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

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

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:

$$d(n) = \prod_{p^\alpha \| n} (\alpha+1) = \prod_{p \mid n} \left(\mathrm{ord}_p(n) + 1\right)$$

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

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

$$d(10) = \prod_{p^\alpha \| 12} (\alpha+1) = \underbrace{(2+1)}_{p=2}\underbrace{(1+1)}_{p=3} = 6$$

$$= \prod_{p \mid 12} \left(\mathrm{ord}_p(12) + 1\right) = \left(\mathrm{ord}_2(12) + 1\right)\left(\mathrm{ord}_3(12) + 1\right)$$

$$= (2+1)(1+1) = 6.$$

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

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

$$\overset{(2)}{=} d(p_1^{\alpha_1})\, d(p_2^{\alpha_2}) \cdots d(p_r^{\alpha_r})$$

$$\overset{(1)}{=} (\alpha_1+1)(\alpha_2+1) \cdots (\alpha_r+1)$$

$$= \prod_{p^\alpha \| n} (\alpha+1) = \prod_{p \mid n} (\mathrm{ord}_p(n)+1) \qquad \square$$

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

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

$$\Rightarrow d(p^k) = \#\{a : 1 \leq a \leq p^k, a \mid p^k\} = \#\{1, p, p^2, \cdots p^k\}$$

$$= k+1. \qquad \square$$

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

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

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

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

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

We define the following set:

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

We define the following map:

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

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 $b \mid m$ and $c \mid n$.

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

This shows that the map is well-defined.

② Assume that $bc = b'c'$.

Suppose that $p \,\|\, b$. 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, $p \mid b'$.

Then we can divide $\frac{bc}{p} = \frac{b'c'}{p}$

$$\frac{b}{p} \cdot c = \frac{b'}{p} \cdot c'$$

We contime this process and we can finally show:

$$c = c'.$$

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

③ Let $a \in A$. Then $a \mid mn$.

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

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

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

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

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

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 construt a bijective map between M and A

Therefore, $\# M = \# A$ and $d(mn) = d(m)d(n)$ (when $\gcd(m,n) = 1$). $\square$