Multiplicative Functions

Theorem : (7.3)

The function d is multiplicative.

Proof. Let m and n be relatively prime. Then, no prime that divides m can divide n and vice versa. Thus, if

$$m = p_1^{e_1} \dots p_k^{e_k} \quad \text{and} \quad n = q_1^{f_1} \dots q_r^{f_r}$$

are the prime power decompositions of m and n, then $p_i \neq q_j$. Then, the prime power decomposition of mn is given by

$$mn = p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}$$

Applying Theorem 7.1, we have that

$$\begin{aligned} d(mn) &= d\left(p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}\right) \\ &= d\left(p_1^{e_1}\right) \dots d\left(p_k^{e_k}\right) d\left(q_1^{f_1}\right) d\left(q_r^{f_r}\right) \\ &= d\left(p_1^{e_1} \dots p_k^{e_k}\right) d\left(q_1^{f_1} \dots q_r^{f_r}\right) \\ &= d(m)\, d(n) \end{aligned}$$

□

Theorem : (7.4)

The function σ is multiplicative.

Proof. Let m and n be relatively prime. Then, no prime that divides m can divide n and vice versa. Thus, if

$$m = p_1^{e_1} \dots p_k^{e_k} \quad \text{and} \quad n = q_1^{f_1} \dots q_r^{f_r}$$

are the prime power decompositions of m and n, then $p_i \neq q_j$. Then, the prime power decomposition of mn is given by

$$mn = p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}$$

Applying Theorem 7.2, we have that

$$\begin{aligned} \sigma(mn) &= \sigma\left(p_1^{e_1} \dots p_k^{e_k} q_1^{f_1} \dots q_r^{f_r}\right) \\ &= \sigma\left(p_1^{e_1}\right) \dots \sigma\left(p_k^{e_k}\right) \sigma\left(q_1^{f_1}\right) \sigma\left(q_r^{f_r}\right) \\ &= \sigma\left(p_1^{e_1} \dots p_k^{e_k}\right) \sigma\left(q_1^{f_1} \dots q_r^{f_r}\right) \\ &= \sigma(m)\, \sigma(n) \end{aligned}$$

□

Theorem : (7.5)

If f is a multiplicative function and the prime power decomposition of n is $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, then

$$f(n) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_k^{e_k}\right)$$

Proof. Base case: $k = 1$: $f(n) = f\left(p_1^{e_1}\right)$. Assume the theorem is true for $k = r$. Now consider $k = r = 1$. Since $\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, p_{r+1}^{e_{r+1}}\right) = 1$, we have from the definition of a multiplicative function that

$$f\left(\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}\right) p_{r+1}^{e_{r+1}}\right) = f\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}\right) f\left(p_{r+1}^{e_{r+1}}\right)$$

From the induction hypothesis, the first factor is

$$f\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}\right) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_r^{e_r}\right)$$

Therefore, we have that

$$f\left(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} p_{r+1}^{e_{r+1}}\right) = f\left(p_1^{e_1}\right) f\left(p_2^{e_2}\right) \dots f\left(p_r^{e_r}\right) f\left(p_{r+1}^{e_{r+1}}\right)$$

□

Perfect Numbers

Definition : Perfect Numbers

A number is called perfect if and only if it is equal to the sum of its positive divisors, excluding itself. That is, a number is perfect if and only if

$$\sigma(n) = 2n$$

Example

Is 6 a perfect number? Is 12 a perfect number?

---

6 is perfect since $6 = 1 + 2 + 3$.

12 is not perfect since $12 \neq 1 + 2 + 3 + 4 + 6$

Theorem : (8.1) (Euclid)

If $2^k - 1$ is prime, then $2^{k-1}\left(2^k - 1\right)$ is perfect.

Proof. Suppose that $n = \left(2^{k-1}\right)\left(2^k - 1\right)$. Since $2^k - 1$ is prime, we know that

$$\sigma\left(2^k - 1\right) = 1 + 2^k - 1 = 2^k$$

Also, notice that 2^{k-1} and $2^k - 1$ are relatively prime. Therefore, n is perfect since

$$\begin{aligned}
\sigma(n) &= \sigma\left(2^{k-1}\left(2^k - 1\right)\right) \\
&= \sigma\left(2^{k-1}\right)\sigma\left(2^k - 1\right) \\
&= \left(2^k - 1\right)2^k \\
&= 2\left(\left(2^k - 1\right)2^{k-1}\right) \\
&= 2n
\end{aligned}$$

□

Lemma

If k is composite, then $2^k - 1$ is composite.

Proof. Suppose $k = ab$, where $a \neq 1$, $b \neq 1$. Then,

$$\begin{aligned} 2^k - 1 &= 2^{ab} - 1 \\ &= (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right) \end{aligned}$$

Therefore, 2^{k-1} can be prime only when k is prime. □

Theorem : (8.2) (Euler)

If n is an even perfect number, then

$$n = 2^{p-1}(2^p - 1)$$

for some prime p and $2^p - 1$ is also prime.

Proof. If n is an even perfect number, $n = 2^e m$, where m is odd and $e \geq 1$. Since $\sigma(m) > m$, we can write $\sigma(m) = m + s$, with $s > 0$. That is, s is the sum of all the divisors of m that are less than m. Therefore, substituting this into the expression for $\sigma(n) = 2n$ gives us that

$$\begin{aligned} \sigma(n) &= 2n \\ \sigma(2^e m) &= 2n \\ \sigma(2^e)\,\sigma(m) &= 2n \\ \left(2^{e+1} - 1\right)(m + s) &= 2^{e+1} m \\ 2^{e+1} m - m + \left(2^{e+1} - 1\right) s &= 2^{e+1} m \\ \left(2^{e+1} - 1\right) s &= m \end{aligned}$$

This means that s is a divisor of m, and $s < m$. But s is the sum of all the divisors of m that are less than m. That is, s is the sum of a group of numbers that includes s. This is only possible if the group consists of one number alone. Therefore the set of divisors of m smaller than m must contain only one element, and that element must be 1. That is, $s = 1$, and hence $m = 2^{e+1} - 1$ is prime. The only numbers of this form that are prime must have $e + 1$ prime. Hence, $m = 2^p - 1$ for some prime $p = e + 1$. Therefore we have

$$\begin{aligned} n &= 2^e m \\ &= 2^e\left(2^{e+1} - 1\right) \\ &= 2^{p-1}(2^p - 1) \end{aligned}$$

□