Theorem 0.1

For $a, b \in \mathbb{Z}$ with $a \neq 0$ say a divides b if $b = a \cdot k$ for some $k \in \mathbb{Z}$

in other words b is a multiple of a

notation: $a|b$

d is a common divisor of a and b if $d|a$ and $d|b$

Greatest common divisor if largest integer that is a common divisor. Denoted by gcd (a, b)

a, b are relatively prime if gcd $(a, b) = 1$

ex. gcd $(48, 40) = 8$

gcd $(49, 39) = 1$

Theorem 0.2

Theorem 2.10 - Let $a, b \in \mathbb{Z} : a, b \neq 0$

There exists $r, s \in \mathbb{Z}$ s.t. gcd $(a, b) = ra + sb$

Example 0.3

gcd $(12, 20) = 2 * 12 - 1 * 20$

gcd $(14, 20) = 3 * 14 - 2 * 20$

Proof. let $S = \{ma + nb : m, n \in \mathbb{Z}$ and $ma + nb > 0\}$

$S \neq 0$ since $a^2 + b^2 > 0$

by W.O.P (well ordering property), let $d = ra + sb$ be least element of S

Claim: gcd $(a, b) = d$

First show that $d|a$ and $d|b$

Second: if $d'|a$ and $d'|b$ then $d'|d$

□

Theorem 0.4

2.9 - Division Algorithm - Review