ANALYTIC NUMBER THEORY

M. ATIF ZAHEER

Contents

1. Arithmetical functions

1.1. Some basic arithmetical functions.

Definition 1.1. The *Möbius function*, denoted μ, 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 seems to be unmotivated right now 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 recover this definition.

Proposition 1.2. 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 $\{1, \dots, k\}$. Hence, 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

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

Problem 1.1. Show that for every $k \in \mathbb{N}$ there are infinitely many n such that

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

Solution. Let $p_1, \ldots, p_k$ be distinct primes. Then by Chinese remainder theorem there are infinitely many n with $n \equiv -j \pmod{p_j^2}$ for $1 \leqslant j \leqslant k$ and so $p_j^2 | (n+j)$ and $\mu(n+j) = 0$.

Definition 1.3. 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 1.4. If $n \geqslant 1$, then

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

Proof. The key idea behind the proof is to partition the set $\{1, \ldots, n\}$ into sets $A_d = \{1 \leqslant k \leqslant n : (k,n) = d\}$, where d is a divisor of n, and to 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

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

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

Proposition 1.5. If $n \geqslant 1$, then we have

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{1.1}$$

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. $\square$

Proposition 1.6. 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 trivially holds. Now let $p_1, \dots, p_k$ be the prime divisors of n let $[k] := \{1, \dots, k\}$. Then expanding the product, we get

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

We now obtain some interesting properties of φ.

Proposition 1.7. 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 (i). 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 $2^r|\varphi(n)$. $\square$

Definition 1.8. 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 1.9. If $n \geqslant 1$, then we have

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

1.2. **Dirichlet multiplication.**

Definition 1.10. 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 1.11. Dirichlet multiplication is commutative and associative, i.e., for any arithmetical functions f, g, h we have

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

Claim 1.12. For any arithmetical function f, we have $e * f = f * e = f$.

Claim 1.13. 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

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

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 1.2 and Proposition 1.4 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 (1.1) follows seamlessly from $\varphi * 1 = N$ by multiplying by μ on both sides; $\varphi = N * \mu$.

Proposition 1.14 (Möbius inversion formula)**.** Let f and g be arithmetical 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 1.4 and Proposition 1.5:

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

1.3. Multiplicative functions.

Definition 1.15. An arithmetical function f is called *multiplicative* if $f \not\equiv 0$ and

$$f(mn) = f(m)f(n) \quad \text{whenever } (m,n) = 1.$$

A multiplicative function f is called *completely multiplicative* (or *totally multiplicative*) if $f \not\equiv 0$ and

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

Example 1.16. We note some common examples of multiplicative functions.

(a) The power function N^α is completely multiplicative.
(b) The identity function E is completely multiplicative.
(c) The Möbius function μ is multiplicative. However, it is not completely multiplicative as $\mu(4) = 0 \neq 1 = \mu(2)^2$.
(d) The Euler totient function φ is multiplicative. However, it is not completely multiplicative as $\varphi(4) = 2 \neq 1 = \varphi(2)^2$.

Claim 1.17. If f is multiplicative, then $f(1) = 1$.

From this property of multiplicative functions it immediately follows that Λ is not multiplicative.

Proposition 1.18. Let f be an arithmetical function with $f(1) = 1$.

(a) f is multiplicative if and only if

$$f(p_1^{a_1} \cdots p_k^{a_k}) = f(p_1^{a_1}) \cdots f(p_k^{a_k}),$$

where $p_1, \ldots, p_k$ are distinct primes.

(b) If f is multiplicative, then f is completely multiplicative if and only if

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

for all primes p and all integers $a \geqslant 1$.

The above result shows that a multiplicative function is uniquely determined by its values on prime powers, and a completely multiplicative function is uniquely determined by its values on primes.

Claim 1.19. If f and g are multiplicative, then so is their Dirichlet product $f * g$.

Proof. Let m and n be relatively prime integers. Then observe that

$$(f * g)(mn) = \sum_{d\mid mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{\substack{a\mid m\\ b\mid n}} f(ab) g\left(\frac{mn}{ab}\right)$$

as every divisor of mn can be uniquely written as ab, where $a|m$ and $b|n$. Using the multiplicativity of f and g we obtain

$$(f * g)(mn) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) = \sum_{a|m}\sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)$$
$$= \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) = (f * g)(m)(f * g)(n). \qquad \square$$

This completes the proof.

The Dirichlet product of two completely multiplicative functions need not be completely multiplicative. For instance, the divisor function $d = 1 * 1$ is not completely multiplicative as $d(4) = 3 \neq 4 = d(2)^2$ whereas 1 clearly is.

Claim 1.20. If f is multiplicative, then so is it's Dirichlet inverse f^{-1}.

Proof. Suppose for the sake of contradiction that f^{-1} is not multiplicative. Then there exist positive integers m and n with $(m, n) = 1$ such that

$$f^{-1}(mn) \neq f^{-1}(m)f^{-1}(n).$$

We choose such a pair m and n for which the product mn is the smallest. Since f is multiplicative therefore $f^{-1}(1) = 1/f(1) = 1$ and hence neither m nor n can be 1. In particular, $mn > 1$. By the construction of the product mn, $f(ab) = f(a)f(b)$ for all positive integers a and b with $(a, b) = 1$ and $ab < mn$. It now follows that

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

This contradiction proves the result.

Second Proof. Let g be an arithmetical function defined as

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

Then g is a multiplicative function by definition and so it suffices to show that $f^{-1} = g$. Note that

$$\begin{aligned}(g * f)(p^k) &= \sum_{d \mid p^k} g(d) f(p^k/d) = \sum_{i=0}^{k} g(p^i) f(p^{k-i}) \\ &= \sum_{i=0}^{k} f^{-1}(p^i) f(p^{k-i}) = \sum_{d \mid p^k} f^{-1}(d) f(p^k/d) = (f^{-1} * f)(p^k) = E(p^k).\end{aligned}$$

Because $g * f$ and E are both multiplicative functions and agree on prime powers, it follows that $g * f = E$ and so $g = f^{-1}$. □

Proposition 1.21. Let f be multiplicative. Then f is completely multiplicative if and only if $f^{-1} = \mu f$.

Proof. Suppose f is completely multiplicative. Then observe that

$$(f * \mu f)(n) = \sum_{d \mid n} \mu(d) f(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d \mid n} \mu(d) = f(n) E(n) = E(n).$$

Conversely, assume that $f^{-1} = \mu f$. Then observe that

$$\sum_{d \mid n} \mu(d) f(d) f\left(\frac{n}{d}\right) = 0$$

for $n > 1$. Let $n = p^a$, where $a \geqslant 1$. Then, we get

$$\mu(1) f(1) f(p^a) + \mu(p) f(p) f(p^{a-1}) = 0.$$

It then follows that

$$f(p^a) = f(p) f(p^{a-1}).$$

This implies that $f(p^a) = f(p)^a$. Thus f is completely multiplicative. □

Example 1.22. Since $\varphi = \mu * N$ we have $\varphi^{-1} = \mu^{-1} * N^{-1}$. But $N^{-1} = \mu N$ since N is completely multiplicative, so

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

Thus we have

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

Proposition 1.23. If f is a multiplicative arithmetical function then

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

Proof. Let $g = 1 * \mu f$. Then g is a multiplicative function. Thus, it suffices to know the value of g at prime powers. We observe that

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

Hence, we obtain

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

as desired.

We earlier gave a product formula for $\varphi(n)$ in Proposition 1.6. This formula also follows from Proposition 1.5 and above proposition by taking $f(n) = 1/n$.