6.2 The Sum and Number of Divisors

In mathematics, function has an important role to play with different topics. For advance study of number theory we have some important aspects related to functions. Any function whose domain is the set of integers are called the number theoretic function or arithmetic functions. The range set may be other than positive integers also. We will start our discussions with the sum and number of divisors.

Definition 6.2.1. *Given a positive integer n, $\tau(n)$ is defined as total number of positive divisors of n.*

For an example if we choose $n = 12$, then $\tau(12) = 6$ as the divisors are $1, 2, 3, 4, 5, 6, 12$. In the following table we have shown few integers and their corresponding number of divisors.

n	2	3	4	5	6	7	8	9	10
$\tau(n)$	2	2	3	2	4	2	4	3	4

Definition 6.2.2. *Given a positive integer n, $\sigma(n)$ is defined as the sum of their divisors.*

For example if we choose $n = 12$, then $\sigma(12) = 1+2+3+4+5+6+12 = 28$. In the following table we have shown few integers and their corresponding sum of divisors.

n	2	3	4	5	6	7	8	9	10
$\sigma(n)$	3	4	7	6	12	8	15	13	18

Before going for further discussions we are going to interpret the symbol $\sum_{d|n} f(d)$ which means 'Sum of values of $f(d)$ as d runs over all positive divisors of n'. This sum is denoted as $F(n)$ and defined as $F(n) = \sum_{d|n} f(d)$. If n is prime then $\tau(n) = 2$ and $\sigma(n) = n + 1$. The converse is also true is justified with the given example: $\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$ i.e. $\tau(n) = \sum_{d|n} 1, \sigma(n) = \sum_{d|n} d$, therefore, $\tau(10) = \sum_{d|10} 1 = 1+1+1+1+1 = 4$ and $\sigma(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18$. Those are already shown in the above two given tables.

The first theorem of the chapter aims to find the positive divisors of a positive integer where the prime factorisation of that positive integer is already known.

Theorem 6.2.1. *If* $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$ *is the prime factorization of* $n > 1$, *then the positive divisors of* n *are precisely, those integers* d *of the form* $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$, *where* $0 \le b_i \le t_i (i = 1, 2, 3, \ldots r)$ *and vice–versa.*

Proof. If $d = 1$, then $b_1 = b_2 = \cdots = b_r = 0$ and $d = n$, then $b_1 = t_1, \ldots, b_r = t_r$. Let $n = dd'$ where $d, d' > 1$ holds. Then they can be expressed as product of primes where $d = q_1 q_2 q_3 \ldots q_s$, $d' = r_1 r_2 r_3 \ldots r_u$ considering q_i, r_j as primes. Hence $p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} = q_1 q_2 q_3 \ldots q_s r_1 r_2 r_3 \ldots r_u$. By uniqueness of primes some of q_i is same as p_j so collecting them we have, $d = q_1 q_2 q_3 \ldots q_s = p_1^{b_1} \cdots p_1^{b_r}$ where $b_i = 0$ is possible.

Conversely, every number $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$ turns out to be the divisor of n. Then we have, $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} = (p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r})(p_1^{t_1 - b_1} p_2^{t_2 - b_2} \cdots p_r^{t_r - b_r}) = dd'$ where $d' = p_1^{t_1 - b_1} p_2^{t_2 - b_2} \cdots p_r^{t_r - b_r}$ and $t_i - b_i \ge 0$ for all i, then $d' > 0$ and $d|n$.

The next theorem deals with the formula for both the number theoretic functions $\tau(n)$ and $\sigma(n)$. The previous two tables on these two functions illustrate, if the integer n is prime then $\tau(n) = 2$ and $\sigma(n) = n + 1$. In particular if $n = p^\alpha$ where p is prime then the divisors of p^α are $1, p, p^2 \cdots p^\alpha$ thus $\tau(p^\alpha) = \alpha + 1$ and $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \dfrac{p^{\alpha+1} - 1}{p - 1}$. Thus the general formula for these two functions are as follows. □

Theorem 6.2.2. *If* $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$ *is prime factorization of* $r > 1$ *then the followings are true.*

1. $\tau(n) = (t_1 + 1)(t_2 + 1)(t_3 + 1) \ldots (t_r + 1)$.

2. $\sigma(n) = \dfrac{p_1^{t_1+1} - 1}{p_1 - 1} \dfrac{p_2^{t_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{t_r+1} - 1}{p_r - 1}$.

Proof. 1. According to the above theorem, the positive divisors of n are precisely those integers $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$ where $0 \le b_i \le t_i$ holds. So there are $t_1 + 1$ choices for $b_1, (t_2 + 1)$ choices for b_2 and continuing we have $t_r + 1$ choices for b_r. Therefore total number of positive divisors are $(t_1 + 1)(t_2 + 1)(t_3 + 1) \ldots (t_r + 1)$. Hence $\tau(n) = (t_1 + 1)(t_2 + 1)(t_3 + 1) \cdots (t_r + 1) = \sum\limits_{1 \le j \le r} (t_j + 1)$.

2. In order to evaluate $\sigma(n)$ we consider the product, $(1 + p_1 + p_1^2 + p_1^3 + \ldots p_1^{t_1})(1 + p_2^2 + p_2^3 + \ldots p_2^{t_2}) \cdots (1 + p_r + p_r^2 + \ldots p_r^{t_r})$ where each term in

brackets are positive divisor of each prime factorisation of n. Therefore

$$\begin{aligned}\sigma(n) &= (1+p_1+p_1^2+p_1^3+\dots p_1^{t_1})(1+p_2^2+p_2^3+\dots p_2^{t_2})\cdots(1+p_r+p_r^2+\dots p_r^{t_r})\\ &= \frac{p_1^{t_1+1}-1}{p_1-1}\frac{p_2^{t_2+1}-1}{p_2-1}\cdots\frac{p_r^{t_r+1}-1}{p_r-1}\\ &= \prod_{1\le i\le r}\frac{p_i^{t_i+1}-1}{p_i-1}.\end{aligned}$$

□

We illustrate this with an example.

Example 6.2.1. *Let* $n = 150 = 2\times3\times5^2$ *then* $\tau(150) = (1+1)(1+1)(2+1) = 12$ *and* $\sigma(150) = \dfrac{2^2-1}{2-1}\dfrac{3^2-1}{3-1}\dfrac{5^3-1}{5-1} = 372$.

Now the following definition deals with a special property of number theoretic functions known to be multiplicative property:

Definition 6.2.3. *A number theoretic function f is said to be multiplicative if, for positive integers m and n, $f(mn) = f(m)f(n)$ where* $\gcd(m,n) = 1$.

Remark 6.2.1. *The function $f(n) = 1,\ \forall\ n \in \mathbb{Z}$ is multiplicative because $f(mn) = 1,\ f(m) = 1\ \&\ f(n) = 1$, so that $f(mn) = f(m)f(n)$. Similarly, the identity function $g(n) = n,\ \forall\ n \in \mathbb{Z}$ is multiplicative, since $g(mn) = mn = g(m)g(n)$. Observe that multiplicative functions f and g with the property $f(mn) = f(m)f(n)$ and $g(mn) = g(m)g(n)$ for all pairs of integers m and n, whether or not* $\gcd(m,n) = 1$*, is said to be completely multiplicative functions.*

Now we are at the stage to discuss the multiplicative property of τ and σ.

Theorem 6.2.3. *The functions τ and σ are both multiplicative.*

Proof. Let m and n be two relatively prime integers both greater than 1, for if any one of them is 1 then the result is trivial. So our primal assumption is both $m,n > 1$. Let $m = p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$ and $n = q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ be prime factorisation of m and n respectively where no $p_i = q_r$ because $\gcd(m,n) = 1$ and if any of p_i's same as any of q_r's then this leads to a contradiction(Why!). Therefore $mn = p_1^{t_1}p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ and

$$\begin{aligned}\tau(mn) &= [(t_1+1)(t_2+1)\cdots(t_r+1)][(j_1+1)(j_2+1)\cdots(j_s+1)]\\ &= \tau(m)\tau(n)\\ \sigma(mn) &= \prod_{1\le i\le r}\frac{p_i^{t_i+1}-1}{p_i-1}\prod_{1\le j\le s}\frac{q_i^{j_s+1}-1}{q_s-1}\\ &= \sigma(m)\sigma(n).\end{aligned}$$

We will continue our study on multiplicative functions of positive divisors for products of relatively prime integers. Next lemma is the first step on this study.

Lemma 6.2.1. *If* $\gcd(m, n) = 1$*, then the set of positive divisors of* mn *consists of all products* $d_1 d_2$ *where* $d_1|m$ *and* $d_2|n$ *and* $\gcd(d_1, d_2) = 1$*.*

Proof. Let us assume $m, n > 1$ and $m = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorization. Therefore

$$mn = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} q_1^{j_1} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}.$$

Hence any positive divisors d of mn represented in the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s},$$

where, $0 \leq a_i \leq t_i$ and $0 \leq b_i \leq j_i$ then $d = d_1 d_2$ where $d_1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where $d_1|m$ and $d_2 = q_1^{b_1} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ where $d_2|n$ and $\gcd(d_1, d_2) = 1$, as $p_i \neq q_j$ because m and n are relatively prime. □

Before proceeding further we will illustrate the idea of a positive divisor by means of an example. Let $m = 4$ and $n = 5$. Also $F(n) = \sum_{d|n} f(d)$ is defined earlier in this section. Here we choose f as an arithmetic function. In this example we will show $F(20) = F(4)F(5)$. Now the divisors of 20 are $1, 2, 4, 5, 10, 20$, therefore $F(20) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$. Also the divisors of 4 are $1, 2, 4$ and of 5 are $1, 5$. Thus we have,

$$\begin{aligned}
F(20) &= f(1) + f(2) + f(4) + f(5) + f(10) + f(20) \\
&= f(1 \cdot 1) + f(1 \cdot 2) + f(1 \cdot 4) + f(1 \cdot 5) + f(2 \cdot 5) + f(4 \cdot 5) \\
&= f(1)f(1) + f(1)f(2) + f(1)f(4) + f(1)f(5) + f(2)f(5) + f(4)f(5) \\
&= (f(1) + f(2) + f(4))(f(1) + f(5)) \\
&= F(4)F(5)
\end{aligned}$$

This shows the arithmetic function F is multiplicative. Now the theorem is as follows,

Theorem 6.2.4. *If* f *is a multiplicative function and* F *is defined by* $F(n) = \sum_{d|n} f(d)$ *then* F *is also multiplicative.*

Proof. Let m, n are relatively prime integer then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2),$$

where $\gcd(d_1, d_2) = 1$ and f is multiplicative, then we have $f(d_1 d_2) = f(d_1)f(d_2)$. Therefore

$$F(mn) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = F(m)F(n).$$

This proves the fact that F is multiplicative. □

6.3 Worked out Exercises

Problem 6.3.1. *Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.*

Solution 6.3.1. *There are infinitely many integers k such that* $\gcd(k, 10) = 1$. *Let us consider $m = 5k, n = 4k$. This implies there exist infinitely many such m, n. Suppose k is prime with $k \neq 2, 5$. Now $m^2 = 5^2k^2$ and $n^2 = 4^2k^2 = 2^4k^2$. Theorem 6.2.2 yields*

$$\sigma(m^2) = \frac{5^3-1}{5-1} \cdot \frac{k^3-1}{k-1} = 31\left(\frac{k^3-1}{k-1}\right).$$
$$\sigma(n^2) = \frac{2^5-1}{2-1} \cdot \frac{k^3-1}{k-1} = 31\left(\frac{k^3-1}{k-1}\right).$$

Thus there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.

Problem 6.3.2. *If n is a square-free integer, prove that $\tau(n) = 2^s$, where s is the number of prime divisors of n.*

Solution 6.3.2. *Since n is square-free, therefore $n = p_1 p_2 \cdots p_r$ where each $p_i \neq p_j \neq$ for $i \neq j$. From Theorem 6.2.2, we obtain*

$$\tau(n) = (k_1+1)(k_2+1)\cdots(k_s+1), \text{ with } k_i = 1 \text{ for all } i.$$

Thus $\tau(n) = (1+1)(1+1)\cdots(1+1) = 2 \cdot 2 \cdots 2 = 2^s$ as there are s terms

Problem 6.3.3. *Prove that the following statements are equivalent:*

1. *$\tau(n)$ is an odd integer.*

2. n is a perfect square.

Solution 6.3.3. *1⇒2:Suppose (1) holds. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Then using Theorem 6.2.2, we have $\tau(n) = (k_1+1)(k_2+1)\cdots(k_s+1)$. Note that each k_i+1 is odd, so k_i is even. Hence $k_i = 2j_i$ implies*

$$n = p_1^{2j_1} p_2^{2j_2} \cdots p_s^{2j_s} = (p_1^{j_1} p_1^{j_2} \cdots p_s^{j_s})^2,$$

which proves n is a perfect-square.

2⇒1:Suppose (2) holds. Then $n = a^2$ for some $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, which implies

$$n = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}.$$

Therefore $\tau(n) = (2k_1+1)(2k_2+1)\cdots(2k_s+1)$. Since each of $2k_i+1$ is odd, therefore $\tau(n)$ is odd.

Problem 6.3.4. *For any positive integer z, prove $\displaystyle\sum_{d|z} \frac{1}{d} = \frac{\sigma(z)}{z}$.*

Solution 6.3.4. *Note that d is a divisor of z if and only if $\dfrac{z}{d}$ is a divisor of z(Why!). Therefore the set of divisors of z are given by $\{d_1, d_2, \ldots, d_s\}$, which further can be expressed as $\left\{\dfrac{z}{d_1}, \dfrac{z}{d_2}, \ldots, \dfrac{z}{d_s}\right\}$. Thus*

$$\sigma(z) = d_1 + d_2 + \ldots + d_s = \frac{z}{d_1} + \frac{z}{d_2} + \ldots + \frac{z}{d_s} = z\left(\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s}\right),$$

implies

$$\frac{\sigma(z)}{z} = \frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s} = \sum_{d|z} \frac{1}{d}.$$

Problem 6.3.5. *If $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ is the prime factorization of $z > 1$, then prove that*

$$1 > \frac{z}{\sigma(z)} > \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_s}\right).$$

Solution 6.3.5. *Since the divisors of z include 1 and z, therefore*

$$\sigma(z) \geq z + 1 > z \Rightarrow \frac{z}{\sigma(z)} < 1.$$

By virtue of Theorem 6.2.2, we obtain

$$\sigma(z) = \frac{q_1^{t_1+1} - 1}{q_1 - 1} \frac{q_2^{t_2+1} - 1}{q_2 - 1} \cdots \frac{q_s^{t_s+1} - 1}{q_s - 1}.$$

Therefore

$$\frac{z}{\sigma(z)} = \frac{q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}}{\frac{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)}{(q_1-1)(q_2-1)\cdots(q_s-1)}}$$
$$= \frac{(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s})(q_1-1)(q_2-1)\cdots(q_s-1)}{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)}$$
$$= \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\frac{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)}{q_1^{t_1} q_2^{t_2}\cdots q_s^{t_s}}}$$
$$= \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\left(q_1 - \frac{1}{q_1^{t_1}}\right)\left(q_2 - \frac{1}{q_2^{t_2}}\right)\cdots\left(q_s - \frac{1}{q_s^{t_s}}\right)}. \qquad (6.3.1)$$

But

$$q_i > q_i - \frac{1}{q_i^{t_i}} \Rightarrow \frac{1}{q_i - \frac{1}{q_i^{t_i}}} > \frac{1}{q_i}.$$

Thus (6.3.1) yields,

$$\frac{z}{\sigma(z)} = \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\left(q_1 - \frac{1}{q_1^{t_1}}\right)\left(q_2 - \frac{1}{q_2^{t_2}}\right)\cdots\left(q_s - \frac{1}{q_s^{t_s}}\right)}$$
$$> \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{q_1 q_2 \cdots q_s}$$
$$= \left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_s}\right).$$

Hence

$$1 > \frac{z}{\sigma(z)} > \left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_s}\right).$$

Problem 6.3.6. *Prove if $z > 1$ is a composite number, then $\sigma(z) > z + \sqrt{z}$.*

Solution 6.3.6. *Since*

$$\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z,$$

its suffices to show that

$$d_1 + d_2 + \ldots + d_s > \sqrt{z}.$$

Since z is composite, there exists d_i (for some i) such that $1 < d_i < z$ and $d_i | z$. Therefore $\frac{z}{d_i} | z$ and $d_i < z$ together implies $1 < \frac{z}{d_i}$ and $1 < d_i \Rightarrow \frac{1}{d_i} < 1 \Rightarrow \frac{z}{d_i} < z$. Therefore

$$1 < \frac{z}{d_i} < z.$$

Now two cases may arise:

Case(i) *If* $d_i > \sqrt{z}$, *then clearly* $1 + d_i > \sqrt{z}$. *So*

$$\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z > z + \sqrt{z}.$$

Case(ii) *If* $d_i \leq \sqrt{z}$, *then*

$$\frac{1}{\sqrt{z}} \leq \frac{1}{d_i} \Rightarrow \sqrt{z} = \frac{z}{\sqrt{z}} \leq \frac{z}{d_i}.$$

Let $d_j = \dfrac{z}{d_i}$. *Then* $d_j|z$ *implies* $d_j \geq \sqrt{z}$. *Therefore* $1 + d_j + z > z + \sqrt{z}$. *Hence from* $\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z$, *it follows* $\sigma(z) > z + \sqrt{z}$.

Thus combining the above cases the assertion follows.

Problem 6.3.7. *For any integer* $k > 1$, *show that*

1. *there exist infinitely many integers* n *for which* $\tau(n) = k$,
2. *but at most finitely many* n *with* $\sigma(n) = k$.

Solution 6.3.7.

1. *Let* p *be any prime and* $n = p^{k-1}$. *Then* $\tau(n) = k$ *(How!). Since there are infinitely many primes, therefore there are infinitely many* n *satisfying* $n = p^{k-1}$ *and* $\tau(n) = k$.
2. *Using Problem (6.3.5), we have* $\sigma(n) > n$, $\forall n$. *If* $\sigma(n) = k$, *for any* k, *then* k *serves as an upper bound to* n. *In fact, for any* $n \geq k$, $\sigma(n) > k$ *(How!). Hence there are at most* $k(> 1)$ *integers such that* $\sigma(n) \leq k$.

Problem 6.3.8. *If pair of successive odd integers* q *and* $q + 2$ *that are both primes, called twin primes. For these* q *and* $q+2$ *prove that* $\sigma(q+2) = \sigma(q)+2$.

Solution 6.3.8. *The only divisors for any prime* q *are* 1 *and* q *itself. Therefore* $\sigma(q) = q + 1$. *Thus* $\sigma(q + 2) = q + 3$ *and* $\sigma(q) + 2 = q + 3$. *Thus* q *and* $q + 2$ *together implies* $\sigma(q + 2) = \sigma(q) + 2$.

Problem 6.3.9. *Let* f *and* g *be multiplicative functions that are not identically zero and have the property that* $f(p^k) = g(p^k)$ *for each prime* p *and* $k \geq 1$. *Prove that* $f = g$.

Solution 6.3.9. *Let* $n > 1$ *be an arbitrary integer with prime factorization given by* $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$. *Then*

$$\begin{aligned} f(n) &= f(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}) \\ &= f(q_1^{t_1}) f(q_2^{t_2}) \cdots f(q_s^{t_s}) \\ &= g(q_1^{t_1}) g(q_2^{t_2}) \cdots g(q_s^{t_s}) \\ &= g(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}) \\ &= g(n). \end{aligned}$$

In particular, if $n = 1$ then $f(1) = g(1) = 1$. Hence combining all $f = g$ holds.

Problem 6.3.10. *For any integer $z > 1$, prove that there exist integers z_1 and z_2 for which $\tau(z_1) + \tau(z_2) = z$.*

Solution 6.3.10. *If z is prime, then $\tau(z) = 2$. Since $tau(1) = 1$, taking $z_1 = z_2 = 1$ gives $\tau(z_1) + \tau(z_2) = \tau(z)$.*

If z is composite, let $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be its prime factorization. Then at least one of $t_i \geq 2$. Let $q_j^{t_j}$ be that factor. Therefore

$$\begin{aligned}\tau(z) &= (t_1 + 1)(t_2 + 1) \cdots (t_j + 1) \cdots (t_s + 1)\\ &= t_j (t_1 + 1)(t_2 + 1) \cdots (t_s + 1) + (t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\end{aligned}$$

Let $z_1 = q_1^{t_1} q_2^{t_2} \cdots q_j^{t_j - 1} \cdots q_s^{t_s}$ and $z_2 = \dfrac{z}{q_j^{t_j}} = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$, where $q_i \neq q_j$. Hence

$$\begin{aligned}\tau(z_1) &= (t_1 + 1)(t_2 + 1) \cdots (t_j - 1 + 1) \cdots (t_s + 1)\\ &= t_j (t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\\ \tau(z_2) &= (t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\end{aligned}$$

Combining we obtain, $\tau(z_1) + \tau(z_2) = \tau(z)$.

Problem 6.3.11. *For any integer $z \geq 1$, prove that $\sum_{d|z} \tau(d)^3 = \left(\sum_{d|z} \tau(d)\right)^2$.*

Solution 6.3.11. *Since $\tau(z)$ is a multiplicative function, therefore $[\tau(mn)]^3 = [\tau(m)\tau(z)]^3 = [\tau(m)]^3[\tau(z)]^3$. This shows $\tau(z)^3$ is a multiplicative function. Hence by virtue of Theorem 6.2.4, $F(z) = \sum\limits_{d|z} \tau(d)^3$ is multiplicative. Moreover, the multiplicative property of $G(z) = \sum_{d|z} \tau(d)$ implies $H(z) = G(z)^2$ is multiplicative(Why!).*

Let $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be its prime factorization. Since F and H both are multiplicative, for $z = q^t$, $F(z) = H(z)$ holds. By similar reasoning, the relation $F(z) = H(z)$ holds true for $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$. Therefore considering $z = q^t$ and applying Theorem 6.2.1, all the divisors of z are given by $1, q, q^2, \ldots, q^t$. Thus

$$\begin{aligned}\sum_{d|q^t}\tau(d)^3 &= \tau(1)^3+\tau(q)^3+\ldots+\tau(q^t)^3\\ &= 1+(1+1)^3+(2+1)^3+\ldots+(t+1)^3\\ &= 1+2^3+3^3+\ldots+(t+1)^3\\ &= \left[\frac{(t+1)(t+2)}{2}\right]^2.\\ \Big(\sum_{d|q^t}\tau(d)\Big)^2 &= [\tau(1)+\tau(q)+\ldots+\tau(q^t)]^2\\ &= [1+(1+1)+(2+1)+\ldots+(t+1)]^2\\ &= \left[\frac{(t+1)(t+2)}{2}\right]^2.\end{aligned}$$

$$\textit{Hence}\ \sum_{d|q^t}\tau(d)^3 = \Big(\sum_{d|q^t}\tau(d)\Big)^2,\ \ \textit{so}\ \ F(z)=H(z)\ \ \textit{for}\ \ z=q^t.$$

Problem 6.3.12. *Given $z \geq 1$, let $\sigma_s(z)$ denote the sum of the sth powers of the positive divisors of z; that is, $\sigma_s(z) = \sum_{d|z} d^s$. Prove that*

$$\sigma_s(z) = \left(\frac{q_1^{s(t_1+1)}-1}{q_1^s-1}\right)\left(\frac{q_2^{s(t_2+1)}-1}{q_2^s-1}\right)\cdots\left(\frac{q_r^{s(t_1+1)}-1}{q_r^s-1}\right),$$

$z = q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}$ being the prime factorization of z.

Solution 6.3.12. *By virtue of Theorem 6.2.1, all divisors of z are of the form*

$$q_1^{a_1}q_2^{a_2}\ldots q_r^{a_r},\ 0 \leq a_i \leq t_i.$$

Therefore all the sth powers of the divisors of z are of the form

$$q_1^{a_1 s}q_2^{a_2 s}\ldots q_r^{a_r s}.$$

Let us consider the product of sums

$$(1+q_1^s+q_1^{2s}+q_1^{t_1 s})\ldots(1+q_r^s+q_r^{2s}+q_r^{t_r s}).$$

Each positive divisor to the sth power occurs only once as a term in the expansion of the product. Therefore

$$\sigma_s(z) = (1+q_1^s+q_1^{2s}+q_1^{t_1 s})\ldots(1+q_r^s+q_r^{2s}+q_r^{t_r s}).$$

Applying the formulae for the sum of the finite geometric series,

$$(1 + q_i^s + q_i^{2s} + q_i^{t_1 s}) = \left(\frac{q_i^{s(t_i+1)} - 1}{q_i^s - 1}\right),$$
$$\Rightarrow \sigma_s(z) = \left(\frac{q_1^{s(t_1+1)} - 1}{q_1^s - 1}\right)\left(\frac{q_2^{s(t_2+1)} - 1}{q_2^s - 1}\right)\cdots\left(\frac{q_r^{s(t_1+1)} - 1}{q_r^s - 1}\right).$$

Problem 6.3.13. *For any positive integer z, show that*

$$\sum_{d|z}\sigma(d) = \sum_{d|z}\frac{z}{d}\tau(d).$$

Solution 6.3.13. *Let $H(n) = \sum_{d|z}\frac{z}{d}\tau(d)$. Then*

$$\begin{aligned}
G(mn) &= \sum_{d|mn}\frac{mn}{d}\tau(d)\\
&= \sum_{d_1|m, d_2|n}\frac{mn}{d_1 d_2}\tau(d_1 d_2)\\
&= \sum_{d_1|m, d_2|n}\frac{mn}{d_1 d_2}\tau(d_1)\tau(d_2)\\
&= \sum_{d_1|m, d_2|n}\frac{m}{d_1}\tau(d_1)\frac{n}{d_2}\tau(d_2),\ \textit{since } \tau(d) \textit{ is multiplicative}\\
&=\Big(\sum_{d_1|m, d_2|n}\frac{m}{d_1}\tau(d_1)\Big)\Big(\sum_{d_1|m, d_2|n}\frac{n}{d_2}\tau(d_2)\Big)\\
&= G(m)G(n).
\end{aligned}$$

Hence G is a multiplicative function. Using multiplicative property of $\sigma(d)$ the function $F(n) = \sum_{d|z}\sigma(d)$ is multiplicative.

Next let $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be its prime factorization. To prove

$$\begin{aligned}
F(z) &= F(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s})\\
&= F(q_1^{t_1})F(q_2^{t_2})\cdots F(q_s^{t_s})\\
&= G(q_1^{t_1})G(q_2^{t_2})\cdots G(q_s^{t_s})\\
&= G(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s})\\
&= G(z),
\end{aligned}$$

its suffices to show $F(q^t) = G(q^t)$. *Now*

$$\begin{aligned} F(q^t) &= \sum_{d|q^t} \sigma(d) \\ &= q^0 + (q^0 + q^1) + \ldots + (q^0 + q^1 + \ldots + q^s) \\ &= (t+1)q^0 + tq^1 + \ldots + (1)q^t \\ &= (1)q^t + \cdots + tq^1 + (t+1). \qquad (6.3.2) \\ G(q^t) &= \sum_{d|q^t} \frac{q^t}{d}\tau(d) \\ &= \frac{q^t}{q^0}\tau(q^0) + \frac{q^t}{q^1}\tau(q^1) + \ldots + \frac{q^t}{q^t}\tau(q^t) \\ &= (1)q^t + 2q^{t-1} + \ldots + tq + (t+1) \\ &= F(q^t), \text{ by (6.3.2)}. \end{aligned}$$

Problem 6.3.14. *For any integer* $z \geq 1$, *prove that* $\tau(z) \leq 2\sqrt{z}$.

Solution 6.3.14. *If* $d|z$, *then either* $d \leq \sqrt{z}$ *or* $\frac{z}{d} \leq \sqrt{z}$. *For if* $d > \sqrt{z}$ *or* $\frac{z}{d} > \sqrt{z}$, *then*

$$d \cdot \frac{z}{d} = z > \sqrt{z}\sqrt{z} = z,$$

a contradiction. Let $d_1, d_2, \ldots, d_t$ *be the divisors of* z *where* $d_1 < d_2 < \ldots < d_t$. *Clearly,* $d_1 = 1, d_t = z$. *Now* $d_i|z \Rightarrow z|d_i$ *and so* $z|d_i$ *must be one of* d_i. *pairing the divisors in such a way that* $d_id_j = z$, *where* $d_j = z|d_i$. *So either* $d_i \leq d_j$ *or* $d_i \geq d_j$.

Case(i) t *is even: Then we have* $\frac{t}{2}$ *unique pairs* $\{d_i, d_j\}(d_i \neq d_j)$ *such that* $d_id_j = z$. *Let us arrange every pair in such a way that* $d_i < d_j$. *Let* $d_{t'}$ *be the largest of the* d_i. *Since there are* $\frac{t}{2}$ *unique pairs, it must be* $\frac{t}{2} \leq d_{t'}$. *But* $\tau(z) = t$ *and from above* $d_{t'} \leq \sqrt{z}$. *Thus,*

$$\frac{\tau(z)}{2} \leq \sqrt{z} \Rightarrow \tau(z) \leq 2\sqrt{z}.$$

Case(ii) t *is odd: Then we have* $\frac{t-1}{2}$ *unique pairs* $\{d_i, d_j\}(d_i \neq d_j)$ *such that* $d_id_j = z$ *and one pair* $\{d_r, d_r\}$ *where* $d_rd_r = z$. *Let us arrange every unique pair in such a way that* $d_i < d_j$. *Let* $d_{t'}$ *be the largest of the* d_i. *Now if* $d_r < d_{t'}$, *considering the pair* $\{d_j, d_{t'}\}$ *and applying the definition of* $d_{t'}$, *we obtain*

$$d_{t'} < d_j, \text{ and } d_{t'}d_j = z.$$

Hence $d_r < d_j \Rightarrow d_r d_r < d_r d_j \Rightarrow z < z$, *a contradiction. Hence* $d_r > d_{t'}$. *But* $d_r^2 = z \Rightarrow d_r = \sqrt{z}$. *As in Case(i),*

$$\frac{t-1}{2} \leq d_{t'} \text{ and } t = \tau(z).$$

Therefore

$$\frac{\tau(z)-1}{2} \leq d_{t'} < d_r = \sqrt{z},$$

which further implies

$$\frac{\tau(z)-1}{2} \leq \sqrt{z}, \tau(z) - 1 < 2\sqrt{z} \Rightarrow \tau(z) \leq 2\sqrt{z}.$$

Hence $\tau(z) \leq 2\sqrt{z}$ *for both even and odd cases.*

Problem 6.3.15. *Find the form of all positive integers* n *satisfying* $\tau(n) = 10$. *What is the smallest positive integer for which this is true?*

Solution 6.3.15. *Let* $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ *be the prime factorization of* n. *Then* $\tau(n) = (t_1+1)(t_2+1)\ldots(t_s+1)$. *If* $\tau(n) = 10$, *then the possibilities are* 10 *and* 5×2. *This implies* $t_1 + 1 = 10$ *or* $(t_1+1)(t_2+1) = 5 \times 2$. *Thus* $n = q_1^9$ *or* $n = q_1^4 q_2$ *where* q_1, q_2 *are distinct primes.*

The smallest of such integers would be 2^9 *or* $2^4 \times 3$ *or* $3^4 \times 2$. *Then the smallest among them is* $2^4 \times 3 = 48$.

6.4 Mobiüs μ-function

In this article, we will discuss an important arithmetic function called Mobiüs μ-function with some of its properties.

Definition 6.4.1. *For a positive integer* n, *define* μ *by the rules*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } p^2 | n \text{ for some prime } p; \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i\text{'s are distinct primes.} \end{cases}$$

For example we see that $\mu(2) = -1, \mu(3) = -1, \mu(4) = 0$. Thus if we choose $n = 15 = 3 \times 5$ then $\mu(15) = \mu(3 \cdot 5) = (-1)^2 = 1$. Now in the next theorem we are going to discuss the multiplicative property on Mobiöus μ function.

Theorem 6.4.1. *The function* μ *is a multiplicative function.*

Proof. Its suffices to show that for any two relatively prime integers m and n, $\mu(mn) = \mu(m)\mu(n)$. This is trivial for $m = n = 1$. Now if we choose either $p^2|n$ or $p^2|m$ then $p^2|mn$. Therefore $\mu(mn) = 0 = \mu(m)\mu(n)$. This case is also trivial. Now we assume m, n to be square-free integers. Then $m = p_1 p_2 \cdots p_a$, $n = q_1 q_2 \cdots q_b$ where p_i and q_j are all distinct, then $\mu(mn) = \mu(p_1 p_2 \cdots p_a q_1 q_2 \cdots q_b) = (-1)^{a+b} = (-1)^a(-1)^b = \mu(m)\mu(n)$. This proves that μ is a multiplicative function. $\square$

Now from the above theorem we can see that both m and n are divisors of mn. A natural question arises how this function behaves with divisors of any integers. If $n = 1$ then the only divisor is $d = 1$ therefore $\sum_{d|1} \mu(d) = \mu(1) = 1$. So we have to discuss the divisors for those $n > 1$ and for that we need to apply the formula $F(n) = \sum_{d|n} \mu(d)$ which has already been discussed in the first section of this chapter. Our next theorem illustrates the clarification of this discussion.

Theorem 6.4.2. *For each positive integer*

$$n \geq 1, \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n > 1. \end{cases}$$

where d is positive divisors of n.

Proof. The assertion is obvious if $n = 1$, then $\sum_{d|n} \mu(d) = \mu(1) = 1$. We proceed by mathematical induction on the number of different prime factors of n when $n > 1$ and if $n = p^\alpha$, then

$$\sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \ldots + \mu(p^\alpha) = 1 + (-1) = 0.$$

Since μ is multiplicative, using Theorem 6.2.4, F is also so. Thus if

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r},$$

then

$$\sum_{d|n} \mu(d) = \sum_{d|p_1^{\alpha_1}} \mu(d) \sum_{d|p_2^{\alpha_2}} \mu(d) \cdots \sum_{d|p_r^{\alpha_r}} \mu(d) = 0.$$

$\square$

To illustrate the above theorem let us consider $n = 12$, the divisors of 12 are $1, 2, 4, 3, 6$ and 12. Thus the required sum is,

$$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$
$$= 1 + (-1) + (-1) + 0 + (-1)^2 + 0 = 0.$$

In mathematics, the classic Mobi*üs* inversion formula was introduced into number theory on 1832 by August Ferdinand Mobi*üs*, stated as follows:

Theorem 6.4.3. *Mobiüs Inversion Formulae: Let F and f be two number theoretic functions related by the formulae $F(n) = \sum_{d|n} f(d)$ and, $f(n) = \sum_{d|n} \mu(d)F(n/d)$ for every n. If either of them is true then they satisfy both the formulae.*

Proof. Let us first choose that $F(n) = \sum_{d|n} f(d)$, then

$$\begin{aligned}\sum_{d|n} \mu(d)F(n|d) &= \sum_{dd'=n} \mu(d)F(d'), \ \text{ since integer } d' \text{ is the quotient when } d|n \\ &= \sum_{dd'=n} \mu(d) \sum_{e|d'} f(e), \ \text{ since } F(n) = \sum_{d|n} f(d) \text{ for each } n \\ &= \sum_{dek=n} \mu(d)f(e), \ \text{ as integer } k \text{ is the quotient when } e|d' \\ &= \sum_{ek'=n} f(e) \sum_{d|k'} \mu(d), \ \text{ taking integer } k' = dh \text{ for some integer } h.\end{aligned}$$

Now if $k' = 1$, then using the Theorem 6.4.2 we have, $\sum_{d|k'} \mu(d) = 1$. Therefore $\sum_{d|n} \mu(d)F(n|d) = f(n)$.

Conversely let, $f(n) = \sum_{d|n} \mu(d)F(n/d)$ holds. Then,

$$\begin{aligned}\sum_{d|n} f(d) &= \sum_{d|n}\left(\sum_{d'|d} \mu(d)F\left(\frac{d}{d'}\right)\right) \\ &= \sum_{d'pq=n} \mu(d')F(p), \quad \text{Since } d = d'p, n = qd = d'pq \text{ for some integer } p \text{ and } q \\ &= \sum_{ph'=n} F(p) \sum_{d'|h'} \mu(d') \quad \text{where, } h' = d'q \text{ for some integer } h'.\end{aligned}$$

Now again applying Theorem 6.4.2 we have, $\sum_{d'|h'} \mu(d') = 1$ if $h' = 1$ holds. Therefore $\sum_{d|n} f(d) = F(n)$. □

Before going to the last result of this section we see from Theorem 6.2.4 that if $f(n)$ is multiplicative then $F(n)$ is also multiplicative for each integer n. Now the question arises, is the converse assertion also true. The following theorem illustrates the answer of it.

Theorem 6.4.4. *If F is a multiplicative function and $F(n) = \sum_{s|n} f(s)$ then f is also multiplicative for any integer n and positive divisor s.*

Proof. Let m, n be relatively prime positive integers then any divisor s of mn can be uniquely written as $s = s_1 s_2$ where $s_1|m$ and $s_2|n$ where $\gcd(s_1, s_2) = 1$. Now by inversion formulae we have,

$$\begin{aligned} f(mn) = \sum_{s|mn} \mu(s) F\left(\frac{mn}{s}\right) &= \sum_{s_1|m, s_2|n} \mu(s_1 s_2) F\left(\frac{mn}{s_1 s_2}\right) \\ &= \left(\sum_{s_1|m} \mu(s_1) F\left(\frac{m}{s_1}\right)\right) \left(\sum_{s_2|n} \mu(s_2) F\left(\frac{n}{s_2}\right)\right) \\ &= f(m) f(n) \text{ (Why!).} \end{aligned}$$

This proves the theorem. □

6.5 Worked out Exercises

Problem 6.5.1. *Suppose a function Λ is defined by*

$$\Lambda(n) = \begin{cases} \ln p, & \textit{if } n = p^k, \textit{ where } p \textit{ is a prime and } k \geq 1; \\ 0, & \textit{otherwise.} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = -\sum_{d/n} \mu(d) \ln d$.

Solution 6.5.1. *Let $n = p^k$. Then*

$$\sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = \mu(p^k) \ln 1 + \mu(p^{k-1}) \ln p + \ldots + \ldots + \mu(p^{k-i}) \ln p^i + \ldots + \mu(p^0) \ln p^k.$$

Case(i) *If $k = 1$, then $\sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = \ln p$ (Verify!).*

Case(ii) *If $k > 1$, then $\mu(p^{k-i}) = 0$ except for $i = 1, 2$. Then the sum is same as $k = 1$.*

Hence $\sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = \ln p = \Lambda(n)$. *Next*

$$\sum_{d/n} \mu(d) \ln d = \mu(p^0) \ln 1 + \mu(p^1) \ln p^1 + \ldots + \ldots + \mu(p^i) \ln p^i + \ldots + \mu(p^k) \ln p^k.$$

For $k > 1$, $\mu(p^k) = 0$ *implies* $\sum_{d/n} \mu(d) \ln d = -\ln p$ *for all* k. *Hence*

$$\sum_{d/n} \mu(d) \ln d = -\Lambda(n).$$

Remark 6.5.1. *The function* Λ *in the Problem 6.5.1 is known as Mangoldt function.*

Problem 6.5.2. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ *be the prime factorization of the integer* $n > 1$. *If* f *is a multiplicative function that is not identically zero, prove that*

$$\sum_{d/n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_s)).$$

Solution 6.5.2. *Since* μ *and* f *is multiplicative, therefore* μf *is also so(Why!). By virtue of Theorem 6.2.4,* $F(n) = \sum_{d/n} \mu(d) f(d)$ *is multiplicative. Consider,*

$$\begin{aligned} F(p^k) &= \sum_{d/p^k} \mu(d) f(d) \\ &= \mu(1) f(1) + \mu(p) f(p) + \cdots + \mu(p^k) f(p^k) \\ &= \mu(1) f(1) + \mu(p) f(p) (Why!) \\ &= 1 f(1) + (-1) f(p) \\ &= f(1) - f(p). \end{aligned}$$

Since for a multiplicative function not identically zero, therefore $f(1) = 1$ *implies* $F(p^k) = 1 - f(p)$. *Thus*

$$\sum_{d/n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_s)).$$

Problem 6.5.3. *Let* $S(n)$ *denote the number of square-free divisors of* n. *Prove that*

$$S(n) = \sum_{d/n} |\mu(d)| = 2^{\omega(n)},$$

where $\omega(n)$ *is the number of distinct prime divisors of* n.

Solution 6.5.3. *Consider,*

$$|\mu(n)| = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } p^2 | n, \ p \text{ being prime }; \\ 1, & \text{if } n = p_1 p_2 \cdots p_s, \ p_i \text{ being distinct.} \end{cases}$$

Let $\gcd(m, n) = 1$. *Then* $|\mu(1)| = 1$. *If* $m = 1$, *then* $|\mu(mn)| = |\mu(n)| = |\mu(m)||\mu(n)|$. *If* $p^2|m$, *then* $p^2|mn$ *implies* $|\mu(mn)| = 0$ *and* $|\mu(m)| = 0$. *Hence* $|\mu(mn)| = |\mu(m)\mu(n)|$. *Assume, both* m, n *are square-free. Let* $m = p_1 p_2 \cdots p_s$, $n = q_1 q_2 \cdots q_r$ *with* $p_i \neq q_j$ *as* $\gcd(m, n) = 1$. *Clearly,* $|\mu(m)| = |\mu(n)| = |\mu(mn)| = 1$. *Hence,* $|\mu(mn)| = |\mu(m)||\mu(n)|$. *This shows* $|\mu(n)|$ *is multiplicative. Using Theorem (6.2.4),* $S(n) = \sum_{d/n} |\mu(n)|$ *is also so.*
Now, consider $n = p^k$. *The divisors of* n *are* $1, p, p^2, \ldots, p^k$. *Therefore*

$$S(n) = \sum_{d/n} |\mu(n)| = 2.$$

The number of square-free divisors of p^k *is* 2 *and is defined by* $\sum_{d/n} |\mu(n)|$. *Given that,* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *From Theorem 6.2.1, all the square divisors of* n *are represented by* $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, $0 \leq a_j \leq 1$. *Here the number of square-free divisors of* p_i *is* 2, *which are* 1 *&* p_i. *It is true for all* $i = 1, 2, 3, \ldots, s$. *Hence the total number of square-free integers is* $2^s = 2^{\omega(n)}$, *where* $\omega(n)$ *is the number of distinct prime divisors of* n. *Therefore*

$$\begin{aligned} S(n) &= S(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= S(p_1^{k_1}) S(p_2^{k_2}) \cdots S(p_s^{k_s}) \\ &= \Bigg(\sum_{d/p_1^{k_1}} |\mu(p_1^{k_1})| \Bigg) \cdots \Bigg(\sum_{d/p_1^{k_1}} |\mu(p_s^{k_s})| \Bigg) \\ &= 2^s = 2^{\omega(n)}. \end{aligned}$$

Problem 6.5.4. *The Liouville* λ *function defined as*

$$\lambda(z) = \begin{cases} (-1)^{t_1 + t_2 + \ldots + t_s}, & \text{if } z = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}, \ z > 1; \\ 1, & \text{if } z = 1. \end{cases}$$

1. *Prove that* λ *is multiplicative.*

2. *For some positive integer* z, *prove that*

$$\sum_{d/z} \lambda(d) = \begin{cases} 1, & \text{if } z = k^2 \text{ for some integer } k; \\ 0, & \text{Otherwise.} \end{cases}$$

Solution 6.5.4. 1. *Let us consider two positive integers* z *and* k *with* $\gcd(z, k) = 1$, *where* $z = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, $k = q_1^{v_1} q_2^{v_2} \cdots q_r^{v_r}$.

Now $zk = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s} q_1^{v_1} q_2^{v_2} \cdots q_r^{v_r},\ p_i \neq q_j$. *Hence*

$$\begin{aligned}\lambda(zk) &= (-1)^{t_1+t_2+\ldots+t_s+v_1+v_2+\ldots+v_r}\\ &= (-1)^{t_1+t_2+\ldots+t_s} \cdot (-1)^{v_1+v_2+\ldots+v_r}\\ &= \lambda(z)\lambda(k).\end{aligned}$$

This shows that $\lambda(z)$ *is multiplicative function.*

2. *Let* $F(z) = \sum_{d/z} \lambda(d)$. *Then by Theorem 6.2.4,* F *is multiplicative. Let* $z = p^t$. *Then,*

$$\begin{aligned}F(z) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \ldots + \lambda(p^t)\\ &= 1 + (-1) + (-1)^2 + (-1)^3 + \ldots + (-1)^{t-1} + (-1)^t.\end{aligned}$$

Now, two cases may arise:

Case(i) t *is even: Then* $z = p^{2\omega}$, $t = 2\omega$ *for some positive integer* ω. *Therefore, taking* $m = p^{\omega}$, *we obtain* $z = m^2$. *Also,* $F(z) = 1$.

Case(ii) t *is odd: Then we have* $F(z) = F(p^t) = 0$. *Let* $n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$. *Since* F *is multiplicative, therefore* $F(n) = F(p_1^{t_1})F(p_2^{t_2}) \cdots F(p_s^{t_s})$. *If* $z = k^2$ *for some integer* k, *then all the* t_i*'s are even. So* $F(p_i^{t_i}) = 1$ *and consequently,* $F(z) = 1$. *Again, if any of the* t_i *is odd, then* $F(p_i^{t_i}) = 0$. *So* $F(z) = 0$.

Problem 6.5.5. *For every integer* $z \geq 3$, *prove that* $\sum_{t=1}^{z} \mu(t!) = 1$.

Solution 6.5.5. *Here* $\mu(4) = 0$*(Why!). If* $n \geq 4$, *then* $z!$ *would contain* 4 *as a factor. Since* μ *is multiplicative, therefore for* $z \geq 4$, $\mu(z!) = 0$. *So, only case need to consider is* $z = 3$. *Now* $\mu(1) = 1$, $\mu(2) = -1 = \mu(3)$ *implies* $\sum_{t=1}^{3} \mu(t!) = 1 + (-1) + 1 = 1$.

6.6 Greatest Integer Function

In this section we are going to discuss a special type of arithmetic function called greatest integer function. The domain of definition of this function is the set of real numbers and the range set is the set of integers. This function is very much useful for calculating continued fractions. The definition of the function as follows.

Definition 6.6.1. *For an arbitrary real number* x, *the largest integer less than or equal to* x *and denoted by* $[x]$ *is called the greatest integer function.*

For an example we have $[2.2] = 2$ and $[-2.2] = -3$. Here for every real number x, there is a unique real number θ such that $x = [x] + \theta, 0 \leq \theta < 1$, where θ is the fractional part of x. This θ sometimes denoted as $\{x\}$ such that $x = [x] + \{x\}, \forall x \in \mathbb{R}$. Actually the greatest integer function for any real number x follows the inequality $x - 1 < [x] \leq x$. In our next proposition we have shown division algorithm using this inequality.

Proposition 6.6.1. *For any $x \in \mathbb{R}$, prove division algorithm by the inequality $x - 1 < [x] \leq x$.*

Proof. Let $q = \left[\frac{m}{n}\right]$ and $r = m - n\left[\frac{m}{n}\right]$, clearly $m = nq + r$ and we will show that the remainder satisfies the above inequality. As $\dfrac{m}{n} \in \mathbb{R}$ then $\left(\frac{m}{n}\right) - 1 < \left[\frac{m}{n}\right] \leq \frac{m}{n}$. Now multiplying by $-n$ the above inequality and changing the order of inequality we have, $-m \leq -n\left[\frac{m}{n}\right] < n - m$. Adding m we get, $0 \leq m - n\left[\frac{m}{n}\right] < n \Rightarrow 0 \leq r < n$. We are to show this q and r are unique. Let us assume that they are not unique then $m = nq_1 + r_1 = nq_2 + r_2$ for q_1, q_2 are quotients and $0 \leq r_1, r_2 < n$ where r_1, r_2 are remainders. Now subtracting these two equations we have, $0 = n(q_1 - q_2) + (r_1 - r_2)$ thus $(r_2 - r_1) = n((q_1 - q_2))$ which implies $n | (r_1 - r_2)$ but this is possible only if $r_1 - r_2 = 0$. Therefore $r_1 = r_2$ and $q_1 - q_2$, which shows that q is unique quotient and r is unique remainder. $\square$

Now we will discuss few properties related to this greatest integer function.

Proposition 6.6.2. *For any $x, y \in \mathbb{R}$ and $m \in \mathbb{Z}$, the greatest integer function satisfies following properties:*

(i) $[x + m] = [x] + m$

(ii) $[x] + [-x] = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \in \mathbb{R} \setminus \mathbb{Z}. \end{cases}$

(iii) $[x] + [y] \leq [x + y]$

(iv) $\left[\dfrac{x}{m}\right] = \left[\dfrac{[x]}{m}\right]$.

Proof. Let $x = n + \theta$ for $n \in \mathbb{Z}, 0 \leq \theta < 1$,

(i) Here, $x + m = (n + m) + \theta$ where $m + n \in \mathbb{Z}$, $0 \leq \theta < 1$. Thus

$$[x + m] = n + m = [x] + m.$$

(ii) Here,

$$-x = \begin{cases} -n - \theta, & 0 \geq -\theta > -1; \\ (-n - 1) + (1 - \theta), & 0 < 1 - \theta \leq 1. \end{cases}$$

Therefore

$$[-x] = \begin{cases} -(1+n), & \text{if } 1-\theta \neq 1; \\ -n, & \text{if } 1-\theta = 1. \end{cases}$$

This proves that

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

(iii) Let $y = r + \theta'$, $r \in \mathbb{Z}$, $0 \leq \theta' < 1$. Therefore

$$x + y = (n + r) + (\theta + \theta'), 0 \leq (\theta + \theta') < 2.$$

Thus we have,

$$[x + y] = \begin{cases} n + r, & \text{if } 0 \leq \theta + \theta' < 1; \\ n + r + 1, & \text{if } \theta + \theta' \geq 1. \end{cases}$$

Hence

$$[x] + [y] = n + r \leq [x + y].$$

(iv) Now let $\dfrac{x}{m} = z + \widetilde{\theta}$, $z \in \mathbb{Z}$ and $0 \leq \widetilde{\theta} < 1$. Then we have

$$x = mz + m\widetilde{\theta},\ mz \in \mathbb{Z} \text{ and } 0 \leq m\widetilde{\theta} < m.$$

Therefore

$$\left[\frac{[x]}{m}\right] = [z] = z \text{ as } x \in \mathbb{Z}.$$

Hence

$$\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right].$$

□

Now we are going to the application part of this greatest integer function. For that we choose an integer 7 whose factorial is $7! = 1{\cdot}2{\cdot}3{\cdot}4{\cdot}5{\cdot}6{\cdot}7 = 2^4{\cdot}3^2{\cdot}5{\cdot}7$. Here we can see that the highest power of 2 which divides 7! is 4. We can find the exponent of any prime which occurs in prime factorization of any factorial of an integer by greatest integer function using the next theorem.

Theorem 6.6.1. *If p is a prime then,* $\displaystyle\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$ *is the exponent of p appearing in the prime factorization of $n!$.*

Proof. If $p > n$ then p does not appear in the prime factorization of $n!$. Thus we have $p \leq n$. Among the first n positive integers those who are divisible by p are $p, 2p, 3p \cdots \left[\frac{n}{p}\right]p$. Thus there exists exactly $\left[\frac{n}{p}\right]$ multiples of p occuring in the product of $n!$. Among those integers $p, 2p, 3p \cdots \left[\frac{n}{p}\right]p$ there are $\left[\frac{n}{p^2}\right]$ integers which are again divisible by p^2 and they are $p^2, 2p^2, 3p^2 \cdots \left[\frac{n}{p^2}\right]p^2$. After continuing these steps finitely many times we get the total number of times p divides $n!$ is $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$. □

Now we will illustrate this theorem by means of an example.

Example 6.6.1. *Let us take* $n = 10$ *and* $p = 2$ *then there are* $\left[\frac{10}{2}\right] = 5$ *integers which are divisible by* $p = 2$ *and they are* $2, 4, 6, 8, 10$. *Among those integers there are* $\left[\frac{10}{2^2}\right] = 2$ *integers which are divisible by* 4 *and they are* $4, 8$. *Now among these two integers there are* $\left[\frac{10}{2^3}\right] = 1$ *integers which are divisible by* 8 *and it is* 8 *itself.Therefore the total number is* $\left[\frac{10}{2}\right] + \left[\frac{10}{2^2}\right] + \left[\frac{10}{2^3}\right] = 8$.*Now* $10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$. *So the highest power of* 2 *is* 8.

In our next two results we are going to find some common well known facts of mathematics by using the last theorem.

Theorem 6.6.2. *If* n *and* r *are positive integers with* $1 \leq r < n$, *then the binomial coefficient* $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ *is an integer.*

Proof. For proving $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ is an integer we are only to show $n!$ is divisible by $r!(n-r)!$. Now from the Theorem 6.6.1 we have the exponent of highest power of prime p that divides $n!$ is $\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$ and the highest power of prime p that divides $\frac{n!}{r!(n-r)!}$ is $\sum_{i=1}^{\infty}\left[\frac{r}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{(n-r)}{p^i}\right]$. Again from the Proposition 6.6.2(iii) we have $[a + b] \geq [a] + [b]$ for any two integers a, b. Then we have,

$$\left[\frac{n}{p^i}\right] \geq \left[\frac{r}{p^i}\right] + \left[\frac{(n-r)}{p^i}\right].$$

Taking the summation we get,

$$\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right] \geq \sum_{i=1}^{\infty}\left[\frac{r}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{(n-r)}{p^i}\right].$$

From the above inequality it follows that p occurs in the numerator of $\frac{n!}{r!(n-r)!}$ at least as many times in the denominator. As p is arbitrary so $r!(n-r)!$ must divide $n!$. Thus $\frac{n!}{r!(n-r)!}$ is an integer. $\square$

Corollary 6.6.1. *For any positive integer r, the product of r consecutive integers is divisible by $r!$.*

Proof. Here we can assume the product of r consecutive integers as $n(n-1)\cdots(n-r+1)$ where n is largest. Here $n(n-1)\cdots(n-r+1) = \frac{n!}{r!(n-r)!} = \left(\frac{n!}{r!(n-r)!}\right) \times r!$ and from the Theorem 6.6.2 we know that $\frac{n!}{r!(n-r)!}$ is an integer.This proves the assertion of this corollary. $\square$

In our later part of discussion on greatest integer function we have shown some valuable relations between this function and other arithmetic functions. Their relationship comes out as,

Theorem 6.6.3. *Let f and F be two arithmetic functions such that $F(n) = \sum_{d|n} f(d)$ where n is a positive integer. Then for any positive integer N, $\sum_{n=1}^{N} F(n) = \sum_{m=1}^{N} f(m)\left[\frac{N}{m}\right]$.*

Proof. We are going to start the theorem by the form of $F(n)$. Taking the sum over this function we have $\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N}\sum_{d|n} f(d)$. Here we are to collect the terms with equal values of $f(d)$. Since each integer divides itself then the assertion for a fixed positive integer $m \leq N$, the term $f(m)$ appears in $\sum_{d|n} f(d)$ if and only if m is a divisor of n is possible. Now to calculate the number of terms in the sum $\sum_{d|n} f(d)$ in which $f(m)$ occurs as a term, it is sufficient to find the number of integers from the set $\{1, 2, \cdots N\}$ which are divisible by m.From the Theorem 6.6.1 there are exactly $\left[\frac{N}{n}\right]$ of them. Thus for each m such that $1 \leq m \leq N$, $f(m)$ is a term of the sum $\sum_{d|n} f(d)$ for $\left[\frac{N}{n}\right]$ different positive integers less than or equal to N. Therefore

$$\sum_{n=1}^{N}\sum_{d|n} f(d) = \sum_{m=1}^{N} f(m)\left[\frac{N}{m}\right] = \sum_{n=1}^{N} F(n)$$

This proves the theorem. $\square$

Our next corollary is the immediate application of this theorem on two arithmetic functions $\tau(n)$ and $\sigma(n)$.

Corollary 6.6.2. *If N is a positive integer then,*

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right] \text{ and } \sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} \left(n\left[\frac{N}{n}\right]\right).$$

Proof. We know that $\tau(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$. Now taking $F(n) = \tau(n)$ and $f(n) = 1$, for all $n \in \mathbb{N}$ we have from the Theorem 6.6.3 $\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$. Again taking $F(n) = \sigma(n)$ and $f(n) = n$, for all $n \in \mathbb{N}$ we have from the Theorem 6.6.3 $\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} \left(n\left[\frac{N}{n}\right]\right)$. $\square$

Now to visualize those two forms of $\tau(n)$ and $\sigma(n)$ we will go through an example given below.

Exercise 6.6.1. *Let us consider $N = 4$ then, $\sum_{n=1}^{4} \tau(n) = \tau(1) + \tau(2) + \tau(3) + \tau(4) = 1 + 2 + 2 + 3 = 8$. Now,*

$$\sum_{n=1}^{4} \left[\frac{4}{n}\right] = [4] + [2] + \left[\frac{4}{3}\right] + [1] = 4 + 2 + 1 + 1 = 8.$$

Also,

$$\sum_{n=1}^{4} \sigma(n) = \sigma(1) + \sigma(2) + \sigma(3) + \sigma(4) = 1 + 3 + 4 + 7 = 15$$

and

$$\sum_{n=1}^{4} \left(n\left[\frac{4}{n}\right]\right) = 1[4] + 2[2] + 3\left[\frac{4}{3}\right] + 4[1] = 4 + 4 + 3 + 4 = 15.$$

6.7 Worked out Exercises

Problem 6.7.1. *Find the highest power of* 5 *dividing* 1000!.

Solution 6.7.1.

$$\left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] = 249 \Rightarrow 5^{249} | 1000!.$$

Problem 6.7.2. *For an integer $z \geq 0$, show that* $\left[\dfrac{z}{2}\right] - \left[-\dfrac{z}{2}\right] = z.$

Solution 6.7.2. *By definition, we have the following inequalities:*

$$\frac{z}{2} - 1 < \left[\frac{z}{2}\right] \leq \frac{z}{2} \tag{6.7.1}$$
$$-\frac{z}{2} - 1 < \left[-\frac{z}{2}\right] \leq -\frac{z}{2}. \tag{6.7.2}$$

From equation (6.7.2), we have $-\left[-\frac{z}{2}\right] < \frac{z}{2} + 1$. *Adding the last inequation with (6.7.1), we obtain*

$$\left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] < \frac{z}{2} + \frac{z}{2} + 1 = z + 1 \leq z. \tag{6.7.3}$$

Further, from inequation (6.7.2), we have $\frac{z}{2} \leq -\left[-\frac{z}{2}\right]$. *Adding the foregoing inequation with (6.7.1), we obtain*

$$z \leq \left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] \text{ (How!)}. \tag{6.7.4}$$

Finally, (6.7.3) and (6.7.4) gives $\left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] = z.$

Problem 6.7.3. *If $z \geq 1$ and q is a prime, then find the exponent of the highest power of q that divides* $\dfrac{(2z)!}{(z!)^2}$.

Solution 6.7.3. *For any prime q, let s be the highest power of q that divides $(2z)!$. If $q|z!$, let k be the highest power of q such that $q^k|z!$. Thus $\frac{q^s}{q^k} = q^{s-k}$. So $s-k$ is the highest power of q satisfying $q^{s-k}\Big|\frac{(2z)!}{(z!)}$. Also, $s-2k$ is the highest power of q satisfying $q^{s-k}\Big|\frac{(2z)!}{(z!)^2}$. By virtue of Theorem 6.6.1, the highest power of q dividing $(2z)!$ is $\sum_{k=1}^{\infty}\left[\frac{2z}{q^k}\right]$ and the highest power of q dividing $z!$ is $\sum_{k=1}^{\infty}\left[\frac{z}{q^k}\right]$. Finally, the highest power of q dividing $\dfrac{(2z)!}{(z!)^2}$ is given by,*

$$\sum_{k=1}^{\infty}\left[\frac{2z}{q^k}\right] - 2\sum_{k=1}^{\infty}\left[\frac{z}{q^k}\right] = \sum_{k=1}^{\infty}\left(\left[\frac{2z}{q^k}\right] - 2\left[\frac{z}{q^k}\right]\right).$$

Problem 6.7.4. *Let the positive integer z be written in terms of powers of the prime q so that we have $z = a_k q^k + \ldots + a_2 q^2 + a_1 q + a_0$, where $0 \leq a_i < q$. Find the exponent of the highest power of q appearing in the prime factorization of $z!$.*

Solution 6.7.4. *Before finding the exponent of the highest power of q, let us state and prove the following lemma viz*

Lemma 6.7.1. *For $q > 1, z > 1$;* $\quad (q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^z}\right) < 1.$

Proof. By principle of mathematical induction we are going to prove the above lemma. For $k = 1$, the lemma is trivial(Verify!). Suppose the lemma is true for $z = k$. Then

$$(q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k}\right) < 1.$$

Therefore

$$\begin{aligned}(q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k} + \frac{1}{q^{k+1}}\right) &= (q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k}\right) + \frac{q-1}{q^{k+1}} \\ &= q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} + \frac{1}{q^k} - \frac{1}{q^{k+1}}.\end{aligned}$$

By hypothesis $q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} < 1$, therefore

$$\begin{aligned}q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} + \frac{1}{q^k} - \frac{1}{q^{k+1}} &< 1 + \frac{1}{q^k} - \frac{1}{q^{k+1}} \\ &< 1 - \frac{1}{q^{k+1}} \\ &< 1.\end{aligned}$$

Hence the lemma is true for $z = k + 1$.

Using Theorem 6.6.1 the exponent of the highest power of q appearing in the prime factorization of $z!$ is

$$\begin{aligned}\sum_{i=1}^{\infty}\left[\frac{z}{q^i}\right] &= \left[a_k q^{k-1} + \ldots + a_2 q + a_1 + \frac{a_0}{q}\right] \\ &\quad + \left[a_k q^{k-2} + \ldots + a_2 + \frac{a_1}{q} + \frac{a_0}{q^2}\right] \\ &\quad + \\ &\quad \vdots \\ &\quad + \\ &\quad + \left[a_k + \ldots + \ldots + \frac{a_1}{q^{k-1}} + \frac{a_0}{q^k}\right] \\ &\quad + \left[\frac{a_k}{q} + \ldots + \ldots + \frac{a_1}{q^k} + \frac{a_0}{q^{k+1}}\right].\end{aligned} \tag{6.7.5}$$

In equation (6.7.5), all $0 \le a_i \le q - 1$. Note that $\left[\frac{z}{q^k}\right] q = a_k q = \left[\frac{z}{q^{k-1}}\right] - a_{k-1}$.

Therefore

$$\begin{aligned}
\left[\frac{z}{q^1}\right] q &= z - a_0 \\
\left[\frac{z}{q^2}\right] q &= \left[\frac{z}{q}\right] - a_1 \\
&\vdots \\
\left[\frac{z}{q^{k-1}}\right] q &= \left[\frac{z}{q^{k-2}}\right] - a_{k-2} \\
\left[\frac{z}{q^k}\right] q &= \left[\frac{z}{q^{k-1}}\right] - a_{k-1} \\
0 &= \left[\frac{z}{q^k}\right] - a_k .
\end{aligned}$$

On adding the left and right column entries, we have

$$\left(\left[\frac{z}{q^1}\right] + \left[\frac{z}{q^2}\right] + \ldots + \left[\frac{z}{q^{k-1}}\right] + \left[\frac{z}{q^k}\right]\right)(q-1) = z - (a_0 + a_1 + \ldots + a_k).$$

Hence

$$\sum_{k=1}^{\infty} \left[\frac{z}{q^k}\right] = \frac{z - (a_0 + a_1 + \ldots + a_k)}{q-1}.$$

Problem 6.7.5. *Using Problem 6.7.4, find the exponent of highest power of p dividing $(p^k - 1)!$.*

Solution 6.7.5. *Hint: Here,*

$$\begin{aligned}
p^k - 1 &= (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1) \\
&= (p-1)p^{k-1} + (p-1)p^{k-2} + \ldots + (p-1)p + (p-1).
\end{aligned}$$

Since, p is prime, $0 \leq p-1 \leq p$ so

$$a_{k-1} = p-1,\ a_{k-2} = p-1, \ldots,\ a_1 = p-1,\ a_0 = p-1.$$

Take $z = p^k - 1$ and apply the formulae in Problem 6.7.4.

Problem 6.7.6. *For any positive integer N, verify the formulae:*

$$\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = [\sqrt{N}].$$

Solution 6.7.6. *Let $F(z) = \sum_{d|z} \lambda(d)$, λ being the Liouville function defined in Problem 6.5.4. Taking help of Theorem 6.6.3, we have $\sum_{z=1}^{N} F(z) = \sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right]$.*

Moreover, by Problem (6.5.4) we have

$$F(z) = \begin{cases} 1, & \text{if } z = m^2 \text{ for some integer } m; \\ 0, & \text{Otherwise.} \end{cases}$$

Therefore $\sum_{z=1}^{N} F(z)$ *monitor the number of perfect squares less than or equal to* N *as* F *assigns a value of* 1 *to each* z *that can be expressed as a perfect square. Thus*

$$\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = \text{Number of squares} \leq N.$$

Next let us consider, $[\sqrt{N}]$ *and perfect squares, which are* $1^2, 2^2, 3^2$, *and so on. For any* $N = m^2$, *there are exactly* m *perfect squares(positive integers) less than or equal to* N. *Suppose* $[\sqrt{N}]$ *is not an integer* m *be the largest integer satisfying* $m^2 < N$. *Therefore* $N < (m+1)^2 \Rightarrow m < \sqrt{N} < m+1$. *Since* $m = \sqrt{N}$, *therefore* $\sqrt{N}$ *is the number of perfect squares less than or equal to* N. *Hence* $\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = [\sqrt{N}]$.

Problem 6.7.7. *If* N *is a positive integer, prove that*

$$\tau(N) = \sum_{z=1}^{N} \left(\left[\frac{N}{z}\right] - \left[\frac{N-1}{z}\right] \right).$$

Solution 6.7.7. *Applying Corollary 6.6.2, yields* $\sum_{z=1}^{N} \left[\frac{N}{z}\right] = \sum_{z=1}^{N} \tau(z)$. *Therefore*

$$\begin{aligned} \sum_{z=1}^{N} \left[\frac{N-1}{z}\right] &= \sum_{z=1}^{N-1} \left[\frac{N-1}{z}\right] + \left[\frac{N-1}{N}\right] \\ &= \sum_{z=1}^{N-1} \tau(z) + \left[\frac{N-1}{N}\right]. \end{aligned}$$

As $\frac{N-1}{z} < 1 (\forall N > 0)$, *therefore* $\left[\frac{N-1}{N}\right] = 0$. *Hence* $\sum_{z=1}^{N} \left[\frac{N-1}{z}\right] = \sum_{z=1}^{N-1} \tau(z)$. *Therefore* $\sum_{z=1}^{N} \left(\left[\frac{N}{z}\right] - \left[\frac{N-1}{z}\right] \right) = \sum_{z=1}^{N} \tau(z) - \sum_{z=1}^{N-1} \tau(z) = \tau(N)$.

Problem 6.7.8. *Given a positive integer* N, *prove:* $\sum_{z=1}^{N} \mu(z) \left[\frac{N}{z}\right] = 1$.

Solution 6.7.8. *Let* $F(z) = \sum_{d|z} \mu(d)$. *By Theorem 6.4.2, we find*

$$F(z) = \begin{cases} 1, & \text{if } z = 1; \\ 0, & \text{if } z > 1. \end{cases}$$

By Theorem 6.6.1, we have

$$\begin{aligned}\sum_{k=1}^{N} F(k) &= \sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] \\ &= F(1)+F(2)+\ldots+F(N) \\ &= 1.\end{aligned}$$

Hence $\sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] = 1$.

Let us illustrate the problem taking $N = 6$.

$$\begin{aligned}\sum_{z=1}^{6} \mu(z)\left[\frac{6}{z}\right] &= \mu(1)\left[\frac{6}{1}\right]+\mu(2)\left[\frac{6}{2}\right]+\mu(3)\left[\frac{6}{3}\right]+\mu(4)\left[\frac{6}{4}\right]+\mu(5)\left[\frac{6}{5}\right]+\mu(6)\left[\frac{6}{6}\right] \\ &= 1\cdot 6+(-1)\cdot 3+(-1)\cdot 2+0\cdot 1+(-1)\cdot 1+1\cdot 1 \\ &= 6-3-2+0-1+1 \\ &= 1.\end{aligned}$$

Problem 6.7.9. *Given a positive integer* N, *prove:* $\left|\sum_{z=1}^{N} \frac{\mu(z)}{z}\right| \leq 1$.

Solution 6.7.9. *From Problem 6.7.8, we obtain*

$$\sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] = 1 \Rightarrow \sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right] + \mu(N) = 1.$$

Dividing by N, *we obtain from foregoing equation*

$$\frac{\mu(N)}{N} = \frac{1}{N} - \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right]. \tag{6.7.6}$$

Again,

$$\begin{aligned}\sum_{z=1}^{N} \frac{\mu(z)}{z} &= \sum_{z=1}^{N-1} \frac{\mu(z)}{z} + \frac{\mu(N)}{N} \\ &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\frac{N}{z} + \frac{\mu(N)}{N}. \end{aligned} \tag{6.7.7}$$

(6.7.6) and (6.7.7) yields

$$\begin{aligned}\sum_{z=1}^{N} \frac{\mu(z)}{z} &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\frac{N}{z} + \frac{1}{N} - \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right] \\ &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left(\frac{N}{z} - \left[\frac{N}{z}\right]\right) + \frac{1}{N}.\end{aligned}$$

Since

$$|a+b| \le |a|+|b|,\ |a\cdot b| = |a|\cdot|b|,\ 0 \le \left|\frac{N}{z} - \left[\frac{N}{z}\right]\right| < 1 \text{ and } \left|\frac{1}{N}\right| = \frac{1}{N},$$

therefore

$$\begin{aligned}\left|\sum_{z=1}^{N}\frac{\mu(z)}{z}\right| &\le \frac{1}{N}\sum_{z=1}^{N-1}|\mu(z)|\left|\frac{N}{z} - \left[\frac{N}{z}\right]\right| + \frac{1}{N}\\ &\le \frac{1}{N}\sum_{z=1}^{N-1}|\mu(z)| + \frac{1}{N}\\ &\le \frac{1}{N}(N-1) + \frac{1}{N} = 1 \text{ as } |\mu(z)| \le 1.\end{aligned}$$

Let us illustrate the problem taking $N = 6$.

$$\begin{aligned}\left|\sum_{z=1}^{6}\frac{\mu(z)}{z}\right| &= \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(5)}{5} + \frac{\mu(6)}{6}\\ &= \left|1 + \left(-\frac{1}{2}\right) + \left(-\frac{1}{3}\right) + \frac{0}{4} + \left(-\frac{1}{5}\right) + \frac{1}{6}\right|\\ &= \left|1 + \left(-\frac{5}{6}\right) + \left(-\frac{1}{5}\right) + \frac{1}{6}\right|\\ &= \left|1 + \left(-\frac{13}{15}\right)\right| = \frac{2}{15} < 1.\end{aligned}$$

6.8 Exercises:

1. Show that $\sigma(n) = \sigma(n+1)$ for $n = 14, 206, 957$.
2. For any positive integer n, prove that $\frac{\sigma(n!)}{n!} \ge 1 + \frac{1}{2} + \ldots + \frac{1}{n}$.
3. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$.
4. Prove that there are no positive integers n satisfying $\sigma(n) = 10$.
5. Show that for $k \ge 2$, if $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.
6. Prove that if f and g are multiplicative functions, then so is their product fg and quotient $\frac{f}{g}$(whenever the latter function is defined).
7. For any positive integer n, show that

$$\sum_{d|z}\frac{z}{d}\sigma(d) = \sum_{d|z} d\tau(d).$$

8. Given $z \geq 1$, let $\sigma_s(z)$ denote the sum of the sth powers of the positive divisors of z; that is, $\sigma_s(z) = \sum_{d|z} d^s$. Prove that σ_s is a multiplicative function.

9. For each positive integer n, verify that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

10. If the integer $n > 1$ has a prime factorization $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, prove the following
    (a) $\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \ldots p_r$;
    (b) $\sum_{d|n} \frac{\mu(d)}{d} = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_r})$.

11. If the integer $n > 1$ has a prime factorization $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, then establish that $\sum_{d|n} \mu(d)\lambda(d) = 2^r$.

12. Find the highest power of 7 dividing 2000!.

13. If $n \geq 1$ and p is a prime, show that $\frac{(2n)!}{(n!)^2}$ is an even integer.

14. Find an integer $n \geq 1$ such that the highest power of 5 contained in $n!$ is 100.

15. Determine the highest power of 3 dividing 80! and the highest power of 7 dividing 2400!.