Arithmetical Functions

LHS Math Team

May 21, 2012

1 Basic Arithmetical Functions

Definition 1.1. *An* arithmetical function *is a function $f : \mathbb{N} \to \mathbb{R}$, where $\mathbb{N}$ denotes the positive integers and $\mathbb{R}$ denotes the real numbers.*

In general, an arithmetical function can be complex valued. However, in this discussion we will be concerned only with real-valued arithmetical functions. Note that by this definition, arithmetical functions and sequences are linked: $f(n) \longleftrightarrow a_n$. We now present a few examples of arithmetical functions.

Example 1.2. *The divisor functions,*

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

are arithmetical functions. When $\alpha = 0$, this is the familiar divisor counting function, denoted $d(n)$ or $\tau(n)$. When $\alpha = 1$, this is the function returning the sum of the divisors.

Example 1.3. *Euler's totient function $\varphi(n)$ that returns the number of positive integers less than or equal to n relatively prime to n is an arithmetical function. It is somewhat well-known and will be stated without proof that*

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

We can prove the following theorem about φ. In the next section, we will prove another theorem about φ that will turn out to be linked to this one.

Theorem 1.4. *For $n \geq 1$,*

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

Proof. For each divisor $d|n$, we count the number of positive integers k such that $\gcd(k, n) = d$. When $\gcd(k, n) = d$, we can write $\gcd(k', n/d) = 1$, where $k' = k/d$. Furthermore, we can see that this is reversible. Thus, the number of positive integers k satisfying $\gcd(k, n) = d$ is exactly $\varphi(n/d)$. Summing over all d, we should get exactly n numbers, so

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d).$$

□

2 The Möbius Function

Definition 2.1. *The* Möbius function μ *is defined for* $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ *as*

$$\mu(n) = \begin{cases} 1 & \text{when } n = 1, \\ (-1)^k & \text{when } a_1 = a_2 = \cdots = a_k = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The following function's definition may seem a little out of place now, but it makes stating the next result marginally easier and it will have importance later.

Definition 2.2. *The* identity function I *is defined as*

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

With these definitions, we now state the following result on the sum of the Möbius function over divisors.

Theorem 2.3. *We have*

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

Proof. When $n = 1$, this is obvious. Otherwise, let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. The only nonzero terms come from $d = 1$ and the products of distinct primes, and basic counting gets

$$\sum_{d|n} \mu(d) = 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0.$$

□

As promised, what follows is another result on Euler's totient function.

Theorem 2.4. *We have*

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

Proof. This follows from comparing this expression with the product formula earlier. □

As an exercise, attempt to find another proof of this fact without using the product formula, which turns out to be equivalent to this theorem. A first step is to write

$$\varphi(n) = \sum_{k=1}^{n} I(\gcd(n,k))$$

and manipulate the double summation from there.

3 Multiplicative Funtions

Definition 3.1. *An arithmetical function f is called* multiplicative *if f is not always zero and if for all m, n satisfying $\gcd(m,n) = 1$, $f(mn) = f(m)f(n)$. We call f* completely multiplicative *if m and n need not be relatively prime.*

Example 3.2. *The identity function I is completely multiplicative.*

Example 3.3. *The Möbius function μ is multiplicative but not completely multiplicative. This can be seen from the definition of μ.*

Example 3.4. *The Euler totient function $\varphi(n)$ is multiplicative. The proof of this is well-known, so it is left as an exercise to the reader who hasn't seen it.*

Theorem 3.5. *If f is multiplicative then $f(1) = 1$.*

Proof. We note that $f(n) = f(1)f(n)$. Since f is not identically zero, it must be the case that $f(1) = 1$. □

4 Dirichlet Products

Definition 4.1. *If f and g are two arithmetical functions, we define their* Dirichlet product *or Dirichlet convolution to be the arithmetical function defined by*

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

Definition 4.2. *Let $N_\alpha(n) = n^\alpha$ for all n. For simplicity, we denote by N the function N_1, so $N(n) = n$.*

Example 4.3. *Theorem 2.4 can be written as $\varphi = \mu * N$.*

It turns out that the Dirichlet product creates an abelian group structure on most arithmetical functions. This is encoded in the following theorems.

Theorem 4.4. *For all f, $I * f = f * I = f$.*

Proof. We write out the sum and get

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

□

Theorem 4.5. *Dirichlet multiplication is commutative and associative.*

Proof. The proofs are left as exercises to the reader. □

Theorem 4.6. *If f is an arithmetical function with $f(1) \neq 0$, then there is a unique arithmetical function f^{-1} such that*

$$f * f^{-1} = f^{-1} * f = I.$$

Proof. We show that $f^{-1}(k)$ is uniquely determined for each k by strong induction.

For $k = 1$, the convolution gives $f(1)f^{-1}(1) = 1$. Since $f(1) \neq 0$, we have a unique value for $f^{-1}(1)$.

For $k \geq 1$, suppose all previous values of f^{-1} were determined uniquely. The convolution formula gives a bunch of determined terms and $f(1)f^{-1}(k)$, and since $f(1) \neq 0$, this determines a unique value for $f^{-1}(k)$, as desired. □

To state our next result, we make use of the following definition.

Definition 4.7. *The* unit function *is the arithmetical function u such that $u(n) = 1$ for all n.*

By Theorem 2.3, $\mu * u = I$. Thus the functions μ and u are inverses of each other. This gives us the *Möbius inversion formula*.

Theorem 4.8. *The equation*

$$f(n) = \sum_{d|n} g(d)$$

is equivalent to the equation

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

Proof. The first equation tells us that $f = g * u$. Multiplication by μ gives $f * \mu = g * u * \mu = g * I = g$, which is the second equation. We can reverse this as well, completing the proof. □

Example 4.9. *Theorems 1.4 and 2.4 are equivalent by the Möbius inversion formula,*

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

5 Combining the Last Two Sections

Theorem 5.1. *If f and g are multiplicative, $f * g$ is multiplicative.*

Proof. Let m and n be relatively prime. Then if $h = f * g$,

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

For each $c|mn$, we can write $c = ab$ where $a|m$ and $b|n$. Furthermore, $\gcd(a, b) = 1$, so

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

□

With a little more effort, one can show that the set of multiplicative functions is a subgroup of the group mentioned earlier under Dirichlet multiplication. We now turn to the inverse of a completely multiplicative function.

Theorem 5.2. *Let f be multiplicative. Then f is completely multiplicative if and only if*

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

Proof. We leave the "if" direction as an exercise for the reader. It suffices to show that this condition implies $f(p^\alpha) = f(p)^\alpha$ for all primes p.

Suppose f is completely multiplicative and let $g(n) = \mu(n)f(n)$. 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 $f(1) = 1$ and $I(n) = 0$ for all $n > 1$. □

One can show as a direct result that $\varphi^{-1} = u * \mu N$ and $\sigma_\alpha^{-1}(n) = (\mu N_\alpha) * \mu$.

6 The von Mangoldt function

Definition 6.1. *The* von Mangoldt function Λ *is defined as*

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

Here, log *denotes the natural logarithm.*

This function turns out to have many applications in analytical number theory, e.g. the Prime Number Theorem. We give one basic but key result here.

Theorem 6.2. *We have*

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

Proof. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. The only nonzero terms in the sum on the right are the divisors of the form p_i^j for $j = 1, 2, \ldots, a_i$ and $i = 1, 2, \ldots, k$. Thus,

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{k} \sum_{j=1}^{a_i} \Lambda(p_i^j) = \sum_{i=1}^{k} a_i \log p_i = \log n.$$

□

We close by noting that *this is the analytic formulation of the fundamental theorem of arithmetic.*

7 Problems

Below are all the things that were left unproven above or proved with little detail.

1. If p denotes a prime, show that

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

2. Find another proof that
$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

3. Show that μ is a multiplicative function.

4. Show that φ is a multiplicative function.

5. Show that Dirichlet multiplication is commutative and associative. That is, $f * g = g * f$ and $f * (g * h) = (f * g) * h$.

6. Show that if f is a multiplicative function satisfying $f^{-1}(n) = \mu(n)f(n)$, f is completely multiplicative.

7. Show that $\varphi^{-1} = u * \mu N$, where fg denotes the actual product $(fg)(n) = f(n)g(n)$.

8. Show that $\sigma_\alpha^{-1}(n) = (\mu N_\alpha) * \mu$.

Below are some additional problems.

1. Find all positive integers n such that $\varphi(n) = \varphi(2n)$.

2. Prove that
$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}.$$

3. Define $\nu(1) = 0$, and for $n > 1$ let $\nu(n)$ be the number of distinct prime factors of n. Let $f = \mu * \nu$ and prove that $f(n)$ is either 0 or 1.

4. If $f(n) > 0$ for all n and if $a(n)$ is real, $a(1) \neq 0$, prove that
$$g(n) = \prod_{d|n} f(d)^{a(n/d)}$$
if, and only if,
$$f(n) = \prod_{d|n} g(d)^{b(n/d)},$$
where $b = a^{-1}$, the Dirichlet inverse of a. This is the *product form* of the Möbius inversion formula.