# NUMBER THEORY

Ariyadi Wijaya

# GCD

- Theorem:

  "If $(a,b)=d$, then there are integer numbers so that $ax+by=d$"

- Proof:

  By using the Division Algorithm

# GCD

- Theorem:

  “If $d|ab$ and $(d,a)=1$ then $d|b$

- Proof:

  Since $(d,a)=1$ then there are x and y so that $dx+ay=1$

  $b(dx)+b(ay)=b \rightarrow d(bx)+y(ab)=b$

  Since $d|ab$ so $d|y(ab)$ and since $d|d(bx)$, so $d|b$

# GCD

- Theorem:

  If $c|a$ and $c|b$ with $(a,b)=d$, then $c|d$

- Proof:

  $(a,b)=d \Rightarrow d=ax+by$

  Since $c|a$ so $c|ax$ ...(i)

  Since $c|b$ then $c|by$ ...(ii)

  From (i) and (ii):

  $c|ax+by \Rightarrow c|d$

# Least Common Multiple (LCM)

- Definition:

  For non zero integers $a_1, a_2, a_3, \dots, a_n$ it is said that they have common multiple b if $a_i|b$ for $i=1,2,3, \dots, n$

- Definition:

  For non zero integers $a_1, a_2, a_3, \dots, a_n$, their LCM is the least number among the common multiples.

  If k is the LCM of a and b, it can be written as $[a,b]=k$

# LCM

- Theorem:
  If m is a common multiple of a and b, so
  $[a,b] \mid m$
- Proof:
  If $[a,b]=k$ so it will be proved that $k|m$
  Assume that $k \nmid m$, so there are q and r so that $m=kq + r$ for $0 < r < k$ ... (i)
  Since m is a CM of a and b so $a|m$ and $b|m$ ... (ii)
  k is the LCM of a and b so $a|k$ and $b|k$ ... (iii)
  From (i), (ii) and (iii), $a|r$ and $b|r$, it is contrary to
  $0 < r < k$ (namely k is the LCM).
  :: $k|m$

# LCM

- Theorem:

  If $m>0$, then $[ma,mb]=m[a,b]$
- Theorem:

  If $a$ and $b$ are positive integers, then $[a,b](a,b)=ab$

# Exercise:

1. Prove that "if $a|b$ and $a>0$ then $(a,b)=a$"
2. Prove that $((a,b),b)=(a,b)$
3. Prove that $(a,b)|(a+b,a)$
4. Is $(a,b)|[a,b]$ a correct statement? Explain
5. Prove that $[a,b]=(a,b)$ iff $a=b$