53

Theorem: If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$

Proof: The positive divisors of n are precisely $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$,

$0 \le a_i \le k_i, \quad i = 1, 2, \ldots r$

There are $k_1 + 1$ choices for a_1

$k_2 + 1$ " a_2

$\vdots$

$k_r + 1$ " a_r

Hence, there are

$(k_1+1)(k_2+1)\cdots(k_r+1)$ possible divisors of n.

$\therefore \tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$

54

Divisors of $p_i^{k_i}$ are $1, p_i, p_i^2, \ldots p_i^{k_i}$
$i = 1, 2, \ldots r$.

$\therefore$

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{k_1}\right).\left(1 + p_2 + \cdots + p_2^{k_2}\right). \ldots \left(1 + p_r + \cdots + p_r^{k_r}\right)$$

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

$$\Rightarrow \quad \sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Notation:

$$\prod_{1 \le d \le 5} f(d) = f(1) f(2) f(3) f(4) f(5)$$

$$\therefore \ \tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

$\tau(180) = 18$ $\qquad 180 = 2^2 \cdot 3^2 \cdot 5$

$\sigma(180) = 546$

55

Def: An arithmetic function is said to be multiplicative if

$f(mn) = f(m)f(n)$ whenever $(m,n) = 1$.

Theorem: Prove that τ and σ are multiplicative functions.

Proof: Let m and n are relatively prime integers. Trivially the result is true for $m = n = 1$ or $m = 1$ or $n = 1$.

Assume $m > 1$, $n > 1$

Let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and

$n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the prime factorization of m and n respectively.

$(m,n) = 1$

$$mn = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$$

$$\tau(mn) = (k_1+1)(k_2+1)\cdots(k_r+1)(t_1+1)\cdots(t_s+1)$$

$$= \tau(m)\,\tau(n)$$

56

$$\sigma(mn) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1} \cdot \frac{q_1^{t_1+1}-1}{q_1-1} \cdots \frac{q_s^{t_s+1}-1}{q_s-1}$$

$$= \sigma(m)\,\sigma(n)$$

Fermat's Theorem: Let p be a prime and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof: Consider the first $p-1$ positive multiples of a, i.e, the integers

$$a, 2a, 3a, \ldots (p-1)a$$

All the numbers above are incongruent modulo p ~~n~~, $\because$ if

$$ra \equiv sa \pmod{p}, \quad 1 \leq r < s \leq p-1$$

$$\Rightarrow \quad r \equiv s \pmod{p}$$

a contradiction as $1 \leq r-s \leq p-1$.

Now, the integers $a, 2a, 3a, \ldots (p-1)a$ are congruent modulo p to

58

1, 2, 3, ..., p−1 taken in some order. Multiply all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

$$a^{p-1} \underline{|p-1} \equiv \underline{|p-1} \pmod{p}$$

since $p \nmid \underline{|p-1}$

$$\therefore \quad a^{p-1} \equiv 1 \pmod{p}$$

<u>Corollary</u>: If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.

If $p \mid a$, then the statement is obviously true as $a^p \equiv 0 \equiv a \pmod{p}$

If $p \nmid a$, then by Fermat's

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{p} \equiv a \pmod{p}$$

Exc: Prove that $5^{38} \equiv 4 \pmod{11}$

$a = 5$

$p = 11$ $\qquad (a, p) = 1$

By Fermat's theorem,

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad 5^{10} \equiv 1 \pmod{11}$$

$$5^{38} = (5^{10})^3 \, 5^8 = (5^{10})^3 (5^2)^4$$

$$\equiv (5^2)^4 \pmod{11}$$

$5^2 \equiv 3 \pmod{11}$

$$\Rightarrow \quad 5^{38} \equiv 3^4 \equiv 4 \pmod{11}$$