Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Multiplicative Functions

Multiplicative Functions

- Recall that the set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group under Dirichlet multiplication.
- An important subgroup consists of the multiplicative functions.

Definition

An arithmetical function f is called **multiplicative** if f is not identically zero and if, whenever $(m, n) = 1$,

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

A multiplicative function f is called **completely multiplicative** if we also have

$$f(mn) = f(m)f(n), \quad \text{for all } m, n.$$

Examples

Example: Let

$$f_\alpha(n) = n^\alpha,$$

where α is a fixed real or complex number.

This function is completely multiplicative.

In particular, the unit function $u = f_0$ is completely multiplicative.

We denote the function f_α by N^α and call it the **power function**.

Example: The identity function

$$I(n) = \left[\frac{1}{n}\right]$$

is completely multiplicative.

Examples

Example: The Möbius function is multiplicative but not completely multiplicative.

This is easily seen from the definition of $\mu(n)$.

Consider two relatively prime integers m and n.

- Suppose either m or n has a prime-square factor. Then so does mn. So both $\mu(mn)$ and $\mu(m)\mu(n)$ are zero.
- Suppose neither has a square factor. 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 we have $\mu(m) = (-1)^s$, $\mu(n) = (-1)^t$ and $\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$.

This shows that μ is multiplicative.

It is not completely multiplicative since $\mu(4) = 0$ but $\mu(2)\mu(2) = 1$.

Example: The Euler totient $\varphi(n)$ is multiplicative.

This is Part (c) of a previous theorem.

It is not completely multiplicative as $\varphi(4) = 2$ but $\varphi(2)\varphi(2) = 1$.

More Examples

Example: The ordinary product fg of two arithmetical functions f and g is defined by the usual formula

$$(fg)(n) = f(n)g(n).$$

Similarly, the quotient f/g is defined by the formula

$$\left(\frac{f}{g}\right)(n) = \frac{f(n)}{g(n)}, \text{ whenever } g(n) \neq 0.$$

- If f and g are multiplicative, so are fg and $\frac{f}{g}$.
- If f and g are completely multiplicative, so are fg and $\frac{f}{g}$.

Multiplicative Functions: Value at 1

Theorem

If f is multiplicative then $f(1) = 1$.

- We have $(n, 1) = 1$, for all n.

  Hence,

  $$f(n) = f(1)f(n).$$

  By hypothesis, f is not identically zero.

  So we have $f(n) \neq 0$, for some n.

  This implies that $f(1) = 1$.

  Note: Since $\Lambda(1) = 0$, the Mangoldt function is not multiplicative.

Characterization of Multiplicativity

Theorem

Given f with $f(1) = 1$. Then:

(a) f is multiplicative if, and only if,

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r}),$$

for all primes p_i and all integers $a_i \geq 1$.

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

$$f(p^a) = f(p)^a.$$

- The proof follows easily from the definitions.

Subsection 2

Multiplicative Functions and Dirichlet Multiplication

Dirichlet Product of Multiplicative Functions

Theorem

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

- Suppose $h = f * g$.

  Choose relatively prime integers m and n.

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

  Every divisor c of mn can be expressed in the form $c = ab$, where:
  - $a \mid m$;
  - $b \mid n$.

  Moreover:
  - $(a, b) = 1$;
  - $(\frac{m}{a}, \frac{n}{b}) = 1$;
  - There is a one-to-one correspondence between the set of products ab and the divisors c of mn.

Dirichlet Product of Multiplicative Functions

- Now we have

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

Warning: The Dirichlet product of two completely multiplicative functions need not be completely multiplicative.

A Partial Converse

Theorem

If both g and $f * g$ are multiplicative, then f is also multiplicative.

- By way of contraposition, assume that f is not multiplicative.

  We deduce that $f * g$ is also not multiplicative.

  Let $h = f * g$.

  By our assumption, there exist positive integers m and n, with $(m, n) = 1$, such that

  $$f(mn) \neq f(m)f(n).$$

  We choose such a pair m and n for which the product mn is as small as possible.

  - Assume, first, that $mn = 1$. Then $f(1) \neq f(1)f(1)$. So $f(1) \neq 1$.
    Now $h(1) = f(1)g(1) = f(1) \neq 1$.
    So h is not multiplicative.

A Partial Converse (Cont'd)

- If $mn > 1$, then we have $f(ab) = f(a)f(b)$, for all positive integers a and b with $(a,b) = 1$ and $ab < mn$.

  Now we argue as in the proof of the preceding theorem.

  In the sum defining $h(mn)$ we separate the term corresponding to $a = m$, $b = n$.

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

  Since $f(mn) \neq f(m)f(n)$, this shows that $h(mn) \neq h(m)h(n)$.

  So h is not multiplicative.

Dirichlet Inverse of Multiplicative Functions

Theorem

If g is multiplicative, so is g^{-1}, its Dirichlet inverse.

- We have $g * g^{-1} = I$.

  Moreover, we know that:
  - g is multiplicative, by hypothesis;
  - I is multiplicative, by a previous example.

  So, by the preceding theorem, g^{-1} is also multiplicative.

  Note: The theorems of this section show that the set of multiplicative functions is a subgroup of the group of all arithmetical functions f with $f(1) \neq 0$.

Subsection 3

The Inverse of a Completely Multiplicative Function

Completely Multiplicative Functions

Theorem

Let f be multiplicative. Then f is completely multiplicative if, and only if,

$$f^{-1}(n) = \mu(n)f(n), \quad \text{for all } n \geq 1.$$

- Let $g(n) = \mu(n)f(n)$.
  Suppose f is completely multiplicative.
  We take into account that $f(1) = 1$ and $I(n) = 0$, for $n > 1$.
  Then, we have
  $$\begin{array}{rcl} (g * f)(n) & = & \sum_{d \mid n} \mu(d)f(d)f(\frac{n}{d}) \\ & = & f(n)\sum_{d \mid n} \mu(d) \\ & = & f(n)I(n) \\ & = & I(n). \end{array}$$
  Hence, $g = f^{-1}$.

Completely Multiplicative Functions (Converse)

- Conversely, assume
$$f^{-1}(n) = \mu(n)f(n).$$
We must show that $f(p^a) = f(p)^a$ for prime powers.
The equation $f^{-1}(n) = \mu(n)f(n)$ implies, for all $n > 1$,
$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0.$$
Hence, taking $n = p^a$, we have
$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0.$$
So
$$f(p^a) = f(p)f(p^{a-1}).$$
This implies $f(p^a) = f(p)^a$.

Example: The Inverse of Euler's φ Function

- Recall that $\varphi = \mu * N$.

  Taking inverses, we get $\varphi^{-1} = \mu^{-1} * N^{-1}$.

  We know that N is completely multiplicative.

  By the theorem,
  $$N^{-1} = \mu N.$$

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

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

A Formula for $\sum_{d|n}\mu(d)f(d)$ for Multiplicative f

Theorem

If f is multiplicative we have

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

- Let $g(n)=\sum_{d|n}\mu(d)f(d)$. Then g is multiplicative.
  To determine $g(n)$ it suffices to compute $g(p^a)$.

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

  Hence,

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

A Formula for φ^{-1}

Corollary

For every n,

$$\varphi^{-1}(n) = \prod_{p|n}(1-p).$$

- By the preceding example, for all n,

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

By the theorem, for f is multiplicative,

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

So, taking $f = N$, we obtain

$$\varphi^{-1}(n) = \prod_{p|n}(1-p).$$

Subsection 4

Liouville's Function $\lambda(n)$

Liouville's Function

Definition

We define $\lambda(1) = 1$, and if $n = p_1^{a_1} \cdots p_k^{a_k}$, we define

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

- The definition shows that λ is completely multiplicative.

Theorem (Divisor Sum of λ)

For every $n \geq 1$, we have

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

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

Divisor Sum of λ

- Let $g(n) = \sum_{d|n} \lambda(d)$.

  Then g is multiplicative.

  To determine $g(n)$ we need only compute $g(p^a)$ for prime powers.

  We have

$$\begin{array}{rcl} g(p^a) & = & \sum_{d|p^a} \lambda(d) \\ & = & 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a) \\ & = & 1 - 1 + 1 - \cdots + (-1)^a \\ & = & \begin{cases} 0, & \text{if } a \text{ is odd} \\ 1, & \text{if } a \text{ is even} \end{cases} \end{array}$$

Divisor Sum of λ (Cont'd)

- Now, if $n = \prod_{i=1}^{k} p_i^{a_i}$, we have

$$g(n) = \prod_{i=1}^{k} g(p_i^{a_i}).$$

  - If any exponent a_i is odd then $g(p_i^{a_i}) = 0$.
    So $g(n) = 0$.
  - If all the exponents a_i are even, then $g(p_i^{a_i}) = 1$, for all i.
    So $g(n) = 1$.

  This shows that $g(n) = 1$ if n is a square, and $g(n) = 0$ otherwise.

  Finally, by a previous theorem,

$$\lambda^{-1}(n) = \mu(n)\lambda(n) = \begin{cases} (-1)^{2k}, & \text{if } n = p_1 \cdots p_k \\ 0, & \text{othewise} \end{cases} = \mu^2(n) = |\mu(n)|.$$

Subsection 5

The Divisor Functions $\sigma_\alpha(n)$

Divisor Functions

Definition

For real or complex α and any integer $n \geq 1$, we define

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

the sum of the α-th powers of the divisors of n.

- The functions σ_α are called **divisor functions**.
- They are multiplicative because

$$\sigma_\alpha = u * N^\alpha,$$

  the Dirichlet product of two multiplicative functions.
- If $\alpha = 0$, $\sigma_0(n)$ is the number of divisors of n, denoted by $d(n)$.
- If $\alpha = 1$, $\sigma_1(n)$ is the sum of the divisors of n, denoted by $\sigma(n)$.

Computing $\sigma_\alpha(n)$

- Since σ_α is multiplicative, we have

$$\sigma_\alpha(p_1^{a_1}\cdots p_k^{a_k}) = \sigma_\alpha(p_1^{a_1})\cdots\sigma_\alpha(p_k^{a_k}).$$

- To compute $\sigma_\alpha(p^a)$ we note that the divisors of a prime power p^a are

$$1, p, p^2, \ldots, p^a.$$

- Hence,

$$\begin{aligned} \sigma_\alpha(p^a) &= 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} \\ &= \begin{cases} \dfrac{p^{a(\alpha+1)}-1}{p^\alpha - 1}, & \text{if } \alpha \neq 0 \\ a+1, & \text{if } \alpha = 0 \end{cases} \end{aligned}$$

Dirichlet Inverse of σ_α

- The Dirichlet inverse of σ_α can also be expressed as a linear combination of the α-th powers of the divisors of n.

Theorem

For $n \geq 1$, we have

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d) \mu\left(\frac{n}{d}\right).$$

- We have the following:
  - $(N^\alpha)^{-1} = \mu N^\alpha$, since N^α is completely multiplicative;
  - $u^{-1} = \mu$.

  Therefore, taking into account $\sigma_\alpha = N^\alpha * u$, we get

$$\sigma_\alpha^{-1} = (N^\alpha)^{-1} * u^{-1} = (\mu N^\alpha) * \mu.$$

Subsection 6

Generalized Convolutions

Generalized Convolutions

- F denotes a real or complex-valued function defined on the positive real axis $(0, +\infty)$, such that $F(x) = 0$, for $0 < x < 1$.
- Sums of the type $\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$ arise frequently in number theory, where α is any arithmetical function.
- The function defined on $(0, +\infty)$ by

$$G(x) = \sum_{n \leq x} \alpha(n) F(\frac{x}{n})$$

  also vanishes for $0 < x < 1$.
- We denote this function G by $\alpha \circ F$:

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Generalized Convolutions

- We defined
$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$
- If $F(x) = 0$, for all nonintegral x, the restriction of F to the integers is an arithmetical function and we find that for all integers $m \geq 1$,
$$(\alpha \circ F)(m) = (a * F)(m).$$
- So the operation $\circ$ can be regarded as a generalization of the Dirichlet convolution $*$.
- The operation $\circ$ is, in general, neither commutative nor associative.

Associative Property Relating $\circ$ and $*$

Theorem (Associative Property Relating $\circ$ and $*$)

For any arithmetical functions α and β we have

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

- For $x > 0$, we have

$$\begin{aligned}
\{\alpha \circ (\beta \circ F)\}(x) &= \sum_{n \le x} \alpha(n) \sum_{m \le x/n} \beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{mn \le x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{k \le x} \left(\sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right)\right) F\left(\frac{x}{k}\right) \\
&= \sum_{k \le x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\
&= \{(\alpha * \beta) \circ F\}(x).
\end{aligned}$$

Generalized Inversion Formula

- Note that the identity function $I(n) = \left[\frac{1}{n}\right]$ for Dirichlet convolution is also a left identity for $\circ$, i.e., $(I \circ F)(x) = \sum_{n \leq x} \left[\frac{1}{n}\right] F(\frac{x}{n}) = F(x)$.

Theorem (Generalized Inversion Formula)

If α has a Dirichlet inverse α^{-1}, then the equation

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \quad \text{implies} \quad F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right)$$

and conversely.

- Suppose $G = \alpha \circ F$. Then, we have

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Thus, we get the left-to-right implication.

The converse is similarly proved.

Generalized Möbius Inversion Formula

- The following special case is of particular importance.

Theorem (Generalized Möbius Inversion Formula)

If α is completely multiplicative we have

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \quad \text{if and only if} \quad F(x) = \sum_{n \leq x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right).$$

- Under the hypothesis, $\alpha^{-1}(n) = \mu(n)\alpha(n)$.

Subsection 7

Formal Power Series

Power Series

- In calculus an infinite series of the form

$$\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \cdots$$

  is called a **power series in** x.
- Both x and the coefficients $a(n)$ are real or complex numbers.
- To each power series there corresponds a radius of convergence $r \geq 0$ (r can be $+\infty$), such that:
  - The series converges absolutely if $|x| < r$;
  - The series diverges if $|x| > r$.

Introducing Formal Power Series

- In this section we consider power series from a different point of view.
- We call them **formal power series** to distinguish them from the ordinary power series of calculus.
- In the theory of formal power series:
  - x is never assigned a numerical value;
  - Questions of convergence or divergence are not of interest.

Formal Power Series

- The object of interest is the sequence of coefficients
$$(a(0), a(1), \ldots, a(n), \ldots).$$
- All that we do with formal power series could also be done by treating the sequence of coefficients as though it were an infinite-dimensional vector with components $a(0), a(1), \ldots$.
- For our purposes it is more convenient to display the terms as coefficients of the power series
$$\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \cdots$$
rather than as components of a vector.
- The symbol x^n is simply a device for locating the position of the n-th coefficient $a(n)$.
- The coefficient $a(0)$ is called the **constant coefficient** of the series.

Algebra on Formal Power Series

- We operate on formal power series algebraically as though they were convergent power series.
- Suppose $A(x)$ and $B(x)$ are two formal power series, say

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \quad \text{and} \quad B(x) = \sum_{n=0}^{\infty} b(n)x^n.$$

- Then we define:

  Equality: $A(x) = B(x)$ means that $a(n) = b(n)$, for all $n \geq 0$.
  Sum: $A(x) + B(x) = \sum_{n=0}^{\infty}(a(n) + b(n))x^n$.
  Product: $A(x)B(x) = \sum_{n=0}^{\infty} c(n)x^n$, where

$$c(n) = \sum_{k=0}^{n} a(k)b(n-k).$$

  The sequence $\{c(n)\}$ is called the **Cauchy product** of the sequences $\{a(n)\}$ and $\{b(n)\}$.

The Ring of Formal Power Series

- The reader can easily verify that the sum and product operations satisfy the commutative and associative laws, and that multiplication is distributive with respect to addition.
- Thus, formal power series form a *ring*.
- This ring has a **zero element** for addition, denoted by 0,

$$0 = \sum_{n=0}^{\infty} a(n)x^n, \text{ where } a(n) = 0, \text{ for all } n \geq 0.$$

- The ring also has an **identity element** for multiplication, denoted by 1,

$$1 = \sum_{n=0}^{\infty} a(n)x^n, \text{ where } a(0) = 1 \text{ and } a(n) = 0, \text{ for } n \geq 1.$$

- A formal power series is called a **formal polynomial** if all its coefficients are 0 from some point on.

Inverse of a Formal Power Series

Claim: For each formal power series $A(x) = \sum_{n=0}^{\infty} a(n)x^n$, with constant coefficient $a(0) \neq 0$, there is a uniquely determined formal power series $B(x) = \sum_{n=0}^{\infty} b(n)x^n$, such that $A(x)B(x) = 1$.

Its coefficients can be determined by solving the infinite system of equations:

$$\begin{aligned} & a(0)b(0) = 1; \\ & a(0)b(1) + a(1)b(0) = 0; \\ & a(0)b(2) + a(1)b(1) + a(2)b(0) = 0; \\ & \qquad\qquad \vdots \end{aligned}$$

We may solve in succession for $b(0), b(1), b(2), \ldots$.

- The series $B(x)$ is called the **inverse** of $A(x)$ and is denoted by $A(x)^{-1}$ or by $\frac{1}{A(x)}$.

The Geometric Series

- The special series
$$A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n$$
is called a **geometric series**.
- Here a is an arbitrary real or complex number.
- Its inverse is the formal polynomial
$$B(x) = 1 - ax.$$
- In other words, we have
$$\frac{1}{1-ax} = 1 + \sum_{n=1}^{\infty} a^n x^n.$$

Subsection 8

The Bell Series of an Arithmetical Function

Bell Series

Definition

Given an arithmetical function f and a prime p, we denote by $f_p(x)$ the formal power series

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n)x^n$$

and call this the **Bell series of** f **modulo** p.

- Bell series are especially useful when f is multiplicative, as we show next.

Uniqueness Theorem Involving Bell Series

Theorem (Uniqueness Theorem)

Let f and g be multiplicative functions. Then $f = g$ if and only if

$$f_p(x) = g_p(x), \quad \text{for all primes } p.$$

- Suppose, first, that $f = g$.

  Then $f(p^n) = g(p^n)$, for all p and all $n \geq 0$.

  So $f_p(x) = g_p(x)$.

  Conversely, suppose $f_p(x) = g_p(x)$, for all p.

  Then $f(p^n) = g(p^n)$, for all $n \geq 0$.

  Since f and g are multiplicative and agree at all prime powers, they agree at all positive integers. So $f = g$.

Bell Series of μ and of φ

- **Möbius Function** μ: We have:
  - $\mu(p) = -1$;
  - $\mu(p^n) = 0$, for $n \geq 2$.

  So we get
  $$\mu_p(x) = 1 - x.$$
- **Euler's Totient** φ: We have
  $$\varphi(p^n) = p^n - p^{n-1}, \quad \text{for } n \geq 1.$$
  So we get
  $$\begin{aligned} \varphi_p(x) &= 1 + \sum_{n=1}^{\infty} (p^n - p^{n-1}) x^n \\ &= \sum_{n=0}^{\infty} p^n x^n - x \sum_{n=0}^{\infty} p^n x^n \\ &= (1 - x) \sum_{n=0}^{\infty} p^n x^n \\ &= \frac{1-x}{1-px}. \end{aligned}$$

Bell Series of a Completely Multiplicative Function

- If f is completely multiplicative then $f(p^n) = f(p)^n$, for all $n \geq 0$.
- So the Bell series $f_p(x)$ is a geometric series,

$$f_p(x) = \sum_{n=0}^{\infty} f(p)^n x^n = \frac{1}{1 - f(p)x}.$$

Particular Cases

- Using $f_p(x) = \sum_{n=0}^{\infty} f(p)^n x^n = \frac{1}{1-f(p)x}$, we get the following Bell series:
  - For the identity function I,
    $$I_p(x) = 1;$$
  - For the unit function u,
    $$u_p(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x};$$
  - For the power function N^α,
    $$N_p^\alpha(x) = 1 + \sum_{n=1}^{\infty} p^{\alpha n} x^n = \frac{1}{1-p^\alpha x};$$
  - For Liouville's function λ,
    $$\lambda_p(x) = \sum_{n=0}^{\infty} (-1)^n x^n = \frac{1}{1+x}.$$

Subsection 9

Bell Series and Dirichlet Multiplication

Multiplication of Bell Series and Dirichlet Multiplication

- We relate multiplication of Bell series to Dirichlet multiplication.

Theorem

For any two arithmetical functions f and g, let $h = f * g$. Then, for every prime p, we have

$$h_p(x) = f_p(x)g_p(x).$$

- The divisors of p^n are $1, p, p^2, \ldots, p^n$.

  So we have

$$h(p^n) = \sum_{d|p^n} f(d)g\left(\frac{p^n}{d}\right) = \sum_{k=0}^{n} f(p^k)g(p^{n-k}).$$

  This completes the proof because the last sum is the Cauchy product of the sequences $\{f(p^n)\}$ and $\{g(p^n)\}$.

Example

- We know that
$$\mu^2(n) = \lambda^{-1}(n).$$
It follows that
$$\mu_p^2(x)\lambda_p(x) = I_p(x) = 1.$$
So the Bell series of μ^2 modulo p is
$$\mu_p^2(x) = \frac{1}{\lambda_p(x)} = 1 + x.$$

Example

- We know that

$$\sigma_\alpha = N^\alpha * u.$$

It follows that the Bell series of σ_α modulo p is

$$\begin{aligned}(\sigma_\alpha)_p(x) &= N_p^\alpha(x)u_p(x)\\ &= \frac{1}{1-p^\alpha x}\cdot\frac{1}{1-x}\\ &= \frac{1}{1-(1+p^\alpha)x+p^\alpha x^2}\\ &= \frac{1}{1-\sigma_\alpha(p)x+p^\alpha x^2}.\end{aligned}$$

Bell Series and Identities of Arithmetical Functions

- This example illustrates how Bell series can be used to discover identities involving arithmetical functions.
- Consider the function ν defined by

$$\nu(n) = \begin{cases} 0, & \text{if } n = 1, \\ k, & \text{if } n = p_1^{a_1} \cdots p_k^{a_k}. \end{cases}$$

- Define

$$f(n) = 2^{\nu(n)}.$$

- The function f is clearly multiplicative.

Bell Series and Identities (Cont'd)

- Recall that:
  - $\mu_p^2(x) = 1 + x$;
  - $u_p(x) = \frac{1}{1-x}$.

  The Bell series of f modulo p is

$$f_p(x) = 1 + \sum_{n=1}^{\infty} 2^{\nu(p^n)} x^n = 1 + \sum_{n=1}^{\infty} 2x^n = 1 + \frac{2x}{1-x} = \frac{1+x}{1-x}.$$

  Hence

$$f_p(x) = \mu_p^2(x) u_p(x).$$

  This implies $f = \mu^2 * u$.

  Equivalently,

$$2^{\nu(n)} = \sum_{d|n} \mu^2(d).$$

Subsection 10

Derivatives of Arithmetical Functions

Derivatives of Arithmetical Functions

Definition

For any arithmetical function f, we define its **derivative** f' to be the arithmetical function given by the equation

$$f'(n) = f(n)\log n, \text{ for } n \geq 1.$$

Examples

Example: We have, for all n,

$$I(n)\log n = 0.$$

So we get

$$I' = 0.$$

Example: We have, for all n, $u(n) = 1$.
So we get

$$u'(n) = \log n.$$

- Recall that, for the Mangoldt function Λ, we have

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

This can be written as

$$\Lambda * u = u'.$$

Properties of Derivatives

- This concept of derivative shares many of the properties of the ordinary derivative discussed in elementary calculus.

Theorem

If f and g are arithmetical functions we have:

(a) $(f+g)' = f' + g'$.

(b) $(f*g)' = f'*g + f*g'$.

(c) $(f^{-1})' = -f'*(f*f)^{-1}$, provided that $f(1) \neq 0$.

(a) We have, for all n,

$$\begin{array}{rcl} (f+g)'(n) & = & (f+g)(n)\log n \\ & = & f(n)\log n + g(n)\log n \\ & = & f'(n) + g'(n) \\ & = & (f'+g')(n). \end{array}$$

Properties of Derivatives (Cont'd)

(b) We use the identity $\log n = \log d + \log\left(\frac{n}{d}\right)$ to write

$$\begin{aligned}(f*g)'(n) &= \sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)\log n \\ &= \sum_{d\mid n} f(d)\log d g\left(\frac{n}{d}\right) + \sum_{d\mid n} f(d)g\left(\frac{n}{d}\right)\log\left(\frac{n}{d}\right) \\ &= (f'*g)(n) + (f*g')(n).\end{aligned}$$

(c) We apply part (b) to the formula $I' = 0$, remembering that $I = f*f'$. This gives us

$$0 = I' = (f*f^{-1})' = f'*f^{-1} + f*(f^{-1})'.$$

So $f*(f^{-1})' = -f'*f^{-1}$.
Multiplication by f^{-1} now gives us

$$\begin{aligned}(f^{-1})' &= -(f'*f^{-1})*f^{-1} \\ &= -f'*(f^{-1}*f^{-1}) \\ &= -f'*(f*f)^{-1}.\end{aligned}$$

Subsection 11

The Selberg Identity

The Selberg Identity

- We quickly derive a formula of Selberg which is sometimes used as the starting point of an elementary proof of the prime number theorem.

Theorem (The Selberg Identity)

For $n \geq 1$, we have

$$\Lambda(n)\log n + \sum_{d|n} \Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\log^2\left(\frac{n}{d}\right).$$

- We saw that $\Lambda * u = u'$.
  Differentiation yields $\Lambda' * u + \Lambda * u' = u''$.
  Since $u' = \Lambda * u$,
  $$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$
  Now we multiply both sides by $\mu = u^{-1}$ to obtain
  $$\Lambda' + \Lambda * \Lambda = u'' * \mu.$$