Definition: Greatest Common Divisor

Definition: Greatest Common Divisor

The **greatest common divisor (GCD)** of two integers is the largest positive integer that divides both numbers.

Definition

Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the unique positive integer d such that:

1. $d \mid a$ and $d \mid b$ (i.e., d divides both a and b)
2. If $c \mid a$ and $c \mid b$ for some integer c, then $c \mid d$

Alternative Characterization

$\gcd(a, b)$ is the largest element in the set:

$$\{d \in \mathbb{Z}^+ : d \mid a \text{ and } d \mid b\}$$

Properties

1. **Commutativity**: $\gcd(a, b) = \gcd(b, a)$
2. **Associativity**: $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$
3. **Identity**: $\gcd(a, 0) = |a|$ for $a \neq 0$
4. **Scaling**: $\gcd(ka, kb) = |k| \cdot \gcd(a, b)$ for any integer k
5. **Bézout's Identity**: There exist integers x, y such that $\gcd(a, b) = ax + by$

Euclidean Algorithm

The GCD can be computed efficiently using the Euclidean algorithm:

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

Repeating until the remainder is 0.

Special Cases

- $\gcd(a, a) = |a|$
- $\gcd(a, 1) = 1$ for any integer a
- If $\gcd(a, b) = 1$, we say a and b are **coprime** or **relatively prime**

Examples

1. $\gcd(12, 18) = 6$
2. $\gcd(17, 19) = 1$ (17 and 19 are coprime)
3. $\gcd(0, 5) = 5$
4. $\gcd(-24, 36) = 12$

Extended Definition

For a finite set of integers $\{a_1, a_2, \ldots, a_n\}$ not all zero:

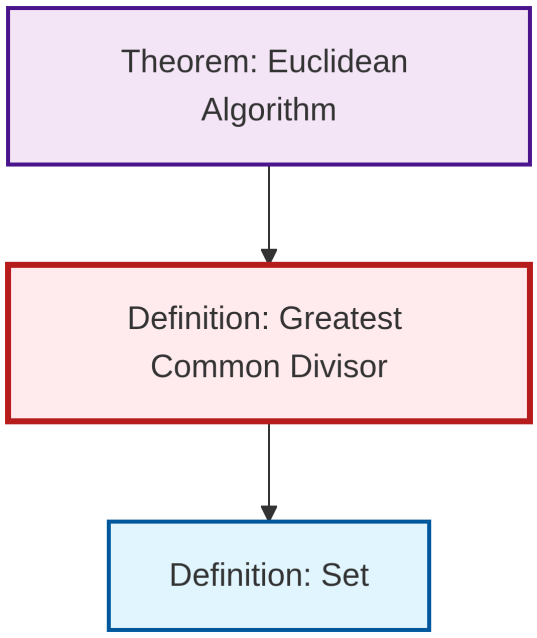
$$\gcd(a_1, a_2, \ldots, a_n) = \gcd(a_1, \gcd(a_2, \ldots, a_n))$$

Mermaid Diagram

```
graph TD
    A[GCD(a,b)] --> B[Largest Common Divisor]
    B --> C[d | a and d | b]
    B --> D[c | a, c | b   c | d]
    A --> E[Properties]
    E --> F[Commutative]
    E --> G[Associative]
    E --> H[Bézout's Identity]
    A --> I[Euclidean Algorithm]
    I --> J[gcd(a,b) = gcd(b, a mod b)]

    style A fill:#f9f,stroke:#333,stroke-width:2px
    style B fill:#bbf,stroke:#333,stroke-width:2px
    style H fill:#bfb,stroke:#333,stroke-width:2px
    style I fill:#bbf,stroke:#333,stroke-width:2px
```

Dependency Graph



Local dependency graph