CH 6- Greatest Common Divisor

Luke Lu • 2025-10-01

Theorem BBD

Info — **Bound By Divisibility**
$\forall a, b \in \mathbb{Z}$, if $b \mid a$ and $a \neq 0$, then $b \leq |a|$

Division Algorithm

$\forall a \in \mathbb{Z}, b$ in positive integers, $\exists$ a unique integers q and r s.t. $a = qb + r$ where $0 \leq r < b$

Greatest Common Divisor

Let a and b be integer. An integer c is called a **common divisor** of a and b if $c \mid a$ and $c \mid b$

If a and b are not both zero, an integer $d > 0$ is the **greatest common divisor** of a and be written $d = \gcd(a, b)$, when

1. d is a common divisor of a and b
2. $\forall$ integers c, if c is a common divisor of a and b, then $c \leq d$

If a and b are both zero, we define $\gcd(a, b) = \gcd(0, 0) = 0$

⚠️ **Warning** — Let $a \in \mathbb{Z}$then
1. $\gcd(a, a) = |a|$
2. $\gcd(0, a) = |a|$

Example:

Let $a, b \in \mathbb{Z}$, prove that $\gcd(3a + b, a) = \gcd(a, b)$

Proof

Let $a, b \in \mathbb{Z}$, let $c = \gcd(3a + b, a)$ and $d = \gcd(a, b)$.

1. Suppose a, b are not both 0:

Note that $3a + b$ and a are not both 0 as well.

Then $c \mid (3a + b), c \mid a$ and $\forall k \in \mathbb{Z}$ if k is a common divisor of $3a + b$ and a, then $k \leq c, c > 0$

Similarly, $d \mid a, d \mid b$, and $\forall l \in \mathbb{Z}$ if l is a common divisor of a and b then $l \leq d, d > 0$

Notice that since $d \mid a$ and $d \mid b$, by DIC, $d \mid (3a + b)$.
This tells us that d is a common divisor of $3a + b$ and a. By definition, $d \leq c$.

Since $c \mid (3a + b)$ and $c \mid a$, then by DIC, $c \mid ((3a + b) + (-3a)) = c \mid b$.
Thus c is a common divisor of a and b. By definition, $c \leq d$

Since $c \leq d$ and $d \leq c \Longrightarrow c = d \Longrightarrow \gcd(3a + b, a) = \gcd(a, b)$

2. Suppose $a = b = 0$ then $\gcd(3a + b, a) = \gcd(a, b) = \gcd(0, 0) = 0$

$\square$

Info — GCD with Remainders
$\forall a, b, q, r \in \mathbb{Z}$, if $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$