3 Arithmetic functions

3.1 Some notational conventions

Divisor sums and products: Let \( n \in \mathbb{N} \).

- \( \sum_{d | n} f(d) \) denotes a sum of \( f(d) \), taken over all positive divisors \( d \) of \( n \).
- \( \sum_{p | n} f(p) \) denotes a sum of \( f(p) \), taken over all prime divisors \( p \) of \( n \).
- \( \sum_{p^\alpha || n} f(p^\alpha) \) denotes a sum of \( f(p^\alpha) \), taken over all prime powers \( p^\alpha \) that occur in the standard prime factorization of \( n \). (Here the double bar in \( p^\alpha || n \) indicates that \( p^\alpha \) is the exact power of \( p \) dividing \( n \), i.e., \( p^\alpha | n \), but \( p^\alpha+1 \nmid n \).)
- Products over \( d | n \), \( p | n \), etc., are defined analogously.

Empty sum/product convention: A sum over an empty set is defined to be 0; a product over an empty set is defined to be 1. Thus, for example, we have
\[
\sum_{p^\alpha || 1} f(p^\alpha) = 0, \quad \prod_{p^\alpha || 1} f(p^\alpha) = 1,
\]
since there is no prime power \( p^\alpha \) satisfying the condition \( p^\alpha || 1 \).

The above notational conventions greatly simplify the statements of formulas involving arithmetic functions. For example, using these conventions the rather clumsy formula
\[
\varphi(n) = \begin{cases} 
1 & \text{if } n = 1, \\
\prod_{i=1}^r p_i^{\alpha_i-1}(p_i - 1) & \text{if } n \geq 2 \text{ and } n = \prod_{i=1}^r p_i^{\alpha_i},
\end{cases}
\]
with distinct primes \( p_i \) and \( \alpha_i \in \mathbb{N} \),
can be rewritten as
\[
\varphi(n) = \prod_{p^\alpha || n} p^\alpha-1(p - 1),
\]
without having to introduce subscripts or single out the case \( n = 1 \). (In the latter case, the product is an empty product, so by the empty product convention, it produces the value 1, which is exactly what we need.)

Sums over 1’s (“Bateman summation”): A sum in which each summand is equal to 1 simply counts the number of terms in it; for example, \( \sum_{d | n} 1 \) is the same as \#\( \{ d \in \mathbb{N} : d \mid n \} \).
While this might seem like a contrived way to represent a counting function, in the context of the general theory of arithmetic functions, such representations are often very useful.

3.2 Multiplicative arithmetic functions

Definition 3.1 (Multiplicative arithmetic function). A function \( f : \mathbb{N} \to \mathbb{C} \) is called an arithmetic function. An arithmetic function \( f \) is called multiplicative if it satisfies the relation
\[
f(n_1n_2) = f(n_1)f(n_2)
\]
whenever \((n_1, n_2) = 1\). If (3.1) holds for all \(n_1, n_2 \in \mathbb{N}\) (i.e., without the restriction \((n_1, n_2) = 1\)), then \(f\) is called \textbf{completely multiplicative}.

**Proposition 3.2** (Multiplicative functions and prime factorization). An arithmetic function \(f\) that is not identically 0 (i.e., such that \(f(n) \neq 0\) for at least one \(n \in \mathbb{N}\)) is multiplicative if and only if it satisfies

\[
  f(n) = \prod_{p} p^{\alpha} f(p^\alpha) \quad (n \in \mathbb{N}).
\]

In particular, any multiplicative function \(f\) that is not identically 0 is uniquely determined by its values \(f(p^\alpha)\) at prime powers and satisfies \(f(1) = 1\).

### 3.3 The Euler phi function and the Carmichael Conjecture

**Definition 3.3** (Euler phi function). The Euler phi function is defined by

\[
  \varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}.
\]

**Proposition 3.4** (Properties of \(\varphi(n)\)).

1. (Multiplicativity) The Euler phi function is multiplicative (though not completely multiplicative).
2. (Explicit formula) For any \(n \in \mathbb{N}\),

\[
  \varphi(n) = \prod_{p^\alpha | n} p^{\alpha - 1}(p - 1) = n \prod_{p | n} \left(1 - \frac{1}{p}\right).
\]
3. (Gauss identity)

\[
  \sum_{d | n} \varphi(d) = n \quad (n \in \mathbb{N}).
\]

**Conjecture** (Carmichael conjecture). Given \(n \in \mathbb{N}\), the equation \(\varphi(x) = n\) has either no solution \(x \in \mathbb{N}\) or more than one solution.

**Remark.** The Carmichael conjecture has several local (UIUC) connections: Its originator, R.D. Carmichael, spent most of his career as a professor here at the U of I, and the conjecture first appeared as an “exercise” in a textbook on number theory he wrote (and which he presumably assigned to his students). Also, most of the current records on this conjecture are held by Kevin Ford, who earned his PhD here in the mid 1990s and is now back as a professor. In particular, Ford showed that the Carmichael conjecture is true for all \(n \leq 10^{10000}\). Moreover, for any \(k \in \mathbb{N}\) except possibly \(k = 1\), there exist infinitely many \(n \in \mathbb{N}\) such that the equation \(\varphi(x) = n\) has exactly \(k\) solutions \(x \in \mathbb{N}\). Thus, only the question of whether multiplicity \(k = 1\) can occur remains open, and this is precisely the question addressed by the Carmichael conjecture.
3.4 The number-of-divisors functions

Definition 3.5 (Number-of-divisors function). The **number-of-divisors function** is defined by
\[ \nu(n) = \# \{ d \in \mathbb{N} : d \mid n \} = \sum_{d \mid n} 1 \quad (n \in \mathbb{N}). \]

This function is often simply called the **divisor function**; alternate, and more common, notations for it are \( d(n) \) (for “divisor”) and \( \tau(n) \) (for “Teiler”, the German word for “divisor”).

Proposition 3.6 (Properties of \( \nu(n) \)).

(i) (Multiplicativity) The function \( \nu(n) \) is multiplicative (though not completely multiplicative).

(ii) (Explicit formula) For any \( n \in \mathbb{N} \),
\[ \nu(n) = \prod_{p^\alpha \mid n} (\alpha + 1) \]

3.5 The sum-of-divisors functions and perfect numbers

Definition 3.7. **Sum-of-divisors function** The **sum-of-divisors function** is defined by
\[ \sigma(n) = \sum_{d \mid n} d \quad (n \in \mathbb{N}). \]

Proposition 3.8 (Properties of \( \sigma(n) \)).

(i) (Multiplicativity) The function \( \sigma(n) \) is multiplicative (though not completely multiplicative).

(ii) (Explicit formula) For any \( n \in \mathbb{N} \),
\[ \sigma(n) = \prod_{p^\alpha \mid n} \frac{p^{\alpha+1} - 1}{p - 1} \]

Definition 3.9 (Perfect numbers). An positive integer \( n \) is called **perfect** if it is equal to the sum of its positive divisors \( d \mid n \), with \( 1 \leq d < n \) (i.e., not counting \( d = n \)). Equivalently, \( n \) is **perfect** if and only if \( \sigma(n) = 2n \).

Example. The first 4 perfect numbers are \( 6 = 1 + 2 + 3 \), \( 28 = 1 + 2 + 4 + 7 + 14 \), 496, and 8128.

Theorem 3.10 (Characterization of even perfect numbers). An even positive integer \( n \) is perfect if and only if it is of the form
\[ n = 2^{p-1}(2^p - 1), \]
where \( 2^p - 1 \) is a Mersenne prime.

Corollary 3.11. There exist infinitely many even perfect numbers if and only if there exist infinitely many Mersenne primes.

Example. The above four perfect numbers 6, 28, 496, 8128 correspond to the first four Mersenne primes, \( 2^2 - 1 = 3 \), \( 2^3 - 1 = 7 \), \( 2^5 - 1 = 31 \), and \( 2^7 - 1 = 127 \).
3.6 The Moebius function and the Moebius inversion formula

Definition 3.12 (Moebius function). The **Moebius function** is defined by

\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1, \\
(-1)^r & \text{if } n = p_1 p_2 \ldots p_r \text{ with distinct primes } p_i, \\
0 & \text{if } n \text{ is not squarefree, i.e., divisible by a prime power } p^\alpha \text{ with } \alpha > 1.
\end{cases}
\]

**Remark.** A very similar function is the **Liouville function** \(\lambda(n)\), which is defined as \((-1)^r\), where \(r\) is the total number of prime factors of \(n\), with multiple prime factors counted multiple times. If \(n\) is squarefree, then \(\lambda(n) = \mu(n)\), but if \(n\) is not squarefree, then \(\mu(n) = 0\), while \(\lambda(n) = \pm 1\) depending on whether \(n\) has an even or an odd number of prime factors.

While the Liouville function has a simpler definition and may seem the more natural of the two functions, the Moebius function is more useful and more important because of results such those below (which would not be valid for the Liouville function).

Proposition 3.13 (Properties of \(\mu(n)\)).

(i) **(Multiplicativity)** The Moebius function is multiplicative (though not completely multiplicative).

(ii) **(Moebius function identity)**

\[
\sum_{d|n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1, \\
0 & \text{otherwise}.
\end{cases}
\]

Theorem 3.14 (Moebius inversion formula). If \(f\) and \(g\) are arithmetic functions satisfying

\[
f(n) = \sum_{d|n} g(d) \quad (n \in \mathbb{N}),
\]

then

\[
g(n) = \sum_{d|n} f(d) \mu(n/d) = \sum_{d|n} \mu(d) f(n/d) \quad (n \in \mathbb{N}).
\]
3.7 Algebraic theory of arithmetic function

In this section we develop an algebraic theory of arithmetic functions based on the notion of a Dirichlet product. This allows us to restate many of the definitions and results encountered earlier in a simple, elegant, and natural form.

We begin by defining some “trivial” arithmetic functions that are needed in this theory and which can be used to build up other arithmetic functions.

Definition 3.15 (Trivial arithmetic functions). The unit function $1$, identity function $\text{id}$, and delta function $\delta$ are the arithmetic functions defined as follows:

- $1(n) = 1 \quad (n \in \mathbb{N})$,
- $\text{id}(n) = n \quad (n \in \mathbb{N})$,
- $\delta(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$

All three of these functions are multiplicative (in fact, completely multiplicative).

Definition 3.16 (Dirichlet product of arithmetic functions). Given two arithmetic functions $f$ and $g$, the Dirichlet product $f \star g$ is the arithmetic function defined by

$$(f \star g)(n) = \sum_{d|n} f(d)g(n/d) \quad (n \in \mathbb{N}).$$

Proposition 3.17 (Algebraic properties of Dirichlet product). Let $f, g, h$ be arithmetic functions.

(i) (Commutativity) $f \star g = g \star f$.
(ii) (Associativity) $(f \star g) \star h = f \star (g \star h)$.
(iii) (Identity element) $f \star \delta = \delta \star f = f$, where $\delta$ is defined as above, i.e., $\delta(1) = 1$ and $\delta(n) = 0$ if $n > 1$.
(iv) (Dirichlet inverse) If $f(1) \neq 0$, then $f$ has a unique Dirichlet inverse $f^{*^{-1}}$, in the sense that $f \star f^{*^{-1}} = \delta$.
(v) (Preservation of multiplicativity) The Dirichlet product of two multiplicative functions is multiplicative.
(vi) (Multiplicativity of inverse) The Dirichlet inverse of a multiplicative function is multiplicative.

Using the Dirichlet product notation, we can now restate many of the definitions, identities, and theorems on arithmetic functions encountered earlier in a simple, elegant, very natural, and easy-to-remember form.

Proposition 3.18 (Dirichlet product versions of identities for arithmetic functions).

(i) Gauss identity: $\varphi \star 1 = \text{id}$
(ii) Definition of the divisor function: $\nu = 1 \star 1$
(iii) Definition of the sum-of-divisors function: $\sigma = 1 \star \text{id}$
(iv) Möbius function identity: $\mu \star 1 = \delta$
(v) Möbius inversion formula: If $f = g \star 1$, then $g = f \star \mu = \mu \star f$. 
3.8 Arithmetic Functions: Summary Table

<table>
<thead>
<tr>
<th>Function</th>
<th>value at $n \in \mathbb{N}$</th>
<th>value at a prime $p$</th>
<th>value at a prime power $p^\alpha$</th>
<th>properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\delta(n)$ (delta function)</td>
<td>1 if $n = 1$, 0 else</td>
<td>0</td>
<td>0</td>
<td>completely multiplicative, $\delta \ast f = f \ast \delta = f$, identity element for Dirichlet product</td>
</tr>
<tr>
<td>$1(n)$ (unit function)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>completely multiplicative</td>
</tr>
<tr>
<td>$\text{id}(n)$ (identity function)</td>
<td>$n$</td>
<td>$p$</td>
<td>$p^\alpha$</td>
<td>completely multiplicative</td>
</tr>
<tr>
<td>$\mu(n)$ (Moebius function)</td>
<td>1 if $n = 1$, $(-1)^\nu$ if $n = \prod_{i=1}^r p_i$ ($p_i$ distinct), 0 otherwise</td>
<td>$-1$</td>
<td>$-1$ if $\alpha = 1$, 0 if $\alpha &gt; 1$</td>
<td>multiplicative, $\mu \ast 1 = \delta$ (Dirichlet inverse of 1)</td>
</tr>
<tr>
<td>$\nu(n)$ (= $d(n) = \tau(n)$) (number-of-divisors function)</td>
<td>$# {d \in \mathbb{N} : d \mid n}$</td>
<td>2</td>
<td>$\alpha + 1$</td>
<td>multiplicative, $\nu = 1 \ast 1$</td>
</tr>
<tr>
<td>$\varphi(n)$ (Euler phi function)</td>
<td>$# {1 \leq m \leq n : (m, n) = 1}$</td>
<td>$p - 1$</td>
<td>$p^\alpha - 1(p - 1)$</td>
<td>multiplicative, $\varphi \ast 1 = \text{id}$ (Gauss identity)</td>
</tr>
<tr>
<td>$\sigma(n)$ (sum-of-divisors function)</td>
<td>$\sum_{d \mid n} d$</td>
<td>$p + 1$</td>
<td>$p^{\alpha + 1} - 1 \over p - 1$</td>
<td>multiplicative, $\sigma = \text{id} \ast 1$</td>
</tr>
</tbody>
</table>

Table 1: Summary of important arithmetic functions