8. MULTIPLICATIVE FUNCTIONS

§8.1. Multiplicative Functions

There are functions F(n) in number theory that have the property that F(mn) = F(m)F(n) whenever m, n are coprime. Functions with this property are called **multiplicative functions**. Of course there are trivial examples such as the constant functions O(n) = 0 and U(n) = 1 or the identity function 1(n) = n. Less trivial examples are the number of divisors and the sum of the divisors of a number.

In Chapter 3 we defined the **Euler function φ(n)** to be the number of numbers from 1 to n that are coprime with n. Equivalently it's the number of units (elements with a multiplicative inverse) in the ring $\mathbb{Z}_m$ of integers modulo m. We proved as a corollary to Theorem 6 in Chapter 3 that φ is a multiplicative function. and that $\varphi(p^n) = p^{n-1}(p - 1)$. We now define two other important multiplicative functions.

Define **δ(n)** to be the number of divisors of n, including 1 and n. Here we're considering only positive numbers and their positive divisors. We define **σ(n)** to be the sum of the (positive) divisors of n.

Theorem 1: $\delta(n)$ and $\sigma(n)$ are multiplicative functions.
Proof: Suppose m, n are coprime. If the divisors of m are $a_1, a_2, ..., a_r$ and the divisors of n are $b_1, b_2, ... b_s$ then every divisor of mn can be expressed uniquely as $a_i b_j$.
Hence $\delta(mn) = rs = \delta(m)\delta(n)$.
And $\sigma(mn) = \sum_{i,j} a_i b_j = (a_1 + ... + a_r)(b_1 + ... + b_s) = \sigma(m)\sigma(n)$.

Theorem 2: If p is prime, $\delta(p^n) = n + 1$ and $\sigma(p^n) = \frac{p^{n+1} - 1}{p - 1}$.
Proof: The divisors of p^n are $1, p, p^2, ..., p^n$.
Hence the number of them is $n + 1$ and their sum is the sum of the GP: $1 + p + p^2 + ... + p^n$.

We can use these theorems to find $\delta(n)$, $\sigma(n)$ and $\varphi(n)$for any n.

Example 1: Find $\delta(600)$, $\sigma(600)$ and $\varphi(600)$.
Solution: $\delta(600) = \delta(2^3.3.5^2) = 4.2.3 = 24$.
$\sigma(600) = \sigma(2^3.3.5^2) = 15.4.31 = 1860$.
$\varphi(600) = \varphi(2^3.3.5^2) = 2^2.2.5.4 = 160$.

§8.2. The Möbius Function

We say that a number is **square-free** if it's not divisible by the square of a prime, that is, if it's the product of distinct primes.

We define the **Möbius function**, **$\mu(n)$**, as follows.

$\mu(n) = (-1)^n$ if n is a product of n distinct primes. [In particular $\mu(1) = 1$],
$\mu(n) = 0$ if n is square free.

This rather strange function in that it takes just three values: –1, 0, 1. Yet it's extremely useful when used in combination with other multiplicative functions.

Example 2: $\mu(30) = \mu(2.3.5) = (-1)^3 = -1$.
$\mu(330) = \mu(2.3.5.11) = (-1)^4 = 1$.
$\mu(990) = \mu(2.3^2.5.11) = 0$.

Theorem 3: $\mu(n)$ is a multiplicative function.
Proof: Suppose that m, n are coprime.
If m or n is divisible by the square of a prime then so is mn and $\mu(mn) = \mu(m)\mu(n) = 0$.
If m is a product of r distinct primes and n is divisible by s distinct primes then mn is divisible by
$r + s$ distinct primes and so $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$.
[Remember that m, n are coprime so the primes dividing m are distinct from those dividing n.]

Example 3: $\mu(30) = \mu(6.5) = \mu(6)\mu(5) = 1(-1) = -1$.

Theorem 4: $\sum_{d|n}\mu(d) = \begin{cases}1 \text{ if } n = 1\\ 0 \text{ if } n > 1\end{cases}$.

Proof: Suppose $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} > 1$.

Then $\sum_{d|n}\mu(d) = 1 + \sum_{i}\mu(p_i) + \sum_{i,j}\mu(p_ip_j) + \sum_{i,j,k}\mu(p_ip_jp_k)$ + ...

$$= 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \ldots$$
$$= (1 - 1)^k$$
$$= 0.$$

Example 4: $\sum_{d|40}\mu(d) =$

$\mu(1) + \mu(2) + \mu(4) + \mu(5) + \mu(8) + \mu(10) + \mu(20) + \mu(40)$
$= 1 - 1 + 0 - 1 + 0 + 1 + 0 + 0$
$= 0.$

§8.3. The Group of Non-Zero Multiplicative Functions

The set of non-zero multiplicative functions can be made into an abelian group. and we can express some multiplicative functions in terms of others. In fact all the ones we consider here can be generated by just the identity function, 1, and the Euler φ-function. But note that 1 is not the identity element of this monoid.

Define Ψ to be the set of all non-zero multiplicative functions from $\mathbb{N}$ to $\mathbb{Z}$.

Define the **Möbius product** $F * G$ of two multiplicative functions F, G by $(F * G)(n) = \sum_{d|n} F(d)G\left(\frac{n}{d}\right)$

$$= \sum_{d|n} F\left(\frac{n}{d}\right)G(d) .$$

We can write this symmetrically as:

$$(F * G)(n) = \sum_{cd=n} F(c)G(d) ,$$

and so $F * G = G * F$ for all multiplicative functions, so the Möbius product is commutative.

Theorem 5 (COOPER):
Ψ is an abelian group under the Möbius product.
Proof:
Closure: Suppose *m*, *n* are coprime. Then every divisor of *mn* has the form *ab* where $a \mid m$ and $b \mid n$. Moreover, the *a*, *b* will be coprime and $\frac{m}{a}$ and $\frac{n}{b}$ will also be coprime.
Suppose that F, G are multiplicative functions.
Then $(F * G)(mn) = \sum_{d|mn} F(d)G\left(\frac{mn}{d}\right)$

$$= \sum_{a \mid m, b \mid n} F(ab)G\left(\frac{mn}{ab}\right)$$

$$= \sum_{a \mid m, b \mid n} F(a)F(b)G\left(\frac{m}{a}\right)G\left(\frac{n}{b}\right)$$

$$= \sum_{a \mid m} F(a)G\left(\frac{m}{a}\right) \sum_{b \mid m} F(b)G\left(\frac{n}{b}\right)$$

$$= (F * G)(m).(F * G)(n).$$

Thus $F * G$ is a multiplicative function.

Associative Law:

The associative law results from the fact that both $(F * G) * H(n)$ and $F * (G * H)(n)$ can be written as $\sum_{abc=n} F(a)G(b)H(c)$.

Identity: Let $I:\mathbb{N} \to \mathbb{N}$ be defined by $I(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise} \end{cases}$

.

This is very clearly a multiplicative function. Moreover, if F is any multiplicative function then

$$(F * I)(n) = \sum_{d \mid n} F(d).I\left(\frac{n}{b}\right).$$

This sum collapses to the single term, namely when $d = n$. This value is $F(n)$.

Hence $F * E = E * F = F$

and so E is the identity of this monoid.

Inverses: Let F be a non-zero multiplicative function. Then F(1) = 1.

For a prime, p, we define $G(p^n)$ inductively as follows:

$G(1) = 1$,

$$G(p^n) = -\sum_{m=0}^{n-1} G(p^m)F(p^{n-m})$$

Then $(G * F)(p^n)$

$$= \sum_{m=0}^{n} G(p^m)F(p^{n-m})$$

$$= G(p^n)F(1) + \sum_{m=0}^{n-1} G(p^m)F(p^{n-m})$$

$$= -\sum_{m=0}^{n-1} G(p^m)F(p^{n-m}) + \sum_{m=0}^{n-1} G(p^m)F(p^{n-m}) = 0.$$

Now we define G(n) for composite n by using the multiplicative property.

Hence, for all n, $(G * F)(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise} \end{cases}$, which means that $G * F = I$.

We're faced with a notational problem here because there are three multiplicative functions that could be considered as an identity function. In fact all three are identities under some appropriate multiplication.

There's the function, 1, that maps n to n. This is the identity under composition of functions. Then there is the function that maps all n to 1. This is the identity under what is called 'point-wise' multiplication, where $(FG)(n) = F(n)G(n)$. Finally we have the function, I, defined above which is the identity for Möbius multiplication.

We shall resolve this problem by denoting these three identities as follows:

Operation	**Identity**	**Defined by**
Möbius multiplication	I	$I(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise} \end{cases}$
Composition	1	$1(n) = n$ for all n
Pointwise multiplication	U	$U(n) = 1$ for all n

Note that all are multiplicative functions but I is the identity in Ψ.

INVERSE OF F
$F^{-1}(1) = 1;$ $F^{-1}(p^n) = -\sum_{m=0}^{n-1} F^{-1}(p^m)F(p^{n-m})$ for $n \geq 1$

Theorem 6: $\mu * U = I$.

Proof: By Theorem 4, $\sum_{d|n} \mu(d) = n$ for all n. The left-hand side of this equation can be expressed as the Möbius product of μ and U. So $\mu * U = I$ and so U and μ are inverses of one another. The Möbius inversion formula is now a simple consequence of the algebra of the group Ψ.

Theorem 7 (MÖBIUS INVERSION FORMULA):
If F is a multiplicative function then $G(n) = \sum_{d|n} F(d)$ if and only if $F(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$.

Proof: The assumption is essentially $G = F * U = F * \mu^{-1}$. Multiplying both sides by μ we get $F = \mu * G$.

It's a simple exercise to show that:

$$\delta = U * U \text{ and } \sigma = 1 * U.$$

Theorem 8: $\varphi = \mu * 1$.

Proof: If p, q, ... are the distinct prime divisors of n then

$$\varphi(n) = n - \sum_{p|n} \frac{n}{p} + \sum_{pq|n} \frac{n}{pq} - \ldots..$$

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

$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) d \text{ by a suitable change of variable.}$$

Hence $\varphi = \mu * 1$.

Example 6: $\varphi(100) = \varphi(2^2.5^2) = \varphi(2^2)\varphi(5^2) = 2.5.4 = 40$.

$$\sum_{d|100} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) + \varphi(25) + \varphi(50) + \varphi(100)$$

$$= 1 + 1 + 2 + 4 + 4 + 8 + 20 + 20 + 40$$

$$= 100.$$

SUMMARY OF MULTIPLICATIVE FUNCTIONS

F	**F(*n*)**
I	1 if $n = 1$, 0 otherwise
U	1
1	n
μ	$\begin{cases} -1 \text{ if product of odd number of distinct primes} \\ 0 \text{ if divisible by a prime square} \\ 1 \text{ if product of even number of distinct primes} \end{cases}$
φ	number of units in $\mathbb{Z}_n^{\#}$
δ	number of positive divisors of n
σ	sum of positive divisors of n

SUMMARY OF SOME RELATIONS IN THE GROUP Ψ

	I	**U**	**1**	**μ**	**φ**	**δ**	**σ**	**in terms of U, φ**
I	I	U	1	μ	φ	δ	σ	1
U	U	δ	σ	I	1			U
1	1	σ	$n\delta$	φ				$U * \varphi$
μ	μ	I	φ			U	1	U^{-1}
φ	φ	1				σ		φ
δ	δ			U	σ			$U * U$
σ	σ			1				$U * U * \varphi$

EXERCISES FOR CHAPTER 8

Exercise 1: Find φ^{-1} in Ψ.

SOLUTIONS FOR CHAPTER 8

Exercise 1: $\varphi^{-1}(n) = -\prod_{\text{prime } p|n}(p-1)$

(If $n = 1$ this evaluates to 1.)

Proof: We prove that $\varphi^{-1}(p^n) = -(p-1)$ for all $n \geq 1$ by induction on n.

Let N be a minimal counter-example.

Clearly $N > 0$.

Then $\varphi^{-1}(p^N)$

$$= -\sum_{m=0}^{N-1} \varphi^{-1}(p^m)\varphi(p^{N-m})$$

$$= -\varphi^{-1}(1)\varphi(p^N) - \sum_{m=1}^{N-1} \varphi^{-1}(p^m)\varphi(p^{N-m})$$

$$= -1.p^{N-1}(p-1) - \sum_{m=1}^{N-1} -(p-1)\ p^{N-m-1}(p-1)$$

$$= -p^{N-1}(p-1) + (p-1)^2 \sum_{m=1}^{N-1} p^{N-m-1}$$

$$= - p^{N-1}(p-1) + (p-1)^2 \left(\frac{p^{N-1}-1}{p-1} \right)$$
$$= - p^{N-1}(p-1) + (p-1)\,(p^{N-1}-1)$$
$$= - p^{N} + p^{N-1} + p^{N} - p - p^{N-1} + 1$$
$$= - (p-1).$$

coopersnotes.net
LIST OF TITLES

GENERAL
- The Mathematics At The Edge Of The Rational Universe

ELEMENTARY
- Basic Mathematics
- Concepts of Algebra
- Concepts of Calculus
- Elementary Algebra
- Elementary Calculus

1st YEAR UNI
- Techniques of Algebra
- Techniques of Calculus
- Matrices

2nd YEAR UNI
- Linear Algebra
- Languages & Machines
- Discrete Mathematics

3rd YEAR UNI
- Group Theory volume 1
- Group Theory volume 2
- Galois Theory
- Graph Theory
- Number Theory
- Geometry
- Topology
- Set Theory

POSTGRADUATE
- Ring Theory
- Representation Theory
- Quadratic Forms
- Group Tables vol 1
- Group Tables vol 2