Divisibility: An integer b is divisible by an integer $a \neq 0$, if $\exists\, x \in \mathbb{Z}$ such that $b = ax$, and we write $a|b$. In case b is not divisible by a, we write $a \nmid b$.

$\mathbb{Z}$ = Set of integers $= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

If $a|b$ and $0 < a < b$, then a is called a proper divisor of b. $a|0 \;\forall\, a \in \mathbb{Z} - \{0\}$.

$a^k \| b \iff a^k | b,\ a^{k+1} \nmid b$, where a is a prime number

① $a|b \Rightarrow a|bc \;\forall\, c \in \mathbb{Z}$

② $a|b$ and $b|c \Rightarrow a|c$

③ $a|b$ and $a|c \Rightarrow a|(bx + cy) \;\forall\, x, y \in \mathbb{Z}$

④ $a|b$ and $b|a \Rightarrow a = \pm b$

⑤ $a|b$, $a > 0$, $b > 0 \Rightarrow a \leq b$

⑥ If $m \neq 0$, $a|b \iff ma|mb$

The division algorithm: Given any integers a and b, with $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r \leq a$. If $a \nmid b$, then r satisfies the stronger inequalities $0 < r < a$.

Let $Z_{a,b} = \{ b - qa \mid q \in \mathbb{Z} \} = \{\ldots, b-2a, b-a, b, b+a, b+2a, \ldots\}$. Let r be the least non-negative element of $Z_{a,b}$. We should have $0 \leq r < a$, otherwise some other $r' < r$ will be the least non-negative element of $Z_{a,b}$. Let $r = b - qa$

$\Rightarrow b = qa + r$ with $0 \leq r < a$.

Let $b = q'a + r'$ with $0 \leq r' < r < a$.

$\Rightarrow qa + r = q'a + r' \Rightarrow (r - r') = (q' - q)a > 0$

$\Rightarrow r - r' \geq a \Rightarrow r \geq a + r' \geq a$, a contradiction.

This proves the uniqueness of r and q. $\underline{r'=r} \Rightarrow \underline{q'=q}$.

$a \nmid b$ and $r=0 \Rightarrow b = qa \Rightarrow a \mid b$, a contradiction.

$\Rightarrow$ If $a \nmid b$, then $0 < r < a$.

<u>Greatest Common Divisor (GCD)</u>: The integer a is a common divisor of b and c in case $a \mid b$ and $a \mid c$. Since there is only a finite number of divisors of any nonzero integer, there is only a finite number of common divisors of b and c, except in the case $b=c=0$. If at least one of b and c is not 0, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by (b,c). Similarly, we denote the greatest common divisor g of the integers $b_1, b_2, \ldots, b_n$, not all zero, by $(b_1, b_2, \ldots, b_n)$.

(b,c) is defined for every pair of integers b, c except $b=c=0$, and we note that $(b,c) \geq 1$.

$\exists\, x_0, y_0 \in \mathbb{Z}$ such that $(b,c) = bx_0 + cy_0$.

Proof is similar to the proof of division algorithm.

Let $\mathbb{Z}_{b,c} = \{ bx + cy \mid x \in \mathbb{Z}, y \in \mathbb{Z} \}$. Let g be the smallest positive element of $\mathbb{Z}_{b,c}$: $g = bx_0 + cy_0$

Claim: $g = (b,c)$.

<u>Proof</u>: Applying division algorithm (dividing b by g):

$b = gq + r \Rightarrow r = b - gq = b - (bx_0 + cy_0)q$

$= b(1 - qx_0) + c(-qy_0) \in \mathbb{Z}_{b,c}$. $0 \leq r < g \Rightarrow r = 0$.

$\Rightarrow g \mid b$. Similarly applying division algorithm (dividing c by g) we get the result that $g \mid c$.

$\Rightarrow g$ is a common divisor of b and c.

If g is not the gcd, then let $g' > g$ be the gcd of b and c. We have: $g' | b$ and $g' | c \Rightarrow g' | (bx_0 + cy_0)$
$\Rightarrow g' | g \Rightarrow g' \leq g$ a contradiction.
$\Rightarrow g = (b, c)$

The gcd g of b and c can be characterized in the following two ways: (1) It is the least positive value of $bx + cy$ where x and y range over all integers; (2) it is the positive common divisor of b and c that is divisible by every common divisor.

Proof of (2): Let $g = bx_0 + cy_0$. Let $g' < g$ be any other common divisor of b and c. $g' | b$ and $g' | c$
$\Rightarrow g' | (bx_0 + cy_0) \Rightarrow g' | g$.

Given any integers $b_1, b_2, \dots, b_n$ not all zero, with gcd g, there exist integers $x_1, x_2, \dots, x_n$ such that

$$g = (b_1, b_2, \dots, b_n) = \sum_{j=1}^{n} b_j x_j .$$

Furthermore, g is the least positive value of the linear form $\sum_{j=1}^{n} b_j y_j$ where the y_j range over all integers; also g is the positive common divisor of $b_1, b_2, \dots, b_n$ that is divisible by every common divisor.

For any positive integer m,

$$(ma, mb) = m(a, b).$$

$$(ma, mb) = \min_{x, y \in \mathbb{Z}} \{ max + mby \} = m \min_{x, y \in \mathbb{Z}} \{ ax + by \}$$
$$= m(a, b).$$