Arithmetic functions and Dirichlet multiplication

Alexander Basler, Anselm Schönbächler

1 Basic examples of arithmetic functions

Definition 1 (arithmetic functions)**.** In general, an arithmetic function is any function going from $\mathbb{N}$ and taking values in $\mathbb{C}$. We will use the convention $0 \notin \mathbb{N}$.

1.1 Möbius function

Definition 2. The function

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by a square number} \\ (-1)^k & \text{otherwise, where } k = \text{number of prime factors of } n \end{cases}.$$

is called the Möbius function. Note that the definition implies $\mu(1) = 1$

Theorem 3. *For every $n \geq 1$ we have*

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{otherwise} \end{cases}.$$

Proof. The statement clearly holds for $n = 1$. For $n \geq 2$, note that all non-zero terms in the sum $\sum_{d|n} \mu(d)$ come from $d = 1$ and those divisors of n, where every prime factor appears at most once. Therefore, if n contains the prime factors $p_1 \cdots p_k$:

$$\sum_{d|n} \mu(d) = \mu(p_1) + \mu(p_2) + \cdots + \mu(p_1 p_2) + \cdots + \mu(p_1 p_2 \cdots p_k) = \sum_{j=0}^{k} \binom{k}{j} (-1)^j = (1-1)^k = 0.$$

□

1.2 Euler's totient function

Definition 4. The function

$$\phi(n) = \sum_{\substack{k \leq n \\ \gcd(k,n)=1}} 1$$

is called Euler's totient function. In words, $\phi(n)$ counts the number of natural numbers smaller than n, that are coprime to n. By convention, $\phi(1) = 1$. There are obviously a number of equivalent definitions, most importantly one could also define $\phi(n)$ to be the number of generators of the cyclic group $\mathbb{Z}/n\mathbb{Z}$.

Theorem 5. *For every $n \geq 1$ we have*

$$\sum_{d|n} \phi(d) = n$$

.

Proof. There are many elementary proofs for this fact, here we will present a proof using group theory which is much shorter. Note that every element in $\mathbb{Z}/n\mathbb{Z}$ generates a subgroup of the form $\mathbb{Z}/d\mathbb{Z}$, where d is a divisor of n. The subgroup $\mathbb{Z}/d\mathbb{Z}$ has exactly $\phi(d)$ generators, therefore the statement follows. □

2 Further properties of μ and ϕ

2.1 The relation between ϕ and μ

Theorem 6. *For $n \geq 1$ we have*

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

Proof. First, fix n. We have

$$\phi(n) = \sum_{k=1}^{n} \mathbb{1}_{\gcd(n,k)=1}$$

The summation property of μ (theorem 3) implies

$$\mathbb{1}_{\gcd(n,k)=1} = \sum_{d|\gcd(n,k)} \mu(d)$$

which means we get

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|\gcd(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d)$$

Now, think about what happens when we fix a divisor d of n. We need to sum over all k smaller than n, which are a multiple of d. So, if we write $k = qd$ we can instead sum over all q smaller than $\frac{n}{d}$, hence

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d}$$

□

2.2 Euler's formula for ϕ

Theorem 7. *For $n \geq 1$ we have*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Proof. For $n = 1$, the product is empty (and therefore by convention equal to 1), since no prime number divides the number 1.
For $n \geq 2$, let $p_1, p_2 \cdots p_r$ be the distinct prime divisors of n. This allows us to rewrite the product as follows:

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \frac{(-1)^r}{p_1 p_2 \cdots p_r}$$

Notice how all the denominators are divisors of n, and how the sign of the numerator changes depending on the number of prime factors of the corresponding divisor in the denominator. In conclusion, one sees that this huge sum can be compactly written as $\sum_{d|n} \frac{\mu(d)}{d}$ and the statement follows from the theorem above (theorem 6). □

3 The dirichlet product

3.1 Definition and basic properties

Definition 8. The function

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

is called the dirichlet product of f and g.

Theorem 9. *For all arithmetic functions f,g,h it holds $f*g = g*f$ and $(f*g)*h = f*(g*h)$; in words, Dirichlet multiplication is commutative and associative.*

Proof. Note that one can write

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b)$$

therefore the commutative property is clear. Similarly, one can see that

$$(f * (g * h))(n) = \sum_{ad=n} f(a) \sum_{bc=d} g(b) h(c) = \sum_{abc=n} f(a) g(b) h(c)$$

and since the analogous rearrangement can be done to get

$$((f * g) * h)(n) = \sum_{abc=n} f(a) g(b) h(c)$$

we get the associative property. □

3.2 The dirichlet inverse

Theorem 10. *For all arithmetic functions f we have $f * I = f$, where $I(n) = \begin{matrix} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{matrix}$ Thus, The set of all arithmetic functions with component-wise addition and dirichlet multiplication form a commutative ring.*

Proof. Simply plugging in the definition:

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = f(n)$$

□

Theorem 11. *Given an arithmetic function f with $f(1) \neq 0$. There exist a unique dirichlet inverse f^{-1} with the property $f * f^{-1} = I$. Moreover, one can recursively calculate f^{-1} with the following recursion formula:*

$$f^{-1}(1) = \frac{1}{f(1)}$$

and for $n > 1$

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

Proof. We need to show that $f^{-1}(n)$ is unique for all n. For $n = 1$ one has to solve the equation

$$(f * f^{-1})(1) = I(1)$$

which is equivalent to

$$f(1)f^{-1}(1) = 1$$

and the first statement follows.
Now, by means of induction, assume that we have proven the uniqueness and calculated the value of $f^{-1}(k)$ for all $k < n$. We see that

$$(f * f^{-1})(n) = I(n)$$

is equivalent to

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

or

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

Solving for $f^{-1}(n)$ we get the result. □

Definition 12. We define the unit function u with

$$u(n) = 1$$

for all n.

Theorem 13. *μ and u are dirichlet inverses of each other.*

Proof. This is exactly the statement of theorem 3, namely

$$\sum_{d|n} \mu(d) = I(n)$$

□

4 Möbius Inversion Formula

Theorem 14 (Möbius inversion formula)**.** *The following equivalence holds:*

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right). \tag{1}$$

Proof. The first equation states that $f = g*u$, which implies $f*\mu = g*u*\mu = g*I = g$ (Dirichlet multiplication is associative), which is the statement of the second equation. Conversely, multiplying the second equation $g = f*\mu$ by the unit function u gives $g*u = f*\mu*u = f*I = f$. □

It is now clear that the pair of formulae

$$n = \sum_{d|n} \phi(d), \quad \phi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

which we've already seen (theorems 5 and 6) are simply special cases of this more general inversion formula.

5 The Mangoldt function $\Lambda(n)$

We introduce the Mangoldt function Λ which is connected to the distribution of primes.

Definition 15. For all natural numbers $n \geq 1$ define

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and } m \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

This means, for example, $\Lambda(3) = \log 3$, $\Lambda(6) = 0$, and $\Lambda(9) = \log 3$. The following theorem and its proof show how Λ arises from the decomposition of natural numbers into products of primes.

Theorem 16. *If $n \geq 1$ we have*

$$\log n = \sum_{d|n} \Lambda(d). \tag{2}$$

Proof. Since $\Lambda(1) = 0$, the theorem holds for $n = 1$ and we can assume $n > 1$. Decomposing n into a product of primes yields

$$n = \prod_{k=1}^{r} p_k^{a_k}.$$

Taking logarithms, we get

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

Considering (2), we see that the only nonzero terms in the sum com from divisors d of the form p_k^m with $m = 1, \ldots, a_k$. Hence,

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n.$$

□

We can utilise the Möbius inversion formula to express Λ in terms of the logarithm:

Theorem 17. *For $n \geq 1$ we have*

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

Proof. The first part follows immediately from the inverting (2). Then we see

$$\sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = I(n) \log n - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d,$$

since $I(n) \log n = 0$ for all n. □

6 Multiplicative functions

Definition 18. An arithmetic function $f \neq 0$ is called multiplicative if

$$f(mn) = f(m)f(n) \quad \text{whenever } \gcd(m,n) = 1.$$

and completely multiplicative if

$$f(mn) = f(m)f(n) \quad \forall m, n.$$

Example 1. The power function $N^\alpha(n) = n^\alpha$ with $\alpha \in \mathbb{C}$ is completely multiplicative.

Example 2. The identity function $I(n) = [1/n]$ is completely multiplicative.

Example 3. The Möbius function is not completely multiplicative since $\mu(4) = 0$, but $\mu(2) = -1$. It is, however, multiplicative: consider two coprime natural numbers m, n. If either of the numbers has a prime-square factor, so does their product and $\mu(mn) = 0 = \mu(m)\mu(n)$. If neither has a square factor we can write $m = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ where the p_i and q_i are distinct primes. Then $\mu(mn) = (-1)^{s+t} = (-1)^s(-1)^t = \mu(m)\mu(n)$.

Example 4. We have already seen that the Euler totient function ϕ is multiplicative. It is not completely multiplicative, as $\phi(4) = 2$, but $\phi(2) = 1$.

Example 5. Finally, if f and g are multiplicative, then so are their pointwise product fg and their pointwise quotient f/g. The same holds in the case of complete multiplicativity.

The following theorem is a very simple result.

Theorem 19. *If f is multiplicative, then $f(1) = 1$.*

Proof. Since $\gcd(n, 1) = 1$ for all natural numbers n, we have $f(n) = f(1)f(n)$. Since $f \neq 0$, there is some n with $f(n) \neq 0$, so $f(1) = 1$. □

It follows immediately that Λ is not multiplicative, since $\Lambda(1) = 0$.

Theorem 20. *Given f with $f(1) = 1$. Then*

(a) f is multiplicative if, and only if, for all primes p_i and all integers $a_i \geq 1$ we have

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r}). \tag{3}$$

(b) If f is multiplicative, then f is completely multiplicative if, and only if, for all primes p and integers $a \geq 1$

$$f(p^a) = f(p)^a. \tag{4}$$

Proof. Suppose f is multiplicative. Then the powers of primes from (a) are all relatively prime, so

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1} \cdots p_{r-1}^{a_{r-1}})f(p_r^{a_r}) = \cdots = f(p_1^{a_1}) \cdots f(p_r^{a_r}).$$

Now suppose instead (3) holds and $n, m \geq 1$ are coprime. We write $n = p_1^{a_1} \cdots p_r^{a_r}$ and $m = q_1^{b_1} \cdots q_s^{b_s}$ with distinct primes. Then

$$f(n)f(m) = f(p_1^{a_1}) \cdots f(p_r^{a_r})f(q_1^{b_1}) \cdots f(q_s^{b_s}) = f(p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}) = f(nm).$$

Since $f(1) = 1$, $f \neq 0$ and f is multiplicative.

We now prove the second part of the theorem. If f is completely multiplicative, then (4) trivially holds. Now suppose (4) holds. For integers $n, m \geq 1$ we write $m = p_1^{a_1} \cdots p_r^{a_r}$ and $n = p_1^{b_1} \cdots p_r^{b_r}$ where the a_i, b_i may be zero. Then

$$\begin{aligned} f(m)f(n) &= f(p_1^{a_1}) \cdots f(p_r^{a_r})f(p_1^{b_1}) \cdots f(p_r^{b_r}) = f(p_1)^{a_1+b_1} \cdots f(p_r)^{a_r+b_r} \\ &= f(p_1^{a_1+b_1}) \cdots f(p_r^{a_r+b_r}) = f(mn). \end{aligned}$$

This concludes the proof of the second equivalence. □

7 Multiplicative functions and Dirichlet multiplication

Theorem 21. *If f and g are multiplicative, so is their Dirichlet product $f * g$.*

Proof. Suppose m, n are relatively prime natural numbers. Then

$$(f * g)(mn) = \sum_{c|mn} f(c) g\left(\frac{mn}{c}\right).$$

Every divisor c of mn can be written as $c = ab$ with $a \mid m$ and $b \mid n$ and since $\gcd(m, n) = 1$, we also have $\gcd(a, b) = 1$ and $\gcd(m/a, n/b) = 1$. Furthermore, there is a one-to-one correspondence between the set of divisors c of mn and the set of products ab. Thus,

$$\begin{aligned}(f * g)(mn) &= \sum_{\substack{a|m \\ b|n}} f(ab) g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a) f(b) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right) = (f * g)(m)(f * g)(n).\end{aligned}$$

□

Remark 1. Since the unit function u is multiplicative, divisor sums $\sum_{d|n} f(d)$ of multiplicative function f are themselves multiplicative.

Remark 2. The theorem does not hold equivalently for completely multiplicative functions. Taking the unit function as an example, we see

$$(u * u)(n) = \sum_{d|n} u(d) u(n/d) = \sum_{d|n} 1.$$

Hence, $(u * u)(4) = 3$, whereas $(u * u)(2) = 2$.

We can prove the next theorem similarly.

Theorem 22. *If both g and $f * g$ are multiplicative, then so is f.*

Proof. We use a proof by contradiction. Suppose f is not multiplicative. Then there are coprime natural numbers m, n such that $f(mn) \neq f(m) f(n)$. We choose such a pair m, n so that the product mn is minimal.

If $mn = 1$, then $f(1) \neq 1$, but since $(f * g)(1) = f(1) g(1) = f(1) \neq 1$, this shows that $f * g$ is not multiplicative.

Otherwise we have $f(ab) = f(a) f(b)$ for all coprime a, b with $ab < mn$. Then, proceeding as in the previous proof, we get

$$\begin{aligned}(f * g)(mn) &= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab) g\left(\frac{mn}{ab}\right) + f(mn) g(1) \\ &= \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right) - f(m) f(n) + f(mn) \\ &= (f * g)(m) \cdot (f * g)(n) - f(m) f(n) + f(mn) \neq (f * g)(m) \cdot (f * g)(n).\end{aligned}$$

□

Corollary 23. If f is multiplicative, so is its Dirichlet inverse f^{-1}.

Proof. Since both f and $f * f^{-1} = I$ are multiplicative, so is f^{-1}. □

Remark 3. We have ultimately now shown in this section, that the set of multiplicative functions is a subgroup of the group of all arithmetic functions f with $f(1) \neq 0$.

8 The inverse of a completely multiplicative function

It is especially easy to determine the Dirichlet inverse of a completely multiplicative function, as the next theorem shows.

Theorem 24. *A multiplicative function f is completely multiplicative if, and only if,*

$$f^{-1}(n) = \mu(n)f(n) \quad \forall n \geq 1.$$

Proof. Let $g(n) := \mu(n)f(n)$. If f is completely multiplicative, then

$$(g * f)(n) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d|n} \mu(d) = f(n)I(n) = I(n),$$

since $(1) = 1$ and $I(n) = 0$ for all $n > 1$. Hence, $g = f^{-1}$.

Conversely, assume $f^{-1}(n) = \mu(n)f(n)$. As we have seen, it suffices to show that $f(p^a) = f(p)^a$ for prime powers p to prove the complete multiplicativity of f. Since $(f^{-1} * f) = I$ we have

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0 \quad \forall n > 1.$$

With $n = p^a$, we get

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0,$$

since $\mu(p^r)$ vanishes for $r \geq 2$. Thus, $f(p^a) = f(p)f(p^{a-1})$, which inductively leads to $f(p^a) = f(p)^a$, so f is completely multiplicative. □

Example 6. Though the Euler totient function ϕ is not completely multiplicative, we can still find its inverse employing the illustrated method. Since $\phi = \mu * N$, we have $\phi^{-1} = N^{-1} * \mu^{-1}$. But N is completely multiplicative, so $N^{-1} = \mu N$, so

$$\phi^{-1} = \mu N * \mu^{-1} = \mu N * u.$$

Hence,

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d).$$

We can manipulate sums divisor sums of this form with the next theorem.

Theorem 25. *If f is multiplicative, then*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p)),$$

where the product is taken over all the primes.

Proof. The sum is equal to $\mu f * u$, which is multiplicative, so it suffices to compute the value of $\mu f * u$ at powers of primes p^a. Now,

$$(\mu f * u)(p^a) = \sum_{d|p^a} \mu(d)f(d) = 1 - f(p).$$

Hence,

$$(\mu f * u)(n) = \prod_{p|n}(\mu f * u)(p^a) = \prod_{p|n}(1 - f(p)).$$

□

Remark 4. Together with our previous observations, this shows

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d) = \prod_{p|n}(1 - p).$$

9 Liouville's function λ

Definition 26. We define the Liouville function by $\lambda(1) = 1$, and if $n = p_1^{a_1} \cdots p_k^{a_k}$ we set

$$\lambda(n) = (-1)^{a_1 + \cdots + a_k}.$$

Clearly λ is completely multiplicative. We now consider the divisor sum of λ and its inverse.

Theorem 27. *For every $n \geq 1$ we have*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, $\lambda^{-1}(n) = |\mu(n)|$.

Proof. As we have already discussed, the divisor sum of a multiplicative function is multiplicative, so it suffices to compute $\lambda * u$ at prime powers p^a. We see

$$(\lambda * u)(p^a) = \sum_{d|p^a} \lambda(d) = \sum_{k=0}^{a} \lambda(p^k) = \sum_{k=0}^{a} (-1)^k = \begin{cases} 0 & \text{if } a \text{ is odd,} \\ 1 & \text{if } a \text{ is even.} \end{cases}$$

Hence, if $n = \prod_{i=1}^{k} p_i^{a_i}$, we have $(\lambda * u)(n) = \prod_{i=1}^{k} (\lambda * u)(p_i^{a_i})$. Consequently, if any exponent a_i is odd, then the divisor sum of λ vanishes. If all the exponents are even, then $\sum_{d|n} \lambda(d) = 1$. Hence, the divisor sum is equal to 1 if n is a square and 0 otherwise. Furthermore, $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$. □