CSE 16 7-23-20

Pre-recorded lecture

Theorem (Fundamental theorem of Arithmetic)

Every $n \in \mathbb{N}$ can be expressed uniquely (up to order) as a Product of (zero or more) Primes.

note

- 'up to order' means order does not count. i.e. $2 \cdot 3 = 3 \cdot 2$ are not different Prime factorizations of 6.
- 'zero or more' extends meaning of Product to include any number of operands.

$1 = 1$ is a Product of zero Primes

$2 = 2$ " " " " 1 Prime

$6 = 2 \cdot 3$ " " " " 2 Primes

Defn

Let $a, b \in \mathbb{Z}$

- The greatest common divisor of a and b is the largest integer that divides both a and b.

  notation: $\gcd(a,b)$

  i.e. $d = \gcd(a,b)$ iff both

  (i) $d \mid a$ and $d \mid b$

  (ii) if $e \mid a$ and $e \mid b$, then $e \leq d$

- The least common multiple of a and b is the smallest (positive) integer that is divisible by both a and b.

  notation: $\operatorname{lcm}(a,b)$

  i.e. $m = \operatorname{lcm}(a,b)$ iff both

  (i) $a \mid m$ and $b \mid m$

  (ii) if $a \mid k$ and $b \mid k$, then $m \leq k$.

<u>Ex.</u> find $\gcd(30,75)$ and $\operatorname{lcm}(30,75)$

divisors of 30 : 1, 2, 3, 5, 10, 15, 30
" " 75 : 1, 3, 5, 15, 25, 75

common divisors : 1, 3, 5, 15

$\therefore \gcd(30,75) = \boxed{15}$

Pos. mult. of 30 : 30, 60, 90, 120, 150, 180, ...
" " " 75 : 75, 150, ...

$\therefore \operatorname{lcm}(30,75) = \boxed{150}$

Observe that

$$30 \cdot 75 = 2250 = 15 \cdot 150$$

Theorem

for any $a, b \in \mathbb{N}$:

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

Lemma 1

let $a, b \in \mathbb{N}$ and $p_1, p_2, \ldots, p_n$ Primes.

suppose

$$a = p_1^{x_1} \cdot p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} \cdot p_2^{y_2} \cdots p_n^{y_n}$$

for some integers $x_i \geq 0, y_i \geq 0$ $(1 \leq i \leq n)$.

Then $a | b$ iff $x_i \leq y_i$ $(1 \leq i \leq n)$.

$\Rightarrow$ / $\Leftarrow$

Proof

observe

$$b = \left(p_1^{x_1} \cdot p_2^{x_2} \cdots p_n^{x_n}\right) \cdot \left(p_1^{y_1 - x_1} \cdot p_2^{y_2 - x_2} \cdots p_n^{y_n - x_n}\right)$$

$$= a \cdot k$$

where $k = p_1^{y_1-x_1} p_2^{y_2-x_2} \cdots p_n^{y_n-x_n}$.

($\Leftarrow$) If $x_i \leq y_i$ for $1 \leq i \leq n$, then $y_i - x_i \geq 0$ $(1 \leq i \leq n)$, so k is an integer. $\therefore$ $a \mid b$

($\Rightarrow$) if $a \mid b$, then $b = ak'$ for some $k' \in \mathbb{Z}$. The uniqueness of prime factorization of b and of k' implies that $k' = k$, hence $k \in \mathbb{Z}$. Therefore $y_i - x_i \geq 0$ $(1 \leq i \leq n)$ and $\therefore$ $x_i \leq y_i$ $(1 \leq i \leq n)$. ∎

<u>Lemma 2</u>

let $a, b \in \mathbb{N}$ and let

$$S = \{p_1, p_2, \ldots, p_n\}$$

be all primes appearing in the prime factorization of a, or b, or both.

So

$$a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}$$

where each $x_i \geq 0$, $y_i \geq 0$ $(1 \leq i \leq n)$.

Then

(1) $\gcd(a,b) = p_1^{\min(x_1,y_1)} p_2^{\min(x_2,y_2)} \cdots p_n^{\min(x_n,y_n)}$

(2) $\operatorname{lcm}(a,b) = p_1^{\max(x_1,y_1)} p_2^{\max(x_2,y_2)} \cdots p_n^{\max(x_n,y_n)}$

<u>Ex</u>

First look at: $a = 30$, $b = 75$.

$$30 = 2 \cdot 3 \cdot 5 = 2^1 \cdot 3^1 \cdot 5^1$$
$$75 = 3 \cdot 5 \cdot 5 = 2^0\, 3^1\, 5^2$$

$\therefore$ $\gcd(30,75) = 2^0 \cdot 3^1 \cdot 5^1 = 15$

$\operatorname{lcm}(30,75) = 2^1 \cdot 3^1 \cdot 5^2 = 150$

Proof of lemma 2

let

$$d = \text{RHS of (1)}$$
$$m = \text{RHS of (2)}$$

we must show d and m satisfy definitions of $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ resp.

Since $\min(x_i, y_i) \le x_i$ for $1 \le i \le n$, lemma 1 implies that

$$d \mid a.$$

similarly $\min(x_i, y_i) \le y_i$ $(1 \le i \le n)$ and lemma 1 gives

$$d \mid b$$

Now suppose $e \mid a$ and $e \mid b$.

Then by lemma 1 we have

$$e = p^{z_1} p_2^{z_2} \cdots p_n^{z_n}$$

where both $z_i \le x_i$ and $z_i \le y_i$ $(1 \le i \le n)$.
Therefore $z_i \le \min(x_i, y_i)$ for $1 \le i \le n$.
so by lemma 1 we have $e | d$.
$\therefore$ $e \le d$. we've shown

$$d = \gcd(a, b).$$

<u>Exercise</u>
complete this proof by showing
that m satisfies the defn.
of $\mathrm{lcm}(a,b)$:

(i) $a | m$ and $b | m$
and (ii) if $a | k$ and $b | k$, then $m \le k$.

$\blacksquare$

Proof of theorem

(*) $$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

let
$$a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$$
$$b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}$$

as in lemma 2. Then

$$*\,\text{LHS} = p_1^{x_1+y_1} \cdot p_2^{x_2+y_2} \cdots p_n^{x_n+y_n}$$

$$*\,\text{RHS} = p_1^{\min(x_1,y_1)+\max(x_1,y_1)} \cdots\cdots p_n^{\min(x_n,y_n)+\max(x_n,y_n)}$$

using lemma 2. But

$$x_i + y_i = \min(x_i, y_i) + \max(x_i, y_i)$$

for $1 \le i \le n$. Therefore

$$*\,\text{LHS} = *\,\text{RHS}$$

as claimed. $\blacksquare$

Euclid invented an efficient algorithm for gcd(a, b)

Ex. $\gcd(16200, 756) = \boxed{108}$.

$$16200 = 21 \cdot 756 + 324$$

$$756 = 2 \cdot 324 + \boxed{108}$$

$$324 = 3 \cdot \boxed{108} + \underline{\underline{0}} \quad \text{(stop)}$$