ARITHMETICAL FUNCTIONS I: MULTIPLICATIVE FUNCTIONS

PETE L. CLARK

1. Arithmetical Functions

Definition: An **arithmetical function** is a function $f : \mathbb{Z}^+ \to \mathbb{C}$.

Truth be told, this definition is a bit embarrassing. It would mean that taking any function from calculus whose domain contains $[1, +\infty)$ and restricting it to positive integer values, we get an arithmetical function. For instance, $\frac{e^{-3x}}{\cos^2 x + (17 \log(x+1))}$ is an arithmetical function according to this definition, although it is, at best, dubious whether this function holds any significance in number theory.

If we were honest, the definition we would like to make is that an arithmetical function is a real or complex-valued function defined for positive integer arguments which *is of some arithmetic significance*, but of course this is not a formal definition at all. Probably it is best to give examples:

Example $A\Omega$: The prime counting function $n \mapsto \pi(n)$, the number of prime numbers p, $1 \leq p \leq n$.

This is the example *par excellence* of an arithmetical function: approximately half of number theory is devoted to understanding its behavior. This function really deserves a whole unit all to itself, and it will get one: we put it aside for now and consider some other examples.

Example 1: The function $\omega(n)$, which counts the number of distinct prime divisors of n.

Example 2: The function $\varphi(n)$, which counts the number of integers k, $1 \leq k \leq n$, with $\gcd(k, n) = 1$. Properly speaking this function is called **the totient function**, but its fame inevitably precedes it and modern times it is usually called just "the phi function" or "Euler's phi function." Since a congruence class $\overline{k}$ modulo n is invertible in the ring $\mathbb{Z}/n\mathbb{Z}$ iff its representative k is relatively prime to n, an equivalent definition is

$$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times,$$

the cardinality of the unit group of the finite ring $\mathbb{Z}/n\mathbb{Z}$.

Example 3: The function $n \mapsto d(n)$, the number of positive divisors of n.

Example 4: For any integer k, the function $\sigma_k(n)$, defined as

$$\sigma_k(n) = \sum_{d \mid n} d^k,$$

the sum of the kth powers of the positive divisors of n. Note that $\sigma_0(n) = d(n)$.

Example 5: The Möbius function $\mu(n)$, defined as follows: $\mu(1) = 1$, $\mu(n) = 0$ if n is not squarefree; $\mu(p_1 \cdots p_r) = (-1)^r$, when $p_1, \ldots, p_r$ are distinct primes.

Example 6: For a positive integer k, the function $r_k(n)$ which counts the number of representations of n as a sum of k integral squares:

$$r_k(n) = \#\{(a_1, \ldots, a_k) \mid a_1^2 + \ldots + a_k^2 = n\}.$$

These examples already suggest many others. Notably, all our examples but Example 5 are special cases of the following general construction: if we have on hand, for any positive integer n, a finite set S_n of arithmetic objects, then we can define an arithmetic function by defining $n \mapsto \#S_n$. This shows the link between number theory and combinatorics. In fact the Möbius function μ is a yet more purely combinatorial gadget, whose purpose we shall learn presently. In general we have lots of choices as to what sets S_n we want to count: the first few examples are "elementary" in the sense that the sets counted are defined directly in terms of such things as divisibility, primality, and coprimality: as we shall, see, they are also elementary in the sense that we can write down exact formulas for them. The example $r_k(n)$ is more fundamentally Diophantine in character: we have a polynomial in several variables – here $P(x_1, \ldots, x_k) = x_1^2 + \ldots + x_k^2$, and the sets we are conunting are just the number of times the value n is taken by this polynomial. This could clearly be much generalized, with the obvious proviso that there should be some suitable restrictions so as to make the number of solutions finite in number (e.g. we would not want to count the number of integer solutions to $ax + by = N$, for that is infinite; however we could restrict x and y to taking non-negative values). Ideally we would like to express these "Diophantine" arithmetical functions like r_k in terms of more elementary arithmetical functions like the divisor sum functions σ_k. Very roughly, this is the arithmetic analogue of the analytical problem expressing a real-valued function $f(x)$ as a combination of simple functions like x^k or $\cos(nx)$, $\sin(nx)$. Of course in analysis most interesting functions are not just polynomials (or trigonometric polynomials), at least not exactly: rather, one either needs to consider approximations to f by elementary functions, or to express f as some sort of limit (e.g. an infinite sum) of elementary functions (or both, of course). A similar philosophy applies here, with a notable exception: even the "elementary" functions like $d(n)$ and $\varphi(n)$ are not really so elementary as they first appear!

2. Multiplicative Functions

2.1. **Definition and basic properties.** An important property shared by many "arithmetically significant" functions is multiplicativity.

Definition: An arithmetical function f is said to be **multiplicative** if:
(M1) $f(1) \neq 0$.
(M2) For all relatively prime positive integers n_1, n_2, $f(n_1 n_2) = f(n_1) \cdot f(n_2)$.

Lemma 1. *If f is multiplicative, then $f(1) = 1$.*

Proof: Taking $n_1 = n_2 = 1$, we have, using (M2)

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1) = f(1)^2.$$

Now by (M1), $f(1) \neq 0$, so that we may cancel $f(1)$'s to get $f(1) = 1$.

Exercise: Suppose an arithmetical function f satisfies (M2) but not (M1). Show that $f \equiv 0$: i.e., $f(n) = 0$ for all $n \in \mathbb{Z}^+$.

The following is a nice characterization of multiplicative functions:

Proposition 2. *For an arithmetical function f, the following are equivalent:*
a) f is multiplicative;
b) f is not identically zero, and for all $n = p_1^{a_1} \cdots p_k^{a_k}$ (the standard form factorization of n), we have $f(n) = \prod_{i=1}^k f(p_i^{a_i})$.

Remark: Here we are using the convention that for $n = 1$, $k = 0$, and a product extending over zero terms is automatically equal to 1 (just as a sum extending over zero terms is automatically equal to 0). (If this is not to your taste, just insert in part b) the condition that $f(1) = 1$!)

Proof: Exercise.

In other words, a multiplicative function f is completely determined by the values it takes on all prime powers p^k. Thus, in trying to understand a function known to be multiplicative, one needs only to "see what it is" on prime power values of n. Note that, conversely, any function f defined only on prime powers p^k – and satisfying $f(1) = 1$ – extends to a unique multiplicative function.

2.2. **Completely multiplicative functions.** If you have never seen this definition before, then something has been bothering you the whole time, and I will now respond to this worry. Namely, wouldn't it make more sense to say that a function f is multiplicative if $f(n_1 \cdots n_2) = f(n_1) \cdot f(n_2)$ for *all* integers n_1 and n_2?

In a purely algebraic sense the answer is yes: the stronger condition (together with $f(1) \neq 0$) says precisely that f is a homomorphism from the monoid $\mathbb{Z}^+$ to the monoid $\mathbb{C}^\times$. This is certainly a very nice property for f to have, and it has a name as well: **complete multiplicativity**. But in practice complete multiplicativity is *too nice*: only very special functions satisfy this property, whereas the class of multiplicative functions is large enough to contain many of our "arithmetically significant functions." For instance, neither σ_k (for any k) nor φ is completely multiplicative, but, as we are about to see, all of these functions are multiplicative.

2.3. **Multiplicativity of the σ_k's.**

Theorem 3. *The functions σ_k (for all $k \in \mathbb{N}$) are multiplicative.*

Proof: It is almost obvious that the Möbius function is multiplicative. Indeed its value at a prime power p^a is: 1 if $a = 0$, -1 if $a = 1$, and 0 if $a \geq 2$. Now there is a unique multiplicative function with these values, and it is easy to see that μ is that function: we have $\mu(p_1^{a_1} \cdots p_k^{a_k}) = 0$ unless $a_i = 1$ for all i – as we should – and

otherwise $\mu(p_1 \cdots p_k) = (-1)^k = \mu(p_1) \cdots \mu(p_k)$. In other words, μ is essentially multiplicative by construction.

Now let us see that σ_k is multiplicative. Observe that – since $\gcd(n_1, n_2) = 1$! – every divisor d of $n_1 \cdot n_2$ can be expressed uniquely as a product $d_1 \cdot d_2$ with $d_i \mid n_i$. So

$$\sigma_k(n_1 n_2) = \sum_{d \mid n_1 n_2} d^k = \sum_{d_1 \mid n_1,\ d_2 \mid n_2} (d_1 d_2)^k = (\sum_{d_1 \mid n_1} d_1^k)(\sum_{d_2 \mid n_2} d_2^k) = \sigma_k(n_1)\sigma_k(n_2).$$

2.4. **CRT and the multiplicativity of the totient.** The multiplicativity of φ is closely connected to the Chinese Remainder Theorem, as we now review. Namely, for coprime n_1 and n_2, consider the map $\Phi : \mathbb{Z}/(n_1 n_2) \to \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2)$ given by

$$k \pmod{n_1 n_2} \mapsto (k \pmod{n_1}, k \pmod{n_2}).$$

This map is a well-defined homomorphism of rings, since if $k_1 \equiv k_2 \pmod{n)_i}$, then $k_1 \equiv k_2 \pmod{n)_1 n_2}$. Because the source and target have the same, finite, cardinality $n_1 n_2$, in order for it to be an isomorphism it suffices to show either that it is injective or that it is surjective. Note that the standard, elementary form of the Chinese Remainder Theorem addresses the surjectivity: given any pair of congruence classes $i \pmod{n_1}$and $j \pmod{n_2}$ the standard proof provides an explicit formula for a class $p(i, j) \pmod{n_1 n_2}$ which maps via Φ onto this pair of classes. However, writing down this formula requires at least a certain amount of cleverness, whereas it is trivial to show the injectivity: as usual, we need only show that the kernel is 0. Well, if $\Phi(\overline{k}) = 0$, then k is 0 mod n_1 and 0 mod n_2, meaning that $n_1 \mid k$ and $n_2 \mid k$. In other words, k is a common multiple of n_1 and n_2, so, as we've shown, k is a multiple of the least common multiple of n_1 and n_2. Since n_1 and n_2 are coprime, this means that $n_1 n_2 \mid k$, i.e., that $k \equiv 0 \pmod{n_1 n_2}$!

Theorem 4. *There is a (canonical) isomorphism of groups*

$$(\mathbb{Z}/(n_1 n_2))^\times \to (\mathbb{Z}/(n_1))^\times \times (\mathbb{Z}/(n_2))^\times.$$

Proof: This follows from the isomorphism of rings discussed above, together with two almost immediate facts of pure algebra. First, if $\Phi : R \to S$ is an isomorphism of rings, then the restriction of Φ to the unit group $R^\times$ of R is an isomorphism onto the unit group $S^\times$ of S. Second, if $S = S_1 \times S_2$ is a product of rings, then $S^\times = S_1^\times \times S_2^\times$, i.e., the units of the product is the product of the units. We leave it to the reader to verify these two facts.

Corollary 5. *The function φ is multiplicative.*

Proof: Since $\varphi(n) = \#(\mathbb{Z}/(n))^\times$, this follows immediately.

Now let us use the "philosophy of multiplicativity" to give exact formulas for $\sigma_k(n)$ and $\varphi(n)$. In other words, we have reduced to the case of evaluating at prime power values of n, but this is much easier. Indeed, the positive divisors of p^a are $1,\ p,\ \ldots, p^a$, so the sum of the kth powers of these divisors is $a + 1$ when $k = 0$ and is otherwise

$$\sigma_k(p^a) = 1 + p^k + p^{2k} + \ldots + p^{ak} = \frac{1 - (p^k)^{a+1}}{1 - p^k} = \frac{1 - p^{(a+1)k}}{1 - p^k}.$$

Similarly, the only numbers $1 \leq i \leq p^a$ which are not coprime to p^a are the multiples of p, of which there are p^{a-1}: $1 \cdot p, 2 \cdot p, \ldots p^{a-1}p = p^a$. So

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1 - \frac{1}{p}).$$

Corollary 6. *Suppose $n = p_1^{a_1} \cdots p_k^{a_k}$. Then:*
a) $d(n) = \prod_{i=1}^k (a_i + 1)$.
b) For $k > 0$, $\sigma_k(n) = \prod_{i=1}^k \frac{1-p^{(a+1)k}}{1-p^k}$.
c) $\varphi(n) = \prod_{i=1}^k p^{a-1}(p-1)$.

The last formula is often rewritten as

$$\frac{\varphi(n)}{n} = \prod_{p \mid n} (1 - \frac{1}{p}). \tag{1}$$

While we are here, we quote the following more general form of the CRT, which is often useful:

Theorem 7. *(Generalized Chinese Remainder Theorem) Let $n_1, \ldots, n_r$ be any r positive integers. Consider the natural map*

$$\Phi : \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$$

which sends an integer k to $(k \pmod{n_1}, \ldots, k \pmod{n_r})$.
a) The kernel of Φ is the ideal $(\mathrm{lcm}(n_1, \ldots, n_r))$.
b) The following are equivalent:
(i) Φ is surjective;
(ii) $\mathrm{lcm}(n_1, \ldots, n_r) = n_1 \cdots n_r$.
(iii) The integers $n_1, \ldots, n_r$ are pairwise relatively prime.

The proof is a good exercise. In fact the result holds essentially verbatim for elements $x_1, \ldots, x_r$ in a PID R, and, in some form, in more general commutative rings.

2.5. **Additive functions.** The function ω is not multiplicative: e.g. $\omega(1) = 0$ and $\omega(2) = 1$. However it satisfies a property which is "just as good" as multiplicativity: $\omega(n_1 n_2) = \omega(n_1) + \omega(n_2)$ when $\gcd(n_1, n_2) = 1$. Such functions are called **additive**. Finally, we have the notion of **complete additivity**: $f(n_1 n_2) = f(n_1) + f(n_2)$ for all $n_1,\ n_2 \in \mathbb{Z}^+$; i.e., f is a homomorphism from the positive integers under multiplication to the complex numbers under addition. We have seen some completely additive functions, namely, ord_p for a prime p.

Proposition 8. *Fix any real number $a > 1$ (e.g. $a = e,\ a = 2$). A function f is additive (respectively, completely additive) iff a^f is multiplicative (respectively, completely multiplicative).*

Proof: An easy exercise.

2.6. **Sums of squares.** The functions r_k are not multiplicative: to represent 1 as a sum of k squares we must take all but one of the x_i equal to 0 and the other equal to ± 1. This amounts to $r_k(1) = 2k > 1$. However, we should not give up so easily! Put $r'_k = \frac{r_k}{2k}$. We can now quote a beautiful theorem, parts of which may be proved later.

Theorem 9. *The function r'_k is multiplicative iff $k = 1,\ 2,\ 4$ or 8.*

2.7. **Perfect numbers.** The ancient Greeks regarded a positive integer n as **perfect** if it is equal to the sum of its proper divisors ("aliquot parts"). They knew some examples, e.g. 6, 28, 496, 8128.

In modern language a perfect number is a solution n of the equation $\sigma(n) - n = n$, or $\sigma(n) = 2n$. Aha, but we have an exact formula for the σ function: perhaps we can use it to write down all perfect numbers? The answer is a resounding "sort of."

Best, as usual, is to examine some data to try to figure out what is going on. Since our formula for σ takes into account the standard form factorization of n, we should probably look at these factorizations of our sample perfect numbers. We find:

$$6 = 2 \cdot 3$$
$$28 = 2^2 \cdot 7$$
$$496 = 2^4 \cdot 31$$
$$8128 = 2^6 \cdot 127.$$

As exercises in pattern recognition go, this is a pretty easy one. We have a power of 2 multiplied by an odd prime. But not just any odd prime, mind you, an odd prime which happens to be exactly one less than a power of 2. And not just any power of 2...anyway, we soon guess the pattern $2^{n-1} \cdot 2^n - 1$. But we're still not done: in our first four examples, n was $2, 3, 5, 7$, all primes. Finally we have a precise conjecture that our knowledge of σ can help us prove:

Proposition 10. *(Euclid) Let p be a prime such that $2^p - 1$ is also prime. Then $N_p = 2^{p-1}(2^p - 1)$ is a perfect number.*

Proof: Since $2^p - 1$ is odd, it is coprime to 2^{p-1}. So

$$\sigma(N_p) = \sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1).$$

But these are both prime power arguments, so are easy to evaluate, as above. We get $\sigma(2^{p-1}) = 2^p - 1$ and $\sigma(2^p - 1) = 2^p$, so overall $\sigma(N_p) = 2^p \cdot (2^p - 1) = 2N_p$.

This is a nice little calculation, but it raises more questions than it answers. The first question is: are there infinitely many primes p such that $2^p - 1$ is prime? Such primes are called **Mersenne primes** after Father Marin Mersenne, a penpal of Fermat. It would be appropriate to make any number of historical remarks about Mersenne and/or his primes, but we refer the reader to Wikipedia for this. Suffice it to say that, in theory, it is a wide open problem to show that there exist infinitely many Mersenne primes, but in practice, we do keep finding successively larger Mersenne primes (at a rate of several a year), meaning that new and ridiculously large perfect numbers are being discovered all the time.

Ah, but the second question: is every perfect number of the form N_p for a Mersenne prime p? Euler was able to show that every **even** perfect number is of this form. The argument is a well-known one (and is found in Silverman's book) so we omit it here. Whether or not there exist any odd perfect numbers is one of the notorious open problems of number theory. At least you should not go searching for odd perfect numbers by hand: it is known that there are no odd perfect numbers $N < 10^{300}$, and that any odd perfect number must satisfy a slew of restrictive conditions (e.g. on the shape of its standard form factorization).