ARITHMETICAL FUNCTIONS

An *arithmetical function* is simply a complex-valued sequence; i.e., it is a function $a : \mathbf{N} \to \mathbf{C}$. Some basic arithmetical functions are defined below:

(a) The *identity function*, denoted $E(n)$, is defined to be 1 if $n = 1$ and 0 elsewhere, i.e, $E(n) = \lfloor 1/n \rfloor$ for $n \in \mathbf{N}$.
(b) For $\alpha \in \mathbf{C}$ the *power function* N^α is defined as $N^\alpha(n) = n^\alpha$. We denote N^1 simply as N.
(c) The *unit function*, denoted 1, is defined to be the constant function 1, i.e., $1(n) = 1$ for every $n \in \mathbf{N}$.

Some basic arithmetical functions and their identities

The *Möbius function*, denoted μ, is an extremely important function which shows up all over in analytic number theory (especially sieve theory). It is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \dots p_k, \text{ where } p_1, \dots, p_k \text{ are distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

Note that μ is the signed characteristic function of the squarefree integers. The definition of μ might seem unmotivated but later we will see that μ is the inverse of the unit function in some group of arithmetical functions. Knowing that the inverse of unit function exists one can easily recover the above definition.

Proposition 1. *If $n \geqslant 1$, then*

$$\sum_{d \mid n} \mu(d) = E(n).$$

Proof. If $n = 1$, then the formula clearly holds as $\mu(1) = 1$. Now suppose that $n = \prod_{i=1}^k p_i^{a_i}$. Because $\mu(d)$ is nonzero if and only if d is squarefree, we can restrict the sum to divisors of the form $\prod_{i \in I} p_i$, where I is a subset of $\{1, \dots, k\}$. Thus we get

$$\sum_{d \mid n} \mu(d) = \sum_{I \subset \{1,\dots,n\}} \mu\left(\prod_{i \in I} p_i\right) = \sum_{I \subset \{1,\dots,n\}} (-1)^{|I|}.$$

Since for each $0 \leqslant r \leqslant k$ there are precisely $\binom{k}{r}$ subsets of $\{1, \dots, k\}$ containing r elements we therefore deduce that

$$\sum_{d \mid n} \mu(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = (-1 + 1)^k = 0. \qquad \square$$

The *Euler's totient function*, denoted φ, is defined to be the number of positive integers not exceeding n which are relatively prime to n, i.e.,

$$\varphi(n) = |\{1 \leqslant k \leqslant n : (k, n) = 1\}|$$

We can rewrite $\varphi(n)$ in the summation notation as

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

Proposition 2. *If $n \geqslant 1$, then*

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

Proof. Partition the set $\{1,\dots,n\}$ into sets $A_d = \{1 \leqslant k \leqslant n : (k,n) = d\}$, where d is a divisor of n, and note that there is a one-to-one bijection between elements of A_d and integers $1 \leqslant r \leqslant n/d$ satisfying $(r, n/d) = 1$. This then implies that

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d),$$

where the last equality follows by the bijection $d \mapsto n/d$ between the divisors of n. $\square$

Proposition 3. *For $n \geqslant 1$ we have*

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

Proof. If $n = 1$, then the product on the right hand side is empty and so the formula holds trivially. Now let $p_1, \dots, p_k$ be the prime divisors of n and let $[k]$ denote the set $\{1,\dots,k\}$. Then expanding the product we get

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = \sum_{I \subset [k]} \prod_{i \in I} \left(-\frac{1}{p_i}\right) = \sum_{I \subset [k]} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i} = \sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}. \qquad \square$$

Proposition 4. *If $n \geqslant 1$, then we have*

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

Proof. We use the formula for the divisor sum of μ to obtain

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

Changing the order of summation we get

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

completing the proof. $\square$

We now obtain some interesting properties of φ.

Proposition 5. *The Euler's totient function has the following properties:*

(a) $\varphi(p^a) = p^a - p^{a-1}$ *for prime p and $a \geqslant 1$.*
(b) $\varphi(mn) = \varphi(m)\varphi(n)(d/\varphi(d))$, *where $d = (m,n)$.*
(c) $\varphi(mn) = \varphi(m)\varphi(n)$ *if $(m,n) = 1$.*

(d) *$n|m$ implies $\varphi(n)|\varphi(m)$.*
(e) *$\varphi(n)$ is even for $n \geqslant 3$. Moreover, if n has r distinct odd prime factors, then $2^r|\varphi(n)$.*

Proof. (a): Follows immediately from the product formula.
(b): Note that

$$\begin{aligned}\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{p}\right) &= \prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{\substack{p|n\\ p\nmid m}}\left(1-\frac{1}{p}\right)\\ &= \prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{\substack{p|n\\ p|m}}\left(1-\frac{1}{p}\right)^{-1}\\ &= \frac{\varphi(m)}{m}\frac{\varphi(n)}{n}\prod_{p|(n,m)}\left(1-\frac{1}{p}\right)^{-1}\\ &= \frac{\varphi(m)}{m}\frac{\varphi(n)}{n}\frac{d}{\varphi(d)},\end{aligned}$$

where $d = (m,n)$.
(c): Follows immediately from part (b).
(d): Let $n = p_1^{a_1}\cdots p_k^{a_k}$ and $m = p_1^{b_1}\cdots p_k^{b_k}$, where a_i are nonnegative. Because $a_i \leqslant b_i$, we have $\varphi(p_i^{a_i})|\varphi(p_i^{b_i})$ due to part (a). This coupled with the fact that φ is multiplicative (due to part (c)) gives us the desired result.
(e): Observe that if $n \geqslant 3$ and $n = 2^a$ for some positive integer a then a must be at least 2 and so $\varphi(2^a) = 2^a - 2^{a-1} = 2(2^{a-1} - 2^{a-2})$ is even. Now note that

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

where the factor $n(\prod_{p|n} p)^{-1}$ is an integer. If n is not of the form 2^a, then an odd prime p divides n, and so the factor on the right must be even which implies that $\varphi(n)$ is even. Finally, if n has r distinct odd prime factors then $2^r|\prod_{p|n}(p-1)$ and hence $2^r|\varphi(n)$. □

One of the famous open problems in number theory is Carmichael's conjecture, which states that for every $n \in \mathbf{N}$ there is a $m \neq n$ such that $\varphi(m) = \varphi(n)$. In other words, if $A(k)$ denotes the number of positive integers n for which $\varphi(n) = k$, then $A(k)$ can never be equal to 1. In 1999, Kevin Ford proved in a paper published in Annals of Mathematics that every other positive integer occurs as a value of $A(k)$. This was known as Sierpinski's conjecture.

The *von-Mangoldt function* (usually referred to as simply Mangoldt function), denoted Λ, is defined as

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

Claim 6. *If $n \geqslant 1$, then we have*

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

Dirichlet multiplication

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

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

Claim 7. *Dirichlet multiplication is commutative and associative, i.e., for any arithmetical functions f, g, h we have*

$$f * g = g * f \quad \textit{and} \quad (f * g) * h = f * (g * h).$$

Claim 8. *For any arithmetical function f, we have $E * f = f * E = f$.*

Claim 9. *If f is an arithmetical function with $f(1) \neq 0$, then there is a unique arithmetical function g such that*

$$g * f = f * g = E.$$

The function g is given by

$$g(1) = \frac{1}{f(1)}, \qquad g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d) f\left(\frac{n}{d}\right) \quad \textit{for } n > 1.$$

The above results show that the set of all arithmetical functions f satisfying $f(1) \neq 0$ form an abelian group under Dirichlet multiplication.

Using the notation of Dirichlet product, we can write the identities in Proposition 1 and Proposition 2 in compact form as

$$\mu * 1 = E \quad \text{and} \quad \varphi * 1 = N.$$

Thus μ and 1 are Dirichlet inverses of each other. Also note that the identity (1) follows seamlessly from $\varphi * 1 = N$ by multiplying by μ on both sides; $\varphi = N * \mu$.

Proposition 10 (Möbius inversion formula)**.** *Let f and g be arithmetic functions. Then*

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

if and only if

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

The Möbius inversion formula has already been illustrated by a pair of identities in Proposition 2 and Proposition 4:

$$n = \sum_{d|n} \varphi(d), \qquad \varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

Exercises

Exercise 1. Show that for every $k \in \mathbf{N}$ there are infinitely many n such that

$$\mu(n+1) = \cdots = \mu(n+k).$$

(Hint: Use Chinese Remainder Theorem.)