Arithmetical functions

Jonathan Lam

February 14, 2020

This is a more explicit understanding of Chapter 2: Arithmetical functions, from Alan Baker's *A concise introduction to the theory of numbers.*

Important results about the floor function

Basic properties of the floor function: $[x+y] \geq [x]+[y]$ (floor function "triangle inequality"); if $n \in \mathbb{Z}$, then $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$ and $[x+n] = [x] + n$.

Theorem 1. *Let p be prime. Let $l(n,p)$ be the largest integer such that p^l divides $n!$. Then the formula for $l(n,p)$ is*

$$l(n,p) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right]$$

Proof. We count.

$$l(n,p) = \sum_{m=1}^{n} \sum_{\substack{j=1 \\ p^j | m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1 \\ p^j | m}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right]$$

If this is confusing, here is a brief explanation of the middle two expressions:

1. The inner summand is the highest power α_i of p that is a factor of m_i. Sum this over all m_is in $1 \dots n$ to get the highest power of p that is a factor of $n!$. I.e., if p^{α_i} is the highest power factor of p in m_i, then $p^{\alpha_1} p^{\alpha_2} \dots p^{\alpha_n} = p^{\sum_{m=1}^{n} \alpha_m} \Rightarrow l = \sum_{m=1} \alpha_m$.
2. This assumes a different interpretation of the problem. Instead of summing over all the powers of p within each m, sum over all of the ms divisible by p_j, and then sum over all of the js. This should give you the same result. The benefit is that the inner sum is easily representable with the floor function.

□

Corollary 1.1. $l(n,p) \leq \left[\frac{n}{p-1}\right]$

Corollary 1.2. *For $m, n \in \mathbb{Z}$, $m \geq n \geq 0$, $\binom{m}{n}$ is an integer. Moreover, if $n_1 + n_2 + \cdots + n_k = m$, then the multinomial coefficient $\binom{m}{n_1, n_2, \ldots, n_k}$ is an integer.*

Proof. Express $m!$, $n!$, and $(m-n)!$ in their prime-factor representations over the same set of primes $\{p_i\}$.

$$m! = \prod_i p_i^{\alpha_i},\ n! = \prod_i p_i^{\beta_i},\ (m-n)! = \prod_i p_i^{\gamma_i},\ n!(m-n)! = \prod_i p_i^{\beta_i+\gamma_i}$$

From the "triangle inequality" for the floor function, observe that

$$\left[\frac{m}{p^j}\right] \geq \left[\frac{n}{p^j}\right] + \left[\frac{m-n}{p^j}\right]$$

By (Theorem 1), for every prime p_i of $\{p_i\}$, $\alpha_i = l(m, p_i)$, $\beta_i = l(n, p_i)$, and $\gamma_i = l(m-n, p_i)$. By the above inequality and the formula for l, $\alpha_i \geq \beta_i + \gamma + i$; i.e., the power α_i of each prime in the prime factorization of $m!$ is at least the power $\beta_i + \gamma_i$ of the same prime in the factorization of $n!(m-n)!$. Thus $n!(m-n)!|m!$. □

Multiplicative functions

Definition 2. *A real function f defined over the positive integers is said to be multiplicative if $f(m)f(n) = f(mn)$ $\forall m, n$ s.t. $(m, n) = 0$.*

Theorem 3. *If f is multiplicative, either f is identically zero or $f(1) = 1$.*

Note that it is often useful to illustrate properties of multiplicative functions by using the fundamental theorem of arithmetic to factor any positive integer into mutually coprime factors.

Notes on divisors of products of coprime integers: Let $m, n \in \mathbb{Z}_+$. Then it is easy to show

$$D = \{d : d|mn\} = \{xy : (x, y) \in \{x : x|m\} \times \{y : y|n\}\}$$

is the set of divisors of mn. If $(m, n) = 1$, then $|D| = |\{x : x|m\}| \times |\{y : y|n\}|$; i.e., every factor of mn is *uniquely* factorable into the product of one divisor of m and one divisor of n. This allows the rewriting of the operation

$$\sum_{d|mn} f(d) = \sum_{(x,y)\in\{x:x|m\}\times\{y:y|n\}}\sum f(xy) = \sum_{x:x|m}\sum_{y:y|n} f(xy)$$

where the summation may be replaced by any other aggregate operation over a set, and f is a generic function defined over positive integers.

Here is the proof of uniqueness of factorization. By the fundamental theorem of arithmetic,

$$m = \prod_{i=1}^{k} p_i^{\alpha_k},\ n = \prod_{j=1}^{l} q_j^{\beta_j}$$

where p_i, q_j are prime for all i, j. Since $(m, n) = 1$, $\{p_i\} \cap \{q_j\} = \varnothing$. Let $a|m$, $b|n$; then

$$a = \prod_{i=1}^{k'} p_i^{\alpha_i},\ b = \prod_{j=1}^{l'} q_j^{\beta_j},\ ab = \prod_{i=1}^{k'} p_i^{\alpha_i} \prod_{j=1}^{l'} q_j^{\beta_j}$$

Since this factorization of ab is unique and $\{p_i\}, \{q_i\}$ are disjoint, it is clear that there is no way to factor this into the product of one divisor of m (the product of some subset of $\{p_i\}$) and one divisor of n (the product of some subset of $\{q_i\}$) except by $a \cdot b$.

Theorem 4. *Let f be a multiplicative function, and define g to be*

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

Then g is multiplicative.

Proof. Let $(m, n) = 1$. Then we can split the single sum over the factors of mn into a double sum over the factors of m and the factors of n (proved above).

$$g(mn) = \sum_{d|mn} f(d) = \sum_{x|m} \sum_{y|n} f(mn) = \sum_{x|m} f(m) \sum_{y|n} f(n) = g(m)g(n)$$

□

Euler's totient function (Sylvester)

Theorem 5 (Euler's totient function)**.**

$$\phi(n) = n \prod_{p_i|k} \left(1 - \frac{1}{p_i}\right)$$

where p_i represents the set of unique prime factors of n.

Proof. Based on an argument provided by Sylvester, and not requiring showing that the totient is multiplicative beforehand. We work backwards, using the known result and showing that it is correct. By expanding the product, we see that this is equivalent to

$$(\phi(n)) = n - \sum_{p_r|n} \frac{n}{p_r} + \sum_{\substack{p_r p_s|n, \\ r<s}} \frac{n}{p_r p_s} - \cdots$$

Note that $\frac{n}{p_r}$ denotes the number of numbers in $1 \dots n$ are divisible by p_r, $\frac{n}{p_r p_s}$ is the number of numbers in that range divisible by $p_r p_s$, and so on. We may reformulate this counting into instead summing over each number m in that range $1 \dots n$, and counting the number of primes or products of primes that divide m. Let $l(m) = |\{p : p|m,\, p|n\}|$; i.e., $l(m)$ denotes the number of common prime factors of m and n and $l(m) = 0 \iff m, n$ are coprime. Thus the above expression is equivalent to

$$(\phi(n)) = \sum_{m=1}^{n} \left(1 - \sum_{\substack{r \\ p_r|m}} 1 + \sum_{\substack{r>s \\ p_r p_s|m}} 1 - \cdots \right)$$

The inner sums are equivalent to combinations over common prime factors of m and n, thus

$$(\phi(n)) = \sum_{m=1}^{n} \left(1 - \binom{l(m)}{1} + \binom{l(m)}{2} - \cdots \right) = \sum_{m=1}^{n} \sum_{r=1}^{l(m)} (-1)^r \binom{l(m)}{r}$$

Note that the inner summation is of the form of a binomial power expansion, i.e.,[1]

$$\sum_{b=0}^{a} (1)^{a-b} (-1)^b \binom{a}{r} = (1-1)^a = \begin{cases} 1 & \text{if } a = 0 \\ 0 & \text{else} \end{cases}$$

Thus

$$c(m) = \sum_{r=1}^{l(m)} (-1)^r \binom{l(m)}{r} = \begin{cases} 1 & \text{if } m, n \text{ coprime} \\ 0 & \text{else} \end{cases}$$

and $c(m)$ is a simple indicator of whether m, n are coprime. This finally simplifies the totient formula down to a clearly correct statement: $\phi(n)$ counts the integers in $1 \dots n$ coprime to n, thus concluding the proof.

$$(\phi(n)) = \sum_{m=1}^{n} c(m)$$

□

Note that, while this proof of the formula for the totient function does not require its multiplicativity, the formula itself may be used to prove its own multiplicativity.

Theorem 6. *Define $g(n)$ as follows:*

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

Then $g(n) = n$.

[1] The following formulation includes first term 1 into the summation, but this introduces the somewhat-iffy 0^0 case. You can see that the value of this summation is clearly 1 when $l(m)$ is zero, as you have no primes to choose from in the pre-simplified version. So this is absolutely correct (and often is, working outside of an analysis context).

Proof. By (Theorem 4), the summation on the left is a multiplicative function. Thus it may be broken up over the prime factorization of n as follows:

$$g(n) = \sum_{d|n} \left((n =) \prod_{p_i|d} p_i^{\alpha_i} \right) = \prod_{p_i|d} \left(\sum_{d|p_i^{\alpha_i}} \phi(p_i^{\alpha_i}) \right)$$

The inner summation can be computed using (Lemma 7):

$$\sum_{d|p_i^{\alpha_i}} \phi(p_i^{\alpha_i}) = 1 + (p-1) + (p^2 - p) + \cdots + (p^{\alpha_i} - p^{\alpha_i - 1}) = p^{\alpha_i}$$

Thus the product in $g(n)$ turns back into the prime factorization for n. Thus

$$g(n) = \prod_{p_i|d} p_i^{\alpha_i} = n$$

□

Euler's totient function (based on multiplicativity)

Lemma 7 (Totient function on prime powers)**.** *Let p be prime. Then*

$$\phi(p^n) = p^n - p^{n-1}$$

Proof. Since p^n has only one unique prime factor p, p must divide any number in $1 \dots p^n$ that shares a common prime factor with p^n. There are $p^n/p = p^{n-1}$ such numbers. Thus the number of numbers in $1 \dots p^n$ that are coprime with p^n is $p^n - p^{n-1}$. □

Corollary 7.1. *Let p be prime. Then $\phi(p) = p - 1$.*

For now, assume that the totient function is multiplicative (which must be shown later). This, along with (Lemma 7), makes the proof for the totient function very simple.

Theorem 8 (Euler's totient function (based on multiplicativity))**.** *Since the totient function is multiplicative and is defined on powers of primes (in a relation given by (Lemma 7)),*

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

Proof. By the fundamental theorem of arithmetic, n is uniquely factorable into a product of its primes, i.e.,

$$n = \prod_{p_r|n} p_r^{\alpha_r}$$

$$\phi(n) = \phi\left(\prod_{p_r|n} p_r^{\alpha_r}\right) = \prod_{p_r|n} \phi(p_r^{\alpha_r}) = \prod_{p_r|n} p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$
$$= \left(\prod_{p_r|n} p_r^{\alpha_r}\right)\left(\prod_{p_r|n}\left(1 - \frac{1}{p_r}\right)\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

□

This proof is clearly much simpler and straightforward than that in the previous section, and doesn't require the clever interpretation and manipulation of counting principles. However, we still need to show multiplicativity of the totient function to finish this proof. This can be done using the formula of the totient function (if proved already by some other manner, such as in the previous section) or using the Chinese remainder theorem (this will be proved later).

The Möbius function $\mu(n)$

The following result is not shown in the book and may be obvious, but it was not immediately apparent to me, so here it is.

Lemma 9. *Let f be an arithmetic function. Then*

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

Proof. The condition for d is symmetric to a condition for $\frac{n}{d}$; i.e., $n|d \iff \frac{n}{d}|d$. The result follows by substituting $d = \frac{n}{d'}$:

$$\sum_{d|n} f(d) = \sum_{\frac{n}{d'}|n} f\left(\frac{n}{d'}\right) = \sum_{d'|n} f\left(\frac{n}{d'}\right)$$

. □

Definition 10. *Let $n \in \mathbb{Z}^+$ have k distinct prime factors. Define the Möbius function $\mu(x)$ as follows:*

$$\mu(x) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ has any repeated prime factors} \\ (-1)^k & \text{else} \end{cases}$$

μ is multiplicative: if $(m, n) = 1$, where m has k_1 distinct prime factors and n has k_2 distinct prime factors, then if m (or n) has a repeated prime factor, then the product will also have a repeated prime factor and $0 \cdot \mu(n) = \mu(m)\mu(n) = \mu(mn) = 0$; otherwise, all of the prime factors will be unique and $(-1)^{k_1}(-1)^{k_n} = \mu(m)\mu(n) = \mu(mn) = (-1)^{k_1+k_2}$. The convention that $\mu(1) = 1$ further makes the Möbius function fit well with multiplicative properties.

Lemma 11. *Define $v(n)$ as follows:*

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

Then

$$v(n) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n > 0 \end{cases}$$

The proof for this lemma is immediate.

Theorem 12 (Möbius inversion formula)**.** *Let $g(x) = \sum_{d|n} f(d)$, where f is an arithmetic function. Then*

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

(i.e., f is the Dirichlet convolution of its sum-function g and μ) and vice versa.

Proof. ($\Rightarrow$) We use (Lemma 9) and manipulate equivalent indexing to achieve the result:

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

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

Note that $d'|d|n \iff \frac{n}{d} | \frac{n}{d'}$, so this becomes

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

Since $v(n/d') = 1 \iff n = d'$ by (Lemma 11), this simplifies to

$$f(n) \cdot 1 + \sum_{\substack{d'|n \\ d' \neq n}} f(d') \cdot 0 = f(n)$$

Proof. ($\Leftarrow$) Let f be defined in the following form:

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

Then

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

$$= \sum_{d'|n} g(d')v\left(\frac{n}{d'}\right) = g(n)$$

(This proof is very similar to that in the forward direction, so some intermediate steps and explanation are not shown here.) □

Some of the reindexing from the book was difficult for me to follow and understand. Online resources such as `https://math.berkeley.edu/~stankova/MathCircle/Multiplicative.pdf` and `https://math.stackexchange.com/a/1757370/96244` were helpful to me.

Theorem 13 (Totient-Möbius relationship)**.**

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

Proof. (Using totient formula) Expanding the totient formula in the same way as in the proof of (Theorem 5), we get

$$\phi(n) = n\left(1 - \sum_{p_r|n} \frac{1}{p_r} + \sum_{\substack{p_r p_s|n,\\ r<s}} \frac{1}{p_r p_s} - \cdots\right)$$

$$= n\left(\frac{\mu(1)(=(-1)^0)}{1} + \sum_{p_r|n} \frac{\mu(p_r)(=(-1)^1)}{p_r} + \sum_{\substack{p_r p_s|n\\ r<s}} \frac{\mu(p_r p_s)(=(-1)^2)}{p_r p_s} + \cdots\right)$$

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

In the original formulation of the totient formula, we are only counting factors of p that have only unique prime factors – this is accommodated nicely for because $\mu(n) = 0$ for all of the other factors (those with repeated prime factors), and thus are implicitly accounted for in this summation.

Proof. (Using Möbius inversion formula) The sum-function $g(n) = \sum_{d|n} \phi(n)$ is equal to n by (Theorem 6). Apply the Möbius inversion formula:

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

□