

Math 453: Elementary Number Theory  
Definitions and Theorems

Version 3/23/2008

# Chapter 3

## Arithmetic functions

### 3.1 Some notational conventions

**Divisor sums and products:** Let  $n \in \mathbf{N}$ .

- $\sum_{d|n} f(d)$  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

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1, \\ \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1) & \text{if } n \geq 2 \text{ and } n = \prod_{i=1}^r p_i^{\alpha_i} \\ & \text{with distinct primes } p_i \text{ and } \alpha_i \in \mathbf{N}, \end{cases}$$

can be rewritten as

$$\varphi(n) = \prod_{p^\alpha \parallel n} p^{\alpha-1}(p-1),$$

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  $\#\{d \in \mathbf{N} : d \mid n\}$ . 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 Arithmetic functions: Definitions and basic examples

Function	value at $n(\in \mathbf{N})$	value at a prime $p$	value at a prime power $p^\alpha$	properties
$\delta(n)$ (delta function)	1 if $n = 1$ , 0 else	0	0	completely multiplicative, $\delta \star f = f \star \delta = f$ , identity element for Dirichlet product
$\mathbf{1}(n)$ (unit function)	1	1	1	completely multiplicative
$\mathbf{i}(n)$ (identity function)	$n$	$p$	$p^\alpha$	completely multiplicative
$\mu(n)$ (Moebius function)	1 if $n = 1$ , $(-1)^r$ if $n = \prod_{i=1}^r p_i$ ( $p_i$ distinct), 0 otherwise	-1	-1 if $\alpha = 1$ , 0 if $\alpha > 1$	multiplicative, $\mu \star \mathbf{1} = \delta$ (Dirichlet inverse of $\mathbf{1}$ )
$\nu(n) (= d(n) = \tau(n)$ (number-of-divisors function)	$\#\{d \in \mathbf{N} : d \mid n\}$	2	$\alpha + 1$	multiplicative, $\nu = \mathbf{1} \star \mathbf{1}$
$\varphi(n)$ (Euler phi function)	$\#\{1 \leq m \leq n : (m, n) = 1\}$	$p - 1$	$p^{\alpha-1}(p - 1)$	multiplicative, $\varphi \star \mathbf{1} = \mathbf{i}$ (Gauss identity)
$\sigma(n)$ (sum-of-divisors function)	$\sum_{d \mid n} d$	$p + 1$	$\frac{p^{\alpha+1} - 1}{p - 1}$	multiplicative, $\sigma = \mathbf{i} \star \mathbf{1}$

Table 3.1: Summary of important arithmetic functions

**Definition (Multiplicative arithmetic function)** A function  $f : \mathbf{N} \rightarrow \mathbf{C}$  is called an **arithmetic function**. An arithmetic function  $f$  is called **multiplicative** if it satisfies the relation

$$(3.1) \quad f(n_1 n_2) = f(n_1) f(n_2)$$

whenever  $((n_1, n_2) = 1)$ . If (3.1) holds for **all**  $n_1, n_2 \in \mathbf{N}$  (i.e., without the restriction  $(n_1, n_2) = 1$ ), then  $f$  is called **completely multiplicative**.

**Proposition 3.1 (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  $n \in \mathbf{N}$ ) is multiplicative if and only if it satisfies*

$$f(n) = \prod_{p^\alpha || n} f(p^\alpha) \quad (n \in \mathbf{N}).$$

*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 algebra of arithmetic functions

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

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

**Proposition 3.2 (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  $f \star f^{*-1} = \delta$ .

**Proposition 3.3 (Dirichlet product of multiplicative functions)** *If  $f$  and  $g$  are multiplicative, then so is their Dirichlet product  $f \star g$ .*

### 3.4 The Moebius function and the Moebius inversion formula

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

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

**Proposition 3.4 (Properties of  $\mu(n)$ )**

- (i) *(Multiplicativity) The Moebius function is multiplicative (though not completely multiplicative).*
- (ii) *(Inverse of the unit function) The function  $\mu$  is the Dirichlet product inverse of the function  $\mathbf{1}$ :  $\mu \star \mathbf{1} = \mathbf{1} \star \mu = \delta$ ; explicitly,*

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

**Theorem 3.5 (Moebius inversion formula)** *If  $f$  and  $g$  are arithmetic functions related by  $f = g \star \mathbf{1}$ , then  $g = f \star \mu = \mu \star f$ ; explicitly, if*

$$f(n) = \sum_{d|n} g(d) \quad (n \in \mathbf{N}),$$

then

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

### 3.5 The Euler phi function. The Carmichael conjecture

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

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

**Proposition 3.6 (Properties of  $\varphi(n)$ )**

- (i) *(Multiplicativity) The Euler phi function is multiplicative (though not completely multiplicative).*
- (ii) *(Explicit formula) For any  $n \in \mathbf{N}$ ,*

$$\varphi(n) = \prod_{p^\alpha || n} p^{\alpha-1} (p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

(iii) (*Gauss identity*)  $\varphi \star 1 = \mathbf{i}$ ; explicitly,

$$\sum_{d|n} \varphi(d) = n \quad (n \in \mathbf{N}).$$

**Conjecture (Carmichael conjecture)** *Given  $n \in \mathbf{N}$ , the equation  $\varphi(x) = n$  has either no solution  $x \in \mathbf{N}$  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 the following:

- (i) The Carmichael conjecture is true for all  $n \leq 10^{1000000000}$ .
- (ii) For any  $k \in \mathbf{N}$  except possibly  $k = 1$ , there exist infinitely many  $n \in \mathbf{N}$  such that the equation  $\varphi(x) = n$  has exactly  $k$  solutions  $x \in \mathbf{N}$ . Thus, only the question of whether multiplicity  $k = 1$  can occur remains open, and this is precisely the question addressed by the Carmichael conjecture.

### 3.6 The number-of-divisors and sum-of-divisors functions. Perfect numbers

**Definition (Number-of-divisors function)** The **number-of-divisors function** is defined by

$$\nu(n) = \#\{d \in \mathbf{N} : d | n\} = \sum_{d|n} 1 = (\mathbf{1} \star \mathbf{1})(n) \quad (n \in \mathbf{N}).$$

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 3.7 (Properties of  $\nu(n)$ )**

- (i) (*Multiplicativity*) *The function  $\nu(n)$  is multiplicative (though not completely multiplicative).*
- (ii) (*Explicit formula*) *For any  $n \in \mathbf{N}$ ,*

$$\nu(n) = \prod_{p^\alpha || n} (\alpha + 1)$$

**Definition** Sum-of-divisors function The **sum-of-divisors function** is defined by

$$\sigma(n) = \sum_{d|n} d = (\mathbf{i} \star \mathbf{1})(n) \quad (n \in \mathbf{N}).$$

**Proposition 3.8 (Properties of  $\sigma(n)$ )**

- (i) *(Multiplicativity)* The function  $\nu(n)$  is multiplicative (though not completely multiplicative).
- (ii) *(Explicit formula)* For any  $n \in \mathbf{N}$ ,

$$\sigma(n) = \prod_{p^\alpha || n} \frac{p^\alpha - 1}{p - 1}$$

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

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

**Theorem 3.9 (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** There exist infinitely many even perfect numbers if and only if there exist infinitely many Mersenne primes.

**Example 2** 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  $2^7 - 1 = 127$ .