Divisor set

We will use $\mathscr{D}(n)$ to denote the set of divisors of n. The size of the set $\mathscr{D}(n)$ is denoted by $\sigma_0(n)$.

Theorem 2.6.1

Let m, n be two integers. The multiplication gives a map

$$\Phi\colon\ \mathscr{D}(m) \times \mathscr{D}(n) \longrightarrow \mathscr{D}(mn).$$

Moreover, if m, n are coprime, Φ is bijective.

Proof. First, the multiplication does give a map Φ: if $a \in \mathscr{D}(m)$ and $b \in \mathscr{D}(n)$, then there are integers u, v such that $m = ua$ and $n = vb$. Hence, $mn = uvab$. Namely, $ab \in \mathscr{D}(mn)$.

It remains to show that Φ is bijective when m, n are coprime.

Now, let's prove Φ is *surjective*. Suppose $c \in \mathscr{D}(mn)$. Let

$$a = \gcd(m, c) \qquad \text{and} \qquad b = \gcd(n, c).$$

Clearly, $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$. It remains to show $ab = c$.

Now, let's prove Φ is *surjective*. Suppose $c \in \mathscr{D}(mn)$. Let

$$a = \gcd(m, c) \qquad \text{and} \qquad b = \gcd(n, c).$$

Clearly, $a \in \mathscr{D}(m)$, $b \in \mathscr{D}(n)$. It remains to show $ab = c$.

Since m, n are coprime, for any prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(c) \leqslant v_p(m) + v_p(n) = v_p(n)$. Therefore, we have

$$v_p(a) = \min\{v_p(m), v_p(c)\} = 0,$$
$$v_p(b) = \min\{v_p(n), v_p(c)\} = v_p(c).$$

In particular, $v_p(a) + v_p(b) = v_p(c)$.

Now, let's prove Φ is *surjective*. Suppose $c \in \mathscr{D}(mn)$. Let

$$a = \gcd(m, c) \qquad \text{and} \qquad b = \gcd(n, c).$$

Clearly, $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$. It remains to show $ab = c$.

Since m, n are coprime, for any prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(c) \leqslant v_p(m) + v_p(n) = v_p(n)$. Therefore, we have

$$v_p(a) = \min\left\{v_p(m), v_p(c)\right\} = 0,$$
$$v_p(b) = \min\left\{v_p(n), v_p(c)\right\} = v_p(c).$$

In particular, $v_p(a) + v_p(b) = v_p(c)$. Similar for the case $v_p(n) = 0$. Since $v_p(a) + v_p(b) = v_p(c)$ for all prime p, we must have $ab = c$.

Now, let's prove Φ is *injective*. Indeed, we only need to show that for all $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$, we have

$$a = \gcd(m, ab) \qquad \text{and} \qquad b = \gcd(n, ab).$$

Now, let's prove Φ is *injective*. Indeed, we only need to show that for all $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$, we have

$$a = \gcd(m, ab) \qquad \text{and} \qquad b = \gcd(n, ab).$$

Since m, n are coprime, for any prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(a) \leqslant v_p(m) = 0$. Therefore,

$$\min\{v_p(m), v_p(ab)\} = 0 = v_p(a),$$
$$\min\{v_p(n), v_p(ab)\} = \min\{v_p(n), v_p(b)\} = v_p(b).$$

Now, let's prove Φ is *injective*. Indeed, we only need to show that for all $a \in \mathscr{D}(m), b \in \mathscr{D}(n)$, we have

$$a = \gcd(m, ab) \qquad \text{and} \qquad b = \gcd(n, ab).$$

Since m, n are coprime, for any prime p, at least one of $v_p(m), v_p(n)$ is 0. Let's say $v_p(m) = 0$. Then we have $v_p(a) \leqslant v_p(m) = 0$. Therefore,

$$\begin{aligned} \min\{v_p(m), v_p(ab)\} &= 0 = v_p(a), \\ \min\{v_p(n), v_p(ab)\} &= \min\{v_p(n), v_p(b)\} = v_p(b). \end{aligned}$$

Similar for the case $v_p(n) = 0$.

Since $\min\{v_p(m), v_p(ab)\} = v_p(a)$ and $\min\{v_p(n), v_p(ab)\} = v_p(b)$ for all prime p, we must have $a = \gcd(m, ab)$ and $b = \gcd(n, ab)$. $\square$

Multiplicative functions

Definition 2.6.2

An *arithmetic function* is a complex-valued function defined on $\mathbb{Z}_+$. An arithmetic function $f(\cdot)$ is *multiplicative** if for every pair of coprime positive integers (a, b),

$$f(ab) = f(a)f(b).$$

*If we remove the requirement on coprimeness, the property is called *completely multiplicative*

Definition 2.6.2

An *arithmetic function* is a complex-valued function defined on $\mathbb{Z}_+$. An arithmetic function $f(\cdot)$ is *multiplicative** if for every pair of coprime positive integers (a, b),

$$f(ab) = f(a)f(b).$$

Example 2.6.3

Theorem 2.6.1 tells us that the function $\sigma_0(\cdot)$ is multiplicative.

$$\sigma_0(mn) = \sigma_0(m)\sigma_0(n)$$

Example 2.6.4

Suppose $f(\cdot)$ is a multiplicative function. If we know

$$f(2) = 4, f(3) = 11, f(4) = 3.$$

Do we know enough to compute $f(6)$? $f(24)$?

$$f(6) = f(2)f(3) \quad \text{“} 6 = 2 \cdot 3 \text{”}$$
$$= 4 \cdot 11 = 44$$

$$f(24) \neq f(4) f(6) = 3 \times 44 \qquad 24 = 4 \cdot 6$$

Not coprime!

$$f(24) = f(8) \cdot f(3) \qquad \text{“} 24 = 2^3 \cdot 3 \text{”}$$

Corollary 2.6.5

Let n be a positive integer. We have

$$\sigma_0(n) = \prod_{p \text{ is prime}} (v_p(n) + 1).$$

Note that only for finitely many primes p, we have $v_p(n) > 0$. Hence, the product is essentially a finite product (since multiply with 1 does nothing).

Corollary 2.6.5

Let n be a positive integer. We have

$$\sigma_0(n) = \prod_{p \text{ is prime}} (v_p(n) + 1).$$

Proof. By the multiplicativity of $\sigma_0(\cdot)$, we only need to prove for all prime p and natural number e that $\sigma_0(p^e) = e + 1$.

Indeed, from the unique prime factorization, it is easy to see that $\mathscr{D}(p^e) = \{1, p, \cdots, p^e\}$. Hence, its size is $e + 1$. $\square$