

Let $n \geq 1$ be an integer. We recall the divisor function:

$$d(n) := \# \{ a : 1 \leq a \leq n, a|n \}$$

In this class, we give an explicit formula for $d(n)$

Theorem Let $n \geq 1$ be an integer.

(1) For a prime p and $k \geq 1$, $d(p^k) = k+1$

(2) If $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$

(3) We have:

$$d(n) = \prod_{p^\alpha \parallel n} (\alpha + 1) = \prod_{p|n} (\text{ord}_p(n) + 1)$$

Example: $d(12) = \# \{ a : 1 \leq a \leq 12, a|12 \}$

$$= \# \{ 1, 2, 3, 4, 6, 12 \} = 6$$

$$d(12) = \prod_{p^\alpha \parallel 12} (\alpha + 1) = \underbrace{(2+1)}_{p=2} \underbrace{(1+1)}_{p=3} = 6$$

$$\begin{aligned} &= \prod_{p|12} (\text{ord}_p(12) + 1) = (\text{ord}_2(12) + 1) (\text{ord}_3(12) + 1) \\ &= (2+1)(1+1) = 6. \end{aligned}$$

Proof of (3): assume that $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

$$d(n) = d(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r})$$

$$\stackrel{(2)}{=} d(p_1^{\alpha_1}) d(p_2^{\alpha_2}) \dots d(p_r^{\alpha_r})$$

$$\stackrel{(1)}{=} (\alpha_1 + 1) (\alpha_2 + 1) \dots (\alpha_r + 1)$$

$$= \prod_{p^{\alpha} \parallel n} (\alpha + 1) = \prod_{p \mid n} (\text{ord}_p(n) + 1) \quad \square$$

Proof of (1): Let p be a prime and $k \geq 1$

$$\{a: 1 \leq a \leq p^k, a \mid p^k\} = \{1, p, p^2, \dots, p^k\}$$

$$\begin{aligned} \Rightarrow d(p^k) &= \#\{a: 1 \leq a \leq p^k, a \mid p^k\} = \#\{1, p, p^2, \dots, p^k\} \\ &= k + 1. \end{aligned} \quad \square$$

Proof of (2): Assume $\text{gcd}(m, n) = 1$

$$A = \{a: 1 \leq a \leq mn, a \mid mn\} \quad \#A = d(mn)$$

$$B = \{b: 1 \leq b \leq m, b \mid m\} \quad \#B = d(m)$$

$$C = \{c: 1 \leq c \leq n, c \mid n\} \quad \#C = d(n)$$

(We need to show: $\#A = \#B \cdot \#C$).

We define the following set:

$$M = \{(b, c) : b \in B, c \in C\} \quad \#M = \#B \cdot \#C.$$

We define the following map:

$$\begin{array}{ccc} M & \xrightarrow{f} & A \\ (b, c) & \longmapsto & bc. \end{array}$$

We need to show:

① The map is well-defined (why $f(b, c) = bc \in A$?)

② The map is injective ($bc = b'c' \Rightarrow b = b'$ and $c = c'$)

③ The map is surjective (for $a \in A$, we can find $b \in B, c \in C$ such that $bc = a$)

①: Let $b \in B$ and $c \in C$. Then $b|m$ and $c|n$.

Then $bc | (mn)$ and hence $bc \in A$.

This shows that the map is well-defined.

② Assume that $bc = b'c'$.

Suppose that $p^a \parallel b$. Then $p \mid b'c'$ and hence

$p \mid b'$ or $p \mid c'$

If $p \mid c'$, then $p \mid \gcd(b, c')$

However $b \mid m$ and $c' \mid n$, then $p \mid \gcd(m, n)$

This contradicts that $\gcd(m, n) = 1$.

Therefore, $p^\alpha \mid b'$.

By primary factorization, $b = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

The above argument shows: $p^\alpha \mid b \Rightarrow p^\alpha \mid b'$

This implies: $b \mid b'$. A similar argument will show: $b' \mid b$.

Therefore: $b = b'$ and

$$\frac{bc}{b} = \frac{b'c'}{b'} \Rightarrow c = c'$$

③ Let $a \in A$. Then $a \mid mn$.

$$\text{Let } m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

$$n = q_1^{\beta_1} \cdots q_s^{\beta_s} \quad \text{with } p_1, \dots, p_r \text{ distinct} \\ q_1, \dots, q_s$$

$$a = p_1^{\gamma_1} \cdots p_r^{\gamma_r} q_1^{\delta_1} \cdots q_s^{\delta_s}$$

$$\text{with } \gamma_i \leq \alpha_i \quad 1 \leq i \leq r \quad (*)$$

$$\delta_j \leq \beta_j \quad 1 \leq j \leq s. \quad (**)$$

$$\text{Set } b = p_1^{\gamma_1} \cdots p_r^{\gamma_r} \quad c = q_1^{\delta_1} \cdots q_s^{\delta_s}$$

$$(*) \Rightarrow b \mid m$$

$$(**) \Rightarrow c \mid n.$$

$$a = bc.$$

By ①, ②, ③, we construct a bijective map between M and A

Therefore, $\# M = \# A$ and $d(mn) = d(m)d(n)$

(when $\gcd(m, n) = 1$).

□