Möbius Inversion Formula

MATH 110 | Introduction to Number Theory | Summer 2023

Student name: [Your Full Name Here]

July 19, 2023

Arithmetic functions play a crucial role in number theory, providing insights into the fundamental properties of integers. The *Möbius inversion formula*, introduced into number theory in 1832 by August Ferdinand Möbius, serves as a bridge between different arithmetic functions, allowing us to deduce properties and reveal hidden relationships between them. In this essay, we will delve into the world of arithmetic functions, introducing relevant concepts and providing a proof of the Möbius inversion formula.

This essay is organized as follows: In Section 1, we will introduce the statement of the formula. Moving on to Section 2, we will delve into the concept of *Dirichlet convolution* and explore its fundamental properties, providing the necessary groundwork for the subsequent proof. In the conclusive Section 3, we will utilize Dirichlet convolution to present a proof of the Möbius inversion formula. Finally, in Section 4, we will demonstrate a practical application of the Möbius inversion formula by showcasing its usage on the *Euler totient function*.

1 The Möbius function and the inversion formula

To state the Möbius inversion formula, we need the following notions.

Definition 1.1. We say that a positive integer n is *square-free* if n is not divisible by p^2 for any prime number p. The *Möbius function* is defined as follows:

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not sqaure-free}, \\ (-1)^t & \text{if } n \text{ is sqaure-free and has exactly } t \text{ prime divisors.} \end{cases}$$

The Möbius function μ is an *arithmetic function*. Namely, it is a complex-valued function defined on the set $\mathbb{Z}_+$ of positive integers.

Definition 1.2. The *Möbius transformation* of an arithmetic function f is the function $\widehat{f}$ defined by the formula

$$\widehat{f}(n) := \sum_{d|n} f(d). \tag{1.1}$$

Then the Möbius inversion formula can be stated as follows.

Theorem 1.3 (Möbius inversion formula). *For any arithmetic function f, we have*

$$f(n) = \sum_{d|n} \mu(\frac{n}{d})\widehat{f}(d). \tag{1.2}$$

2 Dirichlet convolution

To better understand the Möbius inversion formula, we introduce the following concept.

Definition 2.1. Given two arithmetic functions f and g, their *Dirichlet convolution*, denoted as $f \star g$, is defined as follows:

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \tag{2.1}$$

where the summation is taken over the divisor set $\mathscr{D}(n) := \{d \mid d \text{ is a divisor of } n\}$.

The basic property of Dirichlet convolution is the following.

Theorem 2.2. *The set of arithmetic functions, together with the Dirichlet convolution, forms a commutative monoid. Namely, the followings hold.*

1. *The binary operation $\star$ is* associative*: for any arithmetic functions f, g, and h,*

$$(f \star g) \star h = f \star (g \star h). \tag{2.2}$$

2. *The binary operation $\star$ has a* neutral element*. Indeed, let δ be the function defined as follows:*

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

Then δ is a neutral element *for the binary operation $\star$: for any arithmetic function f,*

$$\delta \star f = f \star \delta = f. \tag{2.3}$$

3. *The binary operation $\star$ is* commutative*: for any arithmetic functions f and g,*

$$f \star g = g \star f. \tag{2.4}$$

Proof. (PROOF NEED TO BE FILLED) □

Among all arithmetic functions, the *multiplicative* one usually play special roles.

Definition 2.3. An arithmetic function f is said to be *multiplicative*, if for any pair of coprime positive integers (m, n), we have

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

We can restrict Dirichlet convolution on the subset of multiplicative functions.

Proposition 2.4. *The subset of multiplicative functions, together with the Dirichlet convolution, forms a submonoid of the commutative monoid of all arithmetic functions. Namely, we have:*

1. *The subset of multiplicative functions is closed under the binary operation $\star$: for any arithmetic functions f and g, if both f and g are multiplicative, then $f \star g$ is also multiplicative.*

2. *The subset of multiplicative functions contains the neutral element δ of the binary operation $\star$.*

Proof. (PROOF NEED TO BE FILLED) □

It is worth to note that

Proposition 2.5. *The Möbius function μ is multiplicative.*

Proof. (PROOF NEED TO BE FILLED) □

3 Proof of the Möbius Inversion Formula

With the foundation of Dirichlet convolution in place, we are ready to present the proof of the Möbius inversion formula.

We first note that

Lemma 3.1. *For any arithmetic function f, its Möbius transformation $\widehat{f}$ is $f \star \mathbf{1}$. Where $\mathbf{1}$ is the constant function mapping any positive integer to 1.*

Proof. (PROOF NEED TO BE FILLED) □

Corollary 3.2. *The Möbius transformation of a multiplicative function is also multiplicative.*

Proof. (PROOF NEED TO BE FILLED) □

Moreover, we have

Lemma 3.3. *The Möbius function μ is the inverse of $\mathbf{1}$ under the binary operation $\star$. Namely, $\mathbf{1} \star \mu = \delta$.*

Proof. (PROOF NEED TO BE FILLED) □

Now, we can restate Theorem 1.3 using Dirichlet convolution.

Theorem 3.4. *For any arithmetic function f, we have*

$$f = \widehat{f} \star \mu. \tag{3.1}$$

Indeed, Equations (1.2) and (3.1) are equivalent: (PROOF NEED TO BE FILLED)

We are now able to demonstrate the proof of Theorem 3.4.

Proof. We have

$$\begin{aligned} \widehat{f} \star \mu &= (f \star \mathbf{1}) \star \mu && \text{by Lemma 3.1} \\ &= f \star (\mathbf{1} \star \mu) && \text{by associativity of } \star \\ &= f \star \delta && \text{by Lemma 3.3} \\ &= f && \delta \text{ is the neutral element for } \star. \end{aligned}$$

This proves Equation (3.1). □

We are thus able to extend Corollary 3.2:

Corollary 3.5. *An arithmetic function f is multiplicative if and only if its Möbius transformation $\widehat{f}$ is multiplicative.*

Proof. (PROOF NEED TO BE FILLED) □

4 Euler totient function

We will use the Möbius inversion formula to obtain some properties of the *Euler totient function*.

Definition 4.1. The *Euler totient function* $\varphi(n)$ counts the set $\Phi(n)$ of integers from 0 to $n-1$ which are coprime to n.

Our key step is:

Theorem 4.2. *Let* id *denote the identity map. Then* id *is the Möbius transformation of the Euler totient function* φ*.*

Proof. (PROOF NEED TO BE FILLED) ☐

Then we have the followings.

Corollary 4.3. *The Euler totient function* φ *is multiplicative.*

Proof. First note that id is multiplicative: (PROOF NEED TO BE FILLED).
Since id is the Möbius transformation of φ, by Corollary 3.5, φ is also multiplicative. ☐

Corollary 4.4. *We have the following formula.*

$$\varphi(n) = n \prod_{p \textit{ is a prime divisor of } n} \left(1 - \frac{1}{p}\right). \tag{4.1}$$

Proof. Suppose the prime factorization of n gives

$$n = \prod_{p \text{ is a prime divisor of } n} p^{e_p}.$$

Then by the multiplicativity of φ, we have

$$\varphi(n) = \prod_{p \text{ is a prime divisor of } n} \varphi(p^{e_p}).$$

On the other hand, the right-hand side of Equation (4.1) can be written as

$$\prod_{p \text{ is a prime divisor of } n} \left(p^{e_p}1 - p^{e_p-1}\right).$$

Hence, it suffices to proof the following lemma:

Lemma 4.5. *For any prime* p *and any positive integer* e*, we have* $\varphi(p^e) = p^e - p^{e-1}$*.*

Proof. (PROOF NEED TO BE FILLED) ☐

Now Equation (4.1) follows by previous argument. ☐

References

[TEXT] *An Illustrated Theory of Numbers*, Martin H. Weissman.