# CH 6- Greatest Common Divisor

Luke Lu • 2025-10-06

## 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 $d \leq c \implies c = d \implies \gcd(3a + b, a) = \gcd(a, b)$

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

Euclidean algorithm example:

1. Compute $\gcd(1239, 735)$

$$1239 = 1 \cdot 735 + 504$$

GCDWR says $\gcd(1239, 735) = \gcd(735, 504)$

$$735 = 1 \cdot 504 + 231$$

$\gcd(735, 504) = \gcd(504, 231)$

$$504 = 2 \cdot 231 + 42$$

$\gcd(504, 231) = \gcd(231, 42)$

$$231 = 5 \cdot 42 + 21$$

$\gcd(231, 42) = \gcd(42, 21)$

$$42 = 2 \cdot 21 + 0$$

$\gcd(42, 21) = \gcd(21, 0)$

$$\therefore \gcd(1239, 735) = 21$$

2. Find $x, y \in \mathbb{Z}$ s.t. $1239x + 735y = 21$

We work backwards from the previous example

$$21 = 5 \cdot 42 + 21$$

$$21 = 231 - 5 \cdot (504 - 2 \cdot 231)$$

$$= 11(231) - 5 \cdot 504$$

$$= 11 \cdot 735 - 16 \cdot 504$$

$$= 11 \cdot 735 - 16(1239 - 735)$$

$$= -16 \cdot 1239 + 27 \cdot 735$$

$\therefore -16 \cdot 1239 + 27 \cdot 735 = 21$

$\forall a, b \in \mathbb{Z}$ and non negative integer $d$, if

1. $d$ is a common divisor of $a$ and $b$
2. there exist integers $s$ and $t$ s.t. $as + bt = d$

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

Example:

Let $n \in \mathbb{Z}$. Prove that $\gcd(n, n+1) = 1$

Option 1: Use the definition of GCD

Option 2: Use GCD Characterization Theorem

Let $a = n, b = n + 1, d = 1$.

$d \mid a$ and $d \mid b$ because $d = 1$ divides every integer

Let $s = -1, t = 1$

These will be provide the certificate of correctness to verify that $d = 1$ is the GCD we are looking for.

$as + bt = n(-1) + (n+1)1 = 1$

$\therefore$ by GCD CT $1 = \gcd(n, n+1)$

Option 3: Use GCDWR

$n + 1 = 1 \cdot n + 1$

🐳 **Info — Bézout's Lemma**

$\forall a, b \in \mathbb{Z}, \exists s, t \in \mathbb{Z}$ s.t. $as + bt = d, d = \gcd(a, b)$

🐳 **Info — Extended Euclidean Algorithm**

| $i$ | $x$ | $y$ | $r$ | $q$ |
|---|---|---|---|---|
| $i = 1$ | $1$ | $0$ | $a$ | $0$ |
| $i = 2$ | $0$ | $1$ | $b$ | $0$ |
| $i = 3$ | $x_i = x_{i-2} - q_i x_{i-1}$ | $y_i = y_{i-2} - q_i y_{i-1}$ | $r_i = r_{i-2} - q_i r_{i-1}$ | $\left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$ |

We stop when $r_i = 0$

Note that the last $r \neq 0$ value is the $\gcd(a, b)$

Remember at each row we have $ax_i + by_i = r_i$

Let $n = i - 1$, Then $\gcd(a, b) = r_n$ and $s = x_n$ and $t = y_n$ are certificate of correctness

Numerical Examples:

1. Find $\gcd(56, 35)$ and solve for $s, y \in \mathbb{Z}$ for $56x + 35y = \gcd(56, 35)$

| $i$ | $x$ | $y$ | $r$ | $q$ |
|---|---|---|---|---|
| $i = 1$ | 1 | 0 | 56 | 0 |
| $i = 2$ | 0 | 1 | 35 | 0 |
| $i = 3$ | 1 | $-1$ | 21 | 1 |
| $i = 4$ | $-1$ | 2 | 14 | 1 |
| $i = 5$ | 2 | $-3$ | 7 | 1 |
| $i = 6$ | $-5$ | 8 | 0 | 2 |

So $\gcd(56, 35) = 7$. According to EEA, $s = x_5 = 2$ and $t = y_5 = -3$ are certificate of correctness

Check $56(2) + 35(-3) = 112 - 105 = 7$ which is true

2. Find integers $x, y, d$ s.t. $408x + 170y = d = \gcd(408, 170)$

| $i$ | $x$ | $y$ | $r$ | $q$ |
|---|---|---|---|---|
| $i = 1$ | 1 | 0 | 408 | 0 |
| $i = 2$ | 0 | 1 | 170 | 0 |
| $i = 3$ | 1 | $-2$ | 68 | 2 |
| $i = 4$ | $-2$ | 5 | 34 | 2 |
| $i = 5$ | 5 | $-12$ | 0 | 2 |

So $\gcd(408, 170) = 34$. According to EEA, $s = x_4 = -2$ and $t = y_4 = 5$ are certificate of correctness

Check $408(-2) + 170(5) = 34$ which is true