CSE 547 Discrete Mathematics
Chapter 4: Problem 14

Problem #14

Prove or disprove :

a. gcd(km,kn) = k gcd(m,n);

b. lcm(km,kn) = k lcm(m,n).

Solution

Definitions:

gcd : greatest common divisor

The *greatest common divisor* of two integers m and n is the largest integer that divides them both:

$$gcd(m,n) = \max\{k \mid k\backslash m \text{ and } k\backslash n \}.$$

Continued…

<u>lcm</u> : least common multiple

The least common multiple of two integers m and n is the smallest integer k which is a multiplicative factor of both: i.e.,

$$lcm(m,n) = \min \{ k \mid k>0, m\backslash k \text{ and } n\backslash k \}$$

This is undefined if $m \leq 0$ or $n \leq 0$.

Continued…

Point to note:

In the above definitions, we have used k\m and k\n.

The functionality of '\' is defined by:

$m\backslash n \Leftrightarrow m>0$ and

$n=mk$ for some integer k

Informally, this is nothing but n/m written in the reverse manner.

Continued …

To solve the given problem, it is important to know the following points:

1. Every positive integer n can be written as a product of primes, i.e.,

   $n = p_1 p_2 \ldots\ldots\ldots\ldots p_m = \prod p_k$, $1 \le k \le m$

   and $p_1 \le \ldots\ldots \le p_m$

   (Equation (4.10) on page 106)

   For example, 12 = 2.2.3; 35 = 5.7 etc,.

Continued …

And this expansion (factorization) is unique for every integer. This is called Fundamental Theorem of Arithmetic.

2. This theorem can be stated in another way as :

   Every positive integer can be written uniquely in the form

   $n = \prod_p p$ pow (n_p) , where each $n_p \geq 0$.

   (Equation (4.11) on page 107)

Continued …

The above equation represents n uniquely. So we can think of a sequence $<n_2, n_3, n_5\ldots>$ as a number system for positive integers.

For example, the prime-exponent representation of 12 is <2,1,0,0,…..> and for 18 it is <1,2,0,0,……>.

Continued …

3. To multiply two numbers, we simply add their representations. i.e.,

   $k = mn \iff k_p = m_p + n_p$ for all p.

   (Equation (4.12) on page 107)

   This implies that

   $m \backslash n \iff m_p \le n_p$ for all p,

   (Equation (4.13) on page 107)

Continued …

From the above point, it follows that

$k = \gcd(m,n) \Leftrightarrow k_p = \min(m_p, n_p)$ for all p;

(Equation (4.14) on page 107)

$k = \operatorname{lcm}(m,n) \Leftrightarrow k_p = \max(m_p, n_p)$ for all p.

(Equation (4.15) on page 107)

Example: $12 = 2^2 . 3^1$ and $18 = 2^1 . 3^2$

Continued…

Hence, $\gcd(12,18) = 2^{\min(2,1)} \cdot 3^{\min(1,2)}$

$= 2^1 \cdot 3^1 = 6;$

$\mathrm{lcm}(12,18) = 2^{\max(2,1)} \cdot 3^{\max(1,2)}$

$= 2^2 \cdot 3^2 = 36.$

Now, coming to the given problem,
we want to get the value of gcd(km,kn) and lcm(km,kn) in terms of the gcd(m,n) and lcm(m,n) respectively.

Continued…

Let K = (km) (kn). This implies that

$K_p = (km)_p + (kn)_p$ for all p

(Using equation (4.12))

Again, using the same equation,

if A = km , then $A_p = k_p + m_p$ and

if B = kn , then $B_p = k_p + n_p$

Continued…

Part (a):

L.H.S: X = gcd(km,kn) <=>

$$X_p = \min(A_p , B_p)$$

$$= \min (k_p + m_p , k_p + n_p)$$

(Using equation (4.15))

R.H.S: Y = k {gcd(m,n) } <=>

$$Y_p = k_p + \{\min(m_p , n_p)\}$$

-- According to equation (4.12)

Continued…

Since, k_p is a term added to both m_p and n_p ,it does not matter what the value of k_p is while calculating min ($k_p + m_p$, $k_p + n_p$)

For example, lets assume $m_p < n_p$.

Then, $X_p = (k_p + m_p)$ and $Y_p = k_p + (m_p)$

Hence,

$$gcd(km,kn) = k\ gcd(m,n)$$

Continued…

Now consider Part (b).

lcm(km,kn) = k lcm(m,n)

L.H.S:

X = lcm(km,kn) <=>

$$X_p = \max(A_p , B_p)$$

$$= \max(k_p + m_p , k_p + n_p)$$

Using equation (4.15)

Continued…

R.H.S:

$Y = k\ \{lcm(m,n)\}$ <=>

$$Y_p = k_p + \{max(m_p\ , n_p\ )\}$$

-- According to equation (4.12)

Again following the same argument as for the Part (a),

If $m_p < n_p$, then ,

$X_p = (k_p + n_p)$ and $Y_p = k_p + (n_p)$, which are equal.

Continued…

Hence,

$$\mathrm{lcm}(km,kn) = k\,\mathrm{lcm}(m,n)$$

Therefore,

(a) $\gcd(km,kn) = k \gcd(m,n)$

(b) $\mathrm{lcm}(km,kn) = k\,\mathrm{lcm}(m,n)$