1. Normal order of \( \omega(n) = \sum_{p \mid n} 1 \)

Recall that we defined \( \omega(n) = \sum_{p \mid n} 1 \) and showed, using Mertens’ theorem, that the mean value is \( \log \log n \):

\[
\sum_{n \leq x} \omega(n) = \sum_{n \leq x} \sum_{p \mid n} 1 = \sum_{p \leq x} \left( \frac{x}{p} + O(1) \right) = x \log \log x + O(x) .
\]

In this section we will give a proof of a theorem of Hardy and Ramanujan (1917) stating that for almost all \( n \) that \( \omega(n) = \log \log n (1 + o(1)) \). This means very large integers typically have very few prime factors.

**Definition.** The **density** of a subset \( S \subset \mathbb{N}_{\geq 1} \) is

\[
\lim_{N \to \infty} \frac{|S \cap \{1, 2, \ldots, N\}|}{N}
\]

provided that the limit exists.

**Examples.**
- the density of the even positive integers is \( 1/2 \)
- Chebyshev’s theorem implies the density of the prime numbers is zero.
- We will see that the density of the square-free numbers is \( 1/\zeta(2) \).

**Theorem 1.1** (Hardy-Ramanujan). There exists a density one sub-sequence of positive integers \( \{n_j\} \) such that

\[
\omega(n_j) = \log \log n_j (1 + o(1)) \quad (j \to \infty).
\]

To prove the theorem we will calculate the variance of \( \omega(n) \) and apply Chebyshev’s inequality. This proof was discovered by Turán (1934).

**Lemma 1.2** (Turán).

\[
(1) \quad \sum_{n \leq x} (\omega(n) - \log \log x)^2 = O(x \log \log x)
\]

*Date: March 9, 2022.*
Proof. Squaring out gives
\[
\sum_{n \leq x} (\omega(n) - \log \log x)^2 = \sum_{n \leq x} \omega(n)^2 - 2 \log \log x \sum_{n \leq x} \omega(n) + |x| (\log \log x)^2.
\]
By the lemma we can evaluate the middle term so the left-hand side equals
\[
\sum_{n \leq x} \omega(n)^2 - x (\log \log x)^2 + O(x \log \log x).
\]
To establish (1) it suffices to show that
\[
(2) \sum_{n \leq x} \omega(n)^2 \leq x (\log \log x)^2 + O(x \log \log x).
\]
Observe that
\[
\sum_{n \leq x} \omega(n)^2 = \sum_{n \leq x} \left( \sum_{p \mid n} 1 \right) \left( \sum_{p \mid n} 1 \right) = \sum_{p_1 \leq p_2 \leq x} \sum_{n \leq x} 1.
\]
First, we estimate the terms with \( p_1 = p_2 \)
\[
(4) \sum_{p \leq x} \sum_{n \leq x \atop p \mid n} 1 = \sum_{p \leq x} \left( \frac{x}{p} + O(1) \right) = x \log \log x + O(x).
\]
Next to estimate the terms with \( p_1 \neq p_2 \) note that both \( p_1 \) and \( p_2 \) divide \( n \) iff \( p_1 p_2 \mid n \). This gives that
\[
(5) \leq x \sum_{p_1 p_2 \leq x} \sum_{n \leq x \atop p_1 \neq p_2} \sum_{n \leq x \atop p \mid n, p \mid n} 1
\]
\[= \sum_{p_1 p_2 \leq x \atop p_1 \neq p_2} \left( \frac{x}{p_1 p_2} - \left\{ \frac{x}{p_1 p_2} \right\} \right) \]
\[\leq x \left( \sum_{p \leq x} \frac{1}{p} \right)^2 \leq x (\log \log x)^2 + O(x \log \log x).
\]
Applying (4) and (5) in (3) implies (2). \( \square \)

Proof of the Hardy-Ramanujan theorem. Let
\[
S = \left\{ n \geq 3 : \left| \omega(n) - \log \log n \right| \geq (\log \log n)^{3/4} \right\}
\]
Note that if \( n \notin S \), \((n \geq 3)\), then
\[
\omega(n) = \log \log n(1 + O(1/(\log \log n)^{1/4})).
\]
Therefore it suffices to prove that the density of \( S \) equals zero. For this purpose, we can ignore \( n \leq \sqrt{N} \), and then note that for \( \sqrt{N} < n \leq N \) we have \( \log \log n = \log \log N + O(1) \).

We use Chebyshev’s inequality:
\[
\text{Prob}(|Y - \mathbb{E}(Y)| > \delta) \leq \frac{1}{\delta^2} \mathbb{E}(|Y - \mathbb{E}(Y)|^2) = \frac{1}{\delta^2} \text{Var}(Y).
\]
Applying Chebyshev’s inequality we obtain
\[
\sum_{\sqrt{N} \leq n \leq N \atop n \in S} 1 = \sum_{\sqrt{N} < n \leq N \atop |\omega(n) - \log \log n| \geq (\log \log n)^{3/4}} 1 \leq \sum_{\sqrt{N} < n \leq N \atop |\omega(n) - \log \log n| \geq (\log \log n)^{3/4}} \left| \frac{\omega(n) - \log \log n}{(\log \log n)^{3/4}} \right|^2
\]
Applying Lemma 1.2 yields
\[
\sum_{\sqrt{N} \leq n \leq N \atop n \in S} 1 \ll \frac{1}{(\log \log N)^{3/2}} \sum_{\sqrt{N} < n \leq N} (\omega(n) - \log \log N + O(1))^2 \ll \frac{N}{(\log \log N)^{1/2}} = o(N).
\]
The implies the density of \( S \) is zero, which establishes the claim. \( \square \)

2. **Arithmetic functions**

2.1. Definition and examples of arithmetic functions. An arithmetic function is a complex-valued function on the positive integers \( \alpha : \mathbb{N}_{\geq 1} \to \mathbb{C} \).

Here are some examples:

- the constant function \( 1(n) = 1, \forall n \geq 1 \);
- the delta function \( \delta(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases} \);
- the Möbius function \( \mu \), defined for square-free integers \( n = p_1 \cdots p_k \) to be \((-1)^k\), and is zero otherwise. In particular \( \mu(1) = 1 \);
- the divisor function, giving the number of divisors of an integer:
  \[
  \tau(n) = \{(a, b) : a, b \geq 1, a \cdot b = n\} = \sum_{d|n} 1
  \]
  More generally, we have higher divisor functions, for integer \( r \geq 2 \), defined as
  \[
  \tau_r(n) = \{(a_1, \ldots, a_r) : a_j \geq 1, a_1 \cdot \ldots \cdot a_r = n\}
  \]
- the power functions \( n^s \)
Sum of divisors: If $s \in \mathbb{C}$ then set $\sigma_s(n) = \sum_{d|n} d^s$.

The von Mangoldt function $\Lambda(n) = \begin{cases} \log p, & n = p^k, k \geq 1 \\ 0, & \text{otherwise} \end{cases}$

The set of $\mathcal{A} = \mathbb{C}[\mathbb{N}_{\geq 1}]$ of all arithmetic functions form an algebra over $\mathbb{C}$ under addition and pointwise multiplication.

2.2. Dirichlet convolution. Another useful binary operation is called Dirichlet convolution: If $\alpha, \beta \in \mathcal{A}$, their convolution is defined as

$$\alpha \ast \beta(n) := \sum_{ab=n} \alpha(a)\beta(b) = \sum_{d|n} \alpha(d)\beta\left(\frac{n}{d}\right).$$

Here and elsewhere, the notation $\sum_{d|n}$ denotes the sum over all positive divisors of $n$.

Some elementary properties of Dirichlet convolution are
- Commutativity: $\alpha \ast \beta = \beta \ast \alpha$.
- Associativity $(\alpha \ast \beta) \ast \gamma = \alpha \ast (\beta \ast \gamma)$.
- The delta function is the neutral element for convolution: $\delta \ast \alpha = \alpha$, $\forall \alpha \in \mathcal{A}$.

Using Dirichlet convolution, we can express some of the arithmetic functions we have just seen in terms of others. For instance, by definition

$$\tau = 1 \ast 1$$

and more generally, for $r \geq 2$ (assuming $\tau_1 = 1$)

$$\tau_r = \tau_{r-1} \ast 1,$$

and the sum of divisors functions are given by

$$\sigma_s = 1 \ast n^s.$$

Exercise 1. Show that $\log = \Lambda \ast 1$, that is

$$\sum_{d|n} \Lambda(d) = \log n.$$

2.3. Multiplicative functions. An arithmetic function $\alpha$ is multiplicative if it satisfies $\alpha(1) = 1$ and for any coprime integers $m, n$,

$$\alpha(mn) = \alpha(m)\alpha(n), \quad \gcd(m, n) = 1.$$ (6)

A function is completely multiplicative if $\alpha(mn) = \alpha(m)\alpha(n)$ for any (not necessarily coprime) integers $m, n \geq 1$.

Note: Sometimes one defines a multiplicative function as any function which is not identically zero, and satisfies the relation (6); one then shows that necessarily $\alpha(1) = 1$.

Examples:
- The power functions $n^s$ and the constant function $1$ are strongly multiplicative.
- The delta function $\delta$ is strongly multiplicative.
• \( \mu \) is multiplicative by its definition.

It is clear from the definition that a multiplicative function is determined by its values on prime powers, since by induction if \( n = \prod_j p_j^{e_j} \) is the prime factorization of \( n \), then

\[
\alpha(n) = \prod_j \alpha(p_j^{e_j}).
\]

The basic property that we need it that convolution preserves multiplicativity:

**Proposition 2.1.** If \( \alpha, \beta \in \mathcal{A} \) are multiplicative, then so is \( \alpha \ast \beta \).

**Proof.** Suppose \( \gcd(m, n) = 1 \). Then we claim there is a bijection

\[
\{ \text{divisors } D \mid n \} \leftrightarrow \{ \text{ordered pairs of coprime integers } (c, d), \ c \mid m, \ d \mid n \}
\]

where the maps take \( (c, d) \mapsto c \cdot d =: D \) which is a divisor of \( mn \), and given a divisor \( D \) of \( m \cdot n \), it can be uniquely written as \( D = c \cdot d \) where \( c \mid m \) and \( d \mid n \). This is seen by taking the prime factorization \( m = \prod p_i^{a_i}, \ n = \prod j q_j^{b_j} \) where since \( m, n \) are coprime, \( p_i \neq q_j \). Then if \( D = \prod_i p_i^{u_i} \prod_j q_j^{v_j} \) is the factorization of \( D \), where necessarily \( u_i \leq a_i, \ v_j \leq b_j \) then take \( c = \prod_i p_i^{u_i} \) and \( d = \prod_j q_j^{v_j} \).

Then we compute

\[
\alpha \ast \beta(mn) = \sum_{D \mid mn} \alpha(D) \beta\left(\frac{mn}{D}\right)
\]

\[
= \sum_{c \mid m} \sum_{d \mid n} \alpha(cd) \beta\left(\frac{mn}{cd}\right)
\]

Since \( c, d \) are coprime, \( \alpha(cd) = \alpha(c)\alpha(d) \). Since \( m, n \) are coprime, so are \( m/c \) and \( n/d \) and hence \( \beta\left(\frac{mn}{cd}\right) = \beta\left(\frac{m}{c}\right)\beta\left(\frac{n}{d}\right) \). Hence we find

\[
(\alpha \ast \beta)(mn) = \sum_{c \mid m} \sum_{d \mid n} \alpha(c)\alpha(d) \beta\left(\frac{m}{c}\right)\beta\left(\frac{n}{d}\right)
\]

\[
= \sum_{c \mid m} \alpha(c)\beta\left(\frac{m}{c}\right) \sum_{d \mid n} \alpha(d)\beta\left(\frac{n}{d}\right) = (\alpha \ast \beta)(m) \cdot (\alpha \ast \beta)(n)
\]

proving multiplicativity, after noting that \( \alpha \ast \beta(1) = \alpha(1)\beta(1) = 1 \). \( \square \)

As a corollary, we immediately see that the divisor function \( \tau = \mathbf{1} \ast \mathbf{1} \) is multiplicative, and by induction so are the higher divisor functions \( \tau_r = \tau_{r-1} \ast 1 \).

### 2.4. the Möbius function

We can now use the above to prove a fundamental property of the Möbius function:
Proposition 2.2. $\mu * 1 = \delta$, that is
\[ \sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases} \]

Proof. Since $\mu$ and $1$ are multiplicative, so is $\mu * 1$; and so is $\delta$. Hence it suffices to prove the identity on prime powers. So for a prime power $p^e$, $e \geq 1$, the divisors are $\{1, p, \ldots, p^e\}$ and then
\[ (\mu * 1)(p^e) = \sum_{j=0}^e \mu(p^j) \]
Since $\mu(p^j) = 0$ for $j \geq 2$, and $e \geq 1$, we are left with
\[ \mu * 1(p^e) = \mu(1) + \mu(p) = 1 - 1 = 0 = \delta(p^e) \]
as claimed. $\square$

As a corollary we get the Möbius inversion formula: If $\alpha, \beta \in \mathcal{A}$ satisfy
\[ \alpha(n) = \sum_{d|n} \beta(d) \]
then we can recover $\beta$ from $\alpha$ by
\[ \beta(n) = \sum_{d|n} \mu(d) \alpha\left(\frac{n}{d}\right) \]
Indeed, the first relation says that $\alpha = \beta * 1$. Hence
\[ \alpha * \mu = (\beta * 1) * \mu = \beta * (1 * \mu) = \beta * \delta = \beta \]

2.5. Dirichlet series. An arithmetic function $\alpha \in \mathcal{A}$ has polynomial growth if there is some $A \geq 0$ so that $|\alpha(n)| \ll n^A$, for all $n \gg 1$.

For such an arithmetic function $\alpha$ of polynomial growth, we define an associated Dirichlet series $D_\alpha(s)$ by
\[ D_\alpha(s) := \sum_{n=1}^\infty \frac{\alpha(n)}{n^s} \]
This converges for all complex $s \in \mathbb{C}$ with $\Re(s) > A + 1$, and hence defines an analytic function in that half-plane.

Examples
- The Dirichlet series of $\delta$ is $D_\delta(s) = 1$.
- The constant function $1$ gives the Riemann zeta function
\[ D_\delta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \zeta(s), \quad \Re(s) > 1 \]

Lemma 2.3. If $\alpha, \beta \in \mathcal{A}$ have polynomial growth, then so does their convolution $\alpha * \beta$ and the corresponding Dirichlet series is the product
\[ D_{\alpha * \beta}(s) = D_\alpha(s)D_\beta(s), \quad \Re(s) \gg 1 \]
Proof. For $\Re(s) \gg 1$,

$$D_\alpha(s)D_\beta(s) = \sum \frac{\alpha(m)}{m^s} \sum \frac{\beta(n)}{n^s}$$

$$= \sum_{m,n \geq 1} \frac{\alpha(m)\beta(n)}{(nm)^s}$$

$$= \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{m,n \geq 1, m-n=N} \alpha(m)\beta(n)$$

$$= \sum_{N=1}^{\infty} \frac{1}{N^s} \alpha * \beta(N) = D_{\alpha*\beta}(s)$$

□

As a corollary we see that the Dirichlet series associated to the Möbius function is $1/\zeta(s)$:

$$(8) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}, \quad \Re(s) > 1$$

Indeed, by Möbius inversion,

$$1 = D_\delta(s) = D_{\mu*1}(s) = D_\mu(s) \cdot D_1(s)$$

and since $D_1(s) = \zeta(s)$ we are done.

An important property of the Dirichlet series associated to multiplicative functions is having an Euler product:

**Proposition 2.4.** If $\alpha$ is a multiplicative function of polynomial growth, then

$$D_\alpha(s) = \prod_{p \text{ prime}} \sum_{j=0}^{\infty} \frac{\alpha(p^j)}{p^{js}}, \quad \Re(s) \gg 1$$

As an example, we obtain Euler’s product for the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}, \quad \Re(s) > 1.$$  

3. **Application: The density of squarefree integers**

As a first application of the material of Section 2, we use a very simple sieve to find the density of squarefree integers.

An integer $n$ is *squarefree* if it has no square factors, that is if there is no $d > 1$ so that $d^2 \mid n$. Every integer $n \geq 1$ can be uniquely written in the form

$$n = fs^2, \quad f \text{ squarefree}$$

and $n$ is squarefree if and only if $s = 1$; we will write $s = s(n)$. 

Proposition 3.1. The number \( F(x) \) of squarefree integers up to \( x \) is

\[
\#\{n \leq x : \text{n squarefree}\} = \frac{x}{\zeta(2)} + O(\sqrt{x})
\]

Denote the indicator function of squarefrees by \( \mu_2 \):

\[
\mu_2(n) = \begin{cases} 
1, & \text{n squarefree} \\
0, & \text{otherwise}
\end{cases}
\]

We need a representation of \( \mu_2 \) using the Möbius function:

Lemma 3.2.

\[
\mu_2(n) = \sum_{d \mid n} \mu(d)
\]

Proof. We use the decomposition \( n = f(n)s(n)^2 \) with \( f(n) \) squarefree. Since \( n \) is squarefree if and only if \( s(n) = 1 \), we can write (recall \( \sum_{d \mid s} \mu(d) = 0 \) if \( s > 1 \))

\[
\mu_2(n) = \delta(s(n)) = \sum_{d \mid s(n)} \mu(d)
\]

Now \( d \mid s(n) \) if and only if \( d^2 \mid s(n)^2 \), and since \( f(n) \) is squarefree, this happens if and only if \( d^2 \mid n \). Thus

\[
\sum_{d \mid s(n)} \mu(d) = \sum_{d^2 \mid n} \mu(d)
\]

which proves our claim. \( \square \)

Proof of Proposition 3.1. Using Lemma 3.2, we write

\[
F(x) = \sum_{n \leq x} \mu_2(n) = \sum_{n \leq x} \sum_{d^2 \mid n} \mu(d).
\]

Now we switch order of summation, noting that the \( d \)'s will range up to \( \sqrt{x} \):

\[
F(x) = \sum_{d \leq \sqrt{x}} \sum_{n \leq x \atop d^2 \mid n} \mu(d)
\]

The number of \( n \leq x \), such that \( d^2 \mid n \) is

\[
\left\lfloor \frac{x}{d^2} \right\rfloor = \frac{x}{d^2} + O(1)
\]

and hence we find

\[
F(x) = \sum_{d \leq \sqrt{x}} \mu(d) \left( \frac{x}{d^2} + O(1) \right)
\]

\[
= x \sum_{d \leq \sqrt{x}} \frac{\mu(d)}{d^2} + O(\sum_{d \leq \sqrt{x}} 1)
\]
The series above is given by
\[
\sum_{d \leq \sqrt{x}} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O \left( \sum_{d > \sqrt{x}} \frac{1}{d^2} \right)
\]
where we have used \(|\mu(d)| \leq 1\). The infinite sum is, by (8)
\[
\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)}
\]
and thus we find
\[
F(x) = \frac{x}{\zeta(2)} + O(\sqrt{x})
\]
as claimed. \(\square\)

**Exercise 2.** Let \(k \geq 2\). An integer \(n\) is \(k\)-free if \(d^k \nmid n\) for all \(d > 1\). Show that the number of \(k\)-free integers up to \(x\) is \(x/\zeta(k) + O(x^{1/k})\).