CH 6- Greatest Common Divisor

Luke Lu • 2025-10-24

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

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

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

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

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

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

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

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

🐳 **Info — GCD Characterization Theorem**
$\forall a, b \in \mathbb{Z}$ 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

🐳 **Info — Common Divisor Divides GCD**

$$\forall a, b, c \in \mathbb{Z}, \text{if } c \mid a \text{ and } c \mid b, \text{then } c \mid \gcd(a, b)$$

Examples:

1. Prove $\forall a, b, c, \in \mathbb{Z}$, if $\gcd(ab, c) = 1$, then $\gcd(a, c) = \gcd(b, c) = 1$

Proof

Let $a, b, c \in \mathbb{Z}$. Assume that $\gcd(ab, c) = 1$.
By BL, $\exists s, t \in \mathbb{Z}$ s.t. $ab \cdot s + c \cdot t = 1$
$a(bs) + ct = 1$
$b(as) + ct = 1$
Since $a, b, s, t \in \mathbb{Z}$, $bs \in \mathbb{Z}$ and $as \in \mathbb{Z}$, 1 can be expressed as an integer combination of a and c, as well as an integer combination of b and c.

Meanwhile, 1 is clearly a common divisor of a, c and b, c. Since $1 \mid x \forall z \in \mathbb{Z}$.
$\therefore$ By $\text{GCDCT}, \gcd(a, b) = 1$ and $\gcd(b, c) = 1$

$\square$

2. Is converse of 1. true?

Prime Numbers

💡 **Tip** — Two integers a, b are **comprime** if $\gcd(a, b) = 1$

🐳 **Info** — **Coprimeness Characterization Theorem**

$$\forall a, b \in \mathbb{Z}, \gcd(a, b) = 1 \iff \exists s, t \in \mathbb{Z} \text{ s.t. } as + bt = 1$$

🐳 **Info** — **Division by the GCD**

$$\forall a, b \in \mathbb{Z}, \text{not both zero}, \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \text{ where } d = \gcd(a, b)$$

🐳 **Info** — **Coprimeness and Divisibility**

$$\forall a, b, c \in \mathbb{Z}, \text{if } c \mid ab \text{ and } \gcd(a, c) = 1, \text{then } c \mid b$$

🐳 **Info** — Evey natural number $n > 1$ can be written as a product of primes

Proof

We will prove that the open setnence $P(n)$: the number n can be wirtten as a product of primes is true for all naturanl numbers $n > 1$ by strong induction.

Base case: $n = 2 \Longrightarrow 2 = 2$, so $P(2)$ is true.

Induction Step:
Let $k \in \mathbb{N}, k \geq 2$, assume that $P(2) \land P(3) \land \ldots \land P(k)$ is true. That is $\forall i \in 2, \ldots, k, i$ can be expressed as a product of primes.
Consider $k + 1$:
If $k + 1$ is prime, then $k + 1$ is already a product of primes, so $P(k + 1)$ is true.
If $k + 1$ is composite, meaning $\exists s, r \in \mathbb{N}$ with $2 \leq s, r < k + 1 \Longrightarrow 2 \leq s, r \leq k$ s.t. $k + 1 = r \cdot s$.
By I.H., both s, r can be written as a product or primes. That is $P(k + 1)$is true.
By Principle of Strong Induciton, $P(n)$ is true $\forall n \in \mathbb{N}, n \geq 2$

$\square$

🐳 **Info — Euclid's Lemma**
$\forall a, b \in \mathbb{Z}$, and prime numbers $p, p \mid ab \implies p \mid a \vee p \mid b$

Generalized Euclid's Lemma
Let p be a prime number, $n \in \mathbb{N}$, and $a_1, a_2, ..., a_n \in \mathbb{Z}, p \mid (a_1 a_2 ... a_n) \implies p \mid a_i$ for some $i = 1, 2, ..., n$

🐳 **Info — Unique Prime Factorization**
Every natural number $n > 1$ can be written as a product of primes factors uniquely, apart from the order of factors

Prime Factorization and GCD

🐳 **Info — Divisors From Prime Factorization**
Let n and c be positive integers, and let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} ... p_k^{\alpha_k}$$

be a way to express n as a product of the distinct primes $p_1, p_2, ..., p_n$, where some or all of exponents may be zero. The integer c is a positive divisor of $n \iff c$ can be represented as a product

$$c = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}, \text{where } 0 \leq \beta_i \leq \alpha_i \text{ for} = 1, 2, ..., k$$

Example:
Let $a, b \in \mathbb{Z}$. Prove that $a^2 \mid b^2 \iff a \mid b$

Let $a, b \in \mathbb{Z}$.

1. $(\impliedby)$ Assume $a \mid b$. By definition, $\exists k \in \mathbb{Z}, b = ka \implies b^2 = k^2 a^2$.

$$\therefore a \mid b \implies a^2 \mid b^2$$

2. $(\implies)$ Assume $a^2 \mid b^2$

- Case 1: If $a = 0 \implies a^2 = 0; a^2 \mid b^2 \implies 0 \mid b^2$.

  $$\therefore \exists l \in \mathbb{Z}, b^2 = 0 \cdot l \implies b^2 = 0 \implies b = 0 \implies a \mid b$$

- Case 2: If $a \neq 0$ and $b = 0$ the statement $a \mid b$ becomes $a \mid 0$, which is true $\forall a \in \mathbb{Z}$.
  $\therefore a \mid b$

- Case 3: If $a \neq 0, b \neq 0$, then $|a| > 0, |b| > 0$.

  $|b| = p_1^{\beta_1} ... p_k^{\beta_k}$ and $|a| = p_1^{\alpha_1} ... p_k^{\alpha_k}, p_1, ... p_k$ is a list of all distinct primes that are factors of $|a|$ and $|b|$. then $b^2 = p_1^{2\beta_1} ... p_k^{2\beta_k}, a^2 = p_1^{2\alpha_1} ... p_k^{2\alpha_k}$.
  Now, since $a^2 \mid b^2$, by DFPF, $0 \leq 2\alpha_i \leq 2\beta_i \forall = 1, ..., k$.
  Dividing by $2, 0 \leq \alpha_i \leq \beta_i$. By DFPF, $a \mid b$

🐋 **Info — GCD From Prime Factorization**
Let $a, b \in \mathbb{N}$ and let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

be ways to express a and b as products of the distinct primes $p_1, p_2, \dots, p_k$ where all of the exponenets may be zero. We have

$$\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k} \text{ where } \gamma_i = \min\{\alpha_i, \beta_i\} \text{ for } i = 1, 2, \dots, k$$

Example:

Find the $\gcd(20000, 30000)$

ANS:
$20000 = 2 \cdot 10^4 = 2^5 \cdot 5^4 = 2^5 \cdot 3^0 \cdot 5^4, 30000 = 3 \cdot 10^4 = 2^4 \cdot 3 \cdot 5^4$
By GCDPF: $\gcd(20000, 30000) = 2^4 \cdot 3^0 \cdot 5^4 = 10^4 = 10000$