MATH 335 Lecture 2

Chris Camano: ccamano@sfsu.edu

August 25, 2022

Proposition 0.1. *Let $a, b \in \mathbb{Z}^+$ where a can be written as the following with P as a prime number:*

$$a = \prod_{i=0}^{k} P_i^{\alpha_i}$$

$$b = \prod_{i=0}^{k} P_i^{\beta_i}$$

$$\alpha_i, \beta_i \geq 0$$

Then:

$$gcd(a, b) = \prod_{i=0}^{k} P_i^{\min\{\alpha_i, \beta_i\}}$$

Proof. Let d= $\prod_{i=0}^{k} P_i^{\min\{\alpha_i,\beta_i\}}$, We must show that d is a common divisor and that there does not exist a divisor greater than d. this is to say:

- $d|a$ and $d|b$
- if $e|a$ and $e|b$ then $e|d$
- *Proof.* $d|a$ and $d|b$
  To show this we mush show that $a = dc$ for some $c \in \mathbb{Z}$.

  $$a = \prod_{i=0}^{k} P_i^{\alpha_i} = \left(\prod_{i=0}^{k} P_i^{\min\{\alpha_i,\beta_i\}}\right)\left(\prod_{i=0}^{k} P_i^{\alpha_i - \min\{\alpha_i,\beta_i\}}\right)$$

  Where

  $$\alpha_i - \min\{\alpha_i, \beta_i\} \geq 0 \quad \forall \alpha_i$$

  By similar reasoning we can prove that d—b as well and the proof is complete. □
- *Proof.* if $e|a$ and $e|b$ then $e|d$
  Suppose $e \in \mathbb{Z}$ such that $e|a, e|b$. We now need to show $e|d$ Due to the fact that e

divides both a and b this implies that the prime factorization of e is composed only of the prime factors of the two dividends, or in other words.

$$e = \prod_{i=0}^{k} P_i^{\delta_i}$$

Where $P_1, \ldots, P_k$ are primes only from the set of primes composed by the prime factorization of a and b and $\delta_i \leq \min(\alpha_i, \beta_i)$
Then e—d since the exponents of the primes in d are equal to $\min(\alpha_i, \beta_i)$. □

We have then proven the two conditions required to prove the greatest common divisor. □

Example:

$$30 = 2^1(3^1)(5^1)$$
$$96 = 2^5(3^1)(5^0)$$

Definition 0.2. Let $a, b \in \mathbb{Z}^+$ then an integer d is the least common multiple of a and b, d=lcm(a,b) $\iff$ two conditions are satisfied:

- $a|d$ and $b|d$
- if $a|e$ and $b|e$ then $d|e$

Proposition 0.3. *Let $a, b \in \mathbb{Z}^+$ with the prime factorizations:*

$$a = \prod_{i=0}^{k} P_i^{\alpha_i}$$

$$b = \prod_{i=0}^{k} P_i^{\beta_i}$$

where $P_1, ..., P_k$ are distinct primes and:

$$\alpha_i, \beta_i \geq 0$$

Then the least common multiple of a and b is equal to:

$$lcm(a, b) = \prod_{i=0}^{k} P_i^{\max\{\alpha_i, \beta_i\}}$$