Cse457 Discrete Mathematics

Chapter 4 – Problems 2 and 14

Problem 2, Chapter 4

- Prove that gcd (m, n) x lcm (m, n) = m x n and use this identity to express lcm (m, n) in terms of lcm (n mod m, m), when n mod m != 0.

Representation

- Any number can be written as a product of primes:

$$n = p_1 \cdot p_2 \ldots p_m = \prod_{k=1}^{m} p_k, \; p_1 \le \ldots \le p_m$$

- Example: n = 20; 20 = 2 x 2 x 5

Representation

- Extension: any number can be written as a product over infinitely many primes (powers of primes) where some factors are 1:

$$n = p_2^{n2} \cdot p_3^{n3} \ldots = \prod_p p^{n_p}, n_p \geq 0 \quad \text{(4.11) textbook}$$

- Example: n = 20; $20 = 2^2 \times 3^0 \times 5^1 \times 7^0 \ldots.$

Representation

- Each number is represented as the exponent sequence of all consecutive prime numbers (the representation is unique)
- For $n = p_2^{n2} \cdot p_3^{n3} \ldots = \prod_p p^{n_p}, n_p \geq 0$

  the representation is $(n_2, n_3, n_5 \ldots)$
- Example: n = 20; $20 = 2^2 \times 3^0 \times 5^1 \ldots$

  Representation: (2, 0, 1, 0, …)

Multiplication

- To multiply 2 numbers, we add their representations
- Example: n = 20, m=42;

  $20 = 2^2 \times 3^0 \times 5^1 \ldots.$

  $42 = 2^1 \times 3^1 \times 5^0 \times 7^1 \ldots.$

  $20 \times 42 = 2^{2+1} \times 3^{0+1} \times 5^{1+0} \times 7^{0+1} \ldots.$

  $= 2^3 \times 3^1 \times 5^1 \times 7^1 \ldots.$

$$\begin{array}{r} (2, 0, 1, 0, \ldots) \\ (1, 1, 0, 1, \ldots) \\ \hline (3, 1, 1, 1, \ldots) \end{array}$$

- We can formalize multiplication as:

  $k = m \times n \Leftrightarrow k_p = m_p + n_p$, for all p

(4.12) textbook

GCD

- Example: $n = 20$, $m=42$

$$\gcd(20, 42) = \gcd(2^2 \times 3^0 \times 5^1 \times 7^0,\ 2^1 \times 3^1 \times 5^0 \times 7^1)$$
$$= 2^{\min(2,1)} \times 3^{\min(0,1)} \times 5^{\min(1,0)} \times 7^{\min(0,1)}$$
$$= 2^1 \times 3^0 \times 5^0 \times 7^0 = 2$$

- We can formalize GCD as:

$K = \gcd(m, n)$

$\Leftrightarrow k_p = \min(m_p, n_p)$ for all p

(4.14) textbook

$$\begin{array}{c} (2, 0, 1, 0, \ldots) \\ (1, 1, 0, 1, \ldots) \\ \hline \big\downarrow \text{ min} \\ (1, 0, 0, 0, \ldots) \end{array}$$

LCM

- Example: n = 20, m=42

  lcm (20, 42) = lcm ($2^2 \times 3^0 \times 5^1 \times 7^0$, $2^1 \times 3^1 \times 5^0 \times 7^1$)

  $= 2^{\max(2,1)} \times 3^{\max(0,1)} \times 5^{\max(1,0)} \times 7^{\max(0,1)}$

  $= 2^2 \times 3^1 \times 5^1 \times 7^1 = 420$

- We can formalize multiplication as:

K = lcm (m, n)

$\Leftrightarrow k_p = \max(m_p, n_p)$ for all p

(4.15) textbook

$$
\begin{array}{c}
(2, 0, 1, 0, \ldots) \\
(1, 1, 0, 1, \ldots) \\
\hline
\Big\downarrow \text{max} \\
(2, 1, 1, 1, \ldots)
\end{array}
$$

Our problem – first part

- Prove: gcd (m, n) x lcm (m, n) = m x n
- Each prime factor p (e.g. 2, 3, 5, ...) appears both in m and n.

  gcd (m, n) = $2^{\min(n2,m2)} \times 3^{\min(n3,m3)} \times \ldots$

  lcm (m, n) = $2^{\max(n2,m2)} \times 3^{\max(n3,m3)} \times \ldots$

  m = $2^{m2} \times 3^{m3} \times \ldots$

  n = $2^{n2} \times 3^{n3} \times \ldots$

- For any n_p and m_p exponents, one will be min and one will be max

  => one will appear in gcd and one in lcm

Our problem – first part

- For 2 numbers m_p and n_p, one is min, other is max, therefore:

  $\min(m_p, n_p) + \max(m_p, n_p) = m_p + n_p$
- We apply this for all prime factors p in our number representation and obtain what we had to prove:

  $\gcd(m, n) \times \mathrm{lcm}(m, n) = m \times n$

Our problem – second part

- Problem: Express lcm (m, n) in terms of lcm (n mod m, m), when n mod m != 0
- We start from lcm (n mod m, m):

$$\mathrm{lcm}\,(n \bmod m, m) = \frac{n \bmod m \times m}{\gcd\,(n \bmod m, m)}$$

- From the recurrence in Euclid’s algorithm – Equation 4.4 textbook:
  gcd (m, n) = gcd (n mod m, m), for m>0

We obtain:

$$\mathrm{lcm}\,(n \bmod m, m) = \frac{n \bmod m \times m}{\gcd\,(m, n)}$$

Our problem – second part

- Next, express gcd (m, n) in terms of lcm (m, n):

$$\gcd(m, n) = \frac{m \times n}{\operatorname{lcm}(m, n)}$$

- We obtain:

$$\operatorname{lcm}(n \bmod m, m) = \frac{n \bmod m \times m}{\frac{m \times n}{\operatorname{lcm}(m, n)}} = \frac{n \bmod m}{n} \times \operatorname{lcm}(m, n)$$

- Get lcm (m, n):

$$\operatorname{lcm}(m, n) = \frac{n}{n \bmod m} \times \operatorname{lcm}(n \bmod m, m)$$

Problem 14, Chapter 4

- Prove or disprove:
  - gcd (k x m, k x n) = k x gcd (m, n)
  - lcm (k x m, k x n) = k x lcm (m, n)

Our problem – first part

- Prove or disprove:
  - gcd (k x m, k x n) = k x gcd (m, n)
- Left side - we have: gcd (k x m, k x n)
  - $a = k \times m \Leftrightarrow a_p = k_p + m_p$ for all p

    $b = k \times n \Leftrightarrow b_p = k_p + n_p$ for all p
  - $L = \gcd(k \times m, k \times n)$

    $\Leftrightarrow L = \gcd(a, b)$

    $\Leftrightarrow L_p = \min(a_p, b_p)$

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

    $\Leftrightarrow L_p = k_p + \min(m_p, n_p)$ for all p

Our problem – first part

- Right side - we have: k x gcd (m, n)
  - g = gcd (m, n) $\Leftrightarrow$ $g_p = \min(m_p, n_p)$ for all p
  - R = k x gcd (m, n)

    $\Leftrightarrow$ R = k x g

    $\Leftrightarrow$ $R_p = k_p + g_p$

    $\Leftrightarrow$ $R_p = k_p + \min(m_p, n_p)$ for all p

Our problem – first part

- We had:

  $L = \gcd(k \times m, k \times n)$ and $R = k \times \gcd(m, n)$

- But: $L = R \Leftrightarrow L_p = R_p$ for all p
- We proved that:

  $L_p = R_p = k_p + \min(m_p, n_p)$ for all p

- In conclusion:

  $\gcd(k \times m, k \times n) = k \times \gcd(m, n)$ is TRUE

Our problem – second part

- Prove or disprove:
  - lcm (k x m, k x n) = k x lcm (m, n)
- Left side - we have: lcm (k x m, k x n)
  - a = k x m ⇔ $a_p = k_p + m_p$ for all p

    b = k x n ⇔ $b_p = k_p + n_p$ for all p
  - L = lcm (k x m, k x n)

    ⇔ L = lcm (a, b)

    ⇔ $L_p = \max(a_p, b_p)$

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

    ⇔ $L_p = k_p + \max(m_p, n_p)$ for all p

Our problem – second part

- Right side - we have: k x lcm (m, n)
  - l = lcm (m, n) $\Leftrightarrow$ $l_p = \max(m_p, n_p)$ for all p
  - R = k x lcm (m, n)

    $\Leftrightarrow$ R = k x l

    $\Leftrightarrow$ $R_p = k_p + l_p$

    $\Leftrightarrow$ $R_p = k_p + \max(m_p, n_p)$ for all p

Our problem – second part

- We had:

  $L = \text{lcm}(k \times m, k \times n)$ and $R = k \times \text{lcm}(m, n)$
- But: $L = R \Leftrightarrow L_p = R_p$ for all p
- We proved that:

  $L_p = R_p = k_p + \max(m_p, n_p)$ for all p
- In conclusion:

  $\text{lcm}(k \times m, k \times n) = k \times \text{lcm}(m, n)$ is TRUE