Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Introduction

Introduction

- Number theory often considers sequences of real or complex numbers.
- Such sequences are called arithmetical functions.

Definition

An **arithmetical function** or a **number-theoretic function** is a real- or complex-valued function defined on the positive integers.

- We introduce several arithmetical functions which play an important role in:
  - The study of divisibility properties of integers;
  - The distribution of primes.
- Dirichlet multiplication clarifies some relations between various arithmetical functions.

Subsection 2

The Möbius Function $\mu(n)$

The Möbius Function

Definition

The **Möbius function** μ is defined as follows:

- $\mu(1) = 1$;
- If $n > 1$, write $n = p_1^{a_1} \cdots p_k^{a_k}$. Then:
  - $\mu(n) = (-1)^k$, if $a_1 = a_2 = \cdots = a_k = 1$;
  - $\mu(n) = 0$, otherwise.

Note that $\mu(n) = 0$ if and only if n has a square factor > 1.

- A short table of values of $\mu(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

The Divisor Sum of the Möbius Function

- We consider the sum $\sum_{d|n} \mu(d)$, over the positive divisors of n.
- $[x]$ denotes the greatest integer $\leq x$.

Theorem

If $n \geq 1$, we have

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

- The formula is clearly true if $n = 1$.

  Assume, then, that $n > 1$ and write $n = p_1^{a_1} \cdots p_k^{a_k}$.

  In $\sum_{d|n} \mu(d)$ the only nonzero terms come from $d = 1$ and from those divisors of n which are products of distinct primes.

The Divisor Sum of the Möbius Function (Cont'd)

- Thus,

$$\begin{aligned}\sum_{d|n}\mu(d) &= \mu(1)+\mu(p_1)+\cdots+\mu(p_k)\\ &\quad +\mu(p_1p_2)+\cdots+\mu(p_{k-1}p_k)\\ &\quad +\cdots+\mu(p_1p_2\cdots p_k)\\ &= 1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\cdots+\binom{k}{k}(-1)^k\\ &= (1-1)^k\\ &= 0.\end{aligned}$$

Subsection 3

The Euler Totient Function $\varphi(n)$

The Euler Totient Function

Definition

If $n > 1$, the **Euler totient** $\varphi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n. Thus,

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

where the $'$ indicates that the sum is extended over those k relatively prime to n.

- A short table of values of $\varphi(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

The Divisor Sum of the Totient Function

- There is a simple formula for $\sum_{d|n}\varphi(d)$.

Theorem

If $n \geq 1$, we have

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

- Let S denote the set $\{1, 2, \ldots, n\}$.
  We distribute the integers of S into disjoint sets.
  For each divisor d of n, let

$$A(d) = \{k : (k, n) = d, 1 \leq k \leq n\}.$$

  $A(d)$ contains those elements of S which have the gcd d with n.
  The sets $A(d)$ form a disjoint collection whose union is S.
  So, if $f(d)$ denotes the number of integers in $A(d)$, $\sum_{d|n} f(d) = n$.

The Divisor Sum of the Totient Function (Cont'd)

- We obtained $\sum_{d|n} f(d) = n$.

  Now we have:
  - $(k, n) = d$ if and only if $(k/d, n/d) = 1$;
  - $0 < k \le n$ if and only if $0 < k/d \le n/d$.

  Let $q = k/d$.

  Then there is a one-to-one correspondence between the elements in $A(d)$ and those integers q satisfying $0 < q \le n/d$, $(q, n/d) = 1$.

  The number of such q is $\varphi(n/d)$.

  Hence $f(d) = \varphi(n/d)$.

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

  But, when d runs through all divisors of n, so does n/d.

  So the last equation is equivalent to $\sum_{d|n} \varphi(d) = n$.

Subsection 4

A Relation Connecting μ and φ

A Relation Connecting μ and φ

Theorem

If $n \geq 1$, we have

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

- The sum $\varphi(n) = \sum_{k=1}^{n}{}' 1$ can be rewritten in the form $\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right]$, where k runs through all integers $\leq n$.

  Now we use $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]$, with n replaced by (n,k).

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

A Relation Connecting μ and φ (Cont'd)

- We obtained

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

For a fixed divisor d of n, we must sum over all those k in the range $1 \leq k \leq n$ which are multiples of d.

Write $k = qd$.

Then $1 \leq k \leq n$ if and only if $1 \leq q \leq n/d$.

Hence the last sum for $\varphi(n)$ can be written as

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

Subsection 5

A Product Formula for $\varphi(n)$

A Product Formula for $\varphi(n)$

Theorem (Product Formula for $\varphi(n)$)

For $n \geq 1$, we have

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

- For $n = 1$ the product is empty since no primes divide 1.

  Then it is understood that the product is to be assigned the value 1.

  Let $n > 1$ and $p_1, \ldots, p_r$ be the distinct prime divisors of n.

  The product can be written as

$$\begin{aligned} \textstyle\prod_{p|n}(1 - \frac{1}{p}) &= \textstyle\prod_{i=1}^{r}(1 - \frac{1}{p_r}) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \frac{(-1)^r}{p_1 p_2 \cdots p_r}. \end{aligned}$$

A Product Formula for $\varphi(n)$ (Cont'd)

- We have

$$\prod_{p|n}\left(1-\frac{1}{p}\right)=1-\sum\frac{1}{p_i}+\sum\frac{1}{p_ip_j}-\sum\frac{1}{p_ip_jp_k}+\cdots+\frac{(-1)^r}{p_1p_2\cdots p_r}.$$

On the right, in a term such as $\sum\frac{1}{p_ip_jp_k}$ it is understood that we consider all possible products $p_ip_jp_k$ of distinct prime factors of n taken three at a time.

Note that each term on the right is of the form $\pm\frac{1}{d}$, where d is a divisor of n which is either 1 or a product of distinct primes.

The numerator ± 1 is exactly $\mu(d)$.

We have $\mu(d)=0$ if d is divisible by the square of any p_i.

So the sum is exactly the same as $\sum_{d|n}\frac{\mu(d)}{d}$. Thus,

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

Properties of the Euler Totient Function

Theorem

Euler's totient has the following properties:

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for prime p and $a \geq 1$.

(b) $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, where $d = (m,n)$.

(c) $\varphi(mn) = \varphi(m)\varphi(n)$, if $(m,n) = 1$.

(d) $a \mid b$ implies $\varphi(a) \mid \varphi(b)$.

(e) $\varphi(n)$ is even for $n \geq 3$. Moreover, if n has r distinct odd prime factors, then $2^r \mid \varphi(n)$.

(a) This follows by taking $n = p^\alpha$ in the product formula.

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

Each prime divisor of mn is either a prime divisor of m or of n.

Moreover, those primes which divide both m and n also divide (m,n).

Properties of the Euler Totient Function (Cont'd)

Hence

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

(c) This is a special case of (b).

(d) Since $a \mid b$, we have $b = ac$, where $1 \leq c \leq b$.

- If $c = b$, then $a = 1$. Part (d) is trivially satisfied.
- Assume $c < b$. From (b) we have $\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)}$, where $d = (a, c)$. Now the result follows by induction on b.
  - For $b = 1$ it holds trivially.
  - Suppose that (d) holds for all integers $< b$. Then it holds for c. So $\varphi(d) \mid \varphi(c)$, since $d \mid c$. Hence, the right side of the equation is a multiple of $\varphi(a)$. So $\varphi(a) \mid \varphi(b)$.

Properties of the Euler Totient Function (Cont'd)

(e) If $n = 2^\alpha$, $\alpha \geq 2$, Part (a) shows that $\varphi(n)$ is even.

Suppose n has at least one odd prime factor.

Then we write

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1) = c(n) \prod_{p|n} (p-1),$$

where $c(n)$ is an integer.

The product multiplying $c(n)$ is even.

So $\varphi(n)$ is even.

Moreover, each odd prime p contributes a factor 2 to this product.

So $2^r \mid \varphi(n)$, if n has r distinct odd prime factors.

Subsection 6

The Dirichlet Product of Arithmetical Functions

Introducing the Dirichlet Product

- We proved that

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

- The sum on the right is of a type that occurs frequently in number theory.
- These sums have the form

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

where f and g are arithmetical functions.

- It is fruitful to treat these sums as a new kind of multiplication of arithmetical functions.

The Dirichlet Product of Arithmetical Functions

Definition

If f and g are two arithmetical functions we define their **Dirichlet product** (or **Dirichlet convolution**) to be the arithmetical function h defined by the equation

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

Notation: We write $f * g$ for h and $(f * g)(n)$ for $h(n)$.

- The symbol N will be used for the arithmetical function for which

$$N(n) = n, \text{ for all } n.$$

- In this notation, $\varphi = \mu * N$.

Commutativity and Associativity

Theorem

Dirichlet multiplication is commutative and associative. That is, for any arithmetical functions f, g, k, we have

$$f * g = g * f \quad (\textbf{commutative law});$$
$$(f * g) * k = f * (g * k) \quad (\textbf{associative law}).$$

- First we note that the definition of $f * g$ can also be expressed as follows:

$$(f * g)(n) = \sum_{a \cdot b = n} f(a) g(b),$$

where a and b vary over all positive integers whose product is n.

This makes the commutative property self-evident.

Commutativity and Associativity (Cont'd)

- For the associative property, we let $A = g * k$.

  We consider $f * A = f * (g * k)$.

$$\begin{aligned} (f * A)(n) &= \textstyle\sum_{a \cdot d = n} f(a) A(d) \\ &= \textstyle\sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b) k(c) \\ &= \textstyle\sum_{a \cdot b \cdot c = n} f(a) g(b) k(c). \end{aligned}$$

  Similarly, let $B = f * g$ and consider $B * k$.

  We are led to the same formula for $(B * k)(n)$.

  Hence $f * A = B * k$.

  So the Dirichlet multiplication is associative.

The Identity of the Dirichlet Multiplication

Definition

The arithmetical function I given by

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

is called the **identity function**.

Theorem

For all f, we have $I * f = f * I = f$.

- Note that $\left[\frac{d}{n}\right] = 0$, if $d < n$.
  So we have

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

Subsection 7

Dirichlet Inverses and the Möbius Inversion Formula

The Dirichlet Inverse

Theorem

If f is an arithmetical function with $f(1) \neq 0$, there is a unique arithmetical function f^{-1}, called the **Dirichlet inverse** of f, such that

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

Moreover, f^{-1} is given by the recursion formulas

$$f^{-1}(n) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d \mid n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d), \text{ for } n > 1.$$

- Given f, we shall show that the equation $(f * f^{-1})(n) = I(n)$ has a unique solution for the function values $f^{-1}(n)$.

The Dirichlet Inverse (Base)

- For $n = 1$, we have to solve the equation
$$(f * f^{-1})(1) = I(1).$$
This reduces to
$$f(1)f^{-1}(1) = 1.$$
By hypothesis, $f(1) \neq 0$.
So there is one and only one solution, namely
$$f^{-1}(1) = \frac{1}{f(1)}.$$

The Dirichlet Inverse (Induction Step)

- Assume now that the function values $f^{-1}(k)$ have been uniquely determined for all $k < n$. Then we have to solve the equation $(f * f^{-1})(n) = I(n)$. Equivalently, $\sum_{d|n} f(\frac{n}{d})f^{-1}(d) = 0$. This can be written as

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

  Suppose the values $f^{-1}(d)$ are known for all divisors $d < n$.

  Then, since $f(1) \neq 0$, there is a uniquely determined value for $f^{-1}(n)$:

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

  We have the existence and uniqueness of f^{-1} by induction.

The Group Structure of Arithmetic Functions

- Consider the set of all arithmetical functions f, with $\mathrm{f}(1) \neq 0$.
- It is closed under $*$, since, if $f(1) \neq 0$ and $g(1) \neq 0$, then

$$(f * g)(1) = f(1)g(1) \neq 0.$$

- Moreover, we have seen that $*$ on this set satisfies:
  - The commutative law;
  - The associative law;
  - The existence of an identity I;
  - The existence of an inverse.
- We conclude that the set forms an abelian group with respect to the operation $*$.
- It can be shown that if $f(1) \neq 0$ and $g(1) \neq 0$,

$$(f * g)^{-1} = f^{-1} * g^{-1}.$$

The Unit Function u

Definition

We define the **unit function** u to be the arithmetical function such that

$$u(n) = 1, \quad \text{for all } n.$$

- We saw that
$$\sum_{d|n} \mu(d) = I(n).$$
- In the notation of Dirichlet multiplication this becomes
$$\mu * u = I.$$
- Thus u and μ are Dirichlet inverses of each other,
$$u = \mu^{-1} \quad \text{and} \quad \mu = u^{-1}.$$

The Möbius Inversion Formula

Theorem (Möbius Inversion Formula)

The equation

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

implies

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

and conversely.

- The first equation states that $f = g * u$.
  Multiplication by μ gives

  $$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g.$$

  Conversely, multiplication of $f * \mu = g$ by u gives the first equation.

Example

- We saw that
$$n = \sum_{d|n} \varphi(d).$$
We also saw that
$$\varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

Subsection 8

The Mangoldt Function $\Lambda(n)$

The Mangoldt Function

- Mangoldt's function Λ plays a central role in the distribution of primes.

Definition

For every integer $n \geq 1$, we define

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

- Here is a short table of values of $\Lambda(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

Mangoldt Function and Fundamental Theorem

Theorem

If $n \geq 1$, we have
$$\log n = \sum_{d|n} \Lambda(d).$$

- The theorem is true if $n = 1$, since both members are 0.
  Therefore, assume that $n > 1$ and write $n = \prod_{k=1}^r p_k^{a_k}$.
  Taking logarithms we have $\log n = \sum_{k=1}^r a_k \log p_k$.
  In the sum on the right the only nonzero terms come from those divisors d of the form p_k^m, for $m = 1, 2, \ldots, a_k$ and $k = 1, 2, \ldots, r$.
  Hence,
$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^r \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^r \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^r a_k \log p_k = \log n.$$

Sum Formula for $\Lambda(n)$

- We use Möbius inversion to express $\Lambda(n)$ in terms of the logarithm.

Theorem

If $n \geq 1$, we have

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

- Inverting $\log n = \sum_{d|n} \Lambda(d)$ by the Möbius inversion formula we obtain

$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log \tfrac{n}{d} \\ &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= I(n) \log n - \sum_{d|n} \mu(d) \log d. \end{aligned}$$

But $I(n) \log n = 0$, for all n. This completes the proof.