§1 Divisibility and GCD.

Definition. Let $a, b \in \mathbb{Z}$. We say that a <u>divides</u> b if there exists $d \in \mathbb{Z}$ such that

$$b = d \cdot a.$$

Examples: $-5 \mid 30$, $13 \nmid 19$, $0 \mid 0$.

Notation: $a \mid b$ (a divides b).

Basic properties: $\forall a, b, c \in \mathbb{Z}$

a) $a \mid 0$ $\qquad (0 = 0 \cdot a)$

b) $1 \mid a$ $\qquad (a = a \cdot 1)$

c) $a \mid b,\ b \mid c \Longrightarrow a \mid c$

$\qquad (b = d_1 a,\ c = d_2 b \Longrightarrow c = d_1 d_2 a)$

d) $a \mid b,\ a \mid c \Longrightarrow a \mid mb + nc$ for any integer m, n.

Division with the remainder.

Proposition. Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$. Then there exist unique numbers $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r, \qquad 0 \le r < b.$$

q is called a quotient, r is called a remainder after division of b by a.

Proof. Existence.

Define $S^+ = \{a - kb : k \in \mathbb{Z},\ a - kb \geq 0\}$

S^+ is non-empty $\left(\begin{array}{l} \text{take } k=0 \text{ if } a \geq 0 \\ k = +a \text{ if } a < 0 \end{array}\right)$

By the Least Integer Principle S^+ contains its minimal element

$r = a - qb$.

$r \geq 0$ by construction.

$r - b = a - (q+1)b$ it is not non-negative (it is not in S^+).

Therefore $r - b < 0 \Rightarrow r < b$.

Uniqueness: Assume we have (q, r) and (q', r') with

$a = qb + r = q'b + r'$ $\quad 0 \leq r, r' < b$.

$(q - q')b + r = r'$

If $q > q'$ then $b \leq (q - q')b + r = r' < b$

Contradiction.

Finally $q = q' \Longrightarrow r = r'$. $\square$

Example. $a = 66$, $b = 7$

$$66 = 9 \cdot 7 + 3$$

quotient remainder.

$$\frac{66}{7} = 9.42\ldots$$

quotient.

Remark. a divides b if and only if the remainder after division of b ~~ba~~ a is 0.

§1.2. GCD.

Definition. Let $a, b \in \mathbb{Z}$. An integer d is called a <u>common divisor</u> of a and b if

$$d \mid a, \quad d \mid b$$

An integer g is called the greatest common divisor if it is the biggest integer with this property. We write

$$\gcd(a,b) := \max\{d \in \mathbb{Z} : d \mid a,\ d \mid b\}$$

Convention: $\gcd(0,0) := 0$.

Example: $\gcd(10, 16)$

Divisors of 10: $1, 2, 5, 10$

of 16: $1, 2, 4, 8, 16$

$\gcd(10, 16) = 2$.

Definition: If $\gcd(a, b) = 1$ then a and b are called <u>coprime</u> or <u>relatively prime</u> numbers.

Basic properties.

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

b) If $a \geq 0$ then $\gcd(a, 0) = a$.

c) $\gcd(-a, b) = \gcd(a, b)$.

Lemma. For any $a, b, q \in \mathbb{Z}$ we have

$$\gcd(a,b) = \gcd(a, b-a) = \gcd(a, b-2a) = \ldots$$
$$= \gcd(a, b-qa).$$

Proof. We only prove the first equation.

Consider $d|a$, $d|b \Rightarrow d|a$, $d|b-a$

Therefore $\gcd(a,b)$ is a divisor of a, $b-a$.

$\Rightarrow \gcd(a, b) \leq \gcd(a, b-a)$

Consider $d|a$, $d|b-a \Rightarrow d|a$, $d|(b-a)+a = b$

$\Rightarrow \gcd(a,b) = \gcd(a, b-a)$. $\boxtimes$

Example: $\gcd(345, 92) = \gcd(92, 345)$

$$= \gcd(92, \underbrace{345 - 3 \cdot 92}_{69})$$

$$= \gcd(69, 92) = \gcd(69, \underbrace{92 - 69}_{23})$$

$$= \gcd(23, 69) = \gcd(23, \underbrace{69 - 3 \cdot 23}_{0})$$

$$= 23!$$

Concluding this example we get

Theorem (Euclidean algorithm).

Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$. Then $\gcd(a,b)$ can be computed in the following way:

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\cdots$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

until $r_{n+1} = 0$. Then $\gcd(a,b) = r_n$.