

ARITHMETICAL FUNCTIONS II: CONVOLUTION AND INVERSION

PETE L. CLARK

1. SUMS OVER DIVISORS, CONVOLUTION AND MÖBIUS INVERSION

The proof of the multiplicativity of the functions σ_k , easy though it was, actually establishes a more general result. Namely, suppose that f is a multiplicative function, and define a new function $F = \sum_d f$ as

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

For instance, if we start with the function $f(n) = n^k$, then $F = \sigma_k$. Note that $f(n) = n^k$ is (in fact completely) multiplicative. The generalization of the proof is then the following

Proposition 1. *If f is a multiplicative function, then so is $F(n) = \sum_{d|n} f(d)$.*

Proof: If n_1 and n_2 are coprime, then $F(n_1 n_2) = \sum_{d|n_1 n_2} f(d) =$

$$\sum_{d_1|n_1, d_2|n_2} f(d_1 d_2) = \sum_{d_1|n_1, d_2|n_2} f(d_1) f(d_2) = \left(\sum_{d_1|n_1} f(d_1) \right) \left(\sum_{d_2|n_2} f(d_2) \right) = F(n_1) F(n_2).$$

Note that the process does not preserve completely multiplicative functions.

It turns out that the operation $f \mapsto F$ is of general interest; it gives rise to a certain kind of “duality” among arithmetic functions. Slightly less vaguely, sometimes f is simple and F is more complicated, but sometimes the reverse takes place.

Definition: Define the function δ by $\delta(1) = 1$ and $\delta(n) = 0$ for all $n > 1$. Note that δ is multiplicative. Also write ι for the function $n \mapsto n$.

Proposition 2. *a) For all $n > 1$, $\sum_{d|n} \mu(d) = 0$.*

b) For all $n \in \mathbb{Z}^+$, $\sum_{d|n} \varphi(d) = n$.

In other words, the sum over the divisors of the Möbius function is δ , and the sum over the divisors of φ is ι .

Proof: a) Write $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then $\sum_{d|n} \mu(d) = \sum_{(\epsilon_1, \dots, \epsilon_r)} \mu(p_1^{\epsilon_1} \cdots p_r^{\epsilon_r})$, where the ϵ_i are 0 or 1. Thus

$$\sum_{d|n} \mu(d) = 1 - r + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = (1 - 1)^r = 0.$$

For part b) we take advantage of the fact that since φ is multiplicative, so is the sum over its divisors. Therefore it is enough to verify the identity for a prime power

p^a , and as usual this is significantly easier:

$$\sum_{d \mid p^a} \varphi(p^a) = \sum_{i=0}^a \varphi(p^i) = 1 + \sum_{i=1}^a (p^i - p^{i-1}) = 1 + (p^a - 1) = p^a,$$

where we have cancelled out a telescoping sum.

This indicates that the Möbius function is of some interest. We can go further by asking the question: suppose that $F = \sum_d f$ is multiplicative; must f be multiplicative?

Well, the first question is to what extent f is determined by its divisor sum function: if $F = \sum_d f = \sum_d g = G$, must $f = g$? If so, is there a nice formula which gives f in terms of F ?

Some calculations:

$$f(1) = F(1);$$

for any prime p , $F(p) = f(1) + f(p)$, so $f(p) = F(p) - F(1)$;

$F(p^2) = f(1) + f(p) + f(p^2) = F(p) + f(p^2)$, so $f(p^2) = F(p^2) - F(p)$; indeed

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

For distinct primes p_1, p_2 , we have $F(p_1 p_2) = f(1) + f(p_1) + f(p_2) + f(p_1 p_2) = F(1) + F(p_1) - F(1) + F(p_2) - F(1) + f(p_1 p_2)$, so

$$f(p_1 p_2) = F(p_1 p_2) - F(p_1) - F(p_2) + F(1).$$

This is an enlightening calculation on several accounts; on the one hand, there is some sort of inclusion-exclusion principle at work. On the other hand, and easier to enunciate, we are recovering f in terms of F and μ :

Theorem 3. (*Möbius Inversion Formula*) For any arithmetical function f , let $F(n) = \sum_{d \mid n} f(d)$. Then for all n ,

$$f(n) = \sum_{d \mid n} F(d) \mu(n/d).$$

It is a good exercise to give a direct proof of this. However, playing on a familiar theme, we will introduce a little more algebra to get an easier proof. Namely, we can usefully generalize the construction $f \mapsto \sum_d f = F$ as follows:

Definition: For arithmetical functions f and g , we define their **convolution**, or **Dirichlet product**, as

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

Why is this relevant? Well, define $\mathbf{1}$ as the function $\mathbf{1}(n) = 1$ for all n ;¹ then $F = f * \mathbf{1}$. We have also seen that

$$(1) \quad \mu * \mathbf{1} = \iota,$$

and the inversion formula we want is

$$(f * \mathbf{1}) * \mu = f.$$

Thus we see that if only it is permissible to rewrite $(f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu)$, then the inversion formula is an immediate consequence of Equation (1). In other words, we need to show that convolution is associative. In fact we can prove more:

Proposition 4. *The arithmetical functions form a commutative ring under point-wise addition – i.e., $(f + g)(n) = f(n) + g(n)$ – and convolution. The multiplicative identity is the function δ .*

Proof: In other words, we are making the following assertions: for all arithmetical functions f, g, h :

- (i) $f * g = g * f$.
- (ii) $(f * g) * h = f * (g * h)$.
- (iii) $f * \delta = f$.
- (iv) $f * (g + h) = f * g + f * h$.

To show both (i) and (ii) it is convenient to rewrite the convolution in symmetric form:

$$f * g(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2).$$

The sum extends over all pairs of positive integers d_1, d_2 whose product is n . This already makes the commutativity clear. As for the associativity, writing things out one finds that both $(f * g) * h$ and $f * (g * h)$ are equal to

$$\sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3),$$

and hence they are equal to each other! For (iii), we have

$$(f * \delta)(n) = \sum_{d_1 d_2 = n} f(d_1)\delta(d_2);$$

$\delta(d_2) = 0$ unless $d_2 = 1$, so the sum reduces to $f(n)\delta(1) = f(n)$. The distributivity is easy and left to the reader.

We can now show that $F = \sum_d f$ multiplicative implies f is multiplicative. Indeed, this follows from $f = F * \mu$, the multiplicativity of μ and the following:

Proposition 5. *If f and g are multiplicative, so is $f * g$.*

Proof: Just do it: for coprime m and n , $(f * g)(m)(f * g)(n) =$

$$\begin{aligned} \left(\sum_{a_1 a_2 = m} f(a_1)g(a_2) \right) \left(\sum_{b_1 b_2 = n} f(b_1)g(b_2) \right) &= \sum_{a_1 a_2 b_1 b_2 = mn} f(a_1)f(b_1)g(a_2)g(b_2) = \\ &= \sum_{xy = mn} f(x)g(y) = (f * g)(mn). \end{aligned}$$

¹We now have three similar-looking but different functions floating around: δ , ι and $\mathbf{1}$. It may help the reader to keep on hand a short “cheat sheet” with the definitions of all three functions.

2. SOME APPLICATIONS OF MÖBIUS INVERSION

2.1. Application: another proof of the multiplicativity of the totient. Our first application of Möbius inversion is to give a proof of the multiplicativity of φ which is independent of the Chinese Remainder Theorem. To do this, we will give a direct proof of the identity $\sum_{d|n} \varphi(d) = n$. Note that it is equivalent to write the left hand side as

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

since as d runs through all the divisors of n , so does $\frac{n}{d}$. Now let us classify elements of $\{1, \dots, n\}$ according to their greatest common divisor with n . The greatest common divisor of any such element k is a divisor d of n , and these are exactly the elements k such that $\frac{k}{d}$ is relatively prime to $\frac{n}{d}$, or, in yet other words, the elements $d \cdot l$ with $1 \leq l \leq \frac{n}{d}$ and $\gcd(l, \frac{n}{d}) = 1$, of which there are $\varphi(\frac{n}{d})$. This proves the identity! Now, we can apply Möbius inversion to conclude that $\varphi = \iota \cdot \mu$ is multiplicative.

Here is a closely related approach. Consider the additive group of $\mathbb{Z}/n\mathbb{Z}$, a cyclic group of order n . For a given positive integer d , how many order d elements does it have? Well, by Lagrange's Theorem we need $d|n$. An easier question is how many elements there are of order dividing a given d (itself a divisor of n): these are just the elements $x \in \mathbb{Z}/n\mathbb{Z}$ for which $dx = 0$, i.e., the multiples of n/d , of which there are clearly d . But Möbius Inversion lets us pass from the easier question to the harder question: indeed, define $f(k)$ to be the number of elements of order k in $\mathbb{Z}/n\mathbb{Z}$; then $F(k) = \sum_{d|k} f(d)$ is the number of elements of order dividing k , so we just saw that $F(k) = k$. Applying Möbius inversion, we get that $f(k) = (I * \mu)(k) = \varphi(k)$. On the other hand, it is not hard to see directly that $f(k) = 0$ if k does not divide n and otherwise equals $\varphi(k)$ – e.g., using the fact that there is a unique subgroup of order k for all $k | n$ – and this gives another proof that $\varphi * \mathbf{1} = \iota$.

2.2. A formula for the cyclotomic polynomials. For a positive integer d , let $\Phi_d(x)$ be the monic polynomial whose roots are the primitive d th roots of unity, i.e., those complex numbers which have exact order d in the multiplicative group \mathbb{C}^\times (meaning that $z^d = 1$ and $z^n \neq 1$ for any integer $0 < n < d$). These primitive roots are contained in the group of all d th roots of unity, which is cyclic of order d , so by the above discussion there are exactly $\varphi(d)$ of them: in other words, the degree of the polynomial Φ_d is $\varphi(d)$. It turns out that these important polynomials have entirely integer coefficients, although without a somewhat more sophisticated algebraic background this may well not be so obvious. One might think that to write down formulas for the Φ_d one would have to do a lot of arithmetic with complex numbers, but that is not at all the case. Very much in the spirit of the group-theoretical interpretation of $\sum_{d|n} \varphi(d) = n$, we have

$$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

since, both the left and right-hand sides are monic polynomials whose roots consist of each n th root of unity exactly once.

In fact it follows from this formula, by induction, that the Φ_d 's have integral

²For once, the ancients who fixed the notation have planned ahead!

coefficients. But Möbius inversion gives us an explicit formula. The trick here is to convert the divisor product into a divisor sum by taking logarithms:

$$\log \prod_{d|n} \Phi_d(x) = \sum_{d|n} \log \Phi_d(x) = \log(x^n - 1).$$

Now applying Möbius inversion, we get

$$\begin{aligned} \log \Phi_n(x) &= \sum_{d|n} \log(x^d - 1) \mu\left(\frac{n}{d}\right) \\ &= \log \left(\prod_{d|n} (x^d - 1)^{\mu(n/d)} \right), \end{aligned}$$

so exponentiating back we get a formula which at first looks too good to be true:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

But it is absolutely correct, and, as advertised, reduces the computation of the cyclotomic polynomials to arithmetic (including division!) of polynomials with integer coefficients.

Remark: Our trick of taking logs was done without much worry about rigor. It is not literally true that $\log(x^n - 1)$ is an arithmetical function, since it is not defined for $x = 1$. We can justify what we have done as follows: for fixed n , since the Φ_d 's and $x^n - 1$ are a finite set of monic polynomials with integer coefficients, there exists a large positive integer N such that for all d dividing n and all $x \in \mathbb{Z}^+$, $\Phi_d(x + N) \geq 1$, so that $\log(\Phi_d(x + N))$ and $\log(x + N)^d - 1$ are well-defined arithmetical functions, to which we apply MIF. This gives us the desired identity with $x + N$ in place of x , but being an identity of polynomials, we can substitute $x - N$ for x to get back to the desired identity.

On the other hand, such ad hocery is not so aesthetically pleasing. The formula we obtained suggests that MIF may be valid for functions f defined on \mathbb{Z}^+ but with more general codomains than \mathbb{C} . If R is a commutative ring, then the statement and proof of MIF go through verbatim for “ R -valued arithmetic functions” $f : \mathbb{Z}^+ \rightarrow R$. But this is not the right generalization for the present example: we want a MIF for functions with values in the multiplicative group $\mathbb{C}(x)$ of nonzero rational functions. In fact, for any commutative group A – whose group law we will write as addition, even though in our application it is called multiplication – if one considers A -valued arithmetic functions $f : \mathbb{Z}^+ \rightarrow A$, then there is in general no convolution product (since we can't multiply elements of A), but nevertheless $F(n) = \sum_{d|n} f(d)$ makes sense, as does $\sum_{d|n} F(d) \mu(n/d)$, where for $a \in A$ we interpret $0 \cdot a$ as being the additive identity element 0_A , $1 \cdot a$ as a and $-1 \cdot a$ as the additive inverse $-a$ of a . Then one can check that $\sum_{d|n} F(d) \mu(n/d) = f(n)$ for all f , just as before. We leave the proof as an exercise.

2.3. Finite subgroups of unit groups of fields are cyclic.

Theorem 6. *Let F be a field and $G \subset F^\times$ a finite subgroup of the multiplicative group of units of F . Then G is cyclic.*

Proof: Suppose G has order n . Then, by Lagrange's theorem, we at least know that every element of G has order *dividing* n , and what we would like to know is that it has an element of order *exactly* n . We recognize this as an MIF situation, but this time MIF serves more as inspiration than a tool which is used *per se*.

Namely, for any divisor d of n , let us define G_d to be the set of elements of G of order dividing d . G_d is easily seen to be a subgroup of G , and subgroups of cyclic groups are cyclic, so if what we are trying to prove is true then G_d is a cyclic group of order d . Certainly this is true for $d = 1$! So assume by induction that this is true for all *proper* divisors d of n .

Now let $f(d)$ be the number of elements of order d in G . We know $f(d) = 0$ unless d is a divisor of n . We also know that for any d there are at most d elements in all of F^\times of order d : the polynomial $x^d - 1$ can have at most d roots. Now suppose d is a proper divisor of n : our induction hypothesis implies that there are exactly d roots, namely the elements of G_d ; moreover, since we are assuming that G_d is cyclic, of these d elements, exactly $\varphi(d)$ of them have exact order d . So $f(d) = \varphi(d)$ for all proper divisors d of n . But this means that the number of elements of G whose order is a proper divisor of n is $\sum_{d|n} \varphi(d) - \varphi(n) = n - \varphi(n)$, which leaves us with $n - (n - \varphi(n)) = \varphi(n)$ of elements of a group of order n whose order is not any proper divisor of n . The only possibility is that these elements all have order n , which is what we wanted to show.

2.4. Counting irreducible polynomials. We cannot resist mentioning the following pretty result.

Theorem 7. *For any prime number p and any $n \in \mathbb{Z}^+$, the number of polynomials $P(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ which are irreducible of degree n is*

$$I_n = \frac{N_n}{n} = \frac{\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d}{n}.$$

Remark: All the nonzero terms in N_n have distinct positive ord_p 's, so $\text{ord}_p(N_n)$ is equal to the minimum of these positive numbers, which is less than ∞ : i.e., N_n , and hence I_n , is positive. This implies that there exist finite fields of order p^n for all p and n .

We refer the reader to §7.2 of Ireland and Rosen's *A Classical Introduction to Modern Number Theory* for the short and elegant proof.