned}$$

whence the desired conclusion. □

Our second application concerns prime numbers in arithmetic progressions. Let us write

$$\pi(x;a,q) := \operatorname{card}\{p\leqslant x : p\equiv a \,(\mathrm{mod}\, q)\}$$

so that $\pi(x;a,q)$ is possibly unbounded only when a takes on one of the $\varphi(q)$ values of invertible residues modulo q. It is then natural to conjecture that, under suitable assumptions on the relative values of q and x, we have

$$\pi(x;a,q) \sim \frac{\pi(x)}{\varphi(q)} \sim \frac{x}{\varphi(q)\ln x}.$$

We shall show this in Part II for fixed q (Dirichlet's theorem), and even for $q\leqslant (\ln x)^c$ (Siegel–Walfisz theorem). The large sieve allows us to obtain an upper bound of the same type, equally valid for "short intervals".

Theorem 4.16 (Brun–Titchmarsh)**.** *Let x, y be positive numbers and q, a be integers. If $y/q\to\infty$, we have*

$$\pi(x+y;a,q)-\pi(x;a,q) \leqslant \frac{\{2+o(1)\}y}{\varphi(q)\ln(y/q)}. \tag{4.46}$$

Proof. The left-hand side of (4.46) is at most equal to

$$\sum_n a_n + \pi\big(\sqrt{y/q}\big), \tag{4.47}$$

where $a_n := 1$ if $x < a+nq \leqslant x+y$ and $P^-(a+qn) > \sqrt{y/q}$, and $a_n := 0$ otherwise. The second term in (4.47) is plainly absorbed by the remainder

term in (4.46). With the notation of the large sieve, we have $N \leqslant y/q + 1$ and $w(p) \geqslant 1$ for any prime number p such that $p \leqslant \sqrt{y/q}$ and $p \nmid q$. We therefore obtain that, for all $Q \leqslant \sqrt{y/q}$,

$$\sum_n a_n \leqslant \frac{y/q + Q^2}{L} \tag{4.48}$$

with

$$L := \sum_{m \leqslant Q,\,(m,q)=1} \mu(m)^2 \prod_{p \mid m} \frac{1}{p-1} = \sum_{m \leqslant Q,\,(m,q)=1} \frac{\mu(m)^2}{\varphi(m)}.$$

Noting that each integer $n \leqslant Q$ factorizes uniquely in the form $n = mdt$ with $(m, q) = 1$, $\mu(m)^2 = 1$, $d \mid m^\infty$, $t \mid q^\infty$, we can write

$$\sum_{n \leqslant Q} \frac{1}{n} \leqslant \sum_{m \leqslant Q,\,(m,q)=1} \frac{\mu(m)^2}{m} \sum_{d \mid m^\infty} \frac{1}{d} \sum_{t \mid q^\infty} \frac{1}{t} = \sum_{m \leqslant Q,\,(m,q)=1} \frac{\mu(m)^2}{m} \frac{m}{\varphi(m)} \frac{q}{\varphi(q)}$$

from which we get

$$L \geqslant \frac{\varphi(q)}{q} \ln Q.$$

Inserting this estimate back into (4.48) and selecting $Q = \sqrt{y/q}/\ln(y/q)$, we obtain the stated result. □

4.7. Selberg's sieve

4.7.1. Introduction. Based on an elegant optimization of quadratic forms, the sieve method introduced by Selberg in 1947 has a triple advantage over Brun's sieve, dating from the 1920s: it is simpler in principle, more versatile in its technical implementation, and it provides better estimates, at least in the situations considered in practice.

When the large sieve was discovered and perfected, Selberg's method was merely used for its ability to sieve any sequence and not just the set of integers in an interval—which leads, in certain cases such as that of twin primes, to better constants. From the mid-1970s on, the general idea was that, in the case of an interval, the two techniques are essentially equivalent—see Huxley (1972b), Kobayashi (1973)—but that the large sieve is based on a more fundamental duality principle. This philosophy, in particular, underpins the beautiful book of Elliott (1997).

Subsequently, from the 1980s on, the Rosser–Iwaniec sieve (see the Notes for a precise statement) was, rightly, considered the most efficient in the theory. Besides introducing a great deal of flexibility in the treatment of remainder terms, it allows, in the more propitious cases, to gain asymptotically a constant factor in the main terms of the upper bounds obtained.

The recent and fundamental advances by Goldston, Pintz & Yıldırım (2006) and then Zhang (2014) and Maynard (2014) on small gaps between primes have brought the Selberg sieve out into full light again.

It would take us too far afield to describe these remarkable works. We have chosen to present the Selberg sieve by looking at one of its lesser known aspects: the possibility of sieving by prime powers. This is based on an extension, interesting for its own sake, of the notion of a multiplicative function in one or many variables.

The reader will find, for example, in the book of Halberstam & Richert (1974) or of Greaves (2001), exhaustive expositions about the classical form of Selberg's method, notably the possibility of lower bounds—which we will not mention further here.

4.7.2. Arithmetic functions of several variables. The classic notion of a multiplicative function presented in Chapter I.2 has several drawbacks. One of them is that the structure is not stable if one modifies a finite number of terms in a finite number of factors in the Euler product representing the associated Dirichlet series. Another is that the generalization to several variables is not obvious.

In an article published in 1977, Selberg proposes a new definition which overcomes these two difficulties.

Definition 4.17. *A arithmetic function of r variables $f : (\mathbb{N}^*)^r \to \mathbb{C}$ is said to be multiplicative (in Selberg's sense) if its formal Dirichlet series*

$$F(s_1, \dots, s_r) := \sum_{n_1 \geqslant 1, \dots, n_r \geqslant 1} \frac{f(n_1, \dots, n_r)}{n_1^{s_1} \cdots n_r^{s_r}}$$

is representable as a product

$$F(s_1, \dots, s_r) = \prod_p F_p\big(p^{-s_1}, \dots, p^{-s_r}\big) \tag{4.49}$$

where the F_p are power series in r variables

$$F_p(X_1, \dots, X_r) := \sum_{\nu_1 \geqslant 0, \dots, \nu_r \geqslant 0} f_p(\nu_1, \dots, \nu_r) X_1^{\nu_1} \cdots X_r^{\nu_r}$$

such that $F_p(0, \dots, 0) = 1$ except for at most a finite number of values of p.

We say that f is singular if $f(1, \dots, 1) = 0$, regular if $f(1, \dots, 1) \neq 0$, and normal if $f(1, \dots, 1) = 1$.

Just for this section, we adopt the convention that the term multiplicative arithmetic function in one or many variables should be understood in Selberg's sense.

Condition (4.49) is equivalent to

$$f(n_1,\dots,n_r)=\prod_p f_p(v_p(n_1),\dots,v_p(n_r)) \tag{4.50}$$

where v_p denotes the p-adic valuation and the f_p are such that $f_p(0,\dots,0)=1$ except for a finite number of values of p.

In the case of a single variable, the class of ordinary multiplicative functions coincides with that of normal multiplicative functions in Selberg's sense. We have thus obtained a generalization of the notion. If, for example, f is multiplicative and normal, then $n\mapsto f(kn)$ is multiplicative for all $k\in\mathbb{N}^*$.

In the sequel we shall restrict ourselves to arithmetic functions of two variables.

4.7.3. Generalized convolution.

Definition 4.18. *An arithmetic function f of two variables is said to be symmetric if it satisfies $f(m,n)=f(n,m)$ identically. It is said to be lower triangular if $f(m,n)=0$ whenever $n>m$; it is said to be normal lower triangular if it is lower triangular and satisfies $f(m,m)=1$ for all $m\in\mathbb{N}^*$.*

If t is a normal lower triangular arithmetic function, then, for each fixed integer $m\geqslant 1$, the linear system[2]

$$\sum_{n\leqslant k\leqslant m} t(k,n)x_k=\delta_{mn}\qquad(1\leqslant n\leqslant m)$$

is upper triangular, and so can be solved by Cramer's rule. We denote by

$$x_k=t^*(m,k)\quad(1\leqslant k\leqslant m)$$

its solution. We hence have

$$\sum_{n\leqslant k\leqslant m} t^*(m,k)t(k,n)=\delta_{mn}\qquad(1\leqslant n\leqslant m). \tag{4.51}$$

This relation means that, for each integer $q\geqslant 1$, the lower triangular matrices $T_q^*:=\big(t^*(j,k)\big)_{1\leqslant k\leqslant j\leqslant q}$ and $T_q:=\big(t(r,s)\big)_{1\leqslant s\leqslant r\leqslant q}$ are one another's inverses. By transposition, we obtain the dual relation

$$\sum_{n\leqslant k\leqslant m} t(m,k)t^*(k,n)=\delta_{mn}\qquad(1\leqslant n\leqslant m). \tag{4.52}$$

We then say that the normal lower triangular arithmetic functions t and t^* are each other's inverses.

We recover the classical Dirichlet convolution inverse (see § 2.4) by putting $t(m,n):=h(m/n)$ (resp. $t^*(m,n):=h^*(m/n)$) where h (resp. h^*)

[2]Here and in the sequel we use Kronecker's notation $\delta_{mn}:=1$ if $m=n$, $\delta_{mn}:=0$ if $m\neq n$.

is a function in one variable, with the convention that the right-hand expression is zero if m/n is not an integer. Then, setting $m = Nn$ and making the change of variables $k = dn$ in (4.52), this formula becomes

$$\sum_{d|N} h^*(d)h(N/d) = \delta_{1N} = \delta(N) \qquad (N \in \mathbb{N}^*).$$

This new framework allows us to state inversion formulae that are more general than those arising from Dirichlet convolution, described in Chapter 1.2.

Proposition 4.19. *Let t be a normal lower triangular arithmetic function of two variables.*

(i) If f and g are arithmetic functions of a single variable connected by the relation

$$f(m) = \sum_{1\leqslant n\leqslant m} t(m,n)g(n) \qquad (m \in \mathbb{N}^*), \tag{4.53}$$

then

$$g(m) = \sum_{1\leqslant n\leqslant m} t^*(m,n)f(n) \qquad (m \in \mathbb{N}^*). \tag{4.54}$$

(ii) If f and g are arithmetic functions of a single variable connected by the relation

$$f(n) = \sum_{m\geqslant n} t(m,n)g(m) \qquad (n \in \mathbb{N}^*), \tag{4.55}$$

where the series is assumed to be absolutely convergent for each n, then we have

$$g(n) = \sum_{m\geqslant n} t^*(m,n)f(m) \qquad (n \in \mathbb{N}^*) \tag{4.56}$$

provided that the series is absolutely convergent for each value of n.

Proof. Relation (4.54) results from (4.53) upon inserting the identity

$$f(n) = \sum_{1\leqslant k\leqslant n} t(n,k)g(k)$$

in the left-hand side and inverting summations. A similar manipulation allows us to deduce (4.56) from (4.55), questions of convergence being taken care of by truncating the series in the right-hand side. We omit the details. □

The case when t is multiplicative is of particular practical interest.

Proposition 4.20. *Let $t : (\mathbb{N}^*)^2 \to \mathbb{C}$ be a normal lower triangular multiplicative function. Then its inverse t^* is also normal lower triangular and multiplicative.*

Proof. The power series $T_p(X,Y) := 1 + \sum_{\substack{0\leqslant\nu\leqslant\mu\\(\mu,\nu)\neq(0,0)}} t(p^\mu,p^\nu)X^\mu Y^\nu$ are formally invertible. We have, for any prime p,

$$\begin{aligned} T_p(X,Y)^{-1} &= \sum_{j\geqslant 0}(-1)^j\Bigg\{\sum_{\substack{0\leqslant\nu\leqslant\mu\\(\mu,\nu)\neq(0,0)}} t(p^\mu,p^\nu)X^\mu Y^\nu\Bigg\}^j \\ &= 1 + \sum_{\substack{0\leqslant\nu\leqslant\mu\\(\mu,\nu)\neq(0,0)}} t^*(p^\mu,p^\nu)X^\mu Y^\nu \end{aligned}$$

with $t^*(1,1) = 1$ and, for $0 \leqslant \nu \leqslant \mu$, $(\mu,\nu) \neq (0,0)$,

$$t^*(p^\mu,p^\nu) = \sum_{1\leqslant j\leqslant\nu}(-1)^j \sum_{\substack{\mu_1+\cdots+\mu_j=\mu\\ \nu_1+\cdots+\nu_j=\nu}} \prod_{1\leqslant s\leqslant j} t\big(p^{\mu_s},p^{\nu_s}\big).$$

The normal lower triangular multiplicative function t^* defined by this formula is the sought after inverse. □

Note that, if t is a normal lower triangular multiplicative function, then $t(m,n)$ vanishes whenever $n \nmid m$. The following result is a very useful special case of Proposition 4.19.

Proposition 4.21. *Let t be a normal lower triangular multiplicative function of two variables.*

(i) *If f and g are arithmetic functions in one variable connected by the relation*

$$f(m) = \sum_{d\mid m} t(m,d)g(d) \qquad (m\in\mathbb{N}^*), \tag{4.57}$$

then

$$g(m) = \sum_{d\mid m} t^*(m,d)f(d) \qquad (m\in\mathbb{N}^*). \tag{4.58}$$

(ii) *If f and g are arithmetic functions in one variable connected by the relation*

$$f(n) = \sum_{m\equiv 0\,(\mathrm{mod}\,n)} t(m,n)g(m) \qquad (n\in\mathbb{N}^*), \tag{4.59}$$

where the series is assumed absolutely convergent for each n, then we have

$$g(n) = \sum_{m\equiv 0\,(\mathrm{mod}\,n)} t^*(m,n)f(m) \qquad (n\in\mathbb{N}^*) \tag{4.60}$$

provided that the series is absolutely convergent for each value of n.

Let $k \geqslant 1$ be a fixed integer. An example of a pair (t, t^*) of normal lower triangular multiplicative functions is provided by setting

$$t(m,n) := \tau((m/n,k))\mathbf{1}_{\mathbb{N}}(m/n) \qquad (m,n \in \mathbb{N}^*).$$

Putting $\kappa_p := v_p(k)$, we then have, for any prime p,

$$\sum_{0\leqslant\nu\leqslant\mu} t_p(\mu,\nu)X^\mu Y^\nu = \frac{1-X^{\kappa_p+1}}{(1-X)^2(1-XY)}.$$

It follows that

$$t_p^*(\mu,\nu) = \begin{cases} 1 & \text{if } \mu=\nu=0,\\ -1 & \text{if } \mu=1,\ \nu\in\{0,1\},\ \kappa_p=0,\\ 1 & \text{if } \mu=2,\ \nu=1,\ \kappa_p=0,\\ 1 & \text{if } \mu\equiv 0 \text{ or } 2 \,(\mathrm{mod}\,\kappa_p+1),\ \nu=0,\ \kappa_p\geqslant 1,\\ -2 & \text{if } \mu\equiv 1 \,(\mathrm{mod}\,\kappa_p+1),\ \nu=0,\ \kappa_p\geqslant 1,\\ -1 & \text{if } \mu\equiv 1 \text{ or } 3 \,(\mathrm{mod}\,\kappa_p+1),\ \nu=1,\ \kappa_p\geqslant 1,\\ 2 & \text{if } \mu\equiv 2 \,(\mathrm{mod}\,\kappa_p+1),\ \nu=1,\ \kappa_p\geqslant 1,\\ 0 & \text{in any other case.}\end{cases}$$

4.7.4. Quadratic forms. We denote by $\ell_0(\mathbb{R})$ the set of ultimately vanishing real sequences.

Definition 4.22. *We say that an arithmetic function $f : (\mathbb{N}^*)^2 \to \mathbb{R}$ is positive definite if it is symmetric and if the quadratic form*

$$Q(\boldsymbol{x}) := \sum_{m\geqslant 1,\, n\geqslant 1} f(m,n)x_m x_n \tag{4.61}$$

is strictly positive for any non-zero real sequence $\boldsymbol{x} = \{x_n\}_{n=1}^\infty$ in $\ell_0(\mathbb{R})$.

It follows immediately that, for any integer $N \geqslant 1$, the matrix

$$F_N := \big(f(m,n)\big)_{1\leqslant m,n\leqslant N}$$

associated to a positive definite arithmetic function f is symmetric, invertible, and that all its eigenvalues are strictly positive. A classical theorem on the decomposition of a square matrix into triangular factors (see, for example, Gantmacher (1959, 1966), § 2.4) then allows us to write $F_N = TD\,{}^tT$ where T is lower triangular with 1's along the principal diagonal, D is diagonal and ${}^tT$ denotes the transpose of T. Moreover, the matrices D and T are unique under the conditions indicated. This furnishes the canonical representation

$$f(m,n) = \sum_{1\leqslant k\leqslant \min(m,n)} g(k)t(m,k)t(n,k) \tag{4.62}$$

where t is normal lower triangular and g has strictly positive real values.

Whenever f is multiplicative, this formula takes a simpler form.

Proposition 4.23. *Let f be a positive definite multiplicative function of two variables. Then there exist two normal lower triangular multiplicative functions $g : \mathbb{N}^* \to \mathbb{R}^{+*}$ and $t : (\mathbb{N}^*)^2 \to \mathbb{R}$, such that*

$$f(m,n) = \sum_{d|(m,n)} g(d)t(m,d)t(n,d) \qquad (m,n \in \mathbb{N}^*). \tag{4.63}$$

Furthermore, the functions g and t are uniquely determined by this condition.

Proof. For each prime p, the arithmetic function f_p defined by $f_p(\mu,\nu) := f(p^\mu, p^\nu)$ is positive definite on $\mathbb{N}^2$. Therefore there exist multiplicative functions g_p and t_p, respectively of one and two variables, so that t_p is normal lower triangular and we have the identity

$$f(p^\mu, p^\nu) = \sum_{0 \leqslant \kappa \leqslant \min(\mu,\nu)} g_p(\kappa)t_p(\mu,\kappa)t_p(\nu,\kappa). \tag{4.64}$$

Taking the product over p and defining g and t according to (4.50), we obtain (4.63). The result then follows from the uniqueness of the representation given by (4.62). □

We are presently in a position to solve the problem of constrained optimization for quadratic forms. We restrict ourselves to stating the result for the case of multiplicative functions. The reader will be able to reconstruct the general case without difficulty.

Theorem 4.24. *Let f be a positive definite multiplicative function in two variables, $N \in \mathbb{N}^*$, and g, t, be the two multiplicative functions defined by the canonical representation* (4.63)*. Then, under the conditions $x_1 = 1$ and $n > N \Rightarrow x_n = 0$, the quadratic form* (4.61) *attains its minimum*

$$Q^* := \Big\{ \sum_{m \leqslant N} t^*(m,1)^2/g(m) \Big\}^{-1} \tag{4.65}$$

for the choice

$$x_n := Q^* \sum_{1 \leqslant m \leqslant N} t^*(m,n)t^*(m,1)/g(m) \qquad (1 \leqslant n \leqslant N). \tag{4.66}$$

Proof. Let us put

$$y_d := \sum_{\substack{1 \leqslant m \leqslant N \\ m \equiv 0 \,(\mathrm{mod}\, d)}} t(m,d)x_m \qquad (d \geqslant 1),$$

so that $y_d = 0$ for $d > N$. Substituting (4.63) in (4.61), we obtain

$$Q(\boldsymbol{x}) = \sum_{1 \leqslant d \leqslant N} g(d)y_d^2 \tag{4.67}$$

and, by Proposition 4.21(ii),

$$x_d = \sum_{m \equiv 0 \,(\mathrm{mod}\, d)} t^*(m,d) y_m \qquad (1 \leqslant d \leqslant N). \tag{4.68}$$

In particular, the condition $x_1 = 1$ reads

$$\sum_{1 \leqslant m \leqslant N} t^*(m,1) y_m = 1.$$

It follows that, for all real λ,

$$\begin{aligned} Q(\boldsymbol{x}) &= \lambda + \sum_{1 \leqslant d \leqslant N} \left\{ \sqrt{g(d)}\, y_d - \lambda \frac{t^*(d,1)}{2\sqrt{g(d)}} \right\}^2 - \tfrac{1}{4}\lambda^2 \sum_{1 \leqslant d \leqslant N} \frac{t^*(d,1)^2}{g(d)} \\ &\geqslant \lambda - \tfrac{1}{4}\lambda^2 \sum_{1 \leqslant d \leqslant N} \frac{t^*(d,1)^2}{g(d)} = \lambda - \frac{\lambda^2}{4Q^*}. \end{aligned}$$

The maximum of the right-hand side is achieved for $\lambda = 2Q^*$. We thus obtain $Q(\boldsymbol{x}) \geqslant Q^*$, with equality when $y_d = \lambda t^*(d,1)/2g(d)$ $(1 \leqslant d \leqslant N)$, whence (4.66) by (4.68). □

4.7.5. The Johnsen–Selberg prime power sieve. For each prime power p^ν $(\nu \geqslant 1)$, let $\mathcal{W}(p^\nu)$ be a set of residues modulo p^ν, identified with the class of its representatives in $\mathbb{Z}$. Let us assume that $\mathcal{W}(p^\mu) \cap \mathcal{W}(p^\nu) = \varnothing$ if $\mu \neq \nu$. We then put

$$\mathcal{W}(d) := \bigcap_{p^\nu \| d} \mathcal{W}(p^\nu), \tag{4.69}$$

so that $n \in \mathcal{W}(d)$ if, and only if, $n \in \mathcal{W}(p^\nu)$ whenever $p^\nu \| d$. By convention, let us also set $\mathcal{W}(1) = \mathbb{Z}$.

Let $\mathcal{A}$ be a finite sequence of integers (not necessarily distinct), let $\mathcal{P}$ be a set of primes and let $z \geqslant 2$ be a real number. We put

$$\mathcal{P}_z := \mathcal{P} \cap [1, z].$$

We seek an upper bound for the quantity

$$S(\mathcal{A}, \mathcal{P}; z) := \big|\big\{a \in \mathcal{A} : a \notin \mathcal{W}(p^\nu) \ \ (p \in \mathcal{P}_z,\, \nu \geqslant 1)\big\}\big|.$$

Let us assume we may write

$$\sum_{\substack{a \in \mathcal{A} \\ a \in \mathcal{W}(d)}} 1 = \frac{w(d)}{d} X + r_d \qquad (d \geqslant 1), \tag{4.70}$$

where $X \geqslant 0$ is a quantity independent of d, w is a non-negative multiplicative function, and r_d is, in some appropriate sense, an error term. We can assume with no loss of generality that

$$w(p^\nu) = 0 \qquad (p \notin \mathcal{P}_z,\, \nu \geqslant 1) \tag{4.71}$$

and that

$$\sum_{\nu\geqslant 1}\frac{w(p^\nu)}{p^\nu}<1 \quad (p\in\mathcal{P}_z), \tag{4.72}$$

which, in usual cases of application, is equivalent to the fact that $\bigcup_{\nu\geqslant 1}\mathcal{W}(p^\nu)\neq\mathbb{Z}$ for any prime number p.

We put

$$\vartheta(p^\nu):=1-\sum_{1\leqslant\mu\leqslant\nu}\frac{w(p^\mu)}{p^\mu}>0 \qquad (p\geqslant 2,\nu\geqslant 0). \tag{4.73}$$

Given an arithmetic function f, we also introduce the notation

$$\psi_f(x,y):=\sum_{\substack{n\leqslant x\\ P^+(n)\leqslant y}}\frac{f(n)}{n} \qquad (x\geqslant 1,\ y\geqslant 1).$$

Theorem 4.25. *Under the hypotheses of* (4.70), (4.71) *and* (4.72), *we have, for any integer* $D>1$

$$S(\mathcal{A},\mathcal{P};z)\leqslant\frac{X}{\psi_f(D,z)}+\sum_{\substack{m\leqslant D^2\\ P^+(m)\leqslant z}}3^{\omega(m)}|r_m|, \tag{4.74}$$

where f *is the normal multiplicative function defined by*

$$f(p^\nu):=\frac{p^\nu}{\vartheta(p^\nu)}-\frac{p^\nu}{\vartheta(p^{\nu-1})}=\frac{w(p^\nu)}{\vartheta(p^\nu)\vartheta(p^{\nu-1})} \qquad (\nu\geqslant 1). \tag{4.75}$$

Proof. Let $D>1$. For any real sequence $\{\lambda_d\}_{d\geqslant 1}$ satisfying $\lambda_1=1$ and $\lambda_d=0$ for $d>D$, we have

$$S(\mathcal{A},\mathcal{P};z)\leqslant\sum_{a\in\mathcal{A}}\Big(\sum_{a\in\mathcal{W}(d)}\lambda_d\Big)^2. \tag{4.76}$$

Indeed, the term of index a in the sum in (4.76) is always non-negative (since the λ_d are real) and equals $\lambda_1=1$ if a is counted in $S(\mathcal{A},\mathcal{P};z)$.

Let us introduce the multiplicative function defined by

$$\varepsilon(p^\mu,p^\nu):=\begin{cases}1 & \text{if } \mu=\nu \text{ or } \mu\nu=0,\\ 0 & \text{otherwise.}\end{cases}$$

Our initial disjointness condition for the classes $\mathcal{W}(p^\nu)$ implies that

$$\mathcal{W}(p^\mu)\cap\mathcal{W}(p^\nu)\neq\varnothing$$

is only possible if $\varepsilon(p^\mu,p^\nu)=1$. By multiplicativity, it follows that $\varepsilon(d,d')=1$ whenever $\mathcal{W}(d)\cap\mathcal{W}(d')\neq\varnothing$. Expanding the square in (4.76),

we therefore obtain

$$
\begin{aligned}
S(\mathcal{A},\mathcal{P};z) &\leqslant \sum_{d,\,d'\leqslant D}\lambda_d\lambda_{d'}\sum_{\substack{a\in\mathcal{A}\\ a\in\mathcal{W}(d)\cap\mathcal{W}(d')}}1\\
&= \sum_{d,\,d'\leqslant D}\lambda_d\lambda_{d'}\varepsilon(d,d')\sum_{\substack{a\in\mathcal{A}\\ a\in\mathcal{W}([d,d'])}}1 = XQ+R,
\end{aligned}
\tag{4.77}
$$

where we have put

$$
Q := \sum_{d,\,d'\leqslant D}\lambda_d\lambda_{d'}\varepsilon(d,d')\frac{w([d,d'])}{[d,d']},\quad R := \sum_{d,\,d'\leqslant D}\lambda_d\lambda_{d'}\varepsilon(d,d')r_{[d,d']}.
\tag{4.78}
$$

We may apply Theorem 4.24 to minimize the quadratic form Q. To this end, we must calculate the functions g, t, and t^* associated to the function $F(m,n) := \varepsilon(m,n)w([m,n])/[m,n]$.

Iterating over the pair (μ,ν), we infer from (4.64) that we have, with the notation (4.73),

$$
g(p^\nu) := \{\vartheta(p^{\nu-1}) - \vartheta(p^\nu)\}\frac{\vartheta(p^\nu)}{\vartheta(p^{\nu-1})}\qquad(\nu\geqslant 1),
$$

$$
t(p^\mu,p^\nu) := \begin{cases}\vartheta(p^{\mu-1}) - \vartheta(p^\mu) & \text{if } \nu = 0,\\ -\{\vartheta(p^{\mu-1}) - \vartheta(p^\mu)\}/\vartheta(p^\nu) & \text{if } 0<\nu<\mu,\\ \delta_{\mu\nu} & \text{if } \mu\leqslant\nu,\end{cases}
$$

from which

$$
t^*(p^\mu,p^\nu) := \begin{cases}-\{\vartheta(p^{\mu-1}) - \vartheta(p^\mu)\}/\vartheta(p^{\mu-1}) & \text{if } \nu = 0,\\ \{\vartheta(p^{\mu-1}) - \vartheta(p^\mu)\}/\vartheta(p^{\mu-1}) & \text{if } 0<\nu<\mu,\\ \delta_{\mu\nu} & \text{if } \mu\leqslant\nu.\end{cases}
$$

The minimum Q^* is reached for the value of $\{\lambda_d\}_{d\geqslant 1}$ given by (4.66), namely

$$
\lambda_d := \frac{\sum_{m\leqslant D}t^*(m,d)t^*(m,1)/g(m)}{\sum_{m\leqslant D}t^*(m,1)^2/g(m)}\quad(d\leqslant D),\quad \lambda_d^* := 0\ \ (d>D),
\tag{4.79}
$$

We notice that $t^*(m,1) = 0$ if $P^+(m) > z$. We then deduce from (4.65) that

$$
Q^* = \frac{1}{\sum_{\substack{d\leqslant D\\ P^+(d)\leqslant z}}\prod_{p^\nu\|d}\{1/\vartheta(p^\nu) - 1/\vartheta(p^{\nu-1})\}} = \frac{1}{\psi_f(D,z)}.
\tag{4.80}
$$

On the other hand, since $\sup_d|\lambda_d^*| = 1$, we can write

$$
|R| \leqslant \sum_{\substack{m\leqslant D^2\\ P^+(m)\leqslant z}}\sum_{[d,d']=m}\varepsilon(d,d')|r_m| = \sum_{\substack{m\leqslant D^2\\ P^+(m)\leqslant z}}3^{\omega(m)}|r_m|,
$$

where the inner sum over d,d' has been evaluated by noticing that it is multiplicative in m, and equals exactly 3 whenever m is a prime power. □

When the set $\mathcal{A}$ is an interval of integers, the upper bound (4.74) can take a different form.

Theorem 4.26 (Selberg)**.** *Let $N \in \mathbb{N}^*$ and $\mathcal{A}$ be a set made up of N consecutive integers. If the function $w(d) := |\mathcal{W}(d) \cap [0, d[|$ satisfies* (4.71) *and* (4.72)*, we have, for any integer $D \geqslant 1$,*

$$S(\mathcal{A}, \mathcal{P}; z) \leqslant \frac{N + D^2 - 1}{\psi_f(D, z)}$$

where f is the normal multiplicative function defined by (4.75)*.*

Proof. There exists an integer M such that $\mathcal{A} = \{n \in \mathbb{Z} : M < n \leqslant M+N\}$. Let b be the Beurling function defined by (4.30) with $\delta := 1/D^2$. By the second upper bound in (4.77), we have

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}; z) &\leqslant \sum_{d,\, d' \leqslant D} \lambda_d \lambda_{d'} \varepsilon(d, d') \sum_{\substack{n \in \mathbb{Z} \\ n \in \mathcal{W}([d,d'])}} b(n) \\ &= \sum_{d,\, d' \leqslant D} \lambda_d \lambda_{d'} \varepsilon(d, d') \sum_{\substack{0 \leqslant m < [d,d'] \\ m \in \mathcal{W}([d,d'])}} \sum_{n \equiv m \,(\mathrm{mod}\, [d,d'])} b(n). \end{aligned}$$

The inner sum evaluates to

$$\begin{aligned} &\sum_{n \in \mathbb{Z}} \frac{b(n)}{[d, d']} \sum_{0 \leqslant j < [d,d']} \mathrm{e}\Big(\frac{(n-m)j}{[d, d']}\Big) \\ &\quad = \frac{1}{[d, d']} \sum_{0 \leqslant j < [d,d']} \mathrm{e}\Big(\frac{-mj}{[d, d']}\Big) \sum_{n \in \mathbb{Z}} b(n) \mathrm{e}\Big(\frac{nj}{[d, d']}\Big) = \frac{\widehat{b}(0)}{[d, d']}, \end{aligned}$$

taking account of (4.24). Noticing that $\widehat{b}(0) = N + D^2 - 1$ by (4.31) and summing over m, it follows that, with the notation (4.78),

$$S(\mathcal{A}, \mathcal{P}; z) \leqslant (N + D^2 - 1)Q.$$

The stated result now follows from (4.80). □

We have, for each prime number p,

$$\sum_{\nu \geqslant 0} \frac{f(p^\nu)}{p^\nu} = 1 + \sum_{j \geqslant 1} \frac{1}{\vartheta(p^j)} - \frac{1}{\vartheta(p^{j-1})} = \frac{1}{\lim_{j \to \infty} \vartheta(p^j)} = \Big(1 - \sum_{\nu \geqslant 1} \frac{w(p^\nu)}{p^\nu}\Big)^{-1}.$$

whence

$$\lim_{D \to \infty} \frac{1}{\psi_f(D, z)} = W(z) := \prod_{p \leqslant z} \Big(1 - \sum_{\nu \geqslant 1} \frac{w(p^\nu)}{p^\nu}\Big). \tag{4.81}$$

Under some additional hypotheses, hardly limiting in practice, one may give an optimal estimate for the product $\psi_f(D, z)W(z)$. With this in view,

we assume for example that there are some constants, $r \in \mathbb{N}^*$, $\eta \in]0, \frac{1}{2}[$ and $\kappa > 0$ such that

$$\vartheta(p^\nu) \geqslant \eta \quad (p \in \mathcal{P},\ \nu \geqslant 1), \tag{4.82}$$

$$\sum_p \sum_{1 \leqslant \nu \leqslant r} \frac{w(p^\nu)^2 \log p}{p^{2\nu}} + \sum_p \sum_{\nu > r} \frac{w(p^\nu)}{p^{(1-\eta)\nu}} < \infty, \tag{4.83}$$

and

$$\sum_{\substack{y < p \leqslant t \\ 1 \leqslant \nu \leqslant r}} \frac{w(p^\nu) \ln p}{p^\nu} \leqslant \kappa \ln(t/y) + O(1) \qquad (t \geqslant y \geqslant 1). \tag{4.84}$$

The finer asymptotic behavior of the quantity $\psi_f(D, z)W(z)$ is described in terms of continuous solutions to delay differential equations, the prototype of which is the Dickman function, studied in detail in paragraph III.5.4.

We denote by ϱ_κ the continuous solution of the system

$$\begin{cases} \varrho_\kappa(u) = u^{\kappa-1}/\Gamma(\kappa) & \text{if } 0 < u \leqslant 1, \\ u\varrho'_\kappa(u) + (1-\kappa)\varrho_\kappa(u) + \kappa\varrho_\kappa(u-1) = 0 & \text{if } u > 1, \end{cases} \tag{4.85}$$

where Γ is Euler's function. One may thus establish, by evaluating its Laplace transform,[3] that the generalized Dickman function ϱ_κ is the fractional convolution power of order κ of the Dickman function $\varrho := \varrho_1$. For each κ, the function ϱ_κ inherits from ϱ the rapid decay property. We have, for example,

$$\varrho_\kappa(u) = (u \ln u)^{-u} \mathrm{e}^{O_\kappa(u)} \qquad (u \to \infty),$$

and an asymptotic formula is given in the Notes for this chapter.

Let us further put

$$\lambda_\kappa(u) := \mathrm{e}^{-\gamma\kappa} \int_u^\infty \varrho_\kappa(v)\,\mathrm{d}v, \quad j_\kappa(u) = 1 - \lambda_\kappa(u) \qquad (u \geqslant 0), \tag{4.86}$$

where γ denotes Euler's constant. Proceeding as in the case $\kappa = 1$, described in § III.5.4, one may establish that $\lambda_\kappa(0) = j_\kappa(\infty) = 1$—see, for example, Hensley (1986a).

We state without proof the following result, due to Tenenbaum & Wu (2008a).

[3] See Chapter III.5, where the calculation is performed in the case $\kappa = 1$, which is typical of the general situation.

Theorem 4.27. *Let $\kappa > 0$, $\eta \in]0, \frac{1}{2}[$. Under hypotheses* (4.70), (4.71), (4.82), (4.83), (4.84), *there exists a constant B such that, uniformly for $2 \leqslant z \leqslant D^{1/r}$, we have*

$$\frac{1}{\psi_f(D,z)} \leqslant \frac{W(z)}{j_\kappa(v)}\left\{1 + O\left(\frac{\lambda_\kappa^+(v)}{\ln z}\mathrm{e}^{Bv(\ln v)/\ln z}\right)\right\} \tag{4.87}$$

where $W(z)$ is defined by (4.81) *and where we have put*

$$v := \min\big\{(\ln D)/\{r\ln z\}, 3(\ln D)/(r\eta\ln_2 D)\big\}, \quad \lambda_\kappa^+(v) := \lambda_\kappa(v)v\ln(1+v).$$

We note that the error term, say R, in (4.87) satisfies the upper bound

$$R \ll v^{-v(1-\varepsilon)}/\ln z \qquad (z > z_0(\varepsilon)).$$

4.8. Sums of two squares in an interval

In the form described in the previous section, Selberg's sieve is perfectly adapted to providing an upper bound for the number of integers in an interval which can be represented as sums of two squares.

Let us begin by characterizing this set. The following theorem was conjectured by Girard in 1632 and established by Fermat in 1654.

The proof we give below rests on the fact that, given an odd prime p, the number -1 is a quadratic residue modulo p—or, in other words, the equation $x^2 + 1 \equiv 0 \pmod p$ is solvable— if, and only if, $p \equiv 1 \pmod 4$.

This classic property can easily be derived from the fact that the group $(\mathbb{Z}/p\mathbb{Z})^*$ of invertible residues modulo p is cyclic.[4] Another approach consists in observing that the multiplicative homomorphism

$$f : (\mathbb{Z}/p\mathbb{Z})^* \to \{-1, 1\}$$

defined by $f(x) = x^{(p-1)/2}$ is identically trivial on the subgroup Q_p of quadratic residues. Since the polynomial equation $f(x) = 1$ has at most $\frac{1}{2}(p-1)$ solutions in the field $\mathbb{Z}/p\mathbb{Z}$, it follows that Q_p coincides with the set of its roots. Thus, $f(a)$ assumes the value 1 if a is a quadratic residue modulo p, and the value -1 otherwise. As a rule, this property is expressed in terms of the *Legendre symbol*:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \in Q_p, \\ -1 & \text{if } a \notin Q_p. \end{cases}$$

Theorem 4.28. *For every $a \in (\mathbb{Z}/p\mathbb{Z})^*$, we have*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

[4] See Exercise 232, p. 404.

We are now able to establish the Girard–Fermat theorem in a simple way. Another proof, depending on the theory of continued fractions, is given in Chapter I.7.

Theorem 4.29 (Girard–Fermat)**.** *An odd prime number is the sum of two squares if, and only if, it is congruent to 1 modulo 4.*

Proof. The condition is necessary because a sum of two squares is congruent to 0, 1, or 2 modulo 4. Let us show it is sufficient. Given a prime p such that $p \equiv 1 \pmod 4$, we put $N := \lfloor \sqrt{p} \rfloor$ and consider a solution x of the equation $x^2 \equiv -1 \pmod p$. Amongst the $(N+1)^2 > p$ numbers $u + vx$ with $0 \leqslant u, v \leqslant N$, at least two belong to the same residue class modulo p. By subtraction, we deduce that the congruence $a \equiv bx \pmod p$ has a non-trivial solution in integers a, b such that $\max(|a|, |b|) < \sqrt{p}$. This implies $a^2 \equiv x^2 b^2 \equiv -b^2 \pmod p$, whence $p \mid a^2 + b^2$. Since $0 < a^2 + b^2 < 2p$, we must have $p = a^2 + b^2$. □

Theorem 4.30. *A positive integer n is representable as a sum of two squares if, and only if, for any prime number p such that $p \equiv 3 \pmod 4$, we have $v_p(n) \equiv 0 \pmod 2$.*

Proof. Let h denote the characteristic function of the set of sums of two squares. The identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{4.88}$$

implies that h is super-multiplicative, i.e. satisfies the inequality

$$h(mn) \geqslant h(m)h(n).$$

Taking the Girard–Fermat theorem into account, it follows that any integer satisfying the property stated in the theorem is the sum of two squares.

Conversely, if n has a representation in the form $n = a^2 + b^2$ and if p is an odd prime such that $v_p(n) = 2\nu + 1$ with $\nu \in \mathbb{N}$, let us put $\mu := v_p(a)$, so that $\mu \leqslant \nu$ and hence $v_p(b) = \mu$. Dividing the representation by $p^{2\mu}$, we obtain $\alpha^2 + \beta^2 \equiv 0 \pmod p$ with $p \nmid \alpha\beta$. This implies that -1 is a quadratic residue and therefore $p \equiv 1 \pmod 4$. □

Remark. It results from the above proof that the characteristic function h is in fact multiplicative, defined by

$$h(p^\nu) = \begin{cases} 1 & \text{if } p = 2 \text{ or } p \equiv 1 \pmod 4 \text{ or } 2 \mid \nu, \\ 0 & \text{if } p \equiv 3 \pmod 4 \text{ and } 2 \nmid \nu. \end{cases} \tag{4.89}$$

By standard techniques described in Part II, this allows one to evaluate the summatory function of h. We thus obtain, for example (see Exercise 240, p. 406),

$$\sum_{n\leqslant N} h(n) = \Big\{1 + O\Big(\frac{1}{\ln N}\Big)\Big\}\frac{K_0 N}{\sqrt{\ln N}} \qquad (N \geqslant 2), \tag{4.90}$$

with

$$K_0 := \frac{1}{\sqrt{2}} \prod_{p\equiv 3 \,(\mathrm{mod}\, 4)} \Big(1 - \frac{1}{p^2}\Big)^{-1/2}. \tag{4.91}$$

We can now apply the Johnsen–Selberg sieve to get an upper bound on the number of sums of two squares in an interval. To improve the legibility of the statement, we anticipate, in proving the second part of the following result, the formula

$$\prod_{p>2} \Big(1 - \frac{(-1)^{(p-1)/2}}{p}\Big) = \frac{4}{\pi}\cdot \tag{4.92}$$

This follows, for example, from the prime number theorem for arithmetic progressions in the form given in Theorem II.8.17 and the well-known formula $\sum_{n\geqslant 0}(-1)^n/(2n+1) = \pi/4$.

Theorem 4.31. *Let I be a real interval containing N positive integers. There exists an absolute positive constant K such that the number Z_N of elements of I which can be written as a sum of two squares satisfies*

$$Z_N \leqslant KN \prod_{\substack{p\leqslant N \\ p\equiv 3 \,(\mathrm{mod}\, 4)}} \Big(1 - \frac{1}{p}\Big). \tag{4.93}$$

Furthermore, as N tends to infinity, we have

$$Z_N \leqslant \big\{\pi + o(1)\big\}\frac{K_0 N}{\sqrt{\ln N}}\cdot \tag{4.94}$$

Proof. We apply Theorem 4.26 with the choice

$$\mathcal{P} := \{p \equiv 3 \,(\mathrm{mod}\, 4)\}, \quad \mathcal{W}(p^\nu) := \begin{cases} \{mp^{\nu-1} : p \nmid m\} & \text{if } p \in \mathcal{P},\ 2 \mid \nu, \\ \varnothing & \text{if } p \in \mathcal{P},\ 2 \nmid \nu. \end{cases}$$

Thus, we have

$$w(p^\nu) = \begin{cases} p-1 & \text{if } 2 \mid \nu \text{ and } p \in \mathcal{P}, \\ 0 & \text{if } 2 \nmid \nu \text{ or } p \notin \mathcal{P}. \end{cases}$$

It follows that the hypotheses in Theorem 4.27 are satisfied for $r = 2$: by Theorem 1.10 the value $\kappa = 1$ is trivially admissible—which suffices to

establish (4.93)—and we can in fact select $\kappa = \frac{1}{2}$, anticipating the validity of Theorem II.8.16. We obtain

$$Z_N \leqslant \frac{N+D^2}{j_{1/2}(v)} \prod_{\substack{p\leqslant z\\ p\equiv 3 \,(\mathrm{mod}\, 4)}} \Big(1-\frac{1}{p+1}\Big)\Big\{1+O\Big(\frac{v^{-v/2}}{\ln z}\Big)\Big\},$$

where D is arbitrary and v is defined as indicated in the statement of Theorem 4.27.

Let us choose $D = z^2 := \sqrt{N}/\ln N$, so that $v = 1$ and

$$j_{1/2}(1) = 2\mathrm{e}^{-\gamma/2}/\Gamma(\tfrac{1}{2}) = 2\mathrm{e}^{-\gamma/2}/\sqrt{\pi}.$$

It remains to bound the product, say $W(z)$. We have

$$\begin{aligned} W(z) &= \prod_{\substack{p\leqslant z\\ p\equiv 3 \,(\mathrm{mod}\, 4)}} \Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^2}\Big)^{-1} \\ &= \sqrt{2}\prod_{p\leqslant z}\Big(1-\frac{1}{p}\Big)^{1/2} \prod_{2<p\leqslant z}\Big(1-\frac{(-1)^{(p-1)/2}}{p}\Big)^{-1/2} \prod_{\substack{p\leqslant z\\ p\equiv 3 \,(\mathrm{mod}\, 4)}} \Big(1-\frac{1}{p^2}\Big)^{-1/2} \\ &= \frac{2\sqrt{\pi}\mathrm{e}^{-\gamma/2}K_0+o(1)}{\sqrt{\ln N}}. \end{aligned}$$

□

Remark. The comparison of (4.94) and (4.90) shows that the factor lost by applying the sieve is asymptotically at most π. Since, by the functional equation (4.85), the function $j_{1/2}(v)/\sqrt{v}$ is decreasing for $v \geqslant 1$, it follows that the selection of $v = 1$ made in the preceding proof is optimal for the method used.

Notes

§ 4.2. To estimate the third error term in (4.5), we have appealed to the *parametric method*, presented in detail in chapter 0 of the book by Hall & Tenenbaum (1988). The famous *Rankin's method* (cf. § III.5.1) is another example of this fruitful computational trick, which consists in bounding the characteristic function of a set of integers by a constant multiple of a multiplicative function depending on a parameter to be optimized.

Our application of Brun's method to bounding $\pi(x)$ from above is only a mere illustration of the basic ideas, and should not be considered as a result in itself. Not only, as we observed, does it provides a weaker estimate than Chebyshev's, but one could also object, *stricto sensu*, to a loss of information. Indeed, we appealed to Theorem 1.10, which itself rests on Mertens' first theorem. But this last result immediately yields a Chebyshev-type upper bound for $\pi(x)$ since we have, for large x,

$$\pi(x) - \pi(x/2) \leqslant \frac{x}{\ln x} \sum_{x/2<p\leqslant x} \frac{\ln p}{p} \ll \frac{x}{\ln x}.$$

However, one can easily check that Brun's treatment does not require more than an asymptotic formula for $\sum_{p\leqslant x} 1/p$. This is a much weaker bound than those of Theorems 1.10 or 1.8, and reveals precisely why the scope of this method is so vast.

For other results about $\Phi(x, y)$, see Chapter III.6.

Alladi (1988) has an exposition of some developments of Brun's method for sums of multiplicative functions on certain subsets of $\mathbb{N}$.

The reader interested in the state of the art in the theory of the combinatorial sieve can refer to the survey of Diamond & Halberstam (1985) and the deep articles of Iwaniec (1980a and b, 1981).

A version similar in its principles to that of Brun, but furnishing results of a quality comparable with those of the improvements available in the literature, has been obtained by Hooley (1994) and simplified by Ford and Halberstam (2000), who stated a form that can be deployed "out of the box".

Let us briefly describe the main properties of the coefficients in the Rosser–Iwaniec sieve—see Iwaniec (1980a and b) in the "linear" case, that is to say when the function $w(p)$, representing the number of excluded residue classes modulo p, is bounded by 1 on average, also known as the case of *sieve of dimension* 1. The work of Iwaniec covers the case of any dimension.

Given a set of primes $\mathcal{P}$, we put

$$P(z) := \prod_{p\in\mathcal{P},\, p\leqslant z} p.$$

The Buchstab function $\omega(t)$, vanishing for $0 \leqslant t < 1$, is defined on $[1,\infty[$ as the unique continuous solution of the delay differential equation

$$\big(t\omega(t)\big)' = \omega(t-1) \qquad (t > 2)$$

with the initial condition $t\omega(t) = 1$ for $1 \leqslant t \leqslant 2$. One then defines the sieve functions F and f by

$$F(t) = \mathrm{e}^{\gamma}\{\omega(t) + \varrho(t-1)/t\}, \qquad f(t) = \mathrm{e}^{\gamma}\{\omega(t) - \varrho(t-1)/t\}$$

where γ is Euler's constant and ϱ is the Dickman function. We have $f(t) > 0$ if, and only if, $t > 2$. Moreover (see Corollary III.6.9), we have the asymptotic formulae

$$\begin{matrix} F(t) \\ f(t) \end{matrix} = 1 + O(\varrho(t-1)/t) = 1 + O(t^{-t}) \qquad (t\to\infty).$$

Theorem 4.32 (Iwaniec)**.** *Let $D \geqslant 1$. There exist two sequences $\{\lambda_d^+\}_{d\geqslant 1}$ and $\{\lambda_d^-\}_{d=1}^{\infty}$, vanishing for $d > D$ or $\mu(d) = 0$, satisfying $\lambda_1^{\pm} = 1$, $|\lambda_d^{\pm}| \leqslant 1$, and such that we have*

$$\lambda^- * \mathbf{1} \leqslant \mu * \mathbf{1} \leqslant \lambda^+ * \mathbf{1},$$

and

$$\sum_{d|P(z)} \lambda_d^+ \frac{w(d)}{d} \leqslant \prod_{\substack{p\leqslant z\\ p\in\mathcal{P}}} \Big(1 - \frac{w(p)}{p}\Big)\Big\{F(s) + O\Big(\frac{\mathrm{e}^{\sqrt{L}-s}}{(\ln D)^{1/3}}\Big)\Big\},$$

$$\sum_{d|P(z)} \lambda_d^- \frac{w(d)}{d} \geqslant \prod_{\substack{p\leqslant z\\ p\in\mathcal{P}}} \Big(1 - \frac{w(p)}{p}\Big)\Big\{f(s) + O\Big(\frac{\mathrm{e}^{\sqrt{L}-s}}{(\ln D)^{1/3}}\Big)\Big\}$$

for any $z \in [2, D]$, $D = z^s$, any set $\mathcal{P}$ of prime numbers, and any multiplicative function w satisfying

(i) $\quad 0 < w(p) < p \qquad (p \in \mathcal{P})$,

(ii) $\quad \displaystyle\prod_{u<p\leqslant v,\, p\in\mathcal{P}} \Big(1 - \frac{w(p)}{p}\Big)^{-1} \leqslant \frac{\ln v}{\ln u}\Big(1 + \frac{L}{\ln u}\Big) \qquad (2 \leqslant u \leqslant v \leqslant z).$

§ 4.4. Although (at least for the optimal form of the result) our proof of the analytic large sieve relies on the theory of analytic functions of a complex variable and on a deep result in harmonic analysis, the large sieve may be considered as an essentially elementary tool. We have seen that the proof of the inequality

$$\Delta(N,\delta) \leqslant \tfrac{1}{2}\pi^2(N - 1 + \delta^{-1})$$

is elementary. We also refer to the proofs, all distinct, of Montgomery (1971) [$\Delta \leqslant N + 2/\delta$], Bombieri (1974) [*idem*], and Elliott (1980) [$\Delta \leqslant N + 1/\delta$].

The function $F(z)$ in Lemma 4.11 was studied by Beurling at the end of the 1930s. For an exhaustive study of the optimization problem (4.27)–(4.28) and numerous applications which have been brought about by the various generalizations of this question, see Graham & Vaaler (1981, 1984), Vaaler (1985).

The large sieve is equally useful for estimating mean values of Dirichlet characters—see § II.8.1. Let us set

$$T(\chi) := \sum_{M<n\leqslant M+N} a_n \chi(n).$$

Gallagher (1967) gave a simple proof of the inequality

$$\sum_{\chi}^{*} |T(\chi)|^2 \leqslant \frac{\varphi(q)}{q} \sum_{1\leqslant a\leqslant q,\,(a,q)=1} \Big|S\Big(\frac{a}{q}\Big)\Big|^2$$

where the sum is over the primitive characters modulo q, that is, the characters which are not induced by a character modulo d with $d|q,\ d<q$. We then deduce from (4.33) the upper bound

$$\sum_{q\leqslant Q} \frac{q}{\varphi(q)} \sum_{\chi}^{*} |T(\chi)|^2 \leqslant (N - 1 + Q^2) \sum_{M<n\leqslant M+N} |a_n|^2.$$

This inequality plays an essential role in the study of L-functions (cf. § II.8.2) and the distribution of prime numbers in arithmetic progressions. It is, in particular, one of the fundamental ingredients in the proof of the Bombieri–Vinogradov theorem (1965, 1966)—cf. Chapter II.8, Notes.

§ 4.5. Theorem 4.14 has been used for numerous elegant solutions of arithmetic problems. In particular, it underpins the original proof of Daboussi's theorem (Daboussi & Delange, 1974). It is also the starting point of the new method of Hildebrand (1986c, d, e, 1987a) for studying the mean value of multiplicative functions with modulus at most 1. Hildebrand (1986b) also applies this inequality to manufacture a new elementary proof of the prime number theorem. A variant of Theorem 4.14 has been established by Elliott (1979, lemma 4.7), who shows the inequality (see also Theorem III.3.2)

$$\sum_{p\leqslant N} p\Big|S(p,0) - \frac{1}{p}S(0)\Big|^2 \leqslant 16N \sum_{1\leqslant n\leqslant N} |a_n|^2.$$

The result is not directly comparable to (4.42): the summation over p is longer,[5] but here only one congruence class for each prime number p is considered.

[5]Indeed, (4.42) only implies an upper bound of the same order if $Q \ll \sqrt{N}$.

§ 4.6. The best upper bound currently known for $J(x)$ is due to Wu (2004), improving on results by Fouvry & Grupp (1986) and himself (1990). The factor 8 in Theorem 4.15 is replaced by 3.3996. The basic result for this problem provides a factor 4: see Exercise 82. It is due to Bombieri & Davenport (1966)—cf. Halberstam & Richert (1974). Beside the sieve (Selberg's) the proof requires the Bombieri–Vinogradov theorem—cf. Theorem II.8.34.

The inequality (4.46) in fact holds uniformly *without* an error term, i.e.,

$$\pi(x+y;\ell,k)-\pi(x;\ell,k)<\frac{2y}{\varphi(k)\ln(y/k)}\qquad(1\leqslant k<y\leqslant x).$$

This handy result is due to Montgomery & Vaughan (1973).

§ 4.7. The special case of the prime power sieve where $\mathcal{A}$ is an interval was initially considered by Johnsen (1971) under hypotheses which are noticeably more restrictive than those we assumed. These appear in the work of Selberg (1977), who thus extends his own method. Gallagher (1972, 1973/74) provided a simpler proof of Johnsen's estimate. Motohashi (1979) then obtained a new proof, via the large sieve, of Selberg's result, thereby answering a question posed in Selberg's 1977 work.

The final upper bound for $S(\mathcal{A},\mathcal{P};z)$ is made explicit by Selberg when $\mathcal{A}$ is an interval, which corresponds to Theorem 4.26. In Theorem 4.25 we consider the general formulation by adopting the exposition of Tenenbaum & Wu (2008a).

Theorem 4.27 is obtained by observing that, for any non-negative multiplicative function f, we have

$$\psi_f(D,z)\geqslant\psi_{f_r}(D^{1/r},z)\qquad(D\geqslant 1,\ z\geqslant 1)\tag{4.95}$$

where f_r is the multiplicative function defined by

$$f_r(p^\nu):=\begin{cases}\displaystyle\sum_{1\leqslant j\leqslant r}\frac{f(p^j)}{p^{j-1}} & \text{if } \nu=1,\\ 0 & \text{if } 1<\nu\leqslant r\\ f(p^\nu) & \text{if } \nu>r.\end{cases}$$

Under hypotheses (4.82), (4.83) and (4.84), this allows one to apply th. 3.1 of Tenenbaum–Wu to the function f defined by (4.75).

We now provide some information about the functions ϱ_κ and λ_κ occurring above. Denote by $\xi(u)$ the unique non-zero real solution of $\mathrm{e}^\xi=1+u\xi$

if $u > 0$, $u \neq 1$, and set $\xi(1) = \xi(0) = 0$. Define further

$$\begin{aligned} \xi_\kappa(u) &:= \max\{1,\, \xi(u/\kappa)\}, \\ I(s) &:= \int_0^s \frac{\mathrm{e}^v - 1}{v}\,\mathrm{d}v, \\ \sigma_j(u) &:= \kappa I^{(j)}(\xi_\kappa(u)), \end{aligned} \tag{4.96}$$

so that, by Lemma III.5.11 *infra* and lemma 4.5 of Smida (1991), we have, for any fixed real number $j \geqslant 0$,

$$\begin{aligned} \xi_\kappa(u) &= \ln u + \ln_2 u + O\biggl(\frac{\ln_2 u}{\ln u}\biggr) \\ \sigma_j(u) &= u\biggl\{1 + O\biggl(\frac{1}{\ln u}\biggr)\biggr\} \end{aligned} \qquad (u \to \infty). \tag{4.97}$$

It then follows from theorem 1 of Smida (1991) or from the more general theorem 2 in Hildebrand–Tenenbaum (1993a) that we have

$$\varrho_\kappa(u) = \biggl\{1 + O\biggl(\frac{1}{u}\biggr)\biggr\}\frac{\mathrm{e}^{\gamma\kappa - u\xi_\kappa(u) + \sigma_0(u)}}{\sqrt{2\pi\sigma_2(u)}} \quad (u \to \infty), \tag{4.98}$$

where γ denotes Euler's constant.

As noted in the work of Hanrot, Tenenbaum & Wu (2007)—formula (4.12)—we have

$$\lambda_\kappa(u) = \biggl\{1 + O\biggl(\frac{1}{u}\biggr)\biggr\}\frac{\mathrm{e}^{-\gamma\kappa}\varrho_\kappa(u)}{\xi_\kappa(u)} \qquad (u > 0). \tag{4.99}$$

For a survey exposition of the work of Goldston, Pintz and Yıldırım, see in particular Soundararajan (2007).

Exercises

77. For $x \geqslant z \geqslant y \geqslant 1$, we denote by $\Psi_0(x, y, z)$ the number of integers $n \leqslant x$ having no prime factor in $]y, z]$.

(a) Use Eratosthenes' sieve to show that

$$\lim_{x\to\infty} x^{-1}\Psi_0(x, y, z) = \prod_{y<p\leqslant z} (1 - 1/p).$$

(b) Use Brun's pure sieve to show the existence of an absolute positive constant c such that, uniformly for $1 \leqslant y \leqslant z \leqslant \exp\{c \ln x/ \ln_2 x\}$, we have

$$\Psi_0(x, y, z) \sim x \prod_{y<p\leqslant z} (1 - 1/p) \quad (x \to \infty). \tag{4.100}$$

(c) Extend this result using the fundamental lemma of combinatorial sieve theory.

(d) Assuming the prime number theorem, show that (4.100) does not hold uniformly for $1 \leqslant y < z \leqslant \sqrt{x}$.

78. *Primes and quasi-primes of the form $n^2 + 1$.*

(a) Show that the number $\varrho(p)$ of solutions to the equation

$$\xi^2 + 1 \equiv 0 \pmod p$$

equals 1 if $p = 2$, 2 if $p \equiv 1 \pmod 4$, and 0 if $p \equiv 3 \pmod 4$.

(b) Deduce that the equation $\xi^2 + 1 \equiv 0 \pmod d$ has $\varrho(d) := \prod_{p|d} \varrho(p)$ solutions for each squarefree integer d.

(c) Using the fundamental lemma of combinatorial sieve theory, show that the number $S(x)$ of primes $p \leqslant x$ of the form $p = n^2 + 1$ satisfies

$$S(x) \ll \sqrt{x} \prod_{p\leqslant x,\, p\equiv 1 \,(\mathrm{mod}\, 4)} \Big(1 - \frac{2}{p}\Big).$$

(d) Make the previous calculation more precise by assuming Dirichlet's theorem

$$\sum_{p\leqslant x,\, p\equiv 1 \,(\mathrm{mod}\, 4)} \frac{1}{p} = \tfrac{1}{2} \ln_2 x + O(1).$$

(e) Under the same assumptions, show there is a positive absolute constant B such that

$$\mathrm{card}\,\big\{n \leqslant \sqrt{x} : n^2 + 1 \in Q(B, x)\big\} \asymp \sqrt{x}/ \ln x$$

where $Q(B, x) := \big\{m \leqslant x : p|m \Rightarrow p > x^{1/B}\big\}$.[6]

[6] The elements of this set are usually referred to as "quasi-primes"—see Halberstam & Richert (1974), §2.8. In particular, a quasi-prime only has a bounded number of prime factors. Moreover, $|Q(B, x)| \asymp \pi(x)$.

79. *Almost squares.*

(a) Let p be be a prime > 2. Show that the kernel of the endomorphism of $(\mathbb{Z}/p\mathbb{Z})^* : x \mapsto x^2$ is $\{\pm 1\}$ and deduce that the number of quadratic non-residues modulo p is $(p-1)/2$.

(b) By sieving the set $\mathcal{A} = \{n : n \leqslant x\}$ by the prime numbers $\leqslant \sqrt{x}$ for suitable congruence classes, show that the number S of integers $n \leqslant x$ such that n is a quadratic residue modulo p for all $p \leqslant \sqrt{x}$ satisfies $\lfloor \sqrt{x} \rfloor \leqslant S \leqslant C\sqrt{x}$ where C is an absolute constant to be calculated.

80. Using the large sieve, show that if $\mathcal{A} \subset]M, M+N]$ is a set of integers which, for each prime p, is excluded from $w(p)$ residue classes modulo p with $w(p) \ll 1$, then

$$|\mathcal{A}| \ll N \prod_{p \leqslant N} (1 - w(p)/p).$$

Recover this result using Selberg's sieve.

81. *Majorizing the number of representations in Goldbach's problem.*

Let N be an even integer and let $r(N)$ denote the number of representations of N in the form $N = p + q$ where p and q are primes. According to Goldbach's conjecture, we have $r(N) > 0$ for every even integer $N \geqslant 4$. Probabilistic considerations suggest that we actually have

$$r(N) \sim C_N N/(\ln N)^2 \qquad (N \to \infty)$$

with $C_N := 2\prod_{p>2}(1 - 1/(p-1)^2) \prod_{p|N,\, p>2}((p-1)/(p-2))$.

(a) For any multiplicative function $f \geqslant 0$ with $\mu(m) = 0 \Rightarrow f(m) = 0$, show that we have

$$\sum_{n \leqslant x} f(n) \leqslant \sum_{d|N} f(d) \sum_{m \leqslant x,\, (m,N)=1} f(m) \qquad (1 \leqslant x \leqslant N).$$

(b) Prove the existence of an absolute constant C such that

$$r(N) \leqslant C \prod_{p|N} \Big(1 + \frac{2}{p}\Big) \frac{N}{(\ln N)^2}.$$

(c) Let h be a multiplicative function satisfying the conditions

$$|h(p)| \leqslant 1 \ (p|N), \quad |h(p)| \leqslant p^{-\delta} \ (p \nmid N), \quad |h(p^\nu)| \ll 1 \ (\nu \geqslant 2),$$

where δ is a positive constant. Show that, for $0 \leqslant \alpha \leqslant 1/\ln_2 N$, we have

$$\sum_{d \geqslant 1} |h(d)| d^{\alpha - 1} \ll \ln_2 N.$$

(d) Applying the above result to a suitable function h, establish the inequality

$$r(N) \leqslant (8 + o(1))C_N \frac{N}{(\ln N)^2},$$

which sharpens that obtained in (b).[7]

82. *Generalized twin primes.*

For $k \in \mathbb{N}^*$, $x \geqslant 2$, let us denote by $J_{2k}(x)$ the number of primes p not exceeding x such that $p+2k$ is also prime. By applying Selberg's sieve to the set $\mathcal{A} := \{n(n+2k) : n \leqslant x\}$, show that, whenever $x \to \infty$ and uniformly in $k \geqslant 1$, we have

$$J_{2k}(x) \leqslant \{8C_2 + o(1)\}\frac{g(k)x}{(\ln x)^2}$$

where $C_2 := 2\prod_{p>2}\{1 - 1/(p-1)^2\}$, $g(k) := \prod_{\substack{p|k\\ p>2}}\{1 - 1/(p-1)\}^{-1}$.

Show how the Bombieri–Vinogradov theorem (Theorem II.8.34) allows us to divide this bound asymptotically by 2. Hint: apply Selberg's sieve to the set $\mathcal{A} := \{p + 2k : p \leqslant x,\ p \in \mathbb{P}\}$.

83. *Small gaps between primes.*

Let $\{p_n\}_{n=1}^{\infty}$ be the sequence of prime numbers and set $d_n := p_{n+1} - p_n$ $(n \geqslant 2)$. We intend to show here that $\alpha := \liminf_n d_n/\ln n < 1$.[8]

For $x \geqslant 2$, $0 < \delta < 1$, we put $I_x := \{n \in \mathbb{N}^* : x < p_n < p_{n+1} \leqslant 2x\}$, and

$$N_x(\delta) := \sum_{\substack{n\in I_x\\ 1-\delta<d_n/\ln x\leqslant 1+\delta}} 1, \quad S(x) := \sum_{n\in I_x} d_n.$$

(a) Assuming $\alpha > 1 - \delta$, show that, as x tends to infinity, we have

$$\{1 + \delta + o(1)\}x - 2\delta N_x(\delta)\ln x \leqslant S(x) \leqslant x.$$

(b) Let g be the arithmetic function defined in Exercise 82. By a convolution argument, show that there is a constant $A > 0$ such that

$$\sum_{k\leqslant y} g(k) = \{A + o(1)\}y \qquad (y \to \infty).$$

(c) Show that, for large x, we have $N_x(\delta) < B\delta x/\ln x$ where B is an absolute constant.

(d) Conclude and provide a numerical upper bound for α.

---

[7] This estimate is thus asymptotically equal to eight times the conjectured value for $r(N)$. Employing the Bombieri–Vinogradov theorem—cf. Theorem II.8.34—Bombieri & Davenport (1966) obtain an estimate where the factor 8 is replaced by 4: see Halberstam & Richert—1974, th. 3.11.

[8] This result is due to Erdős (1940). Goldston, Pintz and Yıldırım (2006) established that $\alpha = 0$. Zhang (2014) proved that d_n is bounded on an infinite subsequence of integers n. See also Maynard (2014)

84. *Poisson summation formula.*

Let $f \in L^1(\mathbb{R})$.

(a) Show that the series $\varphi(t) := \sum_{n\in\mathbb{Z}} f(n+t)$ converges for almost all real numbers t.

(b) Assume additionally that f is continuous and of bounded variation on $\mathbb{R}$. Show that Poisson's formula

$$\sum_{n\in\mathbb{Z}} f(n+t) = \lim_{N\to\infty} \sum_{|n|\leqslant N} \widehat{f}(n)\mathrm{e}(tn)$$

holds for all $t \in [0,1[$.

85. *Integers coprime to q.*

For each integer $q \geqslant 1$, set $N_q(x) := |\{n \leqslant x : (n,q) = 1\}|$.

(a) Show that, for each $q \geqslant 1$, we have

$$\lim_{x\to\infty} N_q(x)/x = \varphi(q)/q.$$

(b) For fixed q, show that every integer $n \geqslant 1$ can be written uniquely as $n = hdt$, with $(h,q) = 1$, $d \mid q$, $\mu(d)^2 = 1$, $p \mid t \Rightarrow p \mid d$.

(c) Calculate $\sum_{p|t\Rightarrow p|d} 1/t$.

(d) For $q \geqslant 1$, $Q \geqslant 1$, set $L(q,Q) := \sum_{d|q,\, d\leqslant Q} \mu(d)^2/\varphi(d)$. Show that

$$\ln(Q+1) \leqslant L(q,Q) \prod_{p\leqslant Q,\, p\nmid q} \big(1-1/p\big)^{-1}.$$

Deduce that, for $x \geqslant Q \geqslant 1$, $q \geqslant 1$, $P^+(q) \leqslant x$, we have

$$\frac{1}{L(q,Q)} \leqslant \frac{\mathrm{e}^\gamma \varphi(q)\ln x}{q\ln(Q+1)}\Big\{1 + O\Big(\frac{1}{\ln x}\Big)\Big\}.$$

(e) Show that the upper bound

$$N_q(x) \leqslant \Big\{1 + O\Big(\frac{\ln_2 x}{\ln x}\Big)\Big\} 2\mathrm{e}^\gamma \frac{\varphi(q)}{q} x.$$

holds uniformly for $x \geqslant 3$, $q \geqslant 1$, $P^+(q) \leqslant x$.[9]

86. *Functions of the combinatorial sieve.*

(a) Show that for any arithmetic function χ we have

$$\mu\chi * \mathbf{1}(n) = \sum_{d|m/q} \mu(d)\{\chi(d) - \chi(qd)\} \qquad (n \geqslant 1)$$

with $q := P^-(n)$, $m := \prod_{p|n} p$.

(b) Let $\mathcal{P}$ be a set of prime numbers, and y be a real number; define $P(y) := \prod_{p\leqslant y,\, p\in\mathcal{P}} p$. Show that, if χ_1 and χ_2 satisfy the three properties

[9] This bound can be halved: see Exercise 276, p. 471.

(α) $\chi_i(d) = 0$ or $1 \qquad \big(d \mid P(y)\big)$

(β) $\chi_i(d) = 1 \Rightarrow \chi_i(t) = 1 \qquad (t \mid d)$

(γ) $\chi_i(d)=1$, $\mu(d)=(-1)^{i-1} \Rightarrow \chi_i(pd)=1 \quad \big(pd|P(y),\, p < P^-(d)\big)$,

then, for n dividing $P(y)$ and $q = P^-(n)$, we have

$$(-1)^i\mu(d)\{\chi_i(d) - \chi_i(qd)\} \geqslant 0 \qquad \big(d \mid m/q,\, i = 1, 2\big).$$

Deduce that

$$\mu\chi_1 * \mathbf{1}(n) \leqslant \delta(n) \leqslant \mu\chi_2 * \mathbf{1}(n) \qquad \big(n \mid P(y)\big). \tag{4.101}$$

(c) Show that the functions μ_1, μ_2 described after Theorem 4.3 satisfy relation (4.101).

Chapter III.1

Densities

1.1. Definitions. Natural density

Like other parts of mathematics (and maybe even more so!) number theory is confronted with the problem of rigorously formalizing intuitive notions. Foremost among these figures *the probability that an integer belongs to a given sequence*. The point here is to give a mathematical meaning to statements of the type: one integer in two is even, almost no integer is the sum of two squares, etc.

The first approach which comes to mind is naturally to have recourse to the established theory of probability. Defining a probability measure on $\mathbb{N}^*$ does indeed allow associating a probability with each subset $\mathcal{A}$ of the set of integers. However, the following result shows that such a framework fundamentally contradicts one of our strongest intuitions about numbers: that which suggests that the proportion of integers divisible by $a \geqslant 1$ is exactly $1/a$.

Theorem 1.1. *For $a \in \mathbb{N}^*$, denote by $a\mathbb{N}^*$ the set of positive multiples of a. There exists no probability measure P on $\mathbb{N}^*$ such that*

$$P(a\mathbb{N}^*) = 1/a \qquad (a = 1, 2, \ldots).$$

Proof. Let us argue by contradiction. Since

$$a\mathbb{N}^* \cap b\mathbb{N}^* = ab\mathbb{N}^*$$

whenever $(a, b) = 1$, we see that, under this assumption, the events $a\mathbb{N}^*$ and $b\mathbb{N}^*$ are independent. The same holds for their complements $\mathbb{N}_a$ and $\mathbb{N}_b$,

with the notation $\mathbb{N}_a := \mathbb{N}^* \setminus a\mathbb{N}^*$. Therefore

$$P(\mathbb{N}_a \cap \mathbb{N}_b) = \Big(1 - \frac{1}{a}\Big)\Big(1 - \frac{1}{b}\Big)$$

when $(a, b) = 1$. Inductively, we immediately obtain, for all integers m, n, $m < n$,

$$P(\{m\}) \leqslant P\Big(\bigcap_{m<p\leqslant n} \mathbb{N}_p\Big) = \prod_{m<p\leqslant n} \Big(1 - \frac{1}{p}\Big),$$

where, as usual, the letter p denotes a prime. Since n is arbitrarily large, we deduce from Mertens' theorem that $P(\{m\}) = 0$ for all $m \geqslant 1$, which yields the desired contradiction. □

To define a probability law on $\mathbb{N}^*$ amounts to specifying a convergent series with sum 1, viz.

$$\sum_{n\geqslant 1} \lambda_n = 1,$$

with $0 \leqslant \lambda_n \leqslant 1$ for all n. For any integer sequence[1] $\mathcal{A} \subseteq \mathbb{N}^*$, we then have

$$P(\mathcal{A}) = \sum_{a\in\mathcal{A}} \lambda_a$$

and we can further appreciate the discrepancy between such a model and intuition by noting that the probability of a sequence virtually depends only on its initial terms. Indeed, for each $\varepsilon > 0$ there is an $N = N_\varepsilon$ such that

$$P\big(\{1, 2, \ldots, N\}\big) \geqslant 1 - \varepsilon\ .$$

We thus find ourselves in a typical situation where the only theory at our disposal irrevocably invalidates two natural "theorems", namely

(i) $P(a\mathbb{N}^*) = 1/a \qquad (a = 1, 2, \ldots)$,
(ii) $P(\mathcal{A}) = P(\mathcal{B}) \qquad (|\mathcal{A}\Delta\mathcal{B}| < \infty)$,

where $\mathcal{A}\Delta\mathcal{B}$ denotes the symmetric difference of $\mathcal{A}$ and $\mathcal{B}$.

Making the choice (standard throughout the history of mathematics) of preferring intuitive theorems to established theories, it is not hard to circumvent these difficulties. We introduce a *divergent* series with non-negative terms

$$\sum_{n\geqslant 1} \lambda_n = \infty$$

and define the *density* $d(\mathcal{A})$ of a subset $\mathcal{A} \subseteq \mathbb{N}^*$ as the limit, when it exists, of the ratio

$$d(\mathcal{A}; x) := \sum_{a\leqslant x,\, a\in\mathcal{A}} \lambda_a \Big/ \sum_{n\leqslant x} \lambda_n \tag{1.1}$$

[1] In probabilistic number theory, it is customary to designate as *an integer sequence* a strictly increasing sequence of positive integers, which therefore can also be considered as a subset of $\mathbb{N}^*$.

as $x \to \infty$. It plainly follows that the density of any finite set is zero, but the concept thus introduced is not a measure on $\mathbb{N}^*$:

(iii) sequences possessing a density do not form a σ-algebra,

(iv) density is not countably additive.

The simplest choice consists in setting $\lambda_n = 1$ for all $n \geqslant 1$. We thus obtain the notion of *natural density*, or *asymptotic density*, both terms being commonly used. When it exists, the natural density of $\mathcal{A}$ is given by the formula

$$\mathbf{d}\mathcal{A} := \lim_{x\to\infty} x^{-1}\big|\{a \leqslant x : a \in \mathcal{A}\}\big|. \tag{1.2}$$

One denotes by upper (resp. lower) natural (or asymptotic) density the quantity $\overline{\mathbf{d}}\mathcal{A}$ (resp. $\underline{\mathbf{d}}\,\mathcal{A}$) obtained by replacing the symbol lim by lim sup (resp. lim inf) in (1.2).

Before proceeding further, we make four simple observations.

(a) Every arithmetic progression $n \equiv a \,(\mathrm{mod}\, q)$ has natural density, equal to $1/q$. This is immediate, since in this case we have

$$\big|\{a \leqslant x : a \in \mathcal{A}\}\big| = \lfloor x/q \rfloor + O(1).$$

The intuitive property (i) stated above is thus verified.

(b) A necessary and sufficient condition for the increasing sequence $a_1 < a_2 < a_3 < \dots$ to be of natural density α, $0 \leqslant \alpha \leqslant 1$, is that

$$\lim_{n\to\infty} n/a_n = \alpha. \tag{1.3}$$

The condition is clearly sufficient. We see that it is necessary by noting that, if $\{a_j\}_{j=1}^{\infty}$ has natural density α, then

$$n = \big|\{j : a_j \leqslant a_n\}\big| = \big\{\alpha + o(1)\big\}a_n \qquad (n \to \infty).$$

(c) There exist integer sequences failing to have natural density. Consider, for example, the sequence $\mathcal{A}$ of those integers n with leading digit equal to 1 in the expansion to base 10. We have

$$\mathcal{A} := \bigcup_{k\geqslant 0} \big\{n : 10^k \leqslant n < 2{\cdot}10^k\big\}. \tag{1.4}$$

Writing $A(x) := \big|\mathcal{A} \cap [1, x]\big|$, it follows that, for $m \geqslant 1$,

$$A\big(10^m - 1\big) = \sum_{0\leqslant k<m} 10^k = \tfrac{1}{9}\big(10^m - 1\big),$$

$$A\big(2{\cdot}10^m - 1\big) = \tfrac{1}{9}(10^m - 1) + 10^m = \tfrac{5}{9}\big(2{\cdot}10^m - 1\big) + \tfrac{4}{9}.$$

We easily infer that

$$\underline{\mathbf{d}}\,\mathcal{A} = \tfrac{1}{9}, \qquad \overline{\mathbf{d}}\,\mathcal{A} = \tfrac{5}{9}.$$

(d) A formal link between the notion of density and probability theory can be defined. In the case of natural density, it suffices to observe that, if ν_N denotes the probability measure on $\mathbb{N}^*$ obtained by assigning the uniform weight $1/N$ to each of the first N integers, then we have, subject to existence,

$$\mathbf{d}\mathcal{A} = \lim_{N\to\infty} \nu_N(\mathcal{A}).$$

This explains why the natural density echoes intuitive criteria: the density of a sequence is the limit of its frequency among the first N integers.

1.2. Logarithmic density

The density most used after the natural density is that which is obtained by choosing $\lambda_n = 1/n$ for $n \geqslant 1$. The concept thus defined is called *logarithmic density*. The traditional notation is $\boldsymbol{\delta}\mathcal{A}$, so, assuming existence,

$$\boldsymbol{\delta}\mathcal{A} := \lim_{x\to\infty} \frac{1}{\ln x} \sum_{a\leqslant x,\, a\in\mathcal{A}} \frac{1}{a}. \tag{1.5}$$

The upper $\overline{\boldsymbol{\delta}}\mathcal{A}$ and lower $\underline{\boldsymbol{\delta}}\mathcal{A}$ logarithmic densities are defined in an obvious way.

It is easy to construct examples of sequences failing to possess logarithmic density. The following theorem makes clear that they are to be sought amongst the sequences that do not have a natural density.

Theorem 1.2. *For any integer sequence $\mathcal{A}$, we have*

$$\underline{\mathbf{d}}\,\mathcal{A} \leqslant \underline{\boldsymbol{\delta}}\mathcal{A} \leqslant \overline{\boldsymbol{\delta}}\mathcal{A} \leqslant \overline{\mathbf{d}}\,\mathcal{A}. \tag{1.6}$$

In particular, if the sequence $\mathcal{A}$ has a natural density, then it also has a logarithmic density and the two are equal.

Proof. Define $A(x) := \sum_{a\leqslant x} 1$, and $L(x) := \sum_{a\leqslant x} 1/a$, where the sums are over elements a of $\mathcal{A}$. By partial summation, we have

$$L(x) = \frac{A(x)}{x} + \int_1^x \frac{A(t)}{t^2}\,\mathrm{d}t \qquad (x \geqslant 1). \tag{1.7}$$

Let $\varepsilon > 0$. There exists some $t_0 = t_0(\varepsilon)$ such that

$$\underline{\mathbf{d}}\,\mathcal{A} - \varepsilon \leqslant A(t)/t \leqslant \overline{\mathbf{d}}\mathcal{A} + \varepsilon \qquad (t > t_0).$$

Substituting in (1.7) for $x > t_0$, we infer that

$$\big(\underline{\mathbf{d}}\,\mathcal{A} - \varepsilon\big)\ln\big(x/t_0\big) \leqslant L(x) \leqslant 1 + \ln t_0 + \big(\overline{\mathbf{d}}\mathcal{A} + \varepsilon\big)\ln\big(x/t_0\big).$$

The stated result follows from these bounds upon letting x tend to ∞ and then ε to 0. □

The converse of Theorem 1.2 is false: the existence of logarithmic density in no way implies that of natural density. A counter-example is provided by the sequence (1.4). The following computation shows that it has a logarithmic density $\boldsymbol{\delta}\mathcal{A} = (\ln 2)/\ln 10$. Indeed

$$L(x) = \sum_{a\leqslant x}\frac{1}{a} = \sum_{0\leqslant k\leqslant \ln x/\ln 10}\ \sum_{\substack{10^k\leqslant n<2\cdot 10^k\\ n\leqslant x}}\frac{1}{n}$$

$$= \sum_{0\leqslant k\leqslant \ln x/\ln 10}\Big\{\ln 2 + O\Big(\frac{1}{k+1}\Big)\Big\} + O(1) = \frac{\ln 2}{\ln 10}\ln x + O(\ln_2 x).$$

1.3. Analytic density

The method described in § 1.1 for defining the density of an integer sequence can be formally generalized. Instead of truncating a divergent series $\sum_{n\geqslant 1}\lambda_n$, we consider a continuous family $(P_\sigma)_{\sigma\in S}$ of probability laws on $\mathbb{N}^*$ and define

$$P_\sigma(\{n\}) =: \lambda_n(\sigma)\Big/\sum_{m\geqslant 1}\lambda_m(\sigma)$$

where each series $\sum_{m\geqslant 1}\lambda_m(\sigma)$ ($\sigma\in S$) is convergent. In addition, we consider a point σ_0, in the closure of S but not belonging to S, such that the series $\sum_{m\geqslant 1}\lambda_m(\sigma_0)$, where each term is defined by continuity, diverges. We then define $d(\mathcal{A})$ as the possible limit of the ratio

$$P_\sigma(\mathcal{A}) = \sum_{n\in\mathcal{A}}\lambda_n(\sigma)\Big/\sum_{m\geqslant 1}\lambda_m(\sigma) \tag{1.8}$$

as $\sigma\to\sigma_0$ while remaining in S. The case of Section 1.1 corresponds to $S :=]0,1]$, with $\sigma_0 := 0$, and

$$\lambda_n(\sigma) := \begin{cases}\lambda_n & \big(n\leqslant 1/\sigma\big)\\ 0 & \big(n>1/\sigma\big).\end{cases}$$

The convergence of the series $\sum_{m\geqslant 1}\lambda_m(\sigma)$ for $\sigma\in S$ implies, for each $\varepsilon>0$, the existence of an integer $N = N(\varepsilon,\sigma)$ such that

$$P_\sigma(\mathcal{A}) = \Big(\sum_{n\leqslant N,\, n\in\mathcal{A}}\lambda_n(\sigma)\Big/\sum_{m\leqslant N}\lambda_m(\sigma)\Big) + \vartheta\varepsilon,$$

with $|\vartheta|\leqslant 1$. By choosing $\varepsilon = \varepsilon(\sigma)\to 0$ as $\sigma\to\sigma_0$, we hence recover a definition analogous to that of Section 1.1, but in which the function λ_n also depends on x. In certain circumstances, it may be established by a Tauberian technique that there exists an equivalent procedure which is strictly of type (1.1). Even then, such a framework can be useful: when the series

$\sum \lambda_n(\sigma)$ are well chosen, considering (1.8) instead of (1.1) can notably simplify the calculations, or favor the use of certain analytic techniques. This stems from replacing truncation by a smoother procedure.

The basic example is obtained from the choice $S :=]1, \infty[$, $\sigma_0 := 1$ and $\lambda_n(\sigma) := 1/n^\sigma$ $(n \geqslant 1)$. This yields

$$P_\sigma(\mathcal{A}) = \frac{1}{\zeta(\sigma)} \sum_{n \in \mathcal{A}} \frac{1}{n^\sigma}. \tag{1.9}$$

The presence of the Dirichlet series associated to the indicator function of $\mathcal{A}$ opens the possibility of employing all the analytic and algebraic properties of this class of series—especially those connected to the convolution product—for the computation of density.

The *analytic density* of a sequence $\mathcal{A}$ is defined as the possible limit of the expression (1.9) as $\sigma \to 1+$. Instead of (1.9), we may, of course, equally well consider the quantity

$$(\sigma - 1) \sum_{n \in \mathcal{A}} \frac{1}{n^\sigma} \tag{1.10}$$

but it is often convenient to retain the factor $1/\zeta(\sigma)$ when Euler products are involved.

The expected connection between analytic density and a density of type (1.1) is made explicit in the following result.

Theorem 1.3. *Let $\mathcal{A}$ be an integer sequence. Then $\mathcal{A}$ has analytic density if, and only if, it has logarithmic density. In this case, the two densities are equal.*

Proof. Let us retain the notation $L(x) = \sum_{a \leqslant x} 1/a$ where summation is restricted to elements a of $\mathcal{A}$. By partial summation, we have

$$(\sigma - 1) \sum \frac{1}{a^\sigma} = (\sigma - 1)^2 \int_1^\infty \frac{L(x)}{x^\sigma} \, \mathrm{d}x \qquad (\sigma > 1). \tag{1.11}$$

Suppose first that $\mathcal{A}$ has logarithmic density $\delta = \boldsymbol{\delta}\mathcal{A}$, i.e.,

$$L(x) = \{\delta + o(1)\} \ln x \qquad (x \to \infty).$$

Substituting in the right-hand side of (1.11), we infer that

$$(\sigma - 1) \sum \frac{1}{a^\sigma} = \delta + o(1) \qquad (\sigma \to 1+); \tag{1.12}$$

thus $\mathcal{A}$ has analytic density, equal to δ.

Conversely, if (1.12) holds, we can rewrite (1.11) in the following form, with $h := \sigma - 1$,

$$h \int_0^\infty \mathrm{e}^{-ht} \, \mathrm{d}L(\mathrm{e}^t) = h^2 \int_1^\infty L(x) \frac{\mathrm{d}x}{x^{1+h}} = \delta + o(1) \qquad (h \to 0+).$$

Karamata's Theorem II.7.5 then implies

$$L(\mathrm{e}^t) = \{\delta + o(1)\}t \qquad (t \to \infty),$$

which is equivalent to the required result. □

1.4. Probabilistic number theory

The concepts introduced in the previous sections form the basis of a new branch of number theory. The key idea is that of natural density, which sheds new light on arithmetic functions.

Indeed, these functions usually have the specific property of varying in an intrinsically irregular and erratic manner, with the consequence that classical techniques of analysis are generally powerless to describe their behavior appropriately. Probabilistic number theory corresponds to the challenge, arising naturally in such circumstances, to undertake a statistical study of this behavior. Together with the notions of extremal and average orders, which allow a cursory classification, we shall also define (cf. Chapter III.3) the notion of a *normal order* of an arithmetic function, designed to reflect its "almost certain" behavior. In practice, this involves a process of neglecting a set of integers of zero density (obviously depending on the function considered) so as to eliminate aberrant values. Strikingly, this approach results in order and regularity suddenly emerging from apparent intrinsic chaos. The illuminating focus of the "almost everywhere" concept reveals a new field of investigation, requiring specific methods and yielding distinctive results.

Thus, as remarked by Delange (1982), one ought rather to speak of the "probabilistic theory of arithmetic functions". The typical viewpoint (see remark (d) in § 1.1) is that of considering an arithmetic function f as a random variable on the discrete space formed by the first N integers and equipped with the uniform law. The fundamental question then consists in determining in what sense(s) we can assert that the law of f tends toward a limit law as $N \to \infty$. We shall make this precise in the following chapters.

Notes

§§ 1.1–1.3. Many other types of densities for an integer sequence have been defined in the literature. Let us mention three.

(a) The *multiplicative density* of Davenport & Erdős (1951), connected with the distribution of $\mathcal{A}$ among the different subsequences of $\mathbb{N}^*$ obtained by removing those integers having a "large" prime factor—cf. Exercise 246.

(b) The *Schnirelmann* (1930) density, defined by $\sigma(\mathcal{A}) = \inf_{n\geqslant 1} A(n)/n$. It is connected with the *addition of sequences*; if we define

$$\mathcal{A}+\mathcal{B} := \{a+b : a\in\mathcal{A},\, b\in\mathcal{B}\},$$

an important theorem due to Mann (1942) states that

$$\sigma(\mathcal{A}+\mathcal{B}) \geqslant \min\big\{1, \sigma(\mathcal{A})+\sigma(\mathcal{B})\big\}. \tag{1.13}$$

A fairly simple proof of (1.13) may be found in Halberstam & Roth (1983), chap. I, § 4.

(c) The *divisor density* of Hall (1978). When it exists, this is the unique number $\mathbf{D}\mathcal{A}$ satisfying

$$\sum_{d|n,\, d\in\mathcal{A}} 1 = \big\{\mathbf{D}\mathcal{A}+o(1)\big\}\tau(n) \qquad \text{pp},$$

where the symbol pp (for the French *presque partout*, i.e. almost everywhere) indicates that the relation thus marked occurs as $n\to\infty$ inside some suitable sequence of natural density 1. This definition is quite different from those in §§ 1.1–1.3. For example, for all α,β in $[0,1]$ we can find a sequence $\mathcal{A}$ such that $\mathbf{d}\mathcal{A}=\alpha$, $\mathbf{D}\mathcal{A}=\beta$ (Hall, 1978). Other properties may be found in Hall (1981), Tenenbaum (1982), Dupain, Hall & Tenenbaum (1982), Hall & Tenenbaum (1986). See also Exercises 272 and 273.

§ 1.3. A deeper study of the properties of arithmetic functions in connection with the laws $P_\sigma(\mathcal{A})$ has been undertaken by Nanopoulos (1975, 1977, 1982).

Exercises

Recall that we denote by $P^+(n)$ the largest prime factor of an integer n, with the convention that $P^+(1) = 1$. Except in Exercise 252, we define, for $y \geqslant 2$, and $\mathcal{A} \subseteq \mathbb{N}^*$,

$$\mathcal{A}_y := \mathcal{A} \cap \{n : P^+(n) \leqslant y\}.$$

For each integer $j \geqslant 1$, we let $\mathcal{A}^{(j)}$ denote the finite sequence comprising the j smallest elements of $\mathcal{A}$ and we make the convention that $\mathcal{A}^{(0)} = \varnothing$.

245. For $n \geqslant 1$, write $n_y := \max\{d : d|n,\ P^+(d) \leqslant y\}$. Let $\mathcal{A} \subseteq \mathbb{N}^*$ be an integer sequence satisfying, for some $y \geqslant 2$, $\mathcal{A} = \{n : n_y \in \mathcal{A}_y\}$. Show that, for $s \in \mathbb{C}$, $\sigma > 1$, we have

$$\sum_{n\in\mathcal{A}} \frac{1}{n^s} = \zeta(s) \prod_{p\leqslant y} \Big(1 - \frac{1}{p^s}\Big) \sum_{a\in\mathcal{A}_y} \frac{1}{a^s}\cdot$$

Deduce the existence of $\mathbf{d}\mathcal{A}$ and the formula

$$\mathbf{d}\mathcal{A} = \prod_{p\leqslant y} \big(1 - \frac{1}{p}\big) \sum_{a\in\mathcal{A}_y} \frac{1}{a}\cdot$$

246. *Multiplicative density (Davenport & Erdős, 1951).*

For $y \geqslant 2$, and $\mathcal{A} \subseteq \mathbb{N}^*$, we define

$$\mathbf{m}_y\mathcal{A} := \prod_{p\leqslant y} \big(1 - \frac{1}{p}\big) \sum_{a\in\mathcal{A}_y} \frac{1}{a}\cdot$$

If $\mathbf{m}_y\mathcal{A}$ tends to a limit $\mathbf{m}\mathcal{A}$ as $y \to \infty$, we say that $\mathbf{m}\mathcal{A}$ is the multiplicative density of $\mathcal{A}$. We also set

$$\overline{\mathbf{m}}\mathcal{A} := \limsup_{y\to\infty} \mathbf{m}_y\mathcal{A}, \qquad \underline{\mathbf{m}}\mathcal{A} := \liminf_{y\to\infty} \mathbf{m}_y\mathcal{A}.$$

(a) Show that, for all $\mathcal{A}$, we have $0 \leqslant \underline{\mathbf{m}}\mathcal{A} \leqslant \overline{\mathbf{m}}\mathcal{A} \leqslant 1$.

(b) Show that, for any integer sequence $\mathcal{A}$, we have $\overline{\boldsymbol{\delta}}\mathcal{A} \leqslant \mathrm{e}^{\gamma}\,\overline{\mathbf{m}}\mathcal{A}$.

(c) Let $\mathcal{A} := \{n \geqslant 1 : P^+(n) \leqslant \sqrt{n}\}$. Show that

$$\mathbf{d}\mathcal{A} = 1 - \ln 2, \qquad \mathbf{m}\mathcal{A} = 1 - \mathrm{e}^{-\gamma}.$$

247. *Sequential density of a set of multiples.*[2]

Let $\mathcal{A}$ be an integer sequence. Its *set of multiples* $\mathcal{M}(\mathcal{A})$ is the subset of $\mathbb{N}^*$ defined by $\mathcal{M}(\mathcal{A}) := \{am : a \in \mathcal{A},\ m \geqslant 1\}$.[3]

[2] Davenport & Erdős (1951).

[3] See Halberstam & Roth (1966), Erdős, Hall & Tenenbaum (1994).

(a) Show that, for each $j \geqslant 1$, $\mathcal{M}_j := \mathcal{M}(\mathcal{A}^{(j)}) \setminus \mathcal{M}(\mathcal{A}^{(j-1)})$ has natural density $\mathbf{d}\mathcal{M}_j = \Delta_j(\mathcal{A})$ given by

$$\Delta_j(\mathcal{A}) := \frac{1}{a_j} + \sum_{1 \leqslant k \leqslant j-1} (-1)^k \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant j-1} \frac{1}{[a_{i_1}, \ldots, a_{i_k}, a_j]},$$

where a_j denotes the jth element of $\mathcal{A}$.

(b) Show that $\Delta(\mathcal{A}) := \sum_{j \geqslant 1} \Delta_j(\mathcal{A})$ is finite and satisfies $0 \leqslant \Delta(\mathcal{A}) \leqslant 1$. We say that $\Delta(\mathcal{A})$ is the *sequential density* of the set of multiples $\mathcal{M}(\mathcal{A})$.

(c) Show that, if $\sum_{j \geqslant 1} 1/a_j < \infty$, then $\mathcal{M}(\mathcal{A})$ has natural density and $\mathbf{d}\mathcal{M}(\mathcal{A}) = \Delta(\mathcal{A})$.

248. Let $\mathcal{A} \subseteq \mathbb{N}^*$, $y \geqslant 2$.

(a) Deduce from the results of Exercises 245 and 247 that

$$\mathbf{d}\mathcal{M}(\mathcal{A}_y) = \Delta(\mathcal{A}_y) = \mathbf{m}_y\mathcal{M}(\mathcal{A}).$$

(b) Show that $\mathbf{m}_y\mathcal{M}(\mathcal{A})$ is an increasing function of y.

(c) Let $j \geqslant 1$. Show that, for sufficiently large y, we have

$$\Delta_j(\mathcal{A}_y) = \Delta_j(\mathcal{A}).$$

Deduce that $\mathbf{m}\mathcal{M}(\mathcal{A}) \geqslant \Delta(\mathcal{A})$.

(d) Show that $\Delta(\mathcal{A}_y) \leqslant \Delta(\mathcal{A})$. Deduce that $\mathbf{m}\mathcal{M}(\mathcal{A}) = \Delta(\mathcal{A})$, in other words: *Any set of multiples has multiplicative density, equal to its sequential density* (Davenport–Erdős, 1951).

249. *The Davenport–Erdős theorem (1951).*

Let $\mathcal{A} \subseteq \mathbb{N}^*$, $y \geqslant 2$.

(a) Deduce from Exercise 245 that $\mathbf{d}\mathcal{M}(\mathcal{A}_y) = \mathbf{m}_y\mathcal{M}(\mathcal{A})$.

(b) Let $x > y$. Show that

$$\sum_{\substack{n \in \mathcal{M}(\mathcal{A}) \setminus \mathcal{M}(\mathcal{A}_y) \\ P^+(n) \leqslant x}} \frac{1}{n} = \prod_{p \leqslant x} \Big(1 - \frac{1}{p}\Big)^{-1} \big\{\mathbf{m}_x\mathcal{M}(\mathcal{A}) - \mathbf{m}_y\mathcal{M}(\mathcal{A})\big\}.$$

(c) By applying the result of Exercise 248, show that

$$\overline{\boldsymbol{\delta}}\mathcal{M}(\mathcal{A}) \leqslant \mathbf{m}\mathcal{M}(\mathcal{A}).$$

(d) Show that $\mathbf{m}\mathcal{M}(\mathcal{A}) = \boldsymbol{\delta}\mathcal{M}(\mathcal{A}) = \Delta(\mathcal{A}) = \underline{\mathbf{d}}\,\mathcal{M}(\mathcal{A})$, in other words: *Any set of multiples has a logarithmic density equal to its lower natural density, as well as to its multiplicative and sequential densities.*[4]

[4] A set of multiples does not necessarily have a natural density, cf. Exercise 271.

250. *The Davenport–Erdős theorem (proof of 1937).*

Let $\mathcal{A} \subseteq \mathbb{N}^*$. For $j \geqslant 1$, let $\vartheta_j(n)$ denote the set-theoretic indicator function of $\mathcal{M}_j := \mathcal{M}(\mathcal{A}^{(j)}) \setminus \mathcal{M}(\mathcal{A}^{(j-1)})$ and put $\Theta_j(n) := \sum_{1\leqslant i\leqslant j} \vartheta_i(n)$. We consider the Dirichlet series

$$F_j(s) := \sum_{n\geqslant 1} \frac{\vartheta_j(n)}{n^s}, \qquad F(s) := \sum_{j\geqslant 1} F_j(s) = \sum_{n\in\mathcal{M}(\mathcal{A})} \frac{1}{n^s},$$
$$G_j(s) := F_j(s)/\zeta(s), \qquad G(s) := F(s)/\zeta(s).$$

(a) Show that, for $n \geqslant 1$, $j \geqslant 1$, we have

$$\Theta_j(n) \ln n \geqslant \sum_{d|n} \Theta_j(d)\Lambda(n/d).$$

Deduce that $\sum_{1\leqslant i\leqslant j} G_i(\sigma)$ is a decreasing function of $\sigma > 1$.

(b) With the notation of Exercise 247, show that $G_j(1) = \Delta_j(\mathcal{A})$.

(c) Show that $\lim_{\sigma\to 1+} G(\sigma) = \Delta(\mathcal{A})$.

(d) Show that $\boldsymbol{\delta}\mathcal{M}(\mathcal{A}) = \Delta(\mathcal{A}) \geqslant \underline{\mathbf{d}}\,\mathcal{M}(\mathcal{A})$.

(e) Show that, for each $j \geqslant 1$, we have $\underline{\mathbf{d}}\,\mathcal{M}(\mathcal{A}) \geqslant \sum_{1\leqslant i\leqslant j} \Delta_i(\mathcal{A})$. Deduce that $\underline{\mathbf{d}}\,\mathcal{M}(\mathcal{A}) = \Delta(\mathcal{A})$.

251. *A theorem of Rényi (1955).*

Let $z \in \mathbb{C}$. Write $\varphi_z(n) := z^{\Omega(n)-\omega(n)}$, $\lambda_z(n) := (\varphi_z * \mu)(n)$.

(a) Show that, for $|z| < 2$, we have $\sum_{n\geqslant 1} |\lambda_z(n)|/n < +\infty$.

(b) Deduce an asymptotic formula for $\sum_{n\leqslant x} \varphi_z(n)$.

(c) Show that, for each integer $k \geqslant 0$, the sequence $\{n : \Omega(n)-\omega(n) = k\}$ has natural density d_k, given by the formula

$$\sum_{k\geqslant 0} d_k z^k = \frac{6}{\pi^2} \prod_p \Big(\frac{1 - z/(p+1)}{1 - z/p}\Big) \qquad (|z| < 2).$$

252. *Direct factors of* $\mathbb{N}^*$.

Two subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{N}^*$ are said to form a pair of direct factors if $1 \in \mathcal{A}\cap\mathcal{B}$ and if each integer $n > 1$ decomposes uniquely as a product $n = ab$ with $a \in \mathcal{A}$, $b \in \mathcal{B}$. When this is so, we write $a = \pi_A(n)$, $b = \pi_B(n)$, with the convention that $\pi_A(1) = \pi_B(1) = 1$. For $y \geqslant 2$, $n \geqslant 1$, we denote by n_y the largest divisor of n free of prime factors $> y$, so that $n_y := \prod_{p^\nu \| n,\, p\leqslant y} p^\nu$, and set

$$\mathcal{A}_y := \{n : n \in \mathbb{N}^*,\, n_y \in \mathcal{A}\}, \quad A_y(x) := |\mathcal{A}_y \cap [1, x]|, \quad A(x) := |\mathcal{A} \cap [1, x]|.$$

Throughout the exercise, we let a (resp. b) denote generically an integer in $\mathcal{A}$ (resp. $\mathcal{B}$) where $(\mathcal{A}, \mathcal{B})$ is a given pair of direct factors of $\mathbb{N}^*$.

(a) Show that, for each $y \geqslant 2$, we have

$$\sum_{P^+(a)\leqslant y} \frac{1}{a} \sum_{P^+(b)\leqslant y} \frac{1}{b} = \prod_{p\leqslant y} \Big(1 - \frac{1}{p}\Big)^{-1}.$$

(b) Show the existence of $\mathbf{d}\mathcal{A}_y$ and the formula

$$\mathbf{d}\mathcal{A}_y = \Big(\sum_{P^+(b)\leqslant y} \frac{1}{b} \Big)^{-1}.$$

(c) Let $\varphi_y : \mathcal{A} \to \mathcal{A}_y$ be the map defined by $\varphi_y(a) = \pi_A(a_y)a/a_y$. Show that if $\varphi_y(a) = \varphi_y(a')$, then $a\pi_B(a'_y) = a'\pi_B(a_y)$. Deduce that φ_y is injective and establish that $A(x) \leqslant A_y(x)$ for $x \geqslant 1$, $y \geqslant 2$.

(d) Show that if $\sum 1/b = \infty$ then $\mathbf{d}\mathcal{A} = 0$.

(e) We now assume that $\sum 1/b < \infty$. Let α and β be the respective indicator functions of $\mathcal{A}$ and $\mathcal{B}$. Show that $\alpha = \mathbf{1} - \alpha * (\beta - \delta)$. Using the result of question (c) above, deduce that, for $y \geqslant 2$, we have

$$\underline{\mathbf{d}}\mathcal{A} \geqslant \Big(\sum_{P^+(b)\leqslant y} \frac{1}{b} \Big)^{-1} \Big(1 - \sum_{P^+(b)>y} \frac{1}{b} \Big).$$

(f) Show that $\mathcal{A}$ has a natural density, given by the formula

$$\mathbf{d}\mathcal{A} = \Big(\sum_{b\in\mathcal{B}} \frac{1}{b} \Big)^{-1}$$

where the right-hand side is interpreted as 0 when the series diverges.[5]

[5] This result is due to Saffari (1976) and Erdős, Saffari & Vaughan (1979). The proof presented here is essentially that of Daboussi (1979).