18.781 (Spring 2016): Floor and arithmetic functions

Darij Grinberg

June 19, 2016

Contents

***

These are the extended notes for the 18.786 class on 14 April 2016 (the actual class did about half of what is in these notes). I roughly follow [NiZuMo91, §4.1–§4.3], although not always using the same notations.

I use the notation $\mathbb{N}$ for $\{0, 1, 2, \ldots\}$, and the notation $\mathbb{N}_+$ for $\{1, 2, 3, \ldots\}$.

1. The floor function

1.1. Definition and basic properties

I shall first discuss the floor function, following [NiZuMo91, §4.1].

Definition 1.1.1. Let x be a real number. Then, $\lfloor x \rfloor$ is defined to be the unique integer n satisfying $n \leq x < n+1$. This integer $\lfloor x \rfloor$ is called the *floor* of x, or the *integer part* of x.

Remark 1.1.2. **(a)** Why is $\lfloor x \rfloor$ well-defined? I mean, why does the unique integer n in Definition 1.1.1 exist, and why is it unique? I will not answer this question in general (the answer probably depends on how you define real numbers anyway). However, in the case when x is rational, the proof is simple (see Corollary 1.1.4 below).

(b) What we call $\lfloor x \rfloor$ is typically called $[x]$ in older books (such as [NiZuMo91]). I suggest avoiding the notation $[x]$ wherever possible; it has too many different meanings (whereas $\lfloor x \rfloor$ almost always means the floor of x).

(c) The map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \lfloor x \rfloor$ is called the *floor function* or the *greatest integer function*. There is also a *ceiling function*, which sends each $x \in \mathbb{R}$ to the unique integer n satisfying $n-1 < x \leq n$; this latter integer is called $\lceil x \rceil$. The two functions are connected by the rule $\lceil x \rceil = -\lfloor -x \rfloor$ (for all $x \in \mathbb{R}$).

The floor and the ceiling functions are some of the simplest examples of discontinuous functions.

(d) Here are some examples of floors:

$$\lfloor n \rfloor = n \qquad \text{for every } n \in \mathbb{Z};$$
$$\lfloor 1.32 \rfloor = 1; \qquad \lfloor \pi \rfloor = 3; \qquad \lfloor 0.98 \rfloor = 0;$$
$$\lfloor -2.3 \rfloor = -3; \qquad \lfloor -0.4 \rfloor = -1.$$

(e) You might have the impression that $\lfloor x \rfloor$ is "what remains from x if the digits behind the comma are removed". This impression is highly imprecise. For one, it is completely broken for negative x (for example, $\lfloor -2.3 \rfloor$ is -3, not -2). But more importantly, the operation of "removing the digits behind the comma" from a number is not well-defined; the periodic decimal representations $0.999\ldots$ and $1.000\ldots$ belong to the same real number (1), but removing their digits behind the comma leaves us with different integers.

(f) A related map is the map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \left\lfloor x + \frac{1}{2} \right\rfloor$. It sends each real x to the integer that is closest to x, choosing the larger one in the case of a tie. This is one of the many things that are commonly known as "rounding" a number.

Floors of rational numbers are directly related to division with remainder:

Proposition 1.1.3. Let a and b be integers such that $b > 0$. Let q and r be the quotient and the remainder obtained when dividing a by b. Then, q is the unique integer n satisfying $n \leq \frac{a}{b} < n + 1$.

Proof of Proposition 1.1.3. We know that q and r are the quotient and the remainder obtained when dividing a by b. In other words, we have $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, b-1\}$ and $a = qb + r$.

From $r \in \{0, 1, \ldots, b-1\}$, we obtain $0 \leq r < b$. Now, from $0 \leq r$, we obtain $qb \leq qb + r = a$. Dividing this inequality by b, we obtain $q \leq \frac{a}{b}$ (since $b > 0$). Also, $a = qb + \underbrace{r}_{<b} < qb + b = (q+1)\,b$. Dividing this inequality by b, we obtain $\frac{a}{b} < q + 1$ (since $b > 0$). Thus, $q \leq \frac{a}{b} < q + 1$. Hence, q is an integer n satisfying $n \leq \frac{a}{b} < n + 1$. It thus remains to show that q is the **unique** such integer. In other words, it remains to show that if n is an integer satisfying $n \leq \frac{a}{b} < n + 1$, then $n = q$.

So let n be an integer satisfying $n \leq \frac{a}{b} < n + 1$. We must show that $n = q$.

We have $n \leq \frac{a}{b} < q + 1$. Since n and q are integers, this yields $n \leq (q+1) - 1 = q$.

We have $q \leq \frac{a}{b} < n + 1$. Since q and n are integers, this yields $q \leq (n+1) - 1 = n$. Combining this with $n \leq q$, we obtain $n = q$. As we said, this completes our proof. □

Corollary 1.1.4. Let x be a rational number.

(a) The integer $\lfloor x \rfloor$ is well-defined.

(b) Write x in the form $x = \frac{a}{b}$ where a and b are integers such that $b > 0$. Let q and r be the quotient and the remainder obtained when dividing a by b. Then, $\lfloor x \rfloor = q$.

Proof of Corollary 1.1.4. Write x in the form $x = \frac{a}{b}$ where a and b are integers such that $b > 0$. Let q and r be the quotient and the remainder obtained when dividing a by b. Then, Proposition 1.1.3 yields that q is the unique integer n satisfying $n \leq \frac{a}{b} < n + 1$. In other words, q is the unique integer n satisfying $n \leq x < n + 1$ (since $x = \frac{a}{b}$). Thus, the unique integer n satisfying $n \leq x < n + 1$ exists. Thus, $\lfloor x \rfloor$ is well-defined. This proves Corollary 1.1.4 **(a)**.

(b) We have just seen that q is the unique integer n satisfying $n \leq x < n + 1$. But this latter integer has been denoted by $\lfloor x \rfloor$. Thus, $\lfloor x \rfloor = q$. This proves Corollary 1.1.4 **(b)**. □

Proposition 1.1.5. Let m be an integer, and let x be a real number. Then, $m \leq x$ holds if and only if $m \leq \lfloor x \rfloor$ holds.

Proof of Proposition 1.1.5. Recall that $\lfloor x \rfloor$ is the unique integer n satisfying $n \leq x < n+1$. Thus, $\lfloor x \rfloor$ is an integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

If $m \leq x$ holds, then $m \leq \lfloor x \rfloor$ holds as well[1]. Conversely, if $m \leq \lfloor x \rfloor$ holds, then $m \leq x$ (because $m \leq \lfloor x \rfloor \leq x$). Combining these two implications, we conclude that $m \leq x$ holds if and only if $m \leq \lfloor x \rfloor$ holds. Proposition 1.1.5 is thus proven. □

Corollary 1.1.6. Let x be a real number. Then, $\lfloor x \rfloor$ is the greatest integer that is smaller or equal to x.

Proof of Corollary 1.1.6. Clearly, $\lfloor x \rfloor$ is the greatest integer that is smaller or equal to $\lfloor x \rfloor$. In other words, $\lfloor x \rfloor$ is the greatest integer m satisfying $m \leq \lfloor x \rfloor$. Equivalently, $\lfloor x \rfloor$ is the greatest integer m satisfying $m \leq x$ (since Proposition 1.1.5 shows that the condition $m \leq \lfloor x \rfloor$ for an integer m is equivalent to the condition $m \leq x$). In other words, $\lfloor x \rfloor$ is the greatest integer that is smaller or equal to x. This proves Corollary 1.1.6. □

Corollary 1.1.6 is often used as a definition of $\lfloor x \rfloor$. It is also the reason why the map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \lfloor x \rfloor$ is called the greatest integer function.

Before we come to anything interesting, we shall prove a few more basic properties of the floor function.

Proposition 1.1.7. Let m be an integer. Then, $\lfloor m \rfloor = m$.

Proof of Proposition 1.1.7. Clearly, $m \leq m < m+1$. But $\lfloor m \rfloor$ is the unique integer n satisfying $n \leq m < n+1$ (because this is how $\lfloor m \rfloor$ is defined). Hence, if n is any integer satisfying $n \leq m < n+1$, then $n = \lfloor m \rfloor$. Applying this to $n = m$, we obtain $m = \lfloor m \rfloor$ (since $m \leq m < m+1$). This proves Proposition 1.1.7. □

The next fact that we shall prove is [NiZuMo91, Theorem 4.1 **(5)**]:

Proposition 1.1.8. Let x be a real number. Then,

$$\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases}.$$

[1] *Proof.* Assume that $m \leq x$ holds. We need to prove that $m \leq \lfloor x \rfloor$ holds.

Indeed, assume the contrary. Thus, $m > \lfloor x \rfloor$. Hence, $m \geq \lfloor x \rfloor + 1$ (since m and $\lfloor x \rfloor$ are integers). Thus, $\lfloor x \rfloor + 1 \leq m \leq x$, which contradicts $x < \lfloor x \rfloor + 1$. This contradiction proves that our assumption was wrong. Hence, $m \leq \lfloor x \rfloor$ is proven, qed.

Proof of Proposition 1.1.8. We must be in one of the following two cases:

Case 1: We have $x \in \mathbb{Z}$.

Case 2: We have $x \notin \mathbb{Z}$.

Let us consider Case 1 first. In this case, we have $x \in \mathbb{Z}$. In other words, x is an integer. Hence, $-x$ is an integer as well. Thus, Proposition 1.1.7 (applied to $m = -x$) yields that $\lfloor -x \rfloor = -x$. But Proposition 1.1.7 (applied to $m = x$) yields $\lfloor x \rfloor = x$ (since x is an integer). Thus, $\underbrace{\lfloor x \rfloor}_{=x} + \underbrace{\lfloor -x \rfloor}_{=-x} = x + (-x) = 0$. Comparing this with $\begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases} = 0$ (since $x \in \mathbb{Z}$), we obtain $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases}$. Thus, Proposition 1.1.8 is proven in Case 1.

Let us now consider Case 2. In this case, we have $x \notin \mathbb{Z}$. Recall that $\lfloor x \rfloor$ is the unique integer n satisfying $n \leq x < n+1$ (since this is how $\lfloor x \rfloor$ is defined). Thus, $\lfloor x \rfloor$ is an integer and satisfies $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. In particular, $\lfloor x \rfloor \in \mathbb{Z}$ (since $\lfloor x \rfloor$ is an integer).

We cannot have $\lfloor x \rfloor = x$ (since otherwise, we would have $\lfloor x \rfloor = x \notin \mathbb{Z}$, which would contradict $\lfloor x \rfloor \in \mathbb{Z}$). Thus, $\lfloor x \rfloor \neq x$. Combining this with $\lfloor x \rfloor \leq x$, we obtain $\lfloor x \rfloor < x$.

Now, $x < \lfloor x \rfloor + 1$, so that $-1 - \lfloor x \rfloor < -x$. Thus, $-1 - \lfloor x \rfloor \leq -x$. On the other hand, $\lfloor x \rfloor < x$, so that $-x < -\lfloor x \rfloor = (-1 - \lfloor x \rfloor) + 1$.

Thus, $-1 - \lfloor x \rfloor \leq -x < (-1 - \lfloor x \rfloor) + 1$. But $\lfloor -x \rfloor$ is the unique integer n satisfying $n \leq -x < n+1$ (since this is how $\lfloor -x \rfloor$ is defined). Thus, if n is any integer satisfying $n \leq -x < n+1$, then $n = \lfloor -x \rfloor$. Applying this to $n = -1 - \lfloor x \rfloor$, we obtain $-1 - \lfloor x \rfloor = \lfloor -x \rfloor$ (since $-1 - \lfloor x \rfloor$ is an integer satisfying $-1 - \lfloor x \rfloor \leq -x < (-1 - \lfloor x \rfloor) + 1$). Hence, $-1 = \lfloor x \rfloor + \lfloor -x \rfloor$, so that $\lfloor x \rfloor + \lfloor -x \rfloor = -1$. Comparing this with $\begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases} = -1$ (since $x \notin \mathbb{Z}$), we obtain $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases}$. Thus, Proposition 1.1.8 is proven in Case 2.

We have now proven Proposition 1.1.8 in each of the two Cases 1 and 2. Thus, Proposition 1.1.8 always holds. □

Now, let us prove [NiZuMo91, Theorem 4.1 **(2)**]:

Proposition 1.1.9. Let x be a **nonnegative** real number. Then, $\lfloor x \rfloor = \sum_{\substack{m \in \mathbb{N}_+; \\ m \leq x}} 1$.

Proof of Proposition 1.1.9. First of all, $0 \leq x$ (since x is nonnegative). But Proposition 1.1.5 (applied to $m = 0$) shows that $0 \leq x$ holds if and only if $0 \leq \lfloor x \rfloor$ holds.

Thus, $0 \leq \lfloor x \rfloor$ holds (since $0 \leq x$ holds). Thus, $\lfloor x \rfloor \in \mathbb{N}$ (since $\lfloor x \rfloor$ is an integer). Hence,

$$\sum_{\substack{m \in \mathbb{N}_+; \\ m \leq \lfloor x \rfloor}} 1 = \sum_{m=1}^{\lfloor x \rfloor} 1 = \lfloor x \rfloor .$$

Hence,

$$\lfloor x \rfloor = \sum_{\substack{m \in \mathbb{N}_+; \\ m \leq \lfloor x \rfloor}} 1 = \sum_{\substack{m \in \mathbb{N}_+; \\ m \leq x}} 1$$

(because Proposition 1.1.5 shows that the condition $m \leq \lfloor x \rfloor$ for an integer m is equivalent to the condition $m \leq x$). This proves Proposition 1.1.9. □

We shall next prove [NiZuMo91, Theorem 4.1 **(3)**]:

Proposition 1.1.10. Let x be a real number. Let k be an integer. Then, $\lfloor x + k \rfloor = \lfloor x \rfloor + k$.

Proof of Proposition 1.1.10. Recall that $\lfloor x \rfloor$ is the unique integer n satisfying $n \leq x < n + 1$. Thus, $\lfloor x \rfloor$ is an integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Also, $\lfloor x \rfloor + k$ is an integer (since both $\lfloor x \rfloor$ and k are integers). Also, $\underbrace{\lfloor x \rfloor}_{\leq x} + k \leq x + k$ and $\underbrace{x}_{< \lfloor x \rfloor + 1} + k < \lfloor x \rfloor + 1 + k = (\lfloor x \rfloor + k) + 1$, so that $\lfloor x \rfloor + k \leq x + k < (\lfloor x \rfloor + k) + 1$. Thus, $\lfloor x \rfloor + k$ is an integer n satisfying $n \leq x + k < n + 1$.

But $\lfloor x + k \rfloor$ is the unique integer n satisfying $n \leq x + k < n + 1$ (because this is how $\lfloor x + k \rfloor$ is defined). Hence, if n is any integer satisfying $n \leq x + k < n + 1$, then $n = \lfloor x + k \rfloor$. We can apply this to $n = \lfloor x \rfloor + k$ (since $\lfloor x \rfloor + k$ is an integer n satisfying $n \leq x + k < n + 1$), and thus obtain $\lfloor x \rfloor + k = \lfloor x + k \rfloor$. Proposition 1.1.10 is proven. □

Proposition 1.1.11. Let $n \in \mathbb{N}$ and $b \in \mathbb{N}_+$. Then, $\sum_{\substack{k \in \{1,2,\ldots,n\}; \\ b \mid k}} 1 = \left\lfloor \dfrac{n}{b} \right\rfloor$.

Proof of Proposition 1.1.11. The elements of $\{1, 2, \ldots, n\}$ are precisely the elements

k of $\mathbb{N}_+$ satisfying $k \leq n$. Hence,

$$\sum_{\substack{k \in \{1,2,\ldots,n\};\\ b|k}} 1 = \sum_{\substack{k \in \mathbb{N}_+;\\ k \leq n \\ b|k}} 1 = \sum_{\substack{m \in \mathbb{N}_+;\\ bm \leq n}} 1 \qquad \left(\begin{array}{c}\text{here, we have substituted } bm \text{ for } k \text{ in}\\ \text{the sum (since the } k \in \mathbb{N}_+ \text{ satisfying}\\ b \mid k \text{ are precisely the integers of}\\ \text{the form } bm \text{ with } m \in \mathbb{N}_+)\end{array}\right)$$
$$= \sum_{\substack{m \in \mathbb{N}_+;\\ m \leq \frac{n}{b}}} 1 \qquad \left(\text{since } bm \leq n \text{ is equivalent to } m \leq \frac{n}{b}\right)$$
$$= \left\lfloor \frac{n}{b} \right\rfloor$$

(because Proposition 1.1.9 (applied to $x = \frac{n}{b}$) yields $\left\lfloor \frac{n}{b} \right\rfloor = \sum_{\substack{m \in \mathbb{N}_+;\\ m \leq \frac{n}{b}}} 1$). Thus, Proposition 1.1.11 is proven. □

The floor function is weakly increasing:

Proposition 1.1.12. Let x and y be real numbers such that $x \leq y$. Then, $\lfloor x \rfloor \leq \lfloor y \rfloor$.

Proof of Proposition 1.1.12. Recall that $\lfloor x \rfloor$ is the unique integer n satisfying $n \leq x < n+1$. Thus, $\lfloor x \rfloor$ is an integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Hence, $\lfloor x \rfloor \leq x \leq y$.

Proposition 1.1.5 (applied to $\lfloor x \rfloor$ and y instead of m and x) shows that $\lfloor x \rfloor \leq y$ holds if and only if $\lfloor x \rfloor \leq \lfloor y \rfloor$ holds. Hence, $\lfloor x \rfloor \leq \lfloor y \rfloor$ holds (since $\lfloor x \rfloor \leq y$ holds). This proves Proposition 1.1.12. □

Let us now prove [NiZuMo91, Theorem 4.1 **(4)**]:

Proposition 1.1.13. Let $u \in \mathbb{R}$ and $v \in \mathbb{R}$. Then, $\lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u+v \rfloor \leq \lfloor u \rfloor + \lfloor v \rfloor + 1$.

Proof of Proposition 1.1.13. All of $\lfloor u \rfloor$, $\lfloor v \rfloor$ and $\lfloor u+v \rfloor$ are integers (by their definition).

Recall that $\lfloor u \rfloor$ is the unique integer n satisfying $n \leq u < n+1$. Thus, $\lfloor u \rfloor$ is an integer satisfying $\lfloor u \rfloor \leq u < \lfloor u \rfloor + 1$.

Recall that $\lfloor v \rfloor$ is the unique integer n satisfying $n \leq v < n+1$. Thus, $\lfloor v \rfloor$ is an integer satisfying $\lfloor v \rfloor \leq v < \lfloor v \rfloor + 1$.

Recall that $\lfloor u+v \rfloor$ is the unique integer n satisfying $n \leq u+v < n+1$. Thus, $\lfloor u+v \rfloor$ is an integer satisfying $\lfloor u+v \rfloor \leq u+v < \lfloor u+v \rfloor + 1$.

Proposition 1.1.5 (applied to $m = \lfloor u \rfloor + \lfloor v \rfloor$ and $x = u + v$) shows that $\lfloor u \rfloor + \lfloor v \rfloor \leq u + v$ holds if and only if $\lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u + v \rfloor$ holds. Thus, $\lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u + v \rfloor$ holds (since $\underbrace{\lfloor u \rfloor}_{\leq u} + \underbrace{\lfloor v \rfloor}_{\leq v} \leq u + v$ holds).

We know that $\lfloor v \rfloor + 1$ is an integer (since $\lfloor v \rfloor$ is an integer). Hence, Proposition 1.1.10 (applied to $x = u$ and $k = \lfloor v \rfloor + 1$) yields $\lfloor u + \lfloor v \rfloor + 1 \rfloor = \lfloor u \rfloor + \lfloor v \rfloor + 1$.

But $u + \underbrace{v}_{<\lfloor u \rfloor + 1} < u + \lfloor v \rfloor + 1$. Hence, Proposition 1.1.12 (applied to $x = u + v$ and $y = u + \lfloor v \rfloor + 1$) shows that $\lfloor u + v \rfloor \leq \lfloor u + \lfloor v \rfloor + 1 \rfloor = \lfloor u \rfloor + \lfloor v \rfloor + 1$. Combining this with $\lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u + v \rfloor$, we obtain $\lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u + v \rfloor \leq \lfloor u \rfloor + \lfloor v \rfloor + 1$.

This proves Proposition 1.1.13. □

Finally, let us prove [NiZuMo91, Theorem 4.1 **(6)**]:

Proposition 1.1.14. Let $x \in \mathbb{R}$ and $m \in \mathbb{N}_+$. Then, $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \dfrac{x}{m} \right\rfloor$.

Proof of Proposition 1.1.14. Recall that $\lfloor x \rfloor$ is the unique integer n satisfying $n \leq x < n + 1$. Thus, $\lfloor x \rfloor$ is an integer satisfying $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Recall that $\left\lfloor \dfrac{x}{m} \right\rfloor$ is the unique integer n satisfying $n \leq \dfrac{x}{m} < n + 1$ (by the definition of $\left\lfloor \dfrac{x}{m} \right\rfloor$. Thus, $\left\lfloor \dfrac{x}{m} \right\rfloor$ is an integer satisfying $\left\lfloor \dfrac{x}{m} \right\rfloor \leq \dfrac{x}{m} < \left\lfloor \dfrac{x}{m} \right\rfloor + 1$.

But $m \in \mathbb{N}_+$ and thus $m \geq 1 > 0$. Hence, we can multiply the inequality $\left\lfloor \dfrac{x}{m} \right\rfloor \leq \dfrac{x}{m}$ by m. We thus obtain $m \left\lfloor \dfrac{x}{m} \right\rfloor \leq x$.

But Proposition 1.1.5 (applied to $m \left\lfloor \dfrac{x}{m} \right\rfloor$ instead of m) shows that $m \left\lfloor \dfrac{x}{m} \right\rfloor \leq x$ holds if and only if $m \left\lfloor \dfrac{x}{m} \right\rfloor \leq \lfloor x \rfloor$ holds (since $m \left\lfloor \dfrac{x}{m} \right\rfloor$ is an integer). Thus, $m \left\lfloor \dfrac{x}{m} \right\rfloor \leq \lfloor x \rfloor$ holds (since $m \left\lfloor \dfrac{x}{m} \right\rfloor \leq x$ holds). Dividing this inequality by m, we obtain $\left\lfloor \dfrac{x}{m} \right\rfloor \leq \dfrac{\lfloor x \rfloor}{m}$.

We can divide the inequality $\lfloor x \rfloor \leq x$ by m (since $m > 0$). We thus obtain $\dfrac{\lfloor x \rfloor}{m} \leq \dfrac{x}{m}$. Hence, $\dfrac{\lfloor x \rfloor}{m} \leq \dfrac{x}{m} < \left\lfloor \dfrac{x}{m} \right\rfloor + 1$.

So we have $\left\lfloor \dfrac{x}{m} \right\rfloor \leq \dfrac{\lfloor x \rfloor}{m} < \left\lfloor \dfrac{x}{m} \right\rfloor + 1$. In other words, $\left\lfloor \dfrac{x}{m} \right\rfloor$ is an integer n satisfying $n \leq \dfrac{\lfloor x \rfloor}{m} < n + 1$.

But $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$ is the unique integer n satisfying $n \leq \dfrac{\lfloor x \rfloor}{m} < n + 1$ (because this is how $\left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$ is defined). Hence, if n is any integer satisfying $n \leq \dfrac{\lfloor x \rfloor}{m} < n + 1$, then $n = \left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$. We can apply this to $n = \left\lfloor \dfrac{x}{m} \right\rfloor$ (since $\left\lfloor \dfrac{x}{m} \right\rfloor$ is an integer n

satisfying $n \leq \dfrac{\lfloor x \rfloor}{m} < n+1$), and thus obtain $\left\lfloor \dfrac{x}{m} \right\rfloor = \left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$. Proposition 1.1.14 is proven. □

I refer to [NiZuMo91, §4.1] for further properties of the floor function.

1.2. Interlude: greatest common divisors

Before we move on, let me remind you of some basic facts about coprime numbers and greatest common divisors. First, we recall how greatest common divisors are defined:

Definition 1.2.1. Let b and c be two integers. If $(b,c) \neq (0,0)$, then $\gcd(b,c)$ means the greatest of all common divisors of b and c. We also set $\gcd(0,0) = 0$. Thus, $\gcd(b,c)$ is defined for any two integers b and c.

If b and c are two integers, then $\gcd(b,c)$ is called the *greatest common divisor of b and c* (even if $\gcd(0,0)$ is not literally the greatest of all common divisors of 0 and 0) or, briefly, the *gcd* of b and c. Clearly, $\gcd(b,c) = \gcd(c,b)$, $\gcd(b,c) \mid b$ and $\gcd(b,c) \mid c$ for any two integers b and c. Notice that $\gcd(b,c)$ is a nonnegative integer (and actually a positive integer unless $(b,c) = (0,0)$).

Older books such as [NiZuMo91] tend to denote the gcd of two integers b and c by (b,c) (rather than by $\gcd(b,c)$ as we do); this is a convention that I shall decidedly not follow (since it risks confusion with the notation (b,c) for the ordered pair of b and c).

The most important property of gcds is *Bézout's theorem* ([NiZuMo91, Theorem 1.3]):

Theorem 1.2.2. Let b and c be two integers. Then, there exist integers x and y such that $\gcd(b,c) = bx + cy$.

See [NiZuMo91, Theorem 1.3] for the proof of Theorem 1.2.2 in the case when $(b,c) \neq (0,0)$. In the case when $(b,c) = (0,0)$, Theorem 1.2.2 obviously holds (since we can take $x = 0$ and $y = 0$).

For another proof of Theorem 1.2.2, see the Appendix (Chapter 3) below.

A basic property of gcds that follows directly from Theorem 1.2.2 is the following:

Proposition 1.2.3. Let a, b and c be three integers such that $a \mid b$ and $a \mid c$. Then, $a \mid \gcd(b,c)$.

In words, Proposition 1.2.3 says that any common divisor of two integers must divide the gcd of these two integers.

Proof of Proposition 1.2.3. Theorem 1.2.2 shows that there exist integers x and y such that $\gcd(b,c) = bx + cy$. Consider these x and y. Now, $a \mid b \mid bx$ and $a \mid c \mid cy$. Hence, both integers bx and cy are divisible by a. Thus, their sum $bx + cy$ must also be divisible by a. In other words, $a \mid bx + cy$. In other words, $a \mid \gcd(b,c)$ (since $\gcd(b,c) = bx + cy$). This proves Proposition 1.2.3. □

Corollary 1.2.4. Let a, b, c and d be four integers such that $a \mid c$ and $b \mid d$. Then, $\gcd(a,b) \mid \gcd(c,d)$.

Proof of Corollary 1.2.4. We have $\gcd(a,b) \mid a \mid c$ and $\gcd(a,b) \mid b \mid d$. Thus, Proposition 1.2.3 (applied to $\gcd(a,b)$, c and d instead of a, b and c) shows that $\gcd(a,b) \mid \gcd(c,d)$. This proves Corollary 1.2.4. □

We shall now use Theorem 1.2.2 to derive a slight generalization of [NiZuMo91, Theorem 1.8]:

Proposition 1.2.5. Let a, b and m be three integers such that $\gcd(a,m) = 1$. Then, $\gcd(b,m) = \gcd(ab,m)$.

Proof of Proposition 1.2.5. Theorem 1.2.2 (applied to a and m instead of b and c) shows that there exist integers x and y such that $\gcd(a,m) = ax + my$. Consider these x and y. We have $ax + my = \gcd(a,m) = 1$.

Let $g = \gcd(b,m)$ and $h = \gcd(ab,m)$. Thus, g and h are nonnegative integers.

We have $g = \gcd(b,m) \mid b \mid ab$ and $g = \gcd(b,m) \mid m$. Thus, Proposition 1.2.3 (applied to g, ab and m instead of a, b and c) shows that $g \mid \gcd(ab,m)$. In other words, $g \mid h$ (since $h = \gcd(ab,m)$).

On the other hand, $h = \gcd(ab,m) \mid ab \mid abx$ and $h = \gcd(ab,m) \mid m \mid may$. Thus, both integers abx and may are divisible by h. Therefore, the sum of these two integers must also be divisible by h. In other words, $h \mid abx + may$. Since

$$abx + may = b \underbrace{(ax + my)}_{=1} = b,$$

this rewrites as $h \mid b$. So we have $h \mid b$ and $h \mid m$. Thus, Proposition 1.2.3 (applied to h, b and m instead of a, b and c) shows that $h \mid \gcd(b,m)$. In other words, $h \mid g$ (since $g = \gcd(b,m)$).

But it is well-known that if u and v are two nonnegative integers satisfying $u \mid v$ and $v \mid u$, then $u = v$. We can apply this to $u = g$ and $v = h$ (since g and h are nonnegative integers satisfying $g \mid h$ and $h \mid g$), and thus we obtain $g = h$. Hence, $\gcd(b,m) = g = h = \gcd(ab,m)$. This proves Proposition 1.2.5. □

The following corollary is precisely [NiZuMo91, Theorem 1.8]:

Corollary 1.2.6. Let a, b and m be three integers. Assume that a is coprime to m, and assume that b is coprime to m. Then, ab is coprime to m.

Proof of Corollary 1.2.6. We know that a is coprime to m. In other words, $\gcd(a,m) = 1$. Also, we have assumed that b is coprime to m. In other words, $\gcd(b,m) = 1$. Now, Proposition 1.2.5 yields $\gcd(b,m) = \gcd(ab,m)$. Thus, $\gcd(ab,m) = \gcd(b,m) = 1$. In other words, ab is coprime to m. This proves Corollary 1.2.6. □

The following corollary generalizes Corollary 1.2.6 to n integers instead of the two integers a and b:

Corollary 1.2.7. Let $c_1, c_2, \ldots, c_n$ be n integers. Let m be an integer. Assume that c_u is coprime to m for every $u \in \{1,2,\ldots,n\}$. Then, $c_1c_2\cdots c_n$ is coprime to m.

Proof of Corollary 1.2.7. We shall prove that

$$c_1c_2\cdots c_g \text{ is coprime to } m \qquad \text{for every } g \in \{0,1,\ldots,n\}. \tag{1}$$

Proof of (1): We shall prove (1) by induction on g:

Induction base: We have $c_1c_2\cdots c_0 = (\text{empty product}) = 1$ (since empty products are 1 by definition). But 1 is clearly coprime to m. In other words, $c_1c_2\cdots c_0$ is coprime to m (since $c_1c_2\cdots c_0 = 1$). In other words, (1) holds for $g = 0$. This completes the induction base.

Induction step: Let $G \in \{0,1,\ldots,n\}$ be positive. Assume that (1) holds for $g = G-1$. We must prove that (1) holds for $g = G$.

We have $G \in \{0,1,\ldots,n\}$, and thus $G \in \{1,2,\ldots,n\}$ (since G is positive).

We know that $c_1c_2\cdots c_{G-1}$ is coprime to m (since we assumed that (1) holds for $g = G-1$). Also, we assumed that c_u is coprime to m for every $u \in \{1,2,\ldots,n\}$. Applying this to $u = G$, we see that c_G is coprime to m. Now, Corollary 1.2.6 (applied to $c_1c_2\cdots c_{G-1}$ and c_G instead of a and b) shows that $(c_1c_2\cdots c_{G-1})\,c_G$ is coprime to m. In other words, $c_1c_2\cdots c_G$ is coprime to m (since $(c_1c_2\cdots c_{G-1})\,c_G = c_1c_2\cdots c_G$). In other words, (1) holds for $g = G$. This completes the induction step, and thus (1) is proven.

Now, applying (1) to $g = n$, we conclude that $c_1c_2\cdots c_n$ is coprime to m. This proves Corollary 1.2.7. □

A further consequence of Proposition 1.2.5 is the following fact ([NiZuMo91, Theorem 1.10]):

Proposition 1.2.8. Let x, y and z be three integers such that $x \mid yz$ and $\gcd(x,y) = 1$. Then, $x \mid z$.

Proof of Proposition 1.2.8. We have $x \mid yz$ and $x \mid x$. Hence, Proposition 1.2.3 (applied to x, yz and x instead of a, b and c) shows that $x \mid \gcd(yz,x)$.

We have $\gcd(y,x) = \gcd(x,y) = 1$. Hence, Proposition 1.2.5 (applied to $a = y$, $b = z$ and $m = x$) shows that $\gcd(z,x) = \gcd(yz,x)$. Now, $x \mid \gcd(yz,x) = \gcd(z,x) \mid z$. This proves Proposition 1.2.8. □

Another important result on gcds is the following fact:

Proposition 1.2.9. Let g be a positive integer. Let a and b be two integers. Then, $g \gcd(a,b) = \gcd(ga, gb)$.

Proof of Proposition 1.2.9. Both $\gcd(a,b)$ and g are nonnegative integers; hence, $g \gcd(a,b)$ is a nonnegative integer.

We have $g \underbrace{\gcd(a,b)}_{|a} \mid ga$ and $g \underbrace{\gcd(a,b)}_{|b} \mid gb$. Thus, Proposition 1.2.3 (applied to $g \gcd(a,b)$, ga and gb instead of a, b and c) shows that $g \gcd(a,b) \mid \gcd(ga, gb)$.

On the other hand, Theorem 1.2.2 (applied to a and b instead of b and c) shows that there exist integers x and y such that $\gcd(a,b) = ax + by$. Consider these x and y. We have $\gcd(ga, gb) \mid ga \mid gax$ and $\gcd(ga, gb) \mid gb \mid gby$. Thus, both integers gax and gby are divisible by $\gcd(ga, gb)$. Therefore, their sum $gax + gby$ is also divisible by $\gcd(ga, gb)$. In other words, we have $\gcd(ga, gb) \mid gax + gby$. Since $gax + gby = g \underbrace{(ax + by)}_{=\gcd(a,b)} = g \gcd(a,b)$, this rewrites as $\gcd(ga, gb) \mid g \gcd(a,b)$.

But it is well-known that if u and v are two nonnegative integers satisfying $u \mid v$ and $v \mid u$, then $u = v$. We can apply this to $u = g \gcd(a,b)$ and $v = \gcd(ga, gb)$ (since $g \gcd(a,b)$ and $\gcd(ga, gb)$ are nonnegative integers satisfying $g \gcd(a,b) \mid \gcd(ga, gb)$ and $\gcd(ga, gb) \mid g \gcd(a,b)$), and thus we obtain $g \gcd(a,b) = \gcd(ga, gb)$. This proves Proposition 1.2.9. □

Here is another property of gcds, which we will use later:

Proposition 1.2.10. Let m and n be two coprime positive integers. Let u be an integer. Then, $\gcd(u,m) \cdot \gcd(u,n) = \gcd(u, mn)$.

Proof of Proposition 1.2.10. Set $h = \gcd(u, mn)$, $v = \gcd(u,m)$ and $w = \gcd(u,n)$. We shall prove that $vw = h$.

We have $v = \gcd(u,m) \in \mathbb{N}_+$ (since m is positive) and $w = \gcd(u,n) \in \mathbb{N}_+$ (since n is positive). Thus, both v and w are positive integers; hence, vw is a positive integer. Also, mn is positive (since m and n are positive). Now, $h = \gcd(u, mn) \in \mathbb{N}_+$ (since mn is positive).

We have $v = \gcd(u,m) \mid m$ and $w = \gcd(u,n) \mid n$. Hence, Corollary 1.2.4 (applied to v, w, m and n instead of a, b, c and d) yields $\gcd(v,w) \mid \gcd(m,n) = 1$ (since m and n are coprime). Hence, $\gcd(v,w) = 1$.

We have $w = \gcd(u,n) \mid u$ and thus $\dfrac{u}{w} \in \mathbb{Z}$. Now, $v = \gcd(u,m) \mid u = w \cdot \dfrac{u}{w}$. Thus, Proposition 1.2.8 (applied to v, w and $\dfrac{u}{w}$ instead of x, y and z) shows that $v \mid \dfrac{u}{w}$ (since $\gcd(v,w) = 1$). In other words, $\dfrac{u}{w}/v \in \mathbb{Z}$. Now, $\dfrac{u}{vw} = \dfrac{u}{w}/v \in \mathbb{Z}$, so that $vw \mid u$.

But $v = \gcd(u,m) \mid m$ and thus $\dfrac{m}{v} \in \mathbb{Z}$. Also, $w = \gcd(u,n) \mid n$ and thus $\dfrac{n}{w} \in \mathbb{Z}$. Now, $\dfrac{mn}{vw} = \dfrac{m}{v} \cdot \dfrac{n}{w}$ is the product of two integers (since $\dfrac{m}{v}$ and $\dfrac{n}{w}$ are integers), and thus itself an integer. In other words, $vw \mid mn$.

So we have $vw \mid u$ and $vw \mid mn$. Proposition 1.2.3 (applied to vw, u and mn instead of a, b and c) thus yields $vw \mid \gcd(u,mn) = h$.

Proposition 1.2.9 (applied to n, u and m instead of g, a and b) shows that $n \gcd(u,m) = \gcd(nu,nm)$. Thus, $\gcd(nu,nm) = n \underbrace{\gcd(u,m)}_{=v} = nv = vn$.

Now, $h = \gcd(u,mn) \mid mn = nm$ and $h = \gcd(u,mn) \mid u \mid nu$. Hence, Proposition 1.2.3 (applied to h, nu and nm instead of a, b and c) shows that $h \mid \gcd(nu,nm)$. In other words, $h \mid vn$ (since $\gcd(nu,nm) = vn$).

Proposition 1.2.9 (applied to v, u and n instead of g, a and b) shows that $v \gcd(u,n) = \gcd(vu,vn)$. Thus, $\gcd(vu,vn) = v \underbrace{\gcd(u,n)}_{=w} = vw$.

Now, $h \mid u \mid vu$ and $h \mid vn$. Thus, Proposition 1.2.3 (applied to h, vu and vn instead of a, b and c) shows that $h \mid \gcd(vu,vn)$. In other words, $h \mid vw$ (since $\gcd(vu,vn) = vw$). Combining this with $vw \mid h$, we obtain $h = vw$ (since h and vw are positive integers). Now,

$$\underbrace{\gcd(u,m)}_{=v} \cdot \underbrace{\gcd(u,n)}_{=w} = vw = h = \gcd(u,mn).$$

This proves Proposition 1.2.10. □

1.3. de Polignac's formula

One of the most useful applications of the floor function is computing the p-adic valuation of factorials. Let us first define our notations:

Definition 1.3.1. Let p be a prime. Let n be a nonzero integer. Then, $v_p(n)$ is defined to be the highest nonnegative integer k such that $p^k \mid n$. This nonnegative integer $v_p(n)$ is called the *p-adic valuation* of n.

Remark 1.3.2. Some authors use the notation $e_p(n)$ instead of $v_p(n)$.

Another way to characterize $v_p(n)$ in Definition 1.3.1 is by the following statement: The number $\dfrac{n}{p^{v_p(n)}}$ is an integer not divisible by p.

Yet another (probably simpler) way to define $v_p(n)$ is the following: $v_p(n)$ is the exponent with which p occurs in the prime factorization of n. [2] (This is clearly equivalent to the definition of $v_p(n)$ above.) While I will try to avoid using prime factorizations wherever I can, there should be nothing stopping you from using them; in general, the prime factorization of n is probably the quickest way to get an intuition for $v_p(n)$ (although not the quickest way to compute it!).

Often, the definition of $v_p(n)$ is extended to all rational numbers n. Then, one defines $v_p(n)$ to be the unique integer k (not necessarily nonnegative) such that the rational number $\dfrac{n}{p^k}$ can be written as a fraction whose numerator and denominator are both integers coprime to p. This works when $n \neq 0$. In the case of $n = 0$, one commonly defines $v_p(0)$ to be $-\infty$; here, $-\infty$ is a symbol which (when it comes to comparing it with integers) is smaller than every integer.

Theorem 1.3.3 (de Polignac's formula)**.** Let p be a prime. Let $n \in \mathbb{N}$. Then,

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(The sum on the right hand side is infinite, but only finitely many of its terms are nonzero, and thus it is a well-defined integer.)

Before we prove this theorem, here are two simple lemmas:

Lemma 1.3.4. Let p be a prime. Let n be a nonzero integer. Then,

$$v_p(n) = \sum_{\substack{i \in \mathbb{N}_+; \\ p^i \mid n}} 1.$$

Proof of Lemma 1.3.4. Recall that $v_p(n)$ is defined as the highest nonnegative integer k such that $p^k \mid n$. Thus, $v_p(n)$ is a nonnegative integer satisfying $p^{v_p(n)} \mid n$.

Every $i \in \mathbb{N}_+$ which satisfies $i \leq v_p(n)$ must satisfy $p^i \mid n$ (since $p^i \mid p^{v_p(n)} \mid n$). Conversely, every $i \in \mathbb{N}_+$ satisfying $p^i \mid n$ must satisfy $i \leq v_p(n)$ (since $v_p(n)$ is the **highest** nonnegative integer k such that $p^k \mid n$). Thus, the $i \in \mathbb{N}_+$ which satisfy $i \leq v_p(n)$ are exactly the $i \in \mathbb{N}_+$ which satisfy $p^i \mid n$. Consequently,

$$\sum_{\substack{i \in \mathbb{N}_+; \\ i \leq v_p(n)}} 1 = \sum_{\substack{i \in \mathbb{N}_+; \\ p^i \mid n}} 1.$$

Hence, $\sum_{\substack{i \in \mathbb{N}_+; \\ p^i \mid n}} 1 = \sum_{\substack{i \in \mathbb{N}_+; \\ i \leq v_p(n)}} 1 = \sum_{i=1}^{v_p(n)} 1 = v_p(n)$. This proves Lemma 1.3.4. □

[2]This exponent should be understood as 0 if p does not occur in the prime factorization of n at all.

Lemma 1.3.5. Let p be a prime. Let $a_1, a_2, \ldots, a_n$ be finitely many nonzero integers. Then,

$$v_p\left(a_1 a_2 \cdots a_n\right) = v_p\left(a_1\right) + v_p\left(a_2\right) + \cdots + v_p\left(a_n\right).$$

This lemma is fairly obvious if you follow the "exponent in prime factorization" interpretation of $v_p(n)$. The proof below avoids this interpretation (for the sake of greater generalizability).

Proof of Lemma 1.3.5. Lemma 1.3.5 can be proven straightforwardly by induction over n, provided that the following two claims are shown:

Claim 1: We have $v_p(1) = 0$.

Claim 2: We have $v_p(ab) = v_p(a) + v_p(b)$ whenever a and b are two nonzero integers.

(In fact, Claim 1 settles the induction base, while Claim 2 is used in the induction step.)

Claim 1 is obvious. It thus remains to prove Claim 2.

Proof of Claim 2: Let a and b be two nonzero integers. Recall that $v_p(a)$ is defined as the highest nonnegative integer k such that $p^k \mid a$. Thus, $v_p(a)$ is a nonnegative integer satisfying $p^{v_p(a)} \mid a$, but $p^{v_p(a)+1} \nmid a$. We have $p^{v_p(a)} \mid a$; thus, we can write a in the form $a = p^{v_p(a)} g$ for some $g \in \mathbb{Z}$. Consider this g. If we had $p \mid g$, then we would have $p^{v_p(a)+1} = p^{v_p(a)} \underbrace{p}_{\mid g} \mid p^{v_p(a)} g = a$; this would contradict $p^{v_p(a)+1} \nmid a$. Hence, we cannot have $p \mid g$. We thus must have $p \nmid g$. In other words, g is coprime to p (since p is a prime).

Thus, we have found a $g \in \mathbb{Z}$ which is coprime to p and satisfies $a = p^{v_p(a)} g$. The same argument (but made for b instead of a) shows that there exists an $h \in \mathbb{Z}$ which is coprime to p and satisfies $b = p^{v_p(b)} h$. Consider this h.

Both g and h are coprime to p. Hence, gh is also coprime to p. Multiplying the equalities $a = p^{v_p(a)} g$ and $b = p^{v_p(b)} h$, we obtain $ab = p^{v_p(a)} g p^{v_p(b)} h = p^{v_p(a)} p^{v_p(b)} gh = p^{v_p(a)+v_p(b)} gh$. Hence, $p^{v_p(a)+v_p(b)} \mid ab$.

On the other hand, recall that $v_p(ab)$ is defined as the highest nonnegative integer k such that $p^k \mid ab$. Thus, $v_p(ab)$ is a nonnegative integer and satisfies $p^{v_p(ab)} \mid ab = p^{v_p(a)+v_p(b)} gh$. Since gh is coprime to $p^{v_p(ab)}$ (because gh is coprime to p), this entails that $p^{v_p(ab)} \mid p^{v_p(a)+v_p(b)}$. Therefore, $v_p(ab) \leq v_p(a) + v_p(b)$.

But $v_p(ab)$ is the **highest** nonnegative integer k such that $p^k \mid ab$. Hence, every nonnegative integer k such that $p^k \mid ab$ must satisfy $k \leq v_p(ab)$. Applying this to $k = v_p(a) + v_p(b)$, we obtain $v_p(a) + v_p(b) \leq v_p(ab)$ (since $v_p(a) + v_p(b)$ satisfies $p^{v_p(a)+v_p(b)} \mid ab$). Combined with $v_p(ab) \leq v_p(a) + v_p(b)$, this yields $v_p(ab) = v_p(a) + v_p(b)$. This proves Claim 2; and as we said, this completes the proof of Lemma 1.3.5. □

Proof of Theorem 1.3.3. We have

$$v_p\left(\underbrace{n!}_{=1\cdot 2\cdot\cdots\cdot n}\right) = v_p\left(1\cdot 2\cdot\cdots\cdot n\right) = v_p\left(1\right) + v_p\left(2\right) + \cdots + v_p\left(n\right)$$

$$\text{(by Lemma 1.3.5, applied to } a_i = i\text{)}$$

$$= \underbrace{\sum_{k=1}^{n}}_{=\sum_{k\in\mathbb{N}_+;\ k\leq n}} \underbrace{v_p\left(k\right)}_{\substack{=\sum_{i\in\mathbb{N}_+;\ p^i|k} 1 \\ \text{(by Lemma 1.3.4, applied to } k \\ \text{instead of } n\text{)}}} = \underbrace{\sum_{k\in\mathbb{N}_+;\ k\leq n}\ \sum_{i\in\mathbb{N}_+;\ p^i|k}}_{\substack{=\sum_{i\in\mathbb{N}_+}\sum_{k\in\mathbb{N}_+;\ k\leq n;\ p^i|k} \\ \text{(here, we are interchanging} \\ \text{the order of summation)}}} 1$$

$$= \underbrace{\sum_{i\in\mathbb{N}_+}}_{=\sum_{i=1}^{\infty}} \underbrace{\sum_{k\in\mathbb{N}_+;\ k\leq n;\ p^i|k}}_{\substack{=\sum_{k\in\{1,2,\ldots,n\};\ p^i|k} 1 \\ \text{(since the elements } k \text{ of } \mathbb{N}_+ \\ \text{satisfying } k\leq n \text{ are precisely} \\ \text{the elements of } \{1,2,\ldots,n\}\text{)}}} 1 = \sum_{i=1}^{\infty} \underbrace{\sum_{k\in\{1,2,\ldots,n\};\ p^i|k} 1}_{\substack{=\left\lfloor \frac{n}{p^i}\right\rfloor \\ \text{(by Proposition 1.1.11,} \\ \text{applied to } b=p^i\text{)}}}$$

$$= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

This proves Theorem 1.3.3. ☐

As an application of Theorem 1.3.3, we can check that binomial coefficients are integers (as long as the inputs are integers):

Corollary 1.3.6. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Then, $\dbinom{n}{m} \in \mathbb{Z}$.

Of course, Corollary 1.3.6 can be proven in various simple ways – for example, by induction using the recurrence relation of the binomial coefficients, or combinatorially by interpreting $\dbinom{n}{m}$ as the number of m-element subsets of a given n-element set. But let us prove it using Theorem 1.3.3, just to show how to use the latter:

Lemma 1.3.7. Let a and b be two nonzero integers. Assume that $v_p\left(a\right) \geq v_p\left(b\right)$ for every prime p. Then, $b \mid a$.

First proof of Lemma 1.3.7. Let P be the set of all primes. Every nonzero integer n satisfies $n = \pm \prod_{p \in P} p^{v_p(n)}$ [3]. Thus,

$$a = \pm \prod_{p \in P} p^{v_p(a)} \qquad \text{and} \qquad b = \pm \prod_{p \in P} p^{v_p(b)}. \tag{2}$$

(The two $\pm$ signs may and may not be equal.)

But every $p \in P$ satisfies $p^{v_p(b)} \mid p^{v_p(a)}$ (since $v_p(a) \geq v_p(b)$). Hence, $\prod_{p \in P} p^{v_p(b)} \mid \prod_{p \in P} p^{v_p(a)}$. In light of (2), this becomes $b \mid a$ (indeed, the $\pm$ signs clearly have no effect on the divisibility). This proofs Lemma 1.3.7. □

Second proof of Lemma 1.3.7. Let me, again, give a proof which avoids the use of prime factorizations. As before, this comes at the cost of brevity (but again, it allows leads to more generality).

Let $g = \gcd(a, b)$. Then, $g = \gcd(a, b) \mid a$. Hence, there exists some $a' \in \mathbb{Z}$ such that $a = ga'$. Consider this a'. Clearly, a' is nonzero (since $ga' = a$ is nonzero).

Also, $g = \gcd(a, b) \mid b$. Hence, there exists some $b' \in \mathbb{Z}$ such that $b = gb'$. Consider this b'. Clearly, b' is nonzero (since $gb' = b$ is nonzero). Of course, g is also nonzero (since $g = \gcd(a, b)$ with a and b being nonzero).

Proposition 1.2.9 (applied to a' and b' instead of a and b) shows that $g \gcd(a', b') = \gcd\left(\underbrace{ga'}_{=a}, \underbrace{gb'}_{=b}\right) = \gcd(a, b) = g$. Cancelling g from this equality (since g is nonzero), we obtain $\gcd(a', b') = 1$.

Let p be any prime dividing b'. We shall derive a contradiction (thus concluding that no such primes exist).

We have $p \mid b'$ (since p is a prime dividing b'). But recall that $v_p(b')$ is defined as the highest nonnegative integer k such that $p^k \mid b'$. Thus, every nonnegative integer k such that $p^k \mid b'$ must satisfy $k \leq v_p(b')$. Applying this to $k = 1$, we obtain $1 \leq v_p(b')$ (since $p^1 = p \mid b'$). Hence, $v_p(b') \geq 1$.

Now, Lemma 1.3.5 (applied to $n = 2$, $a_1 = g$ and $a_2 = a'$) yields $v_p(ga') = v_p(g) + v_p(a')$. Thus, $v_p\left(\underbrace{a}_{=ga'}\right) = v_p(ga') = v_p(g) + v_p(a')$. The same argument (used for b and b' instead a and a') yields $v_p(b) = v_p(g) + v_p(b')$. But by assumption, we have $v_p(a) \geq v_p(b)$. Thus, $v_p(g) + v_p(a') = v_p(a) \geq v_p(b) =$

[3] Indeed, for any prime p, we know that $v_p(n)$ is the exponent with which the prime p appears in the prime factorization of n. Hence, the prime factorization of n is $\pm \prod_{p \in P} p^{v_p(n)}$. (The $\pm$ sign is due to the fact that n can be negative.)

$v_p(g) + v_p(b')$. Since $v_p(g)$ is an integer, we can cancel $v_p(g)$ from this inequality, and obtain $v_p(a') \geq v_p(b') \geq 1$.

Recall that $v_p(a')$ is defined as the highest nonnegative integer k such that $p^k \mid a'$. Thus, $p^{v_p(a')} \mid a'$. But $v_p(a') \geq 1$, whence $p \mid p^{v_p(a')} \mid a'$.

Now, $p \mid a'$ and $p \mid b'$. Hence, Proposition 1.2.3 (applied to p, a' and b' instead of a, b and c) shows that $p \mid \gcd(a', b')$, so that $p \mid 1$ (since $\gcd(a', b') = 1$). This is absurd (since p is a prime).

Now, forget that we fixed p. Thus, we have obtained a contradiction for every prime p dividing b'. Therefore, there exist no such primes p. Therefore, b' is either 1 or -1. In either case, $b' \mid 1$. Hence, $b = g \underbrace{b'}_{\mid 1} \mid g1 = g \mid a$. This proves Lemma 1.3.7. □

Proof of Corollary 1.3.6 (sketched). If $m > n$, then $\binom{n}{m} = 0$; thus, Corollary 1.3.6 is obviously correct in this case. Hence, we WLOG assume that we don't have $m > n$. Therefore, $m \leq n$. Consequently, a well-known formula shows that $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$. Hence, in order to prove that $\binom{n}{m} \in \mathbb{Z}$, it suffices to show that $m!(n-m)! \mid n!$. In light of Lemma 1.3.7 (applied to $a = n!$ and $b = m!(n-m)!$), we can achieve this by showing that

$$v_p(n!) \geq v_p(m!(n-m)!) \qquad \text{for every prime } p. \tag{3}$$

Proof of (3): Let p be a prime. Lemma 1.3.5 yields

$$\begin{aligned}
& v_p(m!(n-m)!) \\
&= \underbrace{v_p(m!)}_{\substack{=\sum_{i=1}^{\infty}\left\lfloor \frac{m}{p^i} \right\rfloor \\ \text{(by Theorem 1.3.3)}}} + \underbrace{v_p((n-m)!)}_{\substack{=\sum_{i=1}^{\infty}\left\lfloor \frac{n-m}{p^i} \right\rfloor \\ \text{(by Theorem 1.3.3)}}} \\
&= \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{n-m}{p^i} \right\rfloor = \sum_{i=1}^{\infty} \underbrace{\left(\left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n-m}{p^i} \right\rfloor \right)}_{\substack{\leq \left\lfloor \frac{m}{p^i} + \frac{n-m}{p^i} \right\rfloor \\ \text{(by the formula } \lfloor u \rfloor + \lfloor v \rfloor \leq \lfloor u+v \rfloor \\ \text{from Proposition 1.1.13)}}} \\
&\leq \sum_{i=1}^{\infty} \left\lfloor \underbrace{\frac{m}{p^i} + \frac{n-m}{p^i}}_{=\frac{n}{p^i}} \right\rfloor = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = v_p(n!) \qquad \text{(by Theorem 1.3.3)}.
\end{aligned}$$

This proves (3).

As we know, this completes the proof of Corollary 1.3.6. □

Note that Corollary 1.3.6 also holds for all $n \in \mathbb{Z}$ (not just for all $n \in \mathbb{N}$); but this would require a different method of proof[4].

Our proof of Corollary 1.3.6 using Theorem 1.3.3 was a slight overkill (as I said, there are easier and better ways to achieve the same goal); however, the method is useful, as it also allows proving other results which are harder to obtain in other ways. Here are two examples of such results (without proof):

Proposition 1.3.8. Let $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ and $m \in \mathbb{N}$. Then, $\binom{a/b}{m}$ is a rational number which can be written as a ratio of two integers whose denominator is a power of b. More precisely, $b^{2m-1}\binom{a/b}{m} \in \mathbb{Z}$ when $m > 0$ (and $\binom{a/b}{m} = 1 \in \mathbb{Z}$ when $m = 0$).

Proposition 1.3.9. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Then, $\dfrac{(2m)!\,(2n)!}{m!n!\,(m+n)!} \in \mathbb{Z}$.

2. Arithmetic functions

2.1. Arithmetic functions

Next, I will discuss the notion of arithmetic functions, and some examples thereof; here I will not really follow [NiZuMo91, §4.2] but rather build up the same theory from my perspective.

Definition 2.1.1. An *arithmetic function* shall mean a function from $\mathbb{N}_+$ to $\mathbb{C}$.

My Definition 2.1.1 appears to be slightly incompatible with the definition in [NiZuMo91, §4.2]; indeed, the latter defines an arithmetic function to be a function from $\mathbb{N}_+$ to a subset of $\mathbb{C}$. However, Niven, Zuckerman and Montgomery never specify the target of the arithmetic functions they introduce in [NiZuMo91, §4.2]; thus, I believe that my Definition 2.1.1 is the definition they have actually meant. Anyway, most people are cavalier about the target of an arithmetic function, and prefer to equate any two arithmetic functions which differ only in the choice of target.

[4]The easiest way to reduce the $n \in \mathbb{Z}$ case to the $n \in \mathbb{N}$ case is by using the upper negation formula $\binom{n}{m} = (-1)^m \binom{m-n-1}{m}$.

Let us define a bunch of arithmetic functions:[5]

Definition 2.1.2. We define the following arithmetic functions:

- The function $\phi : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the number of all $k \in \{1, 2, \ldots, n\}$ coprime to n. This function ϕ is called the *Euler totient function*, or the *phi function* (and is often denoted by φ as well).
- The function $\mathrm{d} : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the number of positive divisors of n. This function d is called the *divisor function*.
- The function $\underline{1} : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to 1.
- The function $\underline{0} : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to 0.
- The function $\iota : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to n.
- The function $\sigma : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the sum of all positive divisors of n.
- For each $k \in \mathbb{Z}$, the function $\sigma_k : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the sum of the k-th powers of all positive divisors of n. Note that $\sigma_0 = \mathrm{d}$ and $\sigma_1 = \sigma$.
- The function $\omega : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the number of all distinct primes dividing n. (For example, $\omega(12) = 2$, since the primes dividing 12 are 2 and 3.)
- The function $\Omega : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to the number of all prime factors of n counted with multiplicity. In other words, if $\Omega(n)$ is the $k \in \mathbb{N}$ such that n can be written as a product of k primes (not necessarily distinct primes). (For example, $\Omega(12) = 3$, since $12 = 2 \cdot 2 \cdot 3$.)
- The function $\mu : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to $\begin{cases} (-1)^{\omega(n)}, & \text{if } n \text{ is squarefree;} \\ 0, & \text{otherwise} \end{cases}$. This function μ is called the *Möbius mu function*.
- The function $\lambda : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to $(-1)^{\Omega(n)}$. This function λ is called *Liouville's lambda function*.
- The function $\varepsilon : \mathbb{N}_+ \to \mathbb{C}$ shall send every $n \in \mathbb{N}_+$ to $\begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1 \end{cases}$.

[5]Recall that a positive integer n is said to be *squarefree* if no perfect square other than 1 divides n. Equivalently, a positive integer n is squarefree if and only if n is a product of **distinct** primes. Equivalently, a positive integer n is squarefree if and only if every prime p satisfies $v_p(n) \leq 1$.

Of course, you can come up with more examples easily. Most arithmetic functions that anyone cares about tend to have their images belong to $\mathbb{Z}$, but the added generality of allowing any complex numbers as images does not hurt, so I see no point in restricting it.

We introduce one more standard notation:

Definition 2.1.3. Any summation sign of the form "$\sum\limits_{d\mid n}$" (where n is a given positive integer) will be understood to mean "sum over all **positive** divisors d of n". This similarly applies when there are further conditions under the summation sign; for instance, "$\sum\limits_{\substack{d\mid n;\\ d\leq 3}}$" means "sum over all positive divisors d of n satisfying $d \leq 3$".

Remark 2.1.4. Some of the functions defined in Definition 2.1.2 can easily be reexpressed using the notation from Definition 2.1.3: Namely, for every $n \in \mathbb{N}_+$, we have

$$\mathrm{d}(n) = \sum_{d\mid n} 1; \qquad \sigma(n) = \sum_{d\mid n} d;$$
$$\sigma_k(n) = \sum_{d\mid n} d^k \qquad (\text{for every } k \in \mathbb{Z}).$$

Some of the arithmetic functions defined above can be written explicitly in terms of the prime factorization of n. I will first state some of the explicit representations before I show a method for proving them.

Definition 2.1.5. If n is a nonzero integer, then $\operatorname{PF} n$ will denote the set of all prime factors of n.

Theorem 2.1.6. For every $n \in \mathbb{N}_+$, we have

$$\phi(n) = \prod_{p\in \operatorname{PF} n} \left(p^{v_p(n)-1}(p-1)\right).$$

Theorem 2.1.7. For every $n \in \mathbb{N}_+$, we have

$$\mathrm{d}(n) = \prod_{p\in \operatorname{PF} n} \left(v_p(n)+1\right).$$

Theorem 2.1.8. For every $n \in \mathbb{N}_+$ and every nonzero $k \in \mathbb{Z}$, we have

$$\sigma_k(n) = \prod_{p \in \operatorname{PF} n} \frac{p^{k(v_p(n)+1)} - 1}{p^k - 1}.$$

Theorem 2.1.6 appears in [NiZuMo91, Theorem 2.19] (in a slightly restated form). Theorem 2.1.7 is [NiZuMo91, Theorem 4.3], and Theorem 2.1.8 is a straightforward generalization of [NiZuMo91, Theorem 4.5]. There are simple and elementary ways to prove each of these theorems; I will give a more abstract approach to highlight the theory.

2.2. Multiplicative functions

Definition 2.2.1. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be an arithmetic function.

(a) The function f is said to be *multiplicative* if and only if it satisfies $f(1) = 1$ and

$$f(mn) = f(m) f(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+.$$

(a) The function f is said to be *totally multiplicative* if and only if it satisfies $f(1) = 1$ and

$$f(mn) = f(m) f(n) \qquad \text{for any two } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+.$$

(Another word for "totally multiplicative" is "completely multiplicative".)

It turns out that totally multiplicative functions are somewhat rare, but multiplicative functions abound in number theory. Here are some examples:

Proposition 2.2.2. Consider the functions defined in Definition 2.1.2.

(a) The function ϕ is multiplicative.

(b) The function d is multiplicative.

(c) The function $\underline{1}$ is totally multiplicative and multiplicative.

(d) The function ι is totally multiplicative and multiplicative.

(e) For every $k \in \mathbb{Z}$, the function σ_k is multiplicative. In particular, the function σ is multiplicative.

(f) The function μ is multiplicative.

(g) The function λ is totally multiplicative and multiplicative.

(h) The function ε is totally multiplicative and multiplicative.

(i) Every totally multiplicative function is multiplicative.

(j) Let $f \in \mathbb{Z}[x]$ be a polynomial. Let $N_P : \mathbb{N}_+ \to \mathbb{C}$ be the function which sends every $n \in \mathbb{N}_+$ to the number of solutions of the congruence $f(x) \equiv 0 \bmod n$. Then, the function N_P is multiplicative.

(k) For every integer u, the function $\mathbb{N}_+ \to \mathbb{C},\ n \mapsto \gcd(u, n)$ is multiplicative.

Proof of Proposition 2.2.2 (sketched). **(i)** This is obvious (since the requirements for a totally multiplicative function clearly encompass the requirements for a multiplicative function).

(a) We know that $\phi(1) = 1$. We thus only need to show that $\phi(mn) = \phi(m)\phi(n)$ for any two coprime $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$. But this is precisely the statement of [NiZuMo91, first sentence of Theorem 2.19]. (Here is a brief reminder of the proof: For every $N \in \mathbb{N}_+$, let $\mathcal{R}(N)$ denote the set of all $k \in \{1, 2, \ldots, N\}$ coprime to N. Now, let $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$ be coprime. Then, there is a bijection $\mathcal{R}(mn) \to \mathcal{R}(m) \times \mathcal{R}(n)$ which sends every $k \in \mathcal{R}(mn)$ to $(k', k'') \in \mathcal{R}(m) \times \mathcal{R}(n)$, where k' is the unique element of $\mathcal{R}(m)$ congruent to k modulo m, and where k'' is the unique element of $\mathcal{R}(n)$ congruent to k modulo n. The fact that this map is well-defined and a bijection can be proven using the Chinese Remainder Theorem. Having this bijection in place, we immediately conclude that $|\mathcal{R}(mn)| = |\mathcal{R}(m) \times \mathcal{R}(n)| = |\mathcal{R}(m)| \cdot |\mathcal{R}(n)|$. Since $|\mathcal{R}(N)| = \phi(N)$ for every $N \in \mathbb{N}_+$, this rewrites as $\phi(mn) = \phi(m)\phi(n)$, qed.) Proposition 2.2.2 **(a)** is thus proven.

Proposition 2.2.2 **(j)** is essentially [NiZuMo91, second sentence of Theorem 2.20], and is proven in a similar way as Proposition 2.2.2 **(a)**.

Parts **(c)**, **(d)** and **(h)** of Proposition 2.2.2 are completely straightforward.

(g) We claim that the following two assertions hold:

Assertion 1: We have $\lambda(1) = 1$.

Assertion 2: We have $\lambda(mn) = \lambda(m)\lambda(n)$ for any two $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$.

Proof of Assertion 1: The number 1 can be written as a product of 0 primes (because the empty product equals 1). Hence, $\Omega(1) = 0$ (by the definition of Ω). The definition of λ yields $\lambda(1) = (-1)^{\Omega(1)} = (-1)^0$ (since $\Omega(1) = 0$). Thus, $\lambda(1) = (-1)^0 = 1$. This proves Assertion 1.

Proof of Assertion 2: Let $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$.

Write m as a product of primes; i.e., write m in the form $m = p_1 p_2 \cdots p_k$ for some primes $p_1, p_2, \ldots, p_k$ (which may and may not be distinct). Thus, m is a product of k primes; hence, $\Omega(m) = k$ (by the definition of Ω).

Write n as a product of primes; i.e., write n in the form $n = q_1 q_2 \cdots q_\ell$ for some primes $q_1, q_2, \ldots, q_\ell$ (which may and may not be distinct). Thus, n is a product of ℓ primes; hence, $\Omega(n) = \ell$ (by the definition of Ω).

Now, multiplying the equalities $m = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_\ell$, we obtain $mn = (p_1 p_2 \cdots p_k)(q_1 q_2 \cdots q_\ell) = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell$. Hence, mn is a product of $k + \ell$ primes (since all of $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_\ell$ are primes). Therefore, $\Omega(mn) = k + \ell$ (by the definition of Ω). Hence,

$$\Omega(mn) = \underbrace{k}_{=\Omega(m)} + \underbrace{\ell}_{=\Omega(n)} = \Omega(m) + \Omega(n).$$

Now, the definition of λ yields $\lambda(m) = (-1)^{\Omega(m)}$, $\lambda(n) = (-1)^{\Omega(n)}$ and $\lambda(mn) = (-1)^{\Omega(mn)}$. Hence,

$$\lambda(mn) = (-1)^{\Omega(mn)} = (-1)^{\Omega(m)+\Omega(n)} \qquad (\text{since } \Omega(mn) = \Omega(m) + \Omega(n))$$
$$= \underbrace{(-1)^{\Omega(m)}}_{=\lambda(m)} \underbrace{(-1)^{\Omega(n)}}_{=\lambda(n)} = \lambda(m)\lambda(n).$$

This proves Assertion 2.

Now, the function λ is totally multiplicative if and only if Assertions 1 and 2 hold (by the definition of "totally multiplicative"). Thus, the function λ is totally multiplicative (since Assertions 1 and 2 hold). Consequently, λ is multiplicative (since every totally multiplicative function is multiplicative (by Proposition 2.2.2 **(i)**)). This proves Proposition 2.2.2 **(g)**.

(k) We leave the proof of Proposition 2.2.2 **(k)** to the reader. (It is completely straightforward using Proposition 1.2.10 and the fact that $\gcd(u, 1) = 1$.)

We defer the proofs of parts **(b)** and **(e)** until later. (Actually, we shall also give a second proof of part **(a)** later.) It thus remains to prove Proposition 2.2.2 **(f)**.

(f) The definition of $\omega(1)$ shows that $\omega(1)$ is the number of all distinct primes dividing 1. But the latter number is clearly 0 (since there are no primes dividing 1). Hence, $\omega(1) = 0$.

The integer 1 is squarefree; hence, the definition of μ yields

$$\mu(1) = (-1)^{\omega(1)} = (-1)^0 \qquad (\text{since } \omega(1) = 0)$$
$$= 1.$$

Hence, we only need to show that $\mu(mn) = \mu(m)\mu(n)$ for any two coprime $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$. So let us show this.

Let $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$ be coprime. We must prove the equality $\mu(mn) = \mu(m)\mu(n)$. If mn is not squarefree, then this equality holds[6]. Hence, we WLOG

[6] *Proof.* Assume that mn is not squarefree. Thus, there is some integer $g > 1$ such that $g^2 \mid mn$. Consider this g.

There exists a prime p such that $p \mid g$ (since $g > 1$). Consider such a p. The prime p cannot divide both m and n (since m and n are coprime). Hence, either $p \nmid m$ or $p \nmid n$ (or both). We WLOG assume that $p \nmid m$ (since otherwise, we can simply switch m with n).

The only positive divisors of p^2 are p^α for $\alpha \in \{0, 1, 2\}$ (since p is a prime). Thus, $\gcd(p^2, m)$ has the form p^α for some $\alpha \in \{0, 1, 2\}$ (since $\gcd(p^2, m)$ is a positive divisor of p^2). Consider this α. Thus, $\alpha \in \{0, 1, 2\}$ and $\gcd(p^2, m) = p^\alpha$.

If we had $\alpha \geq 1$, then we would have $p^1 \mid p^\alpha = \gcd(p^2, m) \mid m$, which would contradict $p = p^1 \nmid m$. Hence, we cannot have $\alpha \geq 1$. Thus, we have $\alpha < 1$. Therefore, $\alpha = 0$ (since $\alpha \in \{0, 1, 2\}$). Now, $\gcd(p^2, m) = p^\alpha = p^0$ (since $\alpha = 0$), so that $\gcd(p^2, m) = p^0 = 1$.

Now, $p \mid g$, so that $p^2 \mid g^2 \mid mn$. Hence, Proposition 1.2.8 (applied to p^2, m and n instead of x, y and z) shows that $p^2 \mid n$ (since $\gcd(p^2, m) = 1$). Hence, n is not squarefree (since p^2 is a square $\neq 1$). Therefore, $\mu(n) = 0$ (by the definition of μ). The definition of μ also shows that $\mu(mn) = 0$ (since mn is not squarefree). Now, comparing $\mu(mn) = 0$ with $\mu(m)\underbrace{\mu(n)}_{=0} = 0$, we obtain $\mu(mn) = \mu(m)\mu(n)$, qed.

assume that mn is squarefree. Therefore, m is also squarefree (since any square dividing m would also divide mn). Similarly, n is squarefree.

Since m is squarefree, we have $\mu(m) = (-1)^{\omega(m)}$ (by the definition of μ). Since n is squarefree, we have $\mu(n) = (-1)^{\omega(n)}$ (by the definition of μ). Since mn is squarefree, we have $\mu(mn) = (-1)^{\omega(mn)}$ (by the definition of μ).

But $\omega(mn)$ is the number of all distinct primes dividing mn (by the definition of ω). Thus,

$$\begin{aligned}\omega(mn) &= (\text{the number of distinct primes dividing } mn) \\ &= (\text{the number of distinct primes dividing } m \text{ or dividing } n) \qquad (4)\end{aligned}$$

(since the primes dividing mn are precisely the primes dividing m or dividing n).

Moreover, there is no overlap between the primes dividing m and the primes dividing n (since m and n are coprime). Hence,

$$\begin{aligned}&(\text{the number of distinct primes dividing } m \text{ or dividing } n) \\ &= \underbrace{(\text{the number of distinct primes dividing } m)}_{\substack{=\omega(m) \\ (\text{since this is how } \omega(m) \text{ is defined})}} \\ &\qquad + \underbrace{(\text{the number of distinct primes dividing } n)}_{\substack{=\omega(n) \\ (\text{since this is how } \omega(n) \text{ is defined})}} \\ &= \omega(m) + \omega(n).\end{aligned}$$

Thus, (4) becomes

$$\begin{aligned}\omega(mn) &= (\text{the number of distinct primes dividing } m \text{ or dividing } n) \\ &= \omega(m) + \omega(n). \qquad (5)\end{aligned}$$

Now,

$$\begin{aligned}\mu(mn) &= (-1)^{\omega(mn)} = (-1)^{\omega(m)+\omega(n)} \qquad (\text{by (5)}) \\ &= \underbrace{(-1)^{\omega(m)}}_{=\mu(m)} \underbrace{(-1)^{\omega(n)}}_{=\mu(n)} = \mu(m)\mu(n).\end{aligned}$$

This completes the proof of $\mu(mn) = \mu(m)\mu(n)$. Thus, Proposition 2.2.2 **(f)** holds. □

Note that the function $\underline{0} : \mathbb{N}_+ \to \mathbb{C}$ is not multiplicative; in fact, it fails to satisfy $\underline{0}(1) = 1$.

The pointwise product of multiplicative functions is multiplicative, and the same holds for totally multiplicative functions:

Proposition 2.2.3. Let $g : \mathbb{N}_+ \to \mathbb{C}$ and $h : \mathbb{N}_+ \to \mathbb{C}$ be two arithmetic functions. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be the function defined by

$$f(n) = g(n) h(n) \qquad \text{for every } n \in \mathbb{N}_+. \tag{6}$$

(a) If the functions g and h are multiplicative, then the function f is multiplicative.

(b) If the functions g and h are totally multiplicative, then the function f is totally multiplicative.

Proof of Proposition 2.2.3. **(a)** Assume that the functions g and h are multiplicative. We have to prove that the function f is multiplicative.

The function g is multiplicative. In other words, it satisfies $g(1) = 1$, and

$$g(mn) = g(m) g(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+. \tag{7}$$

The function h is multiplicative. In other words, it satisfies $h(1) = 1$, and

$$h(mn) = h(m) h(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+. \tag{8}$$

Now, we want to prove that f is multiplicative. In order to do so, we shall prove the following two assertions:

Assertion 1: We have $f(1) = 1$.

Assertion 2: We have $f(mn) = f(m) f(n)$ for any two coprime $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$.

Proof of Assertion 1: Applying (6) to $n = 1$, we obtain $f(1) = \underbrace{g(1)}_{=1} \underbrace{h(1)}_{=1} = 1$. This proves Assertion 1.

Proof of Assertion 2: Let $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$ be coprime. Then, (6) (applied to m instead of n) yields $f(m) = g(m) h(m)$. Also, (6) shows that $f(n) = g(n) h(n)$. But (6) (applied to mn instead of n) yields

$$\begin{aligned} f(mn) &= \underbrace{g(mn)}_{\substack{=g(m)g(n) \\ \text{(by (7))}}} \underbrace{h(mn)}_{\substack{=h(m)h(n) \\ \text{(by (8))}}} = (g(m) g(n)) (h(m) h(n)) \\ &= \underbrace{(g(m) h(m))}_{=f(m)} \underbrace{(g(n) h(n))}_{=f(n)} = f(m) f(n). \end{aligned}$$

This proves Assertion 2.

Now we know that Assertions 1 and 2 hold. In other words, the function f is multiplicative (by the definition of "multiplicative"). This proves Proposition 2.2.3 **(a)**.

(b) The proof of Proposition 2.2.3 **(b)** is completely analogous to our above proof of Proposition 2.2.3 **(a)**. (More precisely, we have to replace every "multiplicative" by "totally multiplicative" in our proof of Proposition 2.2.3 **(a)**, and remove the word "coprime" everywhere it appears; this results in a proof of Proposition 2.2.3 **(b)**.) ☐

2.3. The Dirichlet convolution

Let us now define a way to produce a new arithmetic function from two given ones: the *Dirichlet convolution*.

Definition 2.3.1. Let $f : \mathbb{N}_+ \to \mathbb{C}$ and $g : \mathbb{N}_+ \to \mathbb{C}$ be two arithmetic functions. We define a new arithmetic function $f \star g : \mathbb{N}_+ \to \mathbb{C}$ by

$$(f \star g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right) \qquad \text{for every } n \in \mathbb{N}_+.$$

This new function $f \star g$ is called the *Dirichlet convolution* of f and g.

Here is a more symmetric way to rewrite the definition of $f \star g$:

Remark 2.3.2. Let $f : \mathbb{N}_+ \to \mathbb{C}$ and $g : \mathbb{N}_+ \to \mathbb{C}$ be two arithmetic functions. Let $n \in \mathbb{N}_+$. Then,

$$(f \star g)(n) = \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} f(d)\, g(e).$$

Proof of Remark 2.3.2. For every $d \in \mathbb{N}_+$, we have

$$\sum_{\substack{e \in \mathbb{N}_+; \\ de = n}} g(e) = \begin{cases} g\left(\frac{n}{d}\right), & \text{if } d \mid n; \\ 0, & \text{if } d \nmid n \end{cases} \qquad (9)$$

[7]. Now,

$$\underbrace{\sum_{\substack{d\in\mathbb{N}_+;\ e\in\mathbb{N}_+;\\ de=n}} f(d)\,g(e)}_{=\sum_{d\in\mathbb{N}_+}\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}}}$$

$$= \sum_{d\in\mathbb{N}_+}\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} f(d)\,g(e) = \sum_{d\in\mathbb{N}_+} f(d) \underbrace{\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e)}_{\substack{=\begin{cases} g\left(\frac{n}{d}\right), & \text{if } d\mid n; \\ 0, & \text{if } d\nmid n \end{cases} \\ \text{(by (9))}}}$$

$$= \sum_{d\in\mathbb{N}_+} f(d) \begin{cases} g\left(\frac{n}{d}\right), & \text{if } d\mid n; \\ 0, & \text{if } d\nmid n \end{cases}$$

$$= \sum_{\substack{d\in\mathbb{N}_+;\\ d\mid n}} f(d) \underbrace{\begin{cases} g\left(\frac{n}{d}\right), & \text{if } d\mid n; \\ 0, & \text{if } d\nmid n \end{cases}}_{\substack{=g\left(\frac{n}{d}\right) \\ \text{(since } d\mid n\text{)}}} + \sum_{\substack{d\in\mathbb{N}_+;\\ d\nmid n}} f(d) \underbrace{\begin{cases} g\left(\frac{n}{d}\right), & \text{if } d\mid n; \\ 0, & \text{if } d\nmid n \end{cases}}_{\substack{=0 \\ \text{(since } d\nmid n\text{)}}}$$

$$= \sum_{\substack{d\in\mathbb{N}_+;\\ d\mid n}} f(d)\,g\left(\frac{n}{d}\right) + \underbrace{\sum_{\substack{d\in\mathbb{N}_+;\\ d\nmid n}} f(d)\,0}_{=0} = \sum_{\substack{d\in\mathbb{N}_+;\\ d\mid n}} f(d)\,g\left(\frac{n}{d}\right) = \sum_{d\mid n} f(d)\,g\left(\frac{n}{d}\right)$$

$$= (f\star g)(n) \qquad \left(\text{because this is how } (f\star g)(n) \text{ was defined}\right).$$

This proves Remark 2.3.2. □

[7]*Proof.* Let $d\in\mathbb{N}_+$. We must prove the identity (9). In other words, we must prove the following two claims:

Claim 1: If $d\mid n$, then $\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e) = g\left(\frac{n}{d}\right)$.

Claim 2: If $d\nmid n$, then $\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e) = 0$.

Proof of Claim 1: Assume that $d\mid n$. Hence, $\frac{n}{d}\in\mathbb{N}_+$ (since $n\in\mathbb{N}_+$). Thus, there is exactly one $e\in\mathbb{N}_+$ satisfying $de=n$, namely $e=\frac{n}{d}$. Hence, the sum $\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e)$ contains exactly one addend, namely the addend for $e=\frac{n}{d}$. Thus, $\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e) = g\left(\frac{n}{d}\right)$. Claim 1 is proven.

Proof of Claim 2: Assume that $d\nmid n$. Hence, there exists no $e\in\mathbb{N}_+$ satisfying $de=n$. Therefore, the sum $\sum_{\substack{e\in\mathbb{N}_+;\\ de=n}} g(e)$ is empty and thus equals 0. This proves Claim 2.

Now, both Claims 1 and 2 are proven, and (9) follows.

Remark 2.3.3. Here is a little digression which might make the Dirichlet convolution $f \star g$ appear less mysterious (but might also confuse you). I claim that Dirichlet convolution of arithmetic functions is "like multiplication of power series, but with (some) additions replaced by multiplications". Here is what I mean by this:

A power series (say, with complex coefficients) is defined as a sequence $(a_0, a_1, a_2, \ldots)$ of complex numbers. This sequence is usually written in the form $\sum\limits_{i \in \mathbb{N}} a_i X^i$. (For us here, "power series" means "formal power series in one indeterminate X with complex coefficients"; we do not care about any questions of convergence.) The product of two power series $\sum\limits_{i \in \mathbb{N}} a_i X^i$ and $\sum\limits_{i \in \mathbb{N}} b_i X^i$ is defined by

$$\left(\sum_{i \in \mathbb{N}} a_i X^i \right) \left(\sum_{i \in \mathbb{N}} b_i X^i \right) = \sum_{i \in \mathbb{N}} c_i X^i,$$

where

$$c_n = \sum_{m=0}^{n} a_m b_{n-m} = \sum_{\substack{d \in \mathbb{N};\ e \in \mathbb{N}; \\ d+e=n}} a_d b_e. \tag{10}$$

To every arithmetic function $f : \mathbb{N}_+ \to \mathbb{C}$, we can assign a power series $\widehat{f}$ with constant term 0, defined by $\widehat{f} = \sum\limits_{i \in \mathbb{N}_+} f(i) X^i$. This assignment is a 1-to-1 correspondence between the arithmetic functions and the power series (in one indeterminate) with constant term 0. In other words, every power series with constant term 0 can be written as $\widehat{f}$ for a unique arithmetic function f. Thus, we can define a "Dirichlet convolution" on the set of all power series with constant term 0, by setting $\widehat{f} \star \widehat{g} = \widehat{f \star g}$ for every two arithmetic functions f and g. Explicitly, this Dirichlet convolution of power series is given by

$$\left(\sum_{i \in \mathbb{N}_+} a_i X^i \right) \star \left(\sum_{i \in \mathbb{N}_+} b_i X^i \right) = \sum_{i \in \mathbb{N}_+} d_i X^i,$$

where

$$d_n = \sum_{d \mid n} a_d b_{n/d} = \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de=n}} a_d b_e. \tag{11}$$

The similarities between the equations (10) and (11) should be palpable. Roughly speaking, (11) is a "multiplicative" variant of (10): Whereas the sum $\sum\limits_{\substack{d \in \mathbb{N};\ e \in \mathbb{N}; \\ d+e=n}} a_d b_e$ in (10) runs over all decompositions of n into a **sum** of two nonnegative integers d and e, the analogous sum $\sum\limits_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de=n}} a_d b_e$ in (11) runs over all decompositions of n into a **product** of two positive integers d and e. (Yes, the multiplicative analogue of nonnegative integers in this context are positive integers.) So, roughly speaking, Dirichlet convolution is like multiplication of power series, except that two monomials X^m and X^n are taken to X^{mn} and not to X^{m+n}.

This analogy has a consequence: It suggests that Dirichlet convolution should be associative and commutative, and that this should be provable in the same way as one proves the associativity and the commutativity of the multiplication of power series. And, indeed, this is the case: see Theorem 2.3.4 below.

Theorem 2.3.4. **(a)** We have $\varepsilon \star f = f \star \varepsilon = f$ for every arithmetic function f.

(b) We have $f \star (g \star h) = (f \star g) \star h$ for every three arithmetic functions f, g and h.

(c) We have $f \star g = g \star f$ for every two arithmetic functions f and g.

Remark 2.3.5. If you know the notion of a monoid, then you will be able to restate Theorem 2.3.4 as follows: The set of all arithmetic functions is a commutative monoid under the operation $\star$ with neutral element ε.

Actually, we can also define an addition operation on arithmetic functions (namely, pointwise addition: $(f+g)(n) = f(n) + g(n)$). The addition operation $+$ and the Dirichlet convolution $\star$ turn the set of arithmetic functions into a commutative ring.

Proof of Theorem 2.3.4. **(c)** Let f and g be two arithmetic functions. Let $n \in \mathbb{N}_+$. Remark 2.3.2 (applied to g and f instead of f and g) yields

$$(g \star f)(n) = \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} g(d) f(e). \qquad (12)$$

Remark 2.3.2 yields

$$(f \star g)(n) = \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} f(d) g(e) = \underbrace{\sum_{\substack{e \in \mathbb{N}_+;\ d \in \mathbb{N}_+; \\ ed = n}}}_{\substack{= \sum\limits_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ ed = n}} \\ = \sum\limits_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}}}} \underbrace{f(e) g(d)}_{= g(d) f(e)}$$

$$\left(\begin{array}{c} \text{here, we have renamed the summation} \\ \text{indices } d \text{ and } e \text{ as } e \text{ and } d \end{array} \right)$$

$$= \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} g(d) f(e).$$

Comparing this with (12), we obtain $(f \star g)(n) = (g \star f)(n)$.

Now, forget that we fixed n. We thus have shown that $(f \star g)(n) = (g \star f)(n)$ for each $n \in \mathbb{N}_+$. In other words, $f \star g = g \star f$. This proves Theorem 2.3.4 **(c)**.

(a) Let f be an arithmetic function. Every $n \in \mathbb{N}_+$ satisfies

$$(\varepsilon \star f)(n) = \sum_{d|n} \underbrace{\varepsilon(d)}_{\substack{= \begin{cases} 1, & \text{if } d = 1; \\ 0, & \text{if } d \neq 1 \end{cases} \\ \text{(by the definition of } \varepsilon\text{)}}} f\left(\frac{n}{d}\right) \qquad \text{(by the definition of } \varepsilon \star f\text{)}$$

$$= \sum_{d|n} \begin{cases} 1, & \text{if } d = 1; \\ 0, & \text{if } d \neq 1 \end{cases} f\left(\frac{n}{d}\right)$$

$$= \underbrace{\begin{cases} 1, & \text{if } 1 = 1; \\ 0, & \text{if } 1 \neq 1 \end{cases}}_{=1} \underbrace{f\left(\frac{n}{1}\right)}_{=f(n)} + \sum_{\substack{d|n; \\ d \neq 1}} \underbrace{\begin{cases} 1, & \text{if } d = 1; \\ 0, & \text{if } d \neq 1 \end{cases}}_{\substack{=0 \\ \text{(since } d \neq 1\text{)}}} f\left(\frac{n}{d}\right)$$

$$\left(\begin{array}{c} \text{here, we have split off the addend for } d = 1 \text{ from the sum} \\ \text{(since 1 is a positive divisor of } n\text{)} \end{array}\right)$$

$$= f(n) + \underbrace{\sum_{\substack{d|n; \\ d \neq 1}} 0 f\left(\frac{n}{d}\right)}_{=0} = f(n).$$

In other words, $\varepsilon \star f = f$. But Theorem 2.3.4 **(c)** (applied to $g = \varepsilon$) yields $f \star \varepsilon = \varepsilon \star f$. Thus, $f \star \varepsilon = \varepsilon \star f = f$. This proves Theorem 2.3.4 **(a)**.

(b) Let us first make a general observation: If F and G are two arithmetic functions, and if $N \in \mathbb{N}_+$, then

$$(F \star G)(N) = \sum_{\substack{D \in \mathbb{N}_+; \ E \in \mathbb{N}_+; \\ DE = N}} F(D) G(E). \tag{13}$$

(This is simply Remark 2.3.2, with the letters f, g, n, d, e renamed as F, G, N, D, E. We are playing this renaming game in order to avoid collisions between notations.)

Now, let f, g and h be three arithmetic functions. Let $n \in \mathbb{N}_+$. We have

$$\begin{aligned}
&((f \star g) \star h)(n) \\
&= \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = n}} (f \star g)(D)\, h(E) \\
&\qquad \left(\text{by (13), applied to } F = f \star g,\ G = h \text{ and } N = n\right) \\
&= \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} \underbrace{(f \star g)(d)}_{\substack{= \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}} f(D) g(E) \\ \text{(by (13), applied to } F = f,\ G = g \text{ and } N = d)}} h(e) \\
&\qquad \left(\text{here, we have renamed the summation indices } D \text{ and } E \text{ as } d \text{ and } e\right) \\
&= \sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} \left(\sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}} f(D)\, g(E) \right) h(e) \\
&= \underbrace{\sum_{\substack{d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ de = n}} \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}}}_{\substack{= \sum_{d \in \mathbb{N}_+} \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}} \sum_{\substack{e \in \mathbb{N}_+; \\ de = n}} \\ \text{(here, we are interchanging the order of summation)}}} f(D)\, g(E)\, h(e) \\
&= \sum_{d \in \mathbb{N}_+} \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}} \underbrace{\sum_{\substack{e \in \mathbb{N}_+; \\ de = n}}}_{\substack{= \sum_{\substack{e \in \mathbb{N}_+; \\ DEe = n}} \\ \text{(since } d = DE)}} f(D)\, g(E)\, h(e) \\
&= \underbrace{\sum_{d \in \mathbb{N}_+} \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+; \\ DE = d}}}_{= \sum_{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+}} \sum_{\substack{e \in \mathbb{N}_+; \\ DEe = n}} f(D)\, g(E)\, h(e) = \underbrace{\sum_{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+} \sum_{\substack{e \in \mathbb{N}_+; \\ DEe = n}}}_{= \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ DEe = n}}} f(D)\, g(E)\, h(e) \\
&= \sum_{\substack{D \in \mathbb{N}_+;\ E \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ DEe = n}} f(D)\, g(E)\, h(e) \\
&= \sum_{\substack{c \in \mathbb{N}_+;\ d \in \mathbb{N}_+;\ e \in \mathbb{N}_+; \\ cde = n}} f(c)\, g(d)\, h(e) \qquad (14) \\
&\qquad \left(\text{here, we have renamed the summation indices } D \text{ and } E \text{ as } c \text{ and } d\right).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&(f\star(g\star h))(n) \\
&= \sum_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=n}} f(D)(g\star h)(E) \\
&\qquad (\text{by (13), applied to } F=f,\ G=g\star h \text{ and } N=n) \\
&= \sum_{\substack{c\in\mathbb{N}_+;\ d\in\mathbb{N}_+;\\ cd=n}} f(c) \underbrace{(g\star h)(d)}_{\substack{=\sum\limits_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}} g(D)h(E) \\ (\text{by (13), applied to } F=g,\ G=h \text{ and } N=d)}} \\
&\qquad (\text{here, we have renamed the summation indices } D \text{ and } E \text{ as } c \text{ and } d) \\
&= \sum_{\substack{c\in\mathbb{N}_+;\ d\in\mathbb{N}_+;\\ cd=n}} f(c) \left(\sum_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}} g(D)h(E)\right) \\
&= \underbrace{\sum_{\substack{c\in\mathbb{N}_+;\ d\in\mathbb{N}_+;\\ cd=n}} \sum_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}}}_{\substack{=\sum\limits_{d\in\mathbb{N}_+} \sum\limits_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}} \sum\limits_{\substack{c\in\mathbb{N}_+;\\ cd=n}} \\ (\text{here, we are interchanging the order of summation})}} f(c)g(D)h(E) \\
&= \sum_{d\in\mathbb{N}_+} \sum_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}} \underbrace{\sum_{\substack{c\in\mathbb{N}_+;\\ cd=n}}}_{\substack{=\sum\limits_{\substack{c\in\mathbb{N}_+;\\ cDE=n}} \\ (\text{since } d=DE)}} f(c)g(D)h(E) \\
&= \underbrace{\sum_{d\in\mathbb{N}_+} \sum_{\substack{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ DE=d}}}_{=\sum\limits_{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+}} \sum_{\substack{c\in\mathbb{N}_+;\\ cDE=n}} f(c)g(D)h(E) = \underbrace{\sum_{D\in\mathbb{N}_+;\ E\in\mathbb{N}_+} \sum_{\substack{c\in\mathbb{N}_+;\\ cDE=n}}}_{=\sum\limits_{\substack{c\in\mathbb{N}_+;\ D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ cDE=n}}} f(c)g(D)h(E) \\
&= \sum_{\substack{c\in\mathbb{N}_+;\ D\in\mathbb{N}_+;\ E\in\mathbb{N}_+;\\ cDE=n}} f(c)g(D)h(E) = \sum_{\substack{c\in\mathbb{N}_+;\ d\in\mathbb{N}_+;\ e\in\mathbb{N}_+;\\ cde=n}} f(c)g(d)h(e) \\
&\qquad (\text{here, we have renamed the summation indices } D \text{ and } E \text{ as } d \text{ and } e).
\end{aligned}$$

Comparing this with (14), we obtain $(f\star(g\star h))(n) = ((f\star g)\star h)(n)$.

Now, forget that we fixed n. We thus have proven that $(f\star(g\star h))(n) = ((f\star g)\star h)(n)$ for every $n\in\mathbb{N}_+$. In other words, $f\star(g\star h) = (f\star g)\star h$. This proves Theorem 2.3.4 **(b)**. □

2.4. Examples of Dirichlet convolutions

Let us see what Dirichlet convolution does to the arithmetic functions we know. We start with some simple observations:

Proposition 2.4.1. We have $\underline{1} \star \underline{1} = \mathrm{d}$. (See Definition 2.1.2 for the definitions of $\underline{1}$ and d.)

Proof of Proposition 2.4.1. For every $n \in \mathbb{N}_+$, we have

$$\begin{aligned}
\left(\underline{1} \star \underline{1}\right)(n) &= \sum_{d \mid n} \underbrace{\underline{1}(d)}_{\substack{=1 \\ \text{(by the definition of } \underline{1})}} \underbrace{\underline{1}\left(\frac{n}{d}\right)}_{\substack{=1 \\ \text{(by the definition of } \underline{1})}} \qquad \left(\text{by the definition of } \underline{1} \star \underline{1}\right) \\
&= \sum_{d \mid n} 1 = \underbrace{(\text{the number of positive divisors of } n)}_{\substack{=\mathrm{d}(n) \\ \text{(since this is how } \mathrm{d}(n) \text{ was defined)}}} \cdot 1 \\
&= \mathrm{d}(n) \cdot 1 = \mathrm{d}(n).
\end{aligned}$$

In other words, $\underline{1} \star \underline{1} = \mathrm{d}$. This proves Proposition 2.4.1. □

Proposition 2.4.2. **(a)** We have $\iota \star \underline{1} = \sigma$.

(b) Let $k \in \mathbb{Z}$. Let $\iota_k : \mathbb{N}_+ \to \mathbb{C}$ be the function sending each $n \in \mathbb{N}_+$ to n^k. Then, $\iota_k \star \underline{1} = \sigma_k$.

We leave the proof of Proposition 2.4.2 to the reader.

Before we go on, let us show an auxiliary fact:

Lemma 2.4.3. Let $n \in \mathbb{N}_+$. Let $\mathcal{D}(n)$ be the set of all positive divisors of n. Then, the map

$$\mathcal{D}(n) \to \mathcal{D}(n), \qquad d \mapsto n/d$$

is well-defined and bijective.

Proof of Lemma 2.4.3. For every $d \in \mathcal{D}(n)$, we have $n/d \in \mathcal{D}(n)$ [8]. Thus, we can define a map $\rho : \mathcal{D}(n) \to \mathcal{D}(n)$ by

$$\rho(d) = n/d \qquad \text{for every } d \in \mathcal{D}(n).$$

Consider this map ρ. This map ρ is the map

$$\mathcal{D}(n) \to \mathcal{D}(n), \qquad d \mapsto n/d \tag{15}$$

[8] *Proof.* Let $d \in \mathcal{D}(n)$. Thus, d is a positive divisor of n (since $\mathcal{D}(n)$ is the set of all positive divisors of n). Hence, d is a positive integer and satisfies $d \mid n$. Now, n/d is an integer (since $d \mid n$) and is positive (since n and d are positive). Hence, n/d is a positive integer. Thus, n/d is a positive divisor of n (since $n/d \mid n$). In other words, $n/d \in \mathcal{D}(n)$ (since $\mathcal{D}(n)$ is the set of all positive divisors of n). Qed.

(because $\rho(d) = n/d$ for every $d \in \mathcal{D}(n)$). Thus, the map (15) is well-defined.

We have

$$(\rho \circ \rho)(d) = \rho\left(\underbrace{\rho(d)}_{=n/d}\right) = \rho(n/d) = n/(n/d) \qquad \text{(by the definition of } \rho\text{)}$$
$$= d = \text{id}(d)$$

for every $d \in \mathcal{D}(n)$. In other words, $\rho \circ \rho = \text{id}$. Hence, the maps ρ and ρ are mutually inverse. In particular, the map ρ is invertible, i.e., bijective. In other words, the map (15) is bijective (since the map ρ is the map (15)). Thus, we have shown that the map (15) is well-defined and bijective. Lemma 2.4.3 is proven. □

Here is a more interesting result:

Proposition 2.4.4. We have $\phi \star \underline{1} = \iota$.

Before we prove this, let us restate it in a more elementary fashion:

Proposition 2.4.5. We have

$$\sum_{d|n} \phi(d) = n \qquad \text{for every } n \in \mathbb{N}_+.$$

Proposition 2.4.5 is [NiZuMo91, Theorem 4.6]. The proof we are going to give for it here is actually the second proof given for it in [NiZuMo91]:

Proof of Proposition 2.4.5. Fix $n \in \mathbb{N}_+$. Let me first show that

$$\sum_{\substack{k \in \{1,2,\ldots,n\};\\ \gcd(k,n)=d}} 1 = \phi\left(\frac{n}{d}\right) \tag{16}$$

for every positive divisor d of n.

Proof of (16): Let d be a positive divisor of n. Define a set K by

$$K = \{k \in \{1,2,\ldots,n\} \mid \gcd(k,n) = d\}.$$

Thus, $\sum_{\substack{k \in \{1,2,\ldots,n\};\\ \gcd(k,n)=d}} 1 = \sum_{k \in K} 1 = |K| \cdot 1 = |K|$.

On the other hand, define a set F by

$$F = \left\{k \in \left\{1,2,\ldots,\frac{n}{d}\right\} \mid k \text{ is coprime to } \frac{n}{d}\right\}.$$

Then, $|F|$ is the number of all $k \in \left\{1, 2, \ldots, \dfrac{n}{d}\right\}$ coprime to $\dfrac{n}{d}$; this number is $\phi\left(\dfrac{n}{d}\right)$ (since this is how $\phi\left(\dfrac{n}{d}\right)$ is defined). In other words, $|F| = \phi\left(\dfrac{n}{d}\right)$.

But every $u \in K$ satisfies $\dfrac{u}{d} \in F$ [9]. Thus, we can define a map

$$\alpha : K \to F, \qquad u \mapsto \frac{u}{d}.$$

On the other hand, every $v \in F$ satisfies $dv \in K$ [10]. Thus, we can define a map

$$\beta : F \to K, \qquad v \mapsto dv.$$

The two maps α and β that we have now defined are mutually inverse (since one of them divides its input by d, whereas the other multiplies it by d). Hence, α is a bijection. Thus, there is a bijection $K \to F$ (namely, α). Hence, $|F| = |K|$. Now, $\phi\left(\dfrac{n}{d}\right) = |F| = |K| = \sum\limits_{\substack{k \in \{1,2,\ldots,n\};\\ \gcd(k,n)=d}} 1$, and therefore (16) is proven.

Now, let $\mathcal{D}(n)$ be the set of all positive divisors of n. Then, the summation sign $\sum\limits_{d \in \mathcal{D}(n)}$ means the same thing as $\sum\limits_{d \mid n}$ (namely, a summation over all positive divisors d of n).

But Lemma 2.4.3 shows that the map

$$\mathcal{D}(n) \to \mathcal{D}(n), \qquad d \mapsto n/d$$

[9] *Proof.* Let $u \in K$. Thus, u is an element of $\{1, 2, \ldots, n\}$ and satisfies $\gcd(u, n) = d$ (by the definition of K). Now, $d = \gcd(u, n) \mid u$, so that $\dfrac{u}{d}$ is an integer. This integer $\dfrac{u}{d}$ must belong to $\left\{1, 2, \ldots, \dfrac{n}{d}\right\}$ (since u belongs to $\{1, 2, \ldots, n\}$). But Proposition 1.2.9 (applied to d, $\dfrac{u}{d}$ and $\dfrac{n}{d}$ instead of g, a and b) yields $d \gcd\left(\dfrac{u}{d}, \dfrac{n}{d}\right) = \gcd\left(\underbrace{d \cdot \dfrac{u}{d}}_{=u}, \underbrace{d \cdot \dfrac{n}{d}}_{=n}\right) = \gcd(u, n) = d$. Cancelling d from this equality, we obtain $\gcd\left(\dfrac{u}{d}, \dfrac{n}{d}\right) = 1$ (since $d \neq 0$). In other words, $\dfrac{u}{d}$ is coprime to $\dfrac{n}{d}$. Thus, we have shown that $\dfrac{u}{d}$ is an element of $\left\{1, 2, \ldots, \dfrac{n}{d}\right\}$ and is coprime to $\dfrac{n}{d}$. In other words, $\dfrac{u}{d} \in F$ (by the definition of F), qed.

[10] *Proof.* Let $v \in F$. Thus, v is an element of $\left\{1, 2, \ldots, \dfrac{n}{d}\right\}$ and is coprime to $\dfrac{n}{d}$ (by the definition of F). Now, $\gcd\left(v, \dfrac{n}{d}\right) = 1$ (since v is coprime to $\dfrac{n}{d}$). But Proposition 1.2.9 (applied to d, v and $\dfrac{n}{d}$ instead of g, a and b) shows that $d \gcd\left(v, \dfrac{n}{d}\right) = \gcd\left(dv, \underbrace{d \cdot \dfrac{n}{d}}_{=n}\right) = \gcd(dv, n)$, so that $\gcd(dv, n) = d \underbrace{\gcd\left(v, \dfrac{n}{d}\right)}_{=1} = d$. Also, from $v \in \left\{1, 2, \ldots, \dfrac{n}{d}\right\}$, we obtain $dv \in \{1, 2, \ldots, n\}$. Hence, we have shown that dv is an element of $\{1, 2, \ldots, n\}$ and satisfies $\gcd(dv, n) = d$. In other words, $dv \in K$ (by the definition of K), qed.

is well-defined and bijective. Thus, this map is a bijection. Hence, we can substitute $\frac{n}{d}$ for d in the sum $\sum_{d\in\mathcal{D}(n)} \phi(d)$. We thus obtain

$$\sum_{d\in\mathcal{D}(n)} \phi(d) = \underbrace{\sum_{d\in\mathcal{D}(n)}}_{=\sum_{d|n}} \underbrace{\phi\left(\frac{n}{d}\right)}_{\substack{=\sum_{k\in\{1,2,\ldots,n\};\ \gcd(k,n)=d} 1 \\ \text{(by (16))}}} = \underbrace{\sum_{d|n} \sum_{\substack{k\in\{1,2,\ldots,n\};\\ \gcd(k,n)=d}}}_{\substack{=\sum_{k\in\{1,2,\ldots,n\}} \\ \text{(because for every } k\in\{1,2,\ldots,n\}\text{,} \\ \text{the number } \gcd(k,n) \text{ is a positive divisor of } n\text{)}}} 1$$

$$= \sum_{k\in\{1,2,\ldots,n\}} 1 = n.$$

Therefore, $n = \underbrace{\sum_{d\in\mathcal{D}(n)}}_{=\sum_{d|n}} \phi(d) = \sum_{d|n} \phi(d)$. This proves Proposition 2.4.5. □

Proof of Proposition 2.4.4. For every $n \in \mathbb{N}_+$, we have

$$\begin{aligned}(\phi \star \underline{1})(n) &= \sum_{d|n} \phi(d) \underbrace{\underline{1}\left(\frac{n}{d}\right)}_{\substack{=1 \\ \text{(by the definition of } \underline{1}\text{)}}} && \text{(by the definition of } \phi \star \underline{1}\text{)} \\ &= \sum_{d|n} \phi(d) = n && \text{(by Proposition 2.4.5)} \\ &= \iota(n) && \text{(since } \iota(n) \text{ is defined to be } n\text{)}.\end{aligned}$$

In other words, $\phi \star \underline{1} = \iota$. This proves Proposition 2.4.4. □

Here is another important fact about Dirichlet convolution:

Proposition 2.4.6. We have $\mu \star \underline{1} = \varepsilon$.

Again, we shall first restate it in concrete language before proving it:

Proposition 2.4.7. We have

$$\sum_{d|n} \mu(d) = \varepsilon(n) \qquad \text{for every } n \in \mathbb{N}_+.$$

Proposition 2.4.7 is [NiZuMo91, Theorem 4.7], and the book gives two proofs for it. Let us sketch a third:[11]

[11] See [Grinbe15, proof of Theorem 2.6] for a detailed version of this proof.

Proof of Proposition 2.4.7. Fix $n \in \mathbb{N}_+$. We must prove the identity

$$\sum_{d|n} \mu(d) = \varepsilon(n). \tag{17}$$

First of all, we recall that $\mu(1) = 1$. (This has already been proven in our proof of Proposition 2.2.2 **(f)**.) Hence, $\sum_{d|1} \mu(d) = \mu(1) = 1 = \varepsilon(1)$ (because $\varepsilon(1)$ is defined to be 1). In other words, (17) is proven for the case when $n = 1$. Thus, we WLOG assume that $n \neq 1$ from now on. Hence, $\varepsilon(n) = 0$ (by the definition of ε). Also, n has at least one prime divisor (since $n \neq 1$). Pick any prime divisor q of n.

Let D be the set of all squarefree positive divisors d of n satisfying $q \nmid d$.

Let E be the set of all squarefree positive divisors d of n satisfying $q \mid d$.

The map

$$D \to E, \qquad d \mapsto qd$$

is well-defined and a bijection[12]. Moreover, every $d \in D$ satisfies

$$\mu(qd) = -\mu(d) \tag{18}$$

[13].

[12]Check this! (Or see [Grinbe15, proof of Theorem 2.6] for the proof.)

[13]*Proof of (18):* Let $d \in D$. Thus, d is a squarefree positive divisor d of n satisfying $q \nmid d$ (by the definition of D). From $q \nmid d$, we conclude that q is coprime to d (since q is prime). Hence, $\mu(qd) = \mu(q)\mu(d)$ (since the function μ is multiplicative).

But q is a prime; thus, q is squarefree. Hence, the definition of μ yields $\mu(q) = (-1)^{\omega(q)} = (-1)^1$ (since $\omega(q) = 1$ (again since q is a prime)). Thus, $\mu(qd) = \underbrace{\mu(q)}_{=(-1)^1=-1} \mu(d) = -\mu(d)$, qed.

Now,

$$\begin{aligned}
\sum_{d\mid n}\mu(d) &= \sum_{\substack{d\mid n;\\ d\text{ is squarefree}}}\mu(d) + \sum_{\substack{d\mid n;\\ d\text{ is not squarefree}}}\underbrace{\mu(d)}_{\substack{=0\\ \text{(by the definition of }\mu\text{,}\\ \text{since }d\text{ is not squarefree)}}}\\
&= \sum_{\substack{d\mid n;\\ d\text{ is squarefree}}}\mu(d) + \underbrace{\sum_{\substack{d\mid n;\\ d\text{ is not squarefree}}}0}_{=0} = \sum_{\substack{d\mid n;\\ d\text{ is squarefree}}}\mu(d)\\
&= \underbrace{\sum_{\substack{d\mid n;\\ d\text{ is squarefree;}\\ q\mid d}}}_{\substack{=\sum_{d\in E}\\ \text{(by the definition of }E)}}\mu(d) + \underbrace{\sum_{\substack{d\mid n;\\ d\text{ is squarefree;}\\ q\nmid d}}}_{\substack{=\sum_{d\in D}\\ \text{(by the definition of }D)}}\mu(d)\\
&= \sum_{d\in E}\mu(d) + \sum_{d\in D}\mu(d) = \sum_{d\in D}\underbrace{\mu(qd)}_{\substack{=-\mu(d)\\ \text{(by (18))}}} + \sum_{d\in D}\mu(d)\\
&\qquad \left(\begin{array}{c}\text{here, we have substituted }qd\text{ for }d\text{ in the first sum, since}\\ \text{the map }D\to E,\ d\mapsto qd\text{ is a bijection}\end{array}\right)\\
&= \sum_{d\in D}(-\mu(d)) + \sum_{d\in D}\mu(d) = -\sum_{d\in D}\mu(d) + \sum_{d\in D}\mu(d) = 0\\
&= \varepsilon(n) \qquad (\text{since }\varepsilon(n)=0).
\end{aligned}$$

This proves (17). Thus, Proposition 2.4.7 is proven. □

Our proof of Proposition 2.4.7 used a standard technique: In order to prove that a sum is 0, we split the sum into two smaller sums, which cancelled each other out term by term (i.e., every term of one cancelled a term of the other). This kind of proof is widespread in combinatorics and other disciplines.

Proof of Proposition 2.4.6. For every $n \in \mathbb{N}_+$, we have

$$\begin{aligned}
(\mu\star\underline{1})(n) &= \sum_{d\mid n}\mu(d)\underbrace{\underline{1}\left(\frac{n}{d}\right)}_{\substack{=1\\ \text{(by the definition of }\underline{1})}} && (\text{by the definition of }\mu\star\underline{1})\\
&= \sum_{d\mid n}\mu(d) = \varepsilon(n) && (\text{by Proposition 2.4.7}).
\end{aligned}$$

In other words, $\mu\star\underline{1}=\varepsilon$. This proves Proposition 2.4.6. □

The Dirichlet convolutions we have so far computed allow us to compute other Dirichlet convolutions without actually working with sums, but simply by applying Theorem 2.3.4. Here is one result we can obtain in this way:

Proposition 2.4.8. We have $\mu \star \iota = \phi$.

In concrete language, this says the following:

Proposition 2.4.9. We have

$$\sum_{d|n} \mu(d) \frac{n}{d} = \phi(n) \qquad \text{for every } n \in \mathbb{N}_+.$$

Instead of proving the concrete version combinatorially and then deriving the Dirichlet convolution from it, we will go the opposite way this time:

Proof of Proposition 2.4.8. Proposition 2.4.4 yields $\iota = \phi \star \underline{1} = \underline{1} \star \phi$ (by Theorem 2.3.4 **(c)**, applied to $f = \phi$ and $g = \underline{1}$). Now,

$$\begin{aligned} \mu \star \underbrace{\iota}_{=\underline{1}\star\phi} = \mu \star (\underline{1} \star \phi) &= \underbrace{(\mu \star \underline{1})}_{\substack{=\varepsilon \\ \text{(by Proposition 2.4.6)}}} \star \phi \\ &\qquad \text{(by Theorem 2.3.4 (b), applied to } f = \mu,\ g = \underline{1} \text{ and } h = \phi) \\ &= \varepsilon \star \phi = \phi \qquad \text{(by Theorem 2.3.4 (a), applied to } f = \phi). \end{aligned}$$

Thus, Proposition 2.4.8 is proven. ☐

Proof of Proposition 2.4.9. Proposition 2.4.8 yields $\phi = \mu \star \iota$. Thus, every $n \in \mathbb{N}_+$ satisfies

$$\begin{aligned} \underbrace{\phi}_{=\mu\star\iota}(n) = (\mu \star \iota)(n) &= \sum_{d|n} \mu(d) \underbrace{\iota\left(\frac{n}{d}\right)}_{\substack{=\frac{n}{d} \\ \text{(by the definition of } \iota)}} \qquad \text{(by the definition of } \mu \star \iota) \\ &= \sum_{d|n} \mu(d) \frac{n}{d}. \end{aligned}$$

This proves Proposition 2.4.9. ☐

Proposition 2.4.9 is [NiZuMo91, (4.1)].

2.5. Möbius inversion

A particularly useful consequence of the "calculus of Dirichlet convolution" we have established is the so-called *Möbius inversion formula*:

Theorem 2.5.1 (Möbius inversion formula)**.** Let $f : \mathbb{N}_+ \to \mathbb{C}$ and $F : \mathbb{N}_+ \to \mathbb{C}$ be two arithmetic functions. Then, we have the following logical equivalence:

$$\left(F(n) = \sum_{d \mid n} f(d) \text{ for all } n \in \mathbb{N}_+\right)$$
$$\Longleftrightarrow \left(f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) \text{ for all } n \in \mathbb{N}_+\right).$$

Theorem 2.5.1 is [NiZuMo91, Theorems 4.8 and 4.9]. It is merely the most well-known of the many "Möbius inversion formulas" that appear in various parts of mathematics; see [BenGol75] or [Rota64] or [Stanle11, §3.7] for introductions into the more general theory of Möbius functions (of partially ordered sets).

We shall prove Theorem 2.5.1 by rewriting it in the following equivalent form:

Proposition 2.5.2. Let $f : \mathbb{N}_+ \to \mathbb{C}$ and $F : \mathbb{N}_+ \to \mathbb{C}$ be two arithmetic functions. Then, we have the following logical equivalence:

$$(F = f \star \underline{1}) \Longleftrightarrow (f = \mu \star F).$$

Proof of Proposition 2.5.2. We have $f \star \underline{1} = \underline{1} \star f$ (by Theorem 2.3.4 **(c)**, applied to $g = \underline{1}$). Also, $\mu \star \underline{1} = \underline{1} \star \mu$ (by Theorem 2.3.4 **(c)**, applied to μ and $\underline{1}$ instead of f and g). But $\mu \star \underline{1} = \varepsilon$ (by Proposition 2.4.6). Hence, $\underline{1} \star \mu = \mu \star \underline{1} = \varepsilon$.

We must prove the equivalence $(F = f \star \underline{1}) \Longleftrightarrow (f = \mu \star F)$. In other words, we must prove the two implications $(F = f \star \underline{1}) \Longrightarrow (f = \mu \star F)$ and $(F = f \star \underline{1}) \Longleftarrow (f = \mu \star F)$.

Proof of the implication $(F = f \star \underline{1}) \Longrightarrow (f = \mu \star F)$: Assume that $F = f \star \underline{1}$. Then, $F = f \star \underline{1} = \underline{1} \star f$. Hence,

$$\begin{aligned}
\mu \star \underbrace{F}_{= \underline{1} \star f} &= \mu \star (\underline{1} \star f) = \underbrace{(\mu \star \underline{1})}_{= \varepsilon} \star f \\
&\qquad \left(\begin{array}{c}\text{by Theorem 2.3.4 \textbf{(b)}, applied to } \mu, \underline{1} \text{ and } f \\ \text{instead of } f, g \text{ and } h\end{array}\right) \\
&= \varepsilon \star f = f \qquad \text{(by Theorem 2.3.4 \textbf{(a)})}.
\end{aligned}$$

Thus, $f = \mu \star F$. This proves the implication $(F = f \star \underline{1}) \Longrightarrow (f = \mu \star F)$.

Proof of the implication $(F = f \star \underline{1}) \Longleftarrow (f = \mu \star F)$: Assume that $f = \mu \star F$.

Hence,

$$f \star \underline{1} = \underline{1} \star \underbrace{f}_{=\mu \star F} = \underline{1} \star (\mu \star F) = \underbrace{(\underline{1} \star \mu)}_{=\varepsilon} \star F$$

$$\left(\begin{array}{c} \text{by Theorem 2.3.4 } \textbf{(b)}\text{, applied to } \underline{1}, \mu \text{ and } F \\ \text{instead of } f, g \text{ and } h \end{array} \right)$$

$$= \varepsilon \star F = F \qquad \left(\text{by Theorem 2.3.4 } \textbf{(a)}\text{, applied to } F \text{ instead of } f\right).$$

Thus, $F = f \star \underline{1}$. This proves the implication $(F = f \star \underline{1}) \Longleftarrow (f = \mu \star F)$.

Now, both implications are proven; hence, the proof of Proposition 2.5.2 is complete. □

Proof of Theorem 2.5.1. We have the following chain of equivalences:

$$\begin{aligned} & (F = f \star \underline{1}) \\ \Longleftrightarrow\ & (F(n) = (f \star \underline{1})(n) \text{ for all } n \in \mathbb{N}_+) \\ \Longleftrightarrow\ & \left(F(n) = \sum_{d \mid n} f(d) \text{ for all } n \in \mathbb{N}_+ \right) \end{aligned}$$

(since every $n \in \mathbb{N}_+$ satisfies

$$\begin{aligned} (f \star \underline{1})(n) &= \sum_{d \mid n} f(d) \underbrace{\underline{1}\left(\frac{n}{d}\right)}_{\substack{=1 \\ \text{(by the definition of } \underline{1})}} \qquad (\text{by the definition of } f \star \underline{1}) \\ &= \sum_{d \mid n} f(d) \end{aligned}$$

). Hence, we have the following chain of equivalences:

$$\begin{aligned} & \left(F(n) = \sum_{d \mid n} f(d) \text{ for all } n \in \mathbb{N}_+ \right) \\ \Longleftrightarrow\ & (F = f \star \underline{1}) \\ \Longleftrightarrow\ & (f = \mu \star F) \qquad (\text{by Proposition 2.5.2}) \\ \Longleftrightarrow\ & (f(n) = (\mu \star F)(n) \text{ for all } n \in \mathbb{N}_+) \\ \Longleftrightarrow\ & \left(f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) \text{ for all } n \in \mathbb{N}_+ \right) \end{aligned}$$

(since every $n \in \mathbb{N}_+$ satisfies

$$(\mu \star F)(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) \qquad (\text{by the definition of } \mu \star F)$$

). This proves Theorem 2.5.1. □

2.6. Dirichlet convolution and multiplicativity

We will now connect the concept of multiplicative functions with the Dirichlet convolution:

Theorem 2.6.1. Let f and g be two multiplicative arithmetic functions. Then, the arithmetic function $f \star g$ is also multiplicative.

Theorem 2.6.1 is a generalization of [NiZuMo91, Theorem 4.4], and the following proof follows the same ideas as the proof of [NiZuMo91, Theorem 4.4].

Proof of Theorem 2.6.1. The function f is multiplicative. In other words, it satisfies $f(1) = 1$, and

$$f(mn) = f(m) f(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+. \tag{19}$$

The function g is multiplicative. In other words, it satisfies $g(1) = 1$, and

$$g(mn) = g(m) g(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+. \tag{20}$$

The definition of $f \star g$ yields

$$(f \star g)(1) = \sum_{d \mid 1} f(d) g\left(\frac{1}{d}\right) = \underbrace{f(1)}_{=1} \underbrace{g\left(\frac{1}{1}\right)}_{=g(1)=1} = 1.$$

Now, we want to prove that $f \star g$ is multiplicative. In order to do so, we need to verify that $(f \star g)(1) = 1$ and that

$$(f \star g)(mn) = (f \star g)(m) \cdot (f \star g)(n) \tag{21}$$

for any two coprime $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$. Since $(f \star g)(1) = 1$ is already proven, it thus only remains to prove (21).

So let $m \in \mathbb{N}_+$ and $n \in \mathbb{N}_+$ be coprime. We need to prove (21).

For any $N \in \mathbb{N}_+$, let $\mathcal{D}(N)$ be the set of all positive divisors of N.

Consider the map

$$\mathbf{f} : \mathcal{D}(m) \times \mathcal{D}(n) \to \mathcal{D}(mn), \qquad (d, e) \mapsto de.$$

This map $\mathbf{f}$ is well-defined (because if d and e are positive divisors of m and n, respectively, then de is a positive divisor of mn).

Consider the map

$$\mathbf{g} : \mathcal{D}(mn) \to \mathcal{D}(m) \times \mathcal{D}(n), \qquad u \mapsto (\gcd(u, m), \gcd(u, n)).$$

This map $\mathbf{g}$ is well-defined (because if u is a positive divisor of mn, then $\gcd(u, m)$ and $\gcd(u, n)$ are positive divisors of m and n, respectively).

We have $\mathbf{f} \circ \mathbf{g} = \text{id}$ [14] and $\mathbf{g} \circ \mathbf{f} = \text{id}$ [15]. Hence, the maps $\mathbf{f}$ and $\mathbf{g}$ are mutually inverse. In particular, this shows that the map $\mathbf{f}$ is a bijection. In other words, the map $\mathcal{D}(m) \times \mathcal{D}(n) \to \mathcal{D}(mn)$, $(d,e) \mapsto de$ is a bijection (since this map is precisely $\mathbf{f}$).

We make two more simple observations:

1. We have

$$f(de) = f(d) f(e) \qquad \text{for any } d \in \mathcal{D}(m) \text{ and } e \in \mathcal{D}(n). \tag{22}$$

[14] *Proof.* Let $u \in \mathcal{D}(mn)$. Thus, u is a positive divisor of mn. Therefore, $\gcd(u, mn) = u$.

The definition of $\mathbf{g}$ shows that $\mathbf{g}(u) = (\gcd(u,m), \gcd(u,n))$. Now,

$$\begin{aligned}(\mathbf{f} \circ \mathbf{g})(u) &= \mathbf{f}\left(\underbrace{\mathbf{g}(u)}_{=(\gcd(u,m),\gcd(u,n))}\right) = \mathbf{f}(\gcd(u,m), \gcd(u,n)) \\ &= \gcd(u,m) \cdot \gcd(u,n) \qquad (\text{by the definition of } \mathbf{f}) \\ &= \gcd(u, mn) \qquad (\text{by Proposition 1.2.10}) \\ &= u.\end{aligned}$$

Now, forget that we fixed u. We thus have proven that $(\mathbf{f} \circ \mathbf{g})(u) = u$ for every $u \in \mathcal{D}(mn)$. In other words, $\mathbf{f} \circ \mathbf{g} = \text{id}$.

[15] *Proof.* Let $(d,e) \in \mathcal{D}(m) \times \mathcal{D}(n)$. Then, $\mathbf{f}(d,e) = de$ (by the definition of $\mathbf{f}$), and

$$(\mathbf{g} \circ \mathbf{f})(d,e) = \mathbf{g}\left(\underbrace{\mathbf{f}(d,e)}_{=de}\right) = \mathbf{g}(de) = (\gcd(de,m), \gcd(de,n))$$

(by the definition of $\mathbf{g}$).

We have $(d,e) \in \mathcal{D}(m) \times \mathcal{D}(n)$. In other words, $d \in \mathcal{D}(m)$ and $e \in \mathcal{D}(n)$. In other words, d is a positive divisor of m, and e is a positive divisor of n. Thus, $d \mid m$ and $e \mid n$.

Let $d' = \gcd(de, m)$. Then, $d' = \gcd(de, m) \mid m$ and $e \mid n$. Hence, Corollary 1.2.4 (applied to d', e, m and n instead of a, b, c and d) yields $\gcd(d', e) \mid \gcd(m, n) = 1$ (since m and n are coprime). Hence, $\gcd(d', e) = 1$.

Note also that $d' = \gcd(de, m) \mid de = ed$.

Proposition 1.2.8 (applied to $x = d'$, $y = e$ and $z = d$) yields $d' \mid d$ (since $d' \mid ed$ and $\gcd(d', e) = 1$).

On the other hand, $d \mid de$ and $d \mid m$. Thus, Proposition 1.2.3 (applied to d, de and m instead of a, b and c) yields $d \mid \gcd(de, m)$. In other words, $d \mid d'$ (since $d' = \gcd(de, m)$). Combining this with $d' \mid d$, we obtain $d = d'$ (since d and d' are positive integers). Thus, $d = d' = \gcd(de, m)$. In other words, $\gcd(de, m) = d$. The same argument (with the roles of m and n interchanged, and correspondingly also the roles of d and e interchanged) shows that $\gcd(ed, n) = e$. Now,

$$(\mathbf{g} \circ \mathbf{f})(d,e) = \left(\underbrace{\gcd(de,m)}_{=d}, \underbrace{\gcd(de,n)}_{=\gcd(ed,n)=e}\right) = (d,e).$$

Now, forget that we fixed (d,e). We thus have shown that $(\mathbf{g} \circ \mathbf{f})(d,e) = (d,e)$ for each $(d,e) \in \mathcal{D}(m) \times \mathcal{D}(n)$. In other words, $\mathbf{g} \circ \mathbf{f} = \text{id}$.

[16]

2. We have
$$g\left(\frac{mn}{de}\right) = g\left(\frac{m}{d}\right) g\left(\frac{n}{e}\right) \qquad \text{for any } d \in \mathcal{D}(m) \text{ and } e \in \mathcal{D}(n). \qquad (23)$$

[17]

[16] *Proof of (22):* Let $d \in \mathcal{D}(m)$ and $e \in \mathcal{D}(n)$. In other words, d is a positive divisor of m, and e is a positive divisor of n. Hence, $d \mid m$ and $e \mid n$. Therefore, Corollary 1.2.4 (applied to d, e, m and n instead of a, b, c and d) yields $\gcd(d,e) \mid \gcd(m,n) = 1$ (since m and n are coprime). Hence, $\gcd(d,e) = 1$. In other words, d and e are coprime. Hence, (19) (applied to d and e instead of m and n) yields $f(de) = f(d) f(e)$, qed.

[17] *Proof of (23):* Let $d \in \mathcal{D}(m)$ and $e \in \mathcal{D}(n)$. In other words, d is a positive divisor of m, and e is a positive divisor of n. Hence, $d \mid m$ and $e \mid n$. This shows that $\frac{m}{d}$ and $\frac{n}{e}$ are integers; actually, $\frac{m}{d}$ and $\frac{n}{e}$ are positive integers (since m and n are positive).

Moreover, $\frac{m}{d} \mid m$ and $\frac{n}{e} \mid n$. Hence, Corollary 1.2.4 (applied to $\frac{m}{d}$, $\frac{n}{e}$, m and n instead of a, b, c and d) yields $\gcd\left(\frac{m}{d}, \frac{n}{e}\right) \mid \gcd(m,n) = 1$ (since m and n are coprime). Hence, $\gcd\left(\frac{m}{d}, \frac{n}{e}\right) = 1$. In other words, $\frac{m}{d}$ and $\frac{n}{e}$ are coprime. Hence, (20) (applied to $\frac{m}{d}$ and $\frac{n}{e}$ instead of m and n) yields $g\left(\frac{m}{d} \cdot \frac{n}{e}\right) = g\left(\frac{m}{d}\right) g\left(\frac{n}{e}\right)$. Hence, $g\left(\underbrace{\frac{mn}{de}}_{=\frac{m}{d}\cdot\frac{n}{e}}\right) = g\left(\frac{m}{d} \cdot \frac{n}{e}\right) = g\left(\frac{m}{d}\right) g\left(\frac{n}{e}\right)$, qed.

Now, the definition of $f \star g$ yields

$$\begin{aligned}
&(f \star g)(mn) \\
&= \sum_{d \mid mn} f(d)\, g\left(\frac{mn}{d}\right) = \underbrace{\sum_{u \mid mn}}_{= \sum_{u \in \mathcal{D}(mn)}} f(u)\, g\left(\frac{mn}{u}\right) \qquad \left(\begin{array}{c}\text{here, we have renamed the}\\ \text{summation index } d \text{ as } u\end{array}\right) \\
&= \sum_{u \in \mathcal{D}(mn)} f(u)\, g\left(\frac{mn}{u}\right) = \underbrace{\sum_{(d,e) \in \mathcal{D}(m) \times \mathcal{D}(n)}}_{= \sum_{d \in \mathcal{D}(m)} \sum_{e \in \mathcal{D}(n)}} f(de)\, g\left(\frac{mn}{de}\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } de \text{ for } u \text{ in the sum, since the}\\ \text{map } \mathcal{D}(m) \times \mathcal{D}(n) \to \mathcal{D}(mn),\ (d,e) \mapsto de \text{ is a bijection}\end{array}\right) \\
&= \underbrace{\sum_{d \in \mathcal{D}(m)}}_{= \sum_{d \mid m}} \underbrace{\sum_{e \in \mathcal{D}(n)}}_{= \sum_{e \mid n}} \underbrace{f(de)}_{\substack{= f(d) f(e) \\ \text{(by (22))}}} \underbrace{g\left(\frac{mn}{de}\right)}_{\substack{= g\left(\frac{m}{d}\right) g\left(\frac{n}{e}\right) \\ \text{(by (23))}}} \\
&= \sum_{d \mid m} \sum_{e \mid n} f(d)\, f(e)\, g\left(\frac{m}{d}\right) g\left(\frac{n}{e}\right) = \left(\sum_{d \mid m} f(d)\, g\left(\frac{m}{d}\right)\right) \left(\sum_{e \mid n} f(e)\, g\left(\frac{n}{e}\right)\right) \\
&= \left(\sum_{d \mid m} f(d)\, g\left(\frac{m}{d}\right)\right) \left(\sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)\right)
\end{aligned}$$

(here, we renamed the summation index e as d in the second sum). Comparing this with

$$\begin{aligned}
&\underbrace{(f \star g)(m)}_{\substack{= \sum_{d \mid m} f(d) g\left(\frac{m}{d}\right) \\ \text{(by the definition of } f \star g\text{)}}} \cdot \underbrace{(f \star g)(n)}_{\substack{= \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) \\ \text{(by the definition of } f \star g\text{)}}} \\
&= \left(\sum_{d \mid m} f(d)\, g\left(\frac{m}{d}\right)\right) \left(\sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)\right),
\end{aligned}$$

we obtain $(f \star g)(mn) = (f \star g)(m) \cdot (f \star g)(n)$. Thus, (21) is proven. As we have said, this completes the proof of Theorem 2.6.1. □

Notice that Theorem 2.6.1 has no analogue for totally multiplicative functions: The Dirichlet convolution $f \star g$ of two totally multiplicative functions might not be totally multiplicative.

We can use Theorem 2.6.1 to prove (and sometimes reprove) parts of Proposition 2.2.2:

Proof of Proposition 2.2.2 ***(b)***. The arithmetic function $\underline{1}$ is clearly multiplicative (and totally multiplicative). Thus, Theorem 2.6.1 (applied to $f = \underline{1}$ and $g = \underline{1}$) shows that $\underline{1} \star \underline{1}$ is multiplicative. But since $\underline{1} \star \underline{1} = \mathrm{d}$ (by Proposition 2.4.1), this shows that d is multiplicative. This proves Proposition 2.2.2 **(b)**. □

Proof of Proposition 2.2.2 ***(e)***. Let $k \in \mathbb{Z}$. Define the arithmetic function ι_k as in Proposition 2.4.2 **(b)**. This ι_k is clearly multiplicative (and totally multiplicative). We also know that the arithmetic function $\underline{1}$ is clearly multiplicative. Thus, Theorem 2.6.1 (applied to $f = \iota_k$ and $g = \underline{1}$) shows that $\iota_k \star \underline{1}$ is multiplicative. But since $\iota_k \star \underline{1} = \sigma_k$ (by Proposition 2.4.2 **(b)**), this shows that σ_k is multiplicative. Applying this to $k = 1$, we conclude that σ is multiplicative (since $\sigma_1 = \sigma$). This completes the proof of Proposition 2.2.2 **(e)**. □

Second proof of Proposition 2.2.2 ***(a)***. The arithmetic function μ is multiplicative (by Proposition 2.2.2 **(f)**). The arithmetic function ι is clearly multiplicative (and totally multiplicative). Hence, Theorem 2.6.1 (applied to $f = \mu$ and $g = \iota$) shows that $\mu \star \iota$ is multiplicative. But since $\mu \star \iota = \phi$ (by Proposition 2.4.8), this shows that ϕ is multiplicative. This proves Proposition 2.2.2 **(a)** again. □

As an easy consequence of Theorem 2.6.1, we can obtain [NiZuMo91, Theorem 4.4]:

Corollary 2.6.2. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be a multiplicative arithmetic function. Define an arithmetic function $F : \mathbb{N}_+ \to \mathbb{C}$ by

$$F(n) = \sum_{d \mid n} f(d) \qquad \text{for every positive integer } n. \tag{24}$$

Then, the function F is multiplicative.

Proof of Corollary 2.6.2. The arithmetic function $\underline{1}$ is clearly multiplicative (and totally multiplicative). Thus, Theorem 2.6.1 (applied to $g = \underline{1}$) shows that $f \star \underline{1}$ is multiplicative. But every positive integer n satisfies

$$\begin{aligned}(f \star \underline{1})(n) &= \sum_{d \mid n} f(d) \underbrace{\underline{1}\left(\frac{n}{d}\right)}_{\substack{=1 \\ \text{(by the definition of } \underline{1})}} \qquad \text{(by the definition of } f \star \underline{1}) \\ &= \sum_{d \mid n} f(d) = F(n) \qquad \text{(by (24))}.\end{aligned}$$

Hence, $f \star \underline{1} = F$. But recall that $f \star \underline{1}$ is multiplicative. In other words, F is multiplicative (since $f \star \underline{1} = F$). This proves Corollary 2.6.2. □

2.7. Explicit formulas from multiplicativity

One of the nice things about multiplicative arithmetic functions is that, in order to compute their values, it suffices to compute their values on prime powers:

Proposition 2.7.1. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be a multiplicative function. Let $n \in \mathbb{N}_+$. Then,

$$f(n) = \prod_{p \in \operatorname{PF} n} f\left(p^{v_p(n)}\right).$$

(See Definition 2.1.5 for the definition of $\operatorname{PF} n$.)

Applying this proposition to $f = \phi$, $f = \mathrm{d}$ and $f = \sigma_k$, we easily obtain Theorem 2.1.6, Theorem 2.1.7 and Theorem 2.1.8, respectively (once we compute the values $f\left(p^{v_p(n)}\right)$, but this is easy in all three cases).

Proposition 2.7.1 follows from the following fact:

Proposition 2.7.2. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be a multiplicative function. Let $a_1, a_2, \ldots, a_k$ be finitely many pairwise coprime positive integers. Then,

$$f(a_1 a_2 \cdots a_k) = f(a_1) f(a_2) \cdots f(a_k).$$

Both the proof of Proposition 2.7.2 (by induction over k) and the proof of Proposition 2.7.1 (using Proposition 2.7.2) are rather straightforward:

Proof of Proposition 2.7.2. The function f is multiplicative. In other words, it satisfies $f(1) = 1$ and

$$f(mn) = f(m) f(n) \qquad \text{for any two coprime } m \in \mathbb{N}_+ \text{ and } n \in \mathbb{N}_+ \tag{25}$$

(by the definition of "multiplicative").

The integers $a_1, a_2, \ldots, a_k$ are pairwise coprime. In other words,

$$a_u \text{ is coprime to } a_v \tag{26}$$

for any integers u and v satisfying $1 \leq u < v \leq k$.

We shall show that

$$f(a_1 a_2 \cdots a_i) = f(a_1) f(a_2) \cdots f(a_i) \tag{27}$$

for every $i \in \{0, 1, \ldots, k\}$.

Proof of (27): We shall prove (27) by induction over i:

Induction base: We have $a_1 a_2 \cdots a_0 = (\text{empty product}) = 1$. Applying the map f to both sides of this equation, we obtain

$$f(a_1 a_2 \cdots a_0) = f(1) = 1.$$

Comparing this with $f(a_1) f(a_2) \cdots f(a_0) = \text{(empty product)} = 1$, we obtain $f(a_1 a_2 \cdots a_0) = f(a_1) f(a_2) \cdots f(a_0)$. In other words, (27) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \{0, 1, \ldots, k\}$ be positive. Assume that (27) holds for $i = j - 1$. We must prove that (27) holds for $i = j$.

We have assumed that (27) holds for $i = j - 1$. In other words, we have

$$f\left(a_1 a_2 \cdots a_{j-1}\right) = f(a_1) f(a_2) \cdots f\left(a_{j-1}\right).$$

But a_u is coprime to a_j for every $u \in \{1, 2, \ldots, j-1\}$ [18]. Hence, Corollary 1.2.7 (applied to $n = j - 1$, $c_u = a_u$ and $m = a_j$) shows that $a_1 a_2 \cdots a_{j-1}$ is coprime to a_j. Therefore, (25) (applied to $m = a_1 a_2 \cdots a_{j-1}$ and $n = a_j$) yields

$$\begin{aligned} f\left(\left(a_1 a_2 \cdots a_{j-1}\right) a_j\right) &= \underbrace{f\left(a_1 a_2 \cdots a_{j-1}\right)}_{= f(a_1) f(a_2) \cdots f\left(a_{j-1}\right)} f\left(a_j\right) \\ &= \left(f(a_1) f(a_2) \cdots f\left(a_{j-1}\right)\right) f\left(a_j\right) = f(a_1) f(a_2) \cdots f\left(a_j\right). \end{aligned}$$

Comparing this with $f\left(\left(a_1 a_2 \cdots a_{j-1}\right) a_j\right) = f\left(a_1 a_2 \cdots a_j\right)$, we obtain $f\left(a_1 a_2 \cdots a_j\right) = f(a_1) f(a_2) \cdots f\left(a_j\right)$. In other words, (27) holds for $i = j$. Thus, the induction step is complete, and so (27) is proven.

Now, we can apply (27) to $i = k$. As a result, we obtain $f(a_1 a_2 \cdots a_k) = f(a_1) f(a_2) \cdots f(a_k)$. This proves Proposition 2.7.2. □

Let us restate Proposition 2.7.2 in a more convenient form before we come to the proof of Proposition 2.7.1:

Corollary 2.7.3. Let $f : \mathbb{N}_+ \to \mathbb{C}$ be a multiplicative function. Let S be a finite set. Let m_s be a positive integer for each $s \in S$. Assume that the integers m_s and m_t are coprime whenever s and t are two distinct elements of S. Then,

$$f\left(\prod_{s \in S} m_s\right) = \prod_{s \in S} f(m_s).$$

Proof of Corollary 2.7.3. Let $(s_1, s_2, \ldots, s_k)$ be a list of all elements of S (with each element appearing exactly once in the list). Then, $\prod_{s \in S} m_s = m_{s_1} m_{s_2} \cdots m_{s_k}$ and $\prod_{s \in S} f(m_s) = f(m_{s_1}) f(m_{s_2}) \cdots f(m_{s_k})$.

Also, if i and j are two distinct elements of $\{1, 2, \ldots, k\}$, then the integers m_{s_i} and m_{s_j} are coprime[19]. In other words, $m_{s_1}, m_{s_2}, \ldots, m_{s_k}$ are pairwise coprime

[18] *Proof.* Let $u \in \{1, 2, \ldots, j-1\}$. Thus, u is an integer satisfying $1 \leq u \leq j - 1$. Now, $1 \leq u \leq j - 1 < j \leq k$ (since $j \in \{0, 1, \ldots, k\}$). Therefore, (26) (applied to $v = j$) shows that a_u is coprime to a_j. Qed.

[19] *Proof.* Let i and j be two distinct elements of $\{1, 2, \ldots, k\}$.

integers. Hence, Proposition 2.7.2 (applied to $a_i = m_{s_i}$) yields

$$f\left(m_{s_1} m_{s_2} \cdots m_{s_k}\right) = f\left(m_{s_1}\right) f\left(m_{s_2}\right) \cdots f\left(m_{s_k}\right).$$

Thus,

$$f\left(\underbrace{\prod_{s \in S} m_s}_{= m_{s_1} m_{s_2} \cdots m_{s_k}}\right) = f\left(m_{s_1} m_{s_2} \cdots m_{s_k}\right) = f\left(m_{s_1}\right) f\left(m_{s_2}\right) \cdots f\left(m_{s_k}\right) = \prod_{s \in S} f\left(m_s\right).$$

This proves Corollary 2.7.3. ☐

Proof of Proposition 2.7.1. The prime factorization of n is $n = \prod_{p \in \operatorname{PF} n} p^{v_p(n)} = \prod_{s \in \operatorname{PF} n} s^{v_s(n)}$ (here, we renamed the index p as s in the product). Clearly, $s^{v_s(n)}$ is a positive integer for each $s \in \operatorname{PF} n$. Furthermore, the integers $s^{v_s(n)}$ and $t^{v_t(n)}$ are coprime whenever s and t are two distinct elements of $\operatorname{PF} n$ [20]. Hence, Corollary 2.7.3 (applied to $S = \operatorname{PF} n$ and $m_s = s^{v_s(n)}$) yields

$$f\left(\prod_{s \in \operatorname{PF} n} s^{v_s(n)}\right) = \prod_{s \in \operatorname{PF} n} f\left(s^{v_s(n)}\right) = \prod_{p \in \operatorname{PF} n} f\left(p^{v_p(n)}\right)$$

(here, we renamed the index p as s in the product). Thus,

$$f\left(\underbrace{n}_{= \prod_{s \in \operatorname{PF} n} s^{v_s(n)}}\right) = f\left(\prod_{s \in \operatorname{PF} n} s^{v_s(n)}\right) = \prod_{p \in \operatorname{PF} n} f\left(p^{v_p(n)}\right).$$

This proves Proposition 2.7.1. ☐

The list $(s_1, s_2, \ldots, s_k)$ contains no element more than once (because of its definition). In other words, the elements $s_1, s_2, \ldots, s_k$ are pairwise distinct. Hence, $s_i \neq s_j$ (since $i \neq j$). In other words, the elements s_i and s_j are distinct.

But the integers m_s and m_t are coprime whenever s and t are two distinct elements of S. Applying this to $s = s_i$ and $t = s_j$, we conclude that the integers m_{s_i} and m_{s_j} are coprime (since s_i and s_j are distinct). Qed.

[20] *Proof.* Let s and t be two distinct elements of $\operatorname{PF} n$. We must prove that the integers $s^{v_s(n)}$ and $t^{v_t(n)}$ are coprime.

Assume the contrary. Thus, $s^{v_s(n)}$ and $t^{v_t(n)}$ are not coprime. In other words, $\gcd\left(s^{v_s(n)}, t^{v_t(n)}\right) > 1$. Hence, $\gcd\left(s^{v_s(n)}, t^{v_t(n)}\right)$ has a prime divisor q. Consider this q.

All elements of $\operatorname{PF} n$ are primes. Hence, s is a prime (since s is an element of $\operatorname{PF} n$). Thus, the only prime divisor of $s^{v_s(n)}$ is s.

But $q \mid \gcd\left(s^{v_s(n)}, t^{v_t(n)}\right) \mid s^{v_s(n)}$. Thus, q is a prime divisor of $s^{v_s(n)}$ (since q is a prime and divides $s^{v_s(n)}$). Since the only prime divisor of $s^{v_s(n)}$ is s, this shows that $q = s$. The same argument (applied to t instead of s) shows that $q = t$. Hence, $s = q = t$. This contradicts the fact that s and t are distinct. This contradiction proves that our assumption was wrong, qed.

3. Appendix: a proof of Bezout's identity

Let me finally give a proof of Theorem 1.2.2, which was used several times above. Proofs of this theorem abound in the literature; yet I have never seen the following proof written up. I believe that this proof has the advantage of being constructive (unlike the proof in [NiZuMo91, proof of Theorem 1.3], which starts out by choosing the least positive integer in a potentially infinite set) and yet not too messy (unlike some proofs using the extended Euclidean algorithm). Of course, all the standard proofs of Theorem 1.2.2 are "essentially the same", in the sense that they offer different points of view on one and the same idea (viz., that of the Euclidean algorithm).

We first prepare for our proof by showing some simple lemmas:

Lemma 3.0.1. Let b and c be two integers. Then, $\gcd(b,c) = \gcd(c,b)$.

Proof of Lemma 3.0.1. If $(b,c) = (0,0)$, then Lemma 3.0.1 is obvious. Hence, for the rest of this proof, we WLOG assume that $(b,c) \neq (0,0)$. Thus, $(c,b) \neq (0,0)$. Hence, $\gcd(c,b)$ is the greatest of all common divisors of c and b (by the definition of $\gcd(c,b)$). In other words, $\gcd(c,b)$ is the greatest of all common divisors of b and c (since the common divisors of c and b are the same as the common divisors of b and c). On the other hand, $\gcd(b,c)$ is the greatest of all common divisors of b and c (by the definition of $\gcd(b,c)$). Hence, the two numbers $\gcd(c,b)$ and $\gcd(b,c)$ have been characterized in precisely the same way (namely, as the greatest of all common divisors of b and c). Therefore, these two numbers are equal. In other words, $\gcd(b,c) = \gcd(c,b)$. This proves Lemma 3.0.1. □

Lemma 3.0.2. Let b and c be two integers. Then:

(a) We have $\gcd(b,c) = \gcd(-b,c)$.

(b) We have $\gcd(b,c) = \gcd(b,-c)$.

(c) We have $\gcd(b,c) = \gcd(|b|,|c|)$.

Proof of Lemma 3.0.2. If $(b,c) = (0,0)$, then Lemma 3.0.2 is obvious. Hence, for the rest of this proof, we WLOG assume that $(b,c) \neq (0,0)$.

(a) We make the following two observations:

Observation 1: Every common divisor of b and c is a common divisor of $-b$ and c.

Proof of Observation 1. Let d be a common divisor of b and c. We must prove that d is a common divisor of $-b$ and c.

We know that d is a common divisor of b and c; hence, $d \mid b$ and $d \mid c$. Now, $d \mid b \mid (-1)\,b = -b$. So we know that d divides the two integers $-b$ and c (since $d \mid -b$ and $d \mid c$). Hence, d is a common divisor of $-b$ and c. This completes the proof of Observation 1. □

> *Observation 2:* Every common divisor of $-b$ and c is a common divisor of b and c.

Proof of Observation 2. Observation 2 (applied to $-b$ instead of b) shows that every common divisor of $-b$ and c is a common divisor of $-(-b)$ and c. In other words, every common divisor of $-b$ and c is a common divisor of b and c (since $-(-b) = b$). This proves Observation 2. $\square$

Combining Observation 1 with Observation 2, we conclude that the common divisors of b and c are the same as the common divisors of $-b$ and c.

Now, $(-b, c) \neq (0, 0)$ (since $(b, c) \neq (0, 0)$). Hence, $\gcd(-b, c)$ is the greatest of all common divisors of $-b$ and c (by the definition of $\gcd(-b, c)$). In other words, $\gcd(-b, c)$ is the greatest of all common divisors of b and c (since the common divisors of b and c are the same as the common divisors of $-b$ and c). On the other hand, $\gcd(b, c)$ is the greatest of all common divisors of b and c (by the definition of $\gcd(b, c)$). Hence, the two numbers $\gcd(-b, c)$ and $\gcd(b, c)$ have been characterized in precisely the same way (namely, as the greatest of all common divisors of b and c). Therefore, these two numbers are equal. In other words, $\gcd(-b, c) = \gcd(b, c)$. This proves Lemma 3.0.2 **(a)**.

(b) Lemma 3.0.2 **(b)** can be proven in the same way as Lemma 3.0.2 **(a)** (but now we must use the fact that the divisors of c are the same as the divisors of $-c$).

[An alternative proof of Lemma 3.0.2 **(b)** proceeds as follows: We have

$$\begin{aligned} \gcd(b, c) &= \gcd(c, b) && \text{(by Lemma 3.0.1)} \\ &= \gcd(-c, b) && \left(\begin{array}{c}\text{by Lemma 3.0.2 (a), applied to} \\ c \text{ and } b \text{ instead of } b \text{ and } c\end{array}\right) \\ &= \gcd(b, -c) && \left(\begin{array}{c}\text{by Lemma 3.0.1, applied to} \\ -c \text{ and } b \text{ instead of } b \text{ and } c\end{array}\right); \end{aligned}$$

thus, Lemma 3.0.2 **(b)** is proven.]

(c) Lemma 3.0.2 **(c)** can be proven in the same way as Lemma 3.0.2 **(a)** (but now we must use the fact that the divisors of b are the same as the divisors of $|b|$, and that the divisors of c are the same as the divisors of $|c|$).

[Here is an alternative proof of Lemma 3.0.2 **(c)**: Using Lemma 3.0.2 **(a)**, we can find that $\gcd(|b|, c) = \gcd(b, c)$ [21]. Using Lemma 3.0.2 **(b)**, we can find that

[21] *Proof.* We must prove that $\gcd(|b|, c) = \gcd(b, c)$. If $|b| = b$, then this is obvious. Hence, for the rest of this proof, we WLOG assume that $|b| \neq b$.

Clearly, $|b|$ is either b or $-b$. Thus, $|b| = -b$ (since $|b| \neq b$). Hence, $\gcd\left(\underbrace{|b|}_{=-b}, c\right) = \gcd(-b, c) = \gcd(b, c)$ (by Lemma 3.0.2 **(a)**), qed.

$\gcd(|b|, |c|) = \gcd(|b|, c)$ [22]. Hence, $\gcd(|b|, |c|) = \gcd(|b|, c) = \gcd(b, c)$. This proves Lemma 3.0.2 **(c)**.] □

Lemma 3.0.3. Let b, c and u be three integers. Then:
(a) We have $\gcd(b, c) = \gcd(b + uc, c)$.
(b) We have $\gcd(b, c) = \gcd(b, ub + c)$.

Proof of Lemma 3.0.3. **(a)** If $(b, c) = (0, 0)$, then Lemma 3.0.3 is obvious (because if $(b, c) = (0, 0)$, then all four integers b, c, $b + uc$ and $ub + c$ are 0). Hence, for the rest of this proof, we WLOG assume that $(b, c) \neq (0, 0)$.

(a) We make the following two observations:

Observation 1: Every common divisor of $b + uc$ and c is a common divisor of b and c.

Proof of Observation 1. Let d be a common divisor of $b + uc$ and c. We must prove that d is a common divisor of b and c.

We know that d is a common divisor of $b + uc$ and c; hence, $d \mid b + uc$ and $d \mid c$. Now, $d \mid c \mid -uc$. So we know that d divides the two integers $b + uc$ and $-uc$ (since $d \mid b + uc$ and $d \mid -uc$). Hence, d must also divide the sum of these two integers. In other words, we have $d \mid (b + uc) + (-uc) = b$. Now, d divides both b and c (since $d \mid b$ and $d \mid c$). Hence, d is a common divisor of b and c. This completes the proof of Observation 1. □

Observation 2: Every common divisor of b and c is a common divisor of $b + uc$ and c.

Proof of Observation 2. Let d be a common divisor of b and c. We must prove that d is a common divisor of $b + uc$ and c.

We know that d is a common divisor of b and c; hence, $d \mid b$ and $d \mid c$. Now, $d \mid c \mid uc$. So we know that d divides the two integers b and uc (since $d \mid b$ and $d \mid uc$). Hence, d must also divide the sum of these two integers. In other words, we have $d \mid b + uc$. Now, d divides both $b + uc$ and c (since $d \mid b + uc$ and $d \mid c$). Hence, d is a common divisor of $b + uc$ and c. This completes the proof of Observation 2. □

Combining Observation 1 with Observation 2, we conclude that the common divisors of $b + uc$ and c are the same as the common divisors of b and c.

[22] *Proof.* We must prove that $\gcd(|b|, |c|) = \gcd(|b|, c)$. If $|c| = c$, then this is obvious. Hence, for the rest of this proof, we WLOG assume that $|c| \neq c$.

Clearly, $|c|$ is either c or $-c$. Thus, $|c| = -c$ (since $|c| \neq c$).

But Lemma 3.0.2 **(b)** (applied to $|b|$ instead of b) yields $\gcd(|b|, c) = \gcd(|b|, -c)$. Compared with $\gcd\left(|b|, \underbrace{|c|}_{=-c}\right) = \gcd(|b|, -c)$, this yields $\gcd(|b|, |c|) = \gcd(|b|, c)$, qed.

But $(b + uc, c) \neq (0, 0)$ [23]. Hence, $\gcd(b + uc, c)$ is the greatest of all common divisors of $b + uc$ and c (by the definition of $\gcd(b + uc, c)$). In other words, $\gcd(b + uc, c)$ is the greatest of all common divisors of b and c (since the common divisors of $b + uc$ and c are the same as the common divisors of b and c). On the other hand, $\gcd(b, c)$ is the greatest of all common divisors of b and c (by the definition of $\gcd(b, c)$). Hence, the two numbers $\gcd(b + uc, c)$ and $\gcd(b, c)$ have been characterized in precisely the same way (namely, as the greatest of all common divisors of b and c). Therefore, these two numbers are equal. In other words, $\gcd(b + uc, c) = \gcd(b, c)$. This proves Lemma 3.0.3 **(a)**.

(b) One way to prove Lemma 3.0.3 **(b)** is by arguing similarly to how we argued in our proof of Lemma 3.0.3 **(a)**. Let us, however, proceed differently: We have

$$\begin{aligned}
\gcd(b, c) &= \gcd(c, b) \qquad \text{(by Lemma 3.0.1)} \\
&= \gcd\left(\underbrace{c + ub}_{=ub+c}, b\right) \qquad \left(\begin{array}{c}\text{by Lemma 3.0.3 \textbf{(a)}, applied to } c \text{ and } b \\ \text{instead of } b \text{ and } c\end{array}\right) \\
&= \gcd(ub + c, b) \\
&= \gcd(b, ub + c) \qquad \left(\begin{array}{c}\text{by Lemma 3.0.1, applied to} \\ ub + c \text{ and } b \text{ instead of } b \text{ and } c\end{array}\right).
\end{aligned}$$

Thus, Lemma 3.0.3 **(b)** is proven. □

Lemma 3.0.4. Let $a \in \mathbb{N}$.
(a) We have $\gcd(a, 0) = a$.
(b) We have $\gcd(0, a) = a$.

Proof of Lemma 3.0.4. **(a)** We have $\gcd(0, 0) = 0$. In other words, Lemma 3.0.4 **(a)** holds for $a = 0$. Thus, for the rest of the proof of Lemma 3.0.4 **(a)**, we can WLOG assume that $a \neq 0$. Assume this. Thus, a is a positive integer (since $a \in \mathbb{N}$ and $a \neq 0$). Hence, every divisor of a is $\leq a$. Thus, the greatest of all divisors of a is a itself (since a itself is a divisor of a).

We make the following two observations:

Observation 1: Every divisor of a is a common divisor of a and 0.

Proof of Observation 1. Let d be a divisor of a. We must prove that d is a common divisor of a and 0.

We have $d \mid a$ (since d is a divisor of a) and $d \mid 0$ (obviously). Thus, d divides both a and 0. Hence, d is a common divisor of a and 0. This completes the proof of Observation 1. □

[23] *Proof.* Assume the contrary (for the sake of contradiction). Thus, $(b + uc, c) = (0, 0)$. Hence, $b + uc = 0$ and $c = 0$. Now, $0 = b + u \underbrace{c}_{=0} = b$, so that $b = 0$. Combined with $c = 0$, this yields $(b, c) = (0, 0)$, which contradicts $(b, c) \neq (0, 0)$. This contradiction shows that our assumption was false, qed.

Observation 2: Every common divisor of a and 0 is a divisor of a.

Proof of Observation 2. Observation 2 is obvious. □

Combining Observation 1 with Observation 2, we see that the common divisors of a and 0 are the same as the divisors of a.

We have $(a, 0) \neq (0, 0)$ (since $a \neq 0$). Thus, $\gcd(a, 0)$ is the greatest of all common divisors of a and 0 (by the definition of $\gcd(a, 0)$). In other words, $\gcd(a, 0)$ is the greatest of all divisors of a (since the common divisors of a and 0 are the same as the divisors of a). In other words, $\gcd(a, 0)$ is a (since the greatest of all divisors of a is a). This proves Lemma 3.0.4 **(a)**.

(b) We could prove Lemma 3.0.4 **(b)** similarly how we proved Lemma 3.0.4 **(a)**. But we can just as easily derive Lemma 3.0.4 **(b)** from Lemma 3.0.4 **(a)**: We have

$$\gcd(0, a) = \gcd(a, 0) \qquad \left(\begin{array}{c}\text{by Lemma 3.0.1, applied to 0 and } a \\ \text{instead of } b \text{ and } c\end{array}\right)$$
$$= a \qquad (\text{by Lemma 3.0.4 } \textbf{(a)}).$$

This proves Lemma 3.0.4 **(b)**. □

Now, we prove the (trivial) particular case of Theorem 1.2.2 when b and c are nonnegative integers one of which is 0:

Lemma 3.0.5. Let $b \in \mathbb{N}$ and $c \in \mathbb{N}$ be such that either $b = 0$ or $c = 0$ (or both). Then, there exist integers x and y such that $\gcd(b, c) = bx + cy$.

Proof of Lemma 3.0.5. We have either $b = 0$ or $c = 0$. Thus, we are in one of the following two cases:

Case 1: We have $b = 0$.

Case 2: We have $c = 0$.

Let us first consider Case 1. In this case, we have $b = 0$. Thus, $\gcd\left(\underbrace{b}_{=0}, c\right) = \gcd(0, c) = c$ (by Lemma 3.0.4 **(b)**, applied to $a = c$). Compared with $b0 + c1 = c1 = c$, this yields $\gcd(b, c) = b0 + c1$. Hence, there exist integers x and y such that $\gcd(b, c) = bx + cy$ (namely, $x = 0$ and $y = 1$). Thus, Lemma 3.0.5 is proven in Case 1.

Let us now consider Case 2. In this case, we have $c = 0$. Thus, $\gcd\left(b, \underbrace{c}_{=0}\right) = \gcd(b, 0) = b$ (by Lemma 3.0.4 **(a)**, applied to $a = b$). Compared with $b1 + c0 = b1 = b$, this yields $\gcd(b, c) = b1 + c0$. Hence, there exist integers x and y such that $\gcd(b, c) = bx + cy$ (namely, $x = 1$ and $y = 0$). Thus, Lemma 3.0.5 is proven in Case 2.

Hence, Lemma 3.0.5 is proven in each of the two Cases 1 and 2. Thus, Lemma 3.0.5 always holds. □

Next, we prove the particular case of Theorem 1.2.2 when b and c are nonnegative:

Lemma 3.0.6. Let $b \in \mathbb{N}$ and $c \in \mathbb{N}$. Then, there exist integers x and y such that $\gcd(b, c) = bx + cy$.

Proof of Lemma 3.0.6. We shall prove Lemma 3.0.6 by strong induction on $b + c$:

Let $N \in \mathbb{N}$. Assume that Lemma 3.0.6 holds in the case when $b + c < N$. We must prove that Lemma 3.0.6 holds in the case when $b + c = N$.

We have assumed that Lemma 3.0.6 holds in the case when $b + c < N$. In other words, the following holds:

> *Observation 1:* If $b \in \mathbb{N}$ and $c \in \mathbb{N}$ satisfy $b + c < N$, then there exist integers x and y such that $\gcd(b, c) = bx + cy$.

Let now $b \in \mathbb{N}$ and $c \in \mathbb{N}$ be such that $b + c = N$. We are going to show that

$$\text{there exist integers } x \text{ and } y \text{ such that } \gcd(b, c) = bx + cy. \tag{28}$$

If we have either $b = 0$ or $c = 0$ (or both), then (28) is true (by Lemma 3.0.5). Thus, for the rest of this proof of (28), we can WLOG assume that we have neither $b = 0$ nor $c = 0$. Assume this.

We have neither $b = 0$ nor $c = 0$. In other words, we have $b \neq 0$ and $c \neq 0$. Thus, $b > 0$ (since $b \in \mathbb{N}$ and $b \neq 0$) and $c > 0$ (since $c \in \mathbb{N}$ and $c \neq 0$). Now, we are in one of the following two cases:

Case 1: We have $b < c$.

Case 2: We have $b \geq c$.

Let us first consider Case 1. In this case, we have $b < c$. Thus, $b \leq c$, so that $c - b \in \mathbb{N}$. Moreover, $c = (c - b) + \underbrace{b}_{>0} > c - b$, so that $c - b < c$ and thus $b + \underbrace{(c - b)}_{<c} < b + c = N$. Therefore, we can apply Observation 1 to $c - b$ instead of c. As a result, we conclude that there exist integers x and y such that $\gcd(b, c - b) = bx + (c - b) y$. Denote these x and y by x_0 and y_0. Hence, x_0 and y_0 are integers satisfying $\gcd(b, c - b) = bx_0 + (c - b) y_0$.

Lemma 3.0.3 **(b)** (applied to $u = -1$) yields

$$\begin{aligned}
\gcd(b, c) &= \gcd\left(b, \underbrace{(-1) b + c}_{=c-b}\right) = \gcd(b, c - b) = bx_0 + (c - b) y_0 \\
&= bx_0 + cy_0 - by_0 = b(x_0 - y_0) + cy_0.
\end{aligned}$$

Thus, there exist integers x and y such that $\gcd(b, c) = bx + cy$ (namely, $x = x_0 - y_0$ and $z = y_0$). Therefore, (28) is proven in Case 1.

Let us now consider Case 2. In this case, we have $b \geq c$. Thus, $b - c \in \mathbb{N}$. Moreover, $b = (b-c) + \underbrace{c}_{>0} > b - c$, so that $b - c < b$ and thus $\underbrace{(b-c)}_{<b} + c < b + c = N$. Therefore, we can apply Observation 1 to $b - c$ instead of b. As a result, we conclude that there exist integers x and y such that $\gcd(b-c,c) = (b-c)x + cy$. Denote these x and y by x_0 and y_0. Hence, x_0 and y_0 are integers satisfying $\gcd(b-c,c) = (b-c)x_0 + cy_0$.

Lemma 3.0.3 **(a)** (applied to $u = -1$) yields

$$\gcd(b,c) = \gcd\left(\underbrace{b + (-1)c}_{=b-c}, c\right) = \gcd(b-c,c) = (b-c)x_0 + cy_0$$
$$= bx_0 - cx_0 + cy_0 = bx_0 + c(y_0 - x_0).$$

Thus, there exist integers x and y such that $\gcd(b,c) = bx + cy$ (namely, $x = x_0$ and $y = y_0 - x_0$). Therefore, (28) is proven in Case 2.

We have now proven (28) in each of the two Cases 1 and 2. Thus, (28) always holds (since Cases 1 and 2 cover all possibilities). So we have proven that there exist integers x and y such that $\gcd(b,c) = bx + cy$.

Now, forget that we fixed b and c. We thus have shown that if $b \in \mathbb{N}$ and $c \in \mathbb{N}$ are such that $b + c = N$, then there exist integers x and y such that $\gcd(b,c) = bx + cy$. In other words, Lemma 3.0.6 holds in the case when $b + c = N$. This completes the induction step; thus, Lemma 3.0.6 is proven by induction. □

Now, we can finally deliver the coup-de-grâce to Theorem 1.2.2:

Proof of Theorem 1.2.2. We have $|b| \in \mathbb{N}$ and $|c| \in \mathbb{N}$. Hence, Lemma 3.0.6 (applied to $|b|$ and $|c|$ instead of b and c) yields that there exist integers x and y such that $\gcd(|b|,|c|) = |b|x + |c|y$. Denote these x and y by x_0 and y_0. Hence, x_0 and y_0 are integers satisfying $\gcd(|b|,|c|) = |b|x_0 + |c|y_0$.

But $|b|$ is either b or $-b$. In either case, $|b|$ is divisible by b (since both b and $-b$ are divisible by b). Hence, there exists a $\beta \in \mathbb{Z}$ such that $|b| = \beta b$. Similarly, there exists a $\gamma \in \mathbb{Z}$ such that $|c| = \gamma c$. Consider these β and γ. Now, Lemma 3.0.2 **(c)** yields

$$\gcd(b,c) = \gcd(|b|,|c|) = \underbrace{|b|}_{=\beta b} x_0 + \underbrace{|c|}_{=\gamma c} y_0 = \underbrace{\beta b x_0}_{=b(\beta x_0)} + \underbrace{\gamma c y_0}_{=c(\gamma y_0)} = b(\beta x_0) + c(\gamma y_0).$$

Hence, there exist integers x and y such that $\gcd(b,c) = bx + cy$ (namely, $x = \beta x_0$ and $y = \gamma y_0$). This proves Theorem 1.2.2. □

References

[BenGol75] Edward A. Bender, J. R. Goldman, *On the applications of Möbius inversion in combinatorial analysis*, American Mathematical Monthly, vol. 82, October 1975, pp. 789–803.

[Grinbe15] Darij Grinberg, *Mathematical Reflections problem U275*, version of November 2, 2015.
http://web.mit.edu/~darij/www/mrmoeb.pdf

[NiZuMo91] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, Wiley 1991.

[Rota64] Gian-Carlo Rota, *On the Foundations of Combinatorial Theory: I. Theory of Möbius Functions*, Z. Wahrscheinlichkeitstheorie 2, pp. 340–368 (1964).

[Stanle11] Richard P. Stanley, *Enumerative Combinatorics, volume 1*, Cambridge University Press, 2011.
http://math.mit.edu/~rstan/ec/ec1/