Introduction to number theoretic functions

Ümit Işlak*

August 20, 2020

Abstract

We provide a first introduction to multiplicative functions and Möbius inversion formula.

1 Arithmetic functions

Definition 1.1 A function whose domain is the set of positive integers is called a **number theoretic function**, or an **arithmetic function**.

Definition 1.2 (a) We say that an arithmetic function f, which is not identically zero, is **multiplicative** if it has the property

$$f(mn) = f(m)f(n)$$

for all pairs of relatively prime positive integers m and n.¹

(b) An arithmetic function f is said to be additive if it has the property

$$f(mn) = f(m) + f(n)$$

for all pairs of relatively prime positive integers m and n.

Following properties collect some properties of multiplicative functions.

Proposition 1.1 (i) If f is multiplicative, then f(1) = 1.

(ii) If f is multiplicative, and $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where p_i 's are distinct primes, then

$$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_r^{a_r}).$$

(iii) If f and g are multiplicative functions such that $f(p^k) = g(p^k)$ for every prime p and $k \in \mathbb{N}$, then f = g.

Problem 1.1 Prove Lemma 1.1.

^{*}Boğaziçi University, Mathematics department, Istanbul, Turkey. email: umit.islak1@boun.edu.tr

¹Recall that positive integers m and n are relatively prime if their greatest common divisor is 1. 1 is relatively prime with any positive integer.

2 Examples and exercises

Example 2.1 It can be easily checked that the function f(n) = 1, $n \ge 1$ is a multiplicative function.

Example 2.2 Define $\tau : \mathbb{N} \to \mathbb{N}$ by setting

 $\tau(n) = the number of all natural divisors of <math>n = \#\{d > 0 : d \mid n\}.$

Then τ is a multiplicative function. In order to see this it is useful to note that for a given $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_i 's are distinct primes, and $\alpha_i \geq 1$,

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

The rest of the argument is immediate.

Example 2.3 Define $\sigma : \mathbb{N} \to \mathbb{N}$ by setting

$$\sigma(n) = the \ sum \ of \ all \ natural \ divisors \ of \ n = \sum_{d \ | \ n} d.$$

Then σ is a <u>multiplicative function</u>. To see that this is the case, observe that if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_i 's are distinct primes, and $\alpha_i \geq 1$, then we can write

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$

The rest of the argument is easy.

Example 2.4 The function $\pi : \mathbb{N} \to \mathbb{N}$ defined by

 $\pi(n) = the \ product \ of \ all \ natural \ divisors \ of \ n = \Pi_{d \ | \ n} d$

is <u>not</u> multiplicative.

Problem 2.1 Show that π defined in previous problem is not multiplicative.

Problem 2.2 Show that the function $|\mu(n)|$, which is 1 if n is not divisible by a square and 0 otherwise, is multiplicative. Find the value of the function when n is a prime power, and thereby find a formula for its value on any integer n. (This is the characteristic function of square-free integers.)

Problem 2.3 Show that if $\{f(n)\}_{n=1}^{\infty}$ is a multiplicative function, then so is

$$g(n) = \sum_{d|n} f(d), \qquad n = 1, 2, \dots$$

3 Euler totient function

We will need to use Euler's totient function a few times below, so we discuss it briefly here. Letting m be a positive integer, Euler's totient function $\phi(m)$ is defined to be the number of integers between 1 and m which are relatively prime to m. Clearly, if m is prime, then $\phi(m) = m - 1$.

For the more general case, if the distinct prime factors of m are p_1, \ldots, p_n , we claim that

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right) = m\prod_{i=1}^n\left(1 - \frac{1}{p_i}\right).$$
 (1)

We will prove this by using the following form of inclusion-exclusion principle:

Proposition 3.1 Given a finite set of objects which may or may not have any of the properties 1, 2, ..., n, let $N(i_1, ..., i_r)$ be the number of those objects which have at least the r properties $i_1, ..., i_r$. Then the number of objects in the set having at least one of the properties is

$$N(1) + N(2) + \dots + N(n)$$

$$-N(1,2) - N(1,3) - \dots - N(n-1,n)$$

$$+N(1,2,3) + N(1,2,4) + \dots + N(n-2,n-1,n)$$

$$-\dots$$

$$+(-1)^{n-1}N(1,2,\dots,n).$$

Now, let's prove Euler's formula in (1). Let the set of objects in question be $\{1, 2, ..., m\}$, and for $1 \le i \le n$ let 'property i' be that a number is divisible by p_i . Then the integers in that set which are relatively prime to m are precisely those which have none of the properties 1, ..., n. So we must subtract the number of integers with at least one of the properties from m to give (with the usual notation)

$$m$$

$$-N(1) - N(2) \cdots - N(n)$$

$$+N(1,2) + N(1,3) + \cdots + N(n-1,n)$$

$$-N(1,2,3) - N(1,2,4) - \cdots - N(n-2,n-1,n)$$

$$+ \cdots$$

$$+(-1)^{n}N(1,2,\ldots,n).$$

Now N(i) is the number of integers in $\{1, 2, ..., m\}$ which are divisible by p_i and that is precisely m/p_i . Similarly, $N(i,j) = m/p_ip_j$, etc. Hence the required number of integers relatively prime to m is given by

$$\frac{m}{-\frac{m}{p_{1}} - \frac{m}{p_{2}} - \cdots} + \frac{m}{p_{1}p_{2}} + \frac{m}{p_{1}p_{3}} + \cdots + \frac{m}{p_{1}p_{2}p_{3}} - \frac{m}{p_{1}p_{2}p_{4}} - \cdots + (-1)^{n} \frac{m}{p_{1}p_{2} \cdots p_{n}}.$$

It is now straightforward to check that this agrees with the given factorized version of $\phi(m)$, and our claim is proven.

Problem 3.1 Give an alternative proof for the formula for Euler's totient function by using induction.

Remark 3.1 (i) It can be shown that the totient function satisfies

$$\phi(n) \ge \sqrt{n}$$

for all n except n=2 and n=6. In particular, the only values for which $\phi(n)=2$ are n=3,4 and 6.

(ii) When n is composite, one may prove that

$$\phi(n) \le n - \sqrt{n}$$
.

Problem 3.2 Decide whether $\phi(n)$ is multiplicative, additive or neither?

4 Möbius function and Möbius identity

Definition 4.1 The Möbius μ function is defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1. \\ 0, & \text{if } n \text{ is not square free} \\ (-1)^k & \text{if } n = \prod_{i=1}^k p_i. \end{cases}$$

Note that we could alternatively define the Möbius μ function by defining it on prime powers as

$$\mu(p^k) = \begin{cases} 1, & \text{if } k = 0\\ -1, & \text{if } k = 1\\ 0, & \text{if } k \ge 2, \end{cases}$$

and taking its multiplicative extension.

The following identity is of extreme importance.

Theorem 4.1 (Möbius identity) For any $n \in \mathbb{N}$, we have

$$\sum_{d:d|n} \mu(n) = e(n),$$

where

$$e(n) = \begin{cases} 1, & if \ n = 1 \\ 0, & otherwise. \end{cases}$$

Proof: The case for n=1 is clear. For $n\geq 2$, if we let $\prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of n,

then we have

$$\sum_{d:d|n} \mu(d) = \sum_{d:d|n, d \text{ is square free}} \mu(d) = \sum_{I \subset \{1,2,\dots,k\}} \mu\left(\prod_{j \in I} p_j\right)$$

$$= \sum_{I \subset \{1,2,\dots,k\}} (-1)^{|I|}$$

$$= \sum_{j=0}^k \sum_{I \subset \{1,2,\dots,k\}, |I|=j} (-1)^{|I|}$$

$$= \sum_{j=0}^k \binom{k}{j} (-1)^j = 0.$$

Example 4.1 This example is for the use of Möbius identity on removing coprimality condition in summations. Suppose that we are given some integer $k \geq 1$, and that we are willing to evaluate $\sum_{n:(n,k)=1} f(n)$. Then we have

$$\begin{split} \sum_{n:(n,k)=1} f(n) &= \sum_{n} f(n) e((n,k)) = \sum_{n} f(n) \sum_{d:d|(n,k)} \mu(d) &= \sum_{n,d:d|n,d|k} f(n) \mu(d) \\ &= \sum_{d:d|k} \sum_{n:d|n} f(n) \mu(d) \\ &= \sum_{d:d|k} \mu(d) \sum_{n:d|n} f(n) \\ &= \sum_{d:d|k} \mu(d) \sum_{m>1} f(dm). \end{split}$$

That is,

$$\sum_{n:(n,k)=1} f(n) = \sum_{d:d|k} \mu(d) \sum_{m \ge 1} f(dm)$$

. It is often the case that dealing with the right-hand side is easier than the left-hand side with the coprimality condition. \Box

Example 4.2 As an example demonstrating the use of our previous observation we use the Euler totient function. For $k \geq 1$, we have

$$\phi(k) = \sum_{n:1 \le n \le k, (n,k)=1} 1 = \sum_{d:d|k} \mu(d) \sum_{n:1 \le n \le k, d|n} 1 = \sum_{d:d|k} \mu(d) \frac{k}{d}.$$

In particular, we reached at the following conclusion:

$$\frac{\phi(k)}{k} = \sum_{d:d|k} \mu(d) \frac{1}{d}.$$

For other examples, including one on Ramanujan sums, see Hildebrandt. We conclude this section with some notes.

Remark 4.1 (i) Prime number theorem is equivalent to $\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \mu(n) = 0$. This has the following interpretation: If a square free integer is chosen at random, then it is equally likely to have an even and an odd number of prime factors.

(ii) Merten's conjecture states that $\left|\sum_{n\leq x}\mu(n)\right|\leq \sqrt{x}$ for all $x\geq 1$. Staying open for more than a century it was disproved by Odlyzko and H. te Riele in 1985, where they show that

$$\limsup_{x \to \infty} \frac{\sum_{n \le x} \mu(n)}{x} > 1.06.$$

It is still open whether 1.06 can be replaced by an arbitrary c > 1.

5 Dirichlet generating functions

Given a sequence $\{a_n\}_{n\geq 1}$, we say that a formal series

$$D(x) = \sum_{n \ge 1} \frac{a_n}{n^x}$$
$$= a_1 + \frac{a_2}{2^x} + \frac{a_3}{3^x} + \frac{a_4}{4^x} + \cdots$$

is the Dirichlet series generating function of the sequence.

The importance of Dirichlet series stems directly from their multiplication rule. Suppose that D_1 and D_2 are Dirichlet series of the sequences a_n and b_n , respectively. What is then the sequence generated by the product $D_1(x)D_2(x)$? Observe that

$$D_1(x)D_2(x) = (a_1 + a_2 2^{-x} + a_3 3^{-x} + \cdots)(b_1 + b_2 2^{-x} + b_3 3^{-x} + \cdots)$$

$$= (a_1b_1) + (a_1b_2 + a_2b_2)2^{-x} + (a_1b_3 + a_3b_1)3^{-x}$$

$$+ (a_1b_4 + a_2b_2 + a_4b_1)4^{-x} + \cdots$$

So, what is the coefficient of n^{-x} in $D_1(x)D_2(x)$? The pattern above shows that it is the sum of all products of a's and b's where the product of their subscripts is n, i.e., it is

$$\sum_{(r,s): rs=n} a_r b_s.$$

Now if rs = n then r and s are divisors of n, so the above sum can also be written as

$$\sum_{d\mid n} a_d b_{\frac{n}{d}},$$

where $d \mid n$ means that d divides n. Here is the conclusion.

Theorem 5.1 If D_1 and D_2 are Dirichlet series of the sequences $\{a_n\}_{n\geq 0}$ and $\{b_n\}_{n\geq 0}$, then D_1D_2 is the Dirichlet series of the sequence $\left\{\sum_{d\mid n}a_db_{\frac{n}{d}}\right\}_{n=1}^{\infty}$.

Following a similar reasoning we may also understand the kth power of a Dirichlet series D(x).

Observe that we have

$$D(x)^{k} = \left(\sum_{n\geq 1} a_{n} n^{-x}\right)^{k}$$

$$= \sum_{n_{1},\dots,n_{k}\geq 1} a_{n_{1}} \dots a_{n_{k}} (n_{1} n_{2} \dots n_{k})^{-x}$$

$$= \sum_{n\geq 1} n^{-x} \left(\sum_{n_{1} \dots n_{k} = n} a_{n_{1}} \dots a_{n_{k}}\right).$$

So, we reach at

Theorem 5.2 $D(x)^k$ is the Dirichlet series of a sequence whose nth member is the sum, extended over all ordered factorizations of n into k factors, of the products of the members of the sequence whose subscripts are the factors in that factorization.

Example 5.1 What is the Dirichlet series corresponding to the constant sequence $a_n = 1$, $n \ge 1$? It is

$$\zeta(x) = \sum_{n>1} \frac{1}{n^x} = 1^{-x} + 2^{-x} + 3^{-x} + \cdots,$$

which is known to be Riemann zeta function.

Next, what sequence does $\zeta^2(x)$ generate? We have

$$[n^{-x}]\zeta^2(x) = \sum_{d \mid n} 1 \cdot 1 = d(n),$$

where d(n) is the number of divisors of the integer n.

One can go on and study further examples of interesting number- theoretic sequences that are generated by relatives of the Riemann zeta function, but there is a somewhat breathtaking generalization that takes in all of these at a single swoop, so let's prepare the groundwork for that in next section.

Problem 5.1 Find the Dirichlet generating functions of the following two sequences:

$$i \ a_n = n^{\alpha}, \ n = 1, 2, \dots$$

 $ii \ a_n = \ln n, \ n = 1, 2, \dots$

Problem 5.2 Find the Dirichlet generating funtion of the Von Mangoldt function defined by

$$\Lambda(n) = \begin{cases} 0, & otherwise \\ \log p, & if \ n = p^m. \end{cases}$$

6 Euler's prime number identity

Theorem 6.1 (Euler's prime number identity) Let f be a multiplicative number-theoretic function. Then we have the formal identity

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^x} = \prod_p \left(1 + f(p)p^{-x} + f(p^2)p^{-2x} + f(p^3)p^{-3x} + \cdots \right),$$

where the product on right-hand side is taken over all prime numbers p.

Proof: Each factor in the product on right-hand side is an infinite series. The product looks like this, when spread out in detail:

$$(1+f(2)2^{-x}+f(2^{2})2^{-2x}+f(2^{3})2^{-3x})\times$$

$$1+f(3)3^{-x}+f(3^{2})3^{-2x}+f(3^{3})3^{-3x})\times$$

$$(1+f(5)5^{-x}+f(5^{2})5^{-2x}+f(5^{3})5^{-3x})\times$$

$$(1+f(7)7^{-x}+f(7^{2})7^{-2x}+f(7^{3})7^{-3x})\times\cdots$$
(2)

Let n now be some fixed integer, whose prime factorization is given by

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

In order to obtain a term that involves n^{-s} , i.e., that involves $\prod p^{-a_i x}$'s, we must choose the '1' term in every parenthesis on the right side of (2), except for those parentheses that involve the primes p_i that actually occur in n. Inside a parenthesis that belongs to p_i , we must choose the one and only term in which p_i is raised to the power with which it actually occurs in n, else we won't have a chance of getting n^{-x} . Thus we are forced to choose the term $f(p_i^{a_i})p_i^{-a_i x}$ out of the parenthesis that belongs to p_i . This means that the coefficient of n^{-x} in the end will be

$$\prod_{i} f(p_a^{a_i}) = f(n),$$

since f is multiplicative.

The fact that a multiplicative function is completely determined by its values on all prime powers is reflected in Euler's prime number identity. Indeed, on the right side we see only the values of f at prime powers, but on the left, all possible values appear.

Example 6.1 If we take the multiplication function f(n) = 1 for all n, then

$$\zeta(x) = \Pi_p(1 + p^{-x} + p^{-2x} + \cdots) = \Pi_p\left(\frac{1}{1 - p^{-x}}\right) = \frac{1}{\Pi_p(1 - p^{-x})}.$$

7 Möbius inversion

The classical Möbius inversion formula was introduced into number theory during the 19th century by August Ferdinand Möbius. Recall that the Möbius function was defined as the multiplicative extension of

$$\mu(p^a) = \begin{cases} +1, & \text{if } a = 0\\ -1, & \text{if } a = 1\\ 0, & \text{if } a \ge 2. \end{cases}$$

Theorem 6.1 applied on μ gives

$$\sum_{n\geq 1} \frac{\mu(n)}{n^x} = \Pi_p(1 - p^{-x}).$$

Now since $\Pi_p(1-p^{-x}) = \frac{1}{\zeta(x)}$ from our last example in previous subsection, we may conclude that

$$\frac{1}{\zeta(x)} = \sum_{n \ge 1} \frac{\mu(n)}{n^x}.$$

That is $\frac{1}{\zeta(x)}$ is the Dirichlet series for the sequence $\{\mu(n)\}_{n\geq 1}$. Why is this observation useful? Let's see on an example.

Example 7.1 Assume that the two sequences $\{a_n\}_{n\geq 1}$ and $\{b_n\}_{n\geq 1}$ are related to each other by

$$a_n = \sum_{d|n} b_d, \qquad n \ge 1.$$

How can we solve for the b's in terms of a's?

Let the corresponding Dirichlet generating functions be A(s) and B(s). Then by Theorem 5.1

$$A(x) = B(x)\zeta(x),$$

or

$$B(x) = \frac{A(x)}{\zeta(x)}.$$

Now again by Theorem 5.1,

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

We just arrived at the celebrated Möbius Inversion Formula of number theory.

Theorem 7.1 (Möbius Inversion Formula) Assume that the two sequences $\{a_n\}_{n\geq 1}$ and $\{b_n\}_{n\geq 1}$ are related to each other by

$$a_n = \sum_{d|n} b_d, \qquad n \ge 1.$$

Then

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

Problem 7.1 Prove the following variation of the Möbius inversion formula. Let $\{a_n(x)\}$ and $\{b_n(x)\}$ be two sequences of functions that are connected by the relation

$$a_n(x) = \sum_{d|n} b_{\frac{n}{d}}(x^d), \qquad n = 1, 2, \dots$$

Then we have

$$b_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d^{x^{n/d}}.$$

7.1 Application I: Primitive bit strings

How many strings of n 0's and 1's are primitive, in the sense that such a string is not expressible as a concatenation of several identical smaller strings?

For instance, 100100100 is not primitive, but 1101 is.

There are a total of 2^n strings of length n. Suppose f(n) of these are primitive. Every string of length n is uniquely expressible as a concatenation of some number, n/d, of identical primitive strings of length d, where d is a divisor of n.

Thus we have

$$2^n = \sum_{d \mid n} f(d)$$
 $n = 1, 2, \dots$

Therefore

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) 2^d$$
 $n = 1, 2, \dots$

7.2 Application II: Cyclotomic polynomials

In general, the equation $x^n = 1$ has n roots that are given by $w_i = e^{2\pi i k/n}$, k = 0, 1, ..., n-1. The **primitive** nth roots of unity are defined as the subset

$${e^{2\pi ik/n}: 0 \le k \le n-1, (k,n) = 1}.$$

Recalling that the number of positive integers that are relatively prime to n is given by Euler's totient function, we see that the set of primitive nth roots of unity contain $\phi(n)$ terms. The question here is to determine the polynomial of order $\phi(n)$ which has the primitive nth roots of unity as its roots. This polynomial is called nth order cyclotomic polynomial, and is denoted by $\Phi_n(x)$. In other words, the cyclotomic polynomials are given by

$$\Phi_n(x) = \prod_{0 \le k \le n-1, (k,n)=1} (x - e^{2\pi i k/n}), n \ge 2.$$

We will need the following fact whose proof is left for you:

Fact: $\Phi_n(x)$ satisfies

$$\prod_{d|n} \Phi_d(x) = 1 - x^n.$$

Using this we have

$$\sum_{d|n} \log \Phi_d(x) = \log(1 - x^n),$$

which after usign Möbius inversion gives

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}, \qquad n = 1, 2, \dots$$

Proposition 7.1 The nth order cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}.$$

Example 7.2 Using the proposition, it is immediate that

$$\Phi_{12}(x) = (1-x)^{\mu(12)} (1-x^3)^{\mu(4)} (1-x^4)^{\mu(3)} (1-x^6)^{\mu(2)} (1-x^{12})^{\mu(1)}
= \frac{(1-x^2)(1-x^{12})}{(1-x^4)(1-x^6)}
= 1-x^2+x^4.$$

8 The Von Mangoldt function

Definition 8.1 The Von Mangoldt function is defined by

$$\Lambda(n) = \begin{cases} 0, & otherwise \\ \log p, & if \ n = p^m. \end{cases}$$

Problem 8.1 Check that Λ is neither additive nor multiplicative.

Theorem 8.1 We have

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

Proof: Letting $n = \prod_{i=1}^k p_i^{\alpha_i}$ be the prime factorization of n,

$$\sum_{d:d|n} \Lambda(d) = \sum_{j=1}^k \sum_{r=1}^{\alpha_j} \Lambda(p_j^{\alpha_r}) = \sum_{j=1}^k \sum_{r=1}^{\alpha_j} \log p$$

$$= \sum_{j=1}^k \alpha_j \log p$$

$$= \sum_{j=1}^k \log(p_j^{\alpha_j})$$

$$= \log \left(\prod_{i=1}^k p_i^{\alpha_i}\right)$$

$$= \log n.$$

9 Exercises

Problem 9.1 Let f be a multiplicative function satisfying $\lim_{p^m \to \infty} f(p^m) = 0$. Show that $\lim_{n \to \infty} f(n) = 0$.

Problem 9.2 *Show that, for every positive integer* $n \geq 2$ *,*

$$\sum_{1 \le k \le n-1, (k,n)=1} k = \frac{n}{2} \phi(n).$$

Problem 9.3 Evaluate the function

$$f(n) = \sum_{d^2 \mid n} \mu(d)$$

(where the summation runs over all positive integers d such that $d^2|n$), in the sense of expressing it in terms of familiar arithmetic functions.

Problem 9.4 Let $f(n) = \sum_{d|n} \mu(d) \log d$. Find a simple expression for f(n) in terms of familiar arithmetic functions.

Problem 9.5 Let $f(n) = \#\{(n_1, n_2) \in \mathbb{N}^2 : [n_1, n_2] = n\}$ where $[n_1, n_2]$ is the least common multiple of n_1 and n_2 . Show that f is multiplicative and evaluate f at prime powers.

References

- [1] Bryant, Victor. Aspects of Combinatorics: A wide-ranging introduction. Cambridge University Press, 1993.
- [2] Hildebrand, A. J., Introduction to analytic number theory, 2005.
- [3] Wilf, Herbert S. Generating functionology. Elsevier, 2013.