Info

This note, that was found here, as a part of a collection
is written (completely with human hands) by Rupadarshi Ray,
was created on March 13, 2026 6:24:18 PM,
was last modified on September 7, 2026 1:56:03 PM, and
was exported on September 7, 2026 3:04:03 PM.

$\gcd$ of integers

Definition. Let $a, b \in \mathbb{Z}, a \neq 0$. Then b **is divisible by** a or a **divides** b if

$$b \in a\mathbb{Z}$$

Definition.

$$\gcd(a, b) := \max \{d \geq 1 | a, b \in d\mathbb{Z}\}$$

Let $a, b \in \mathbb{Z}$, not both zero. Then

$$\gcd(a, b) = \min \mathbb{Z}\{a, b\} \cap \mathbb{Z}_{>0}$$

Consider

$$S := \mathbb{Z}\{a, b\} \cap \mathbb{Z}_{>0}$$

- If $a \neq 0$ then $\pm a \in S$, so S is not empty.
- Consider

$$d := \min S = \min \mathbb{Z}\{a, b\} \cap \mathbb{Z}_{>0}$$

and

$$d = ax + by$$

- By

Let $a, b \in \mathbb{Z}, b > 0$ then there exists unique $q, r \in \mathbb{Z}$ such that $r \in [0, b)$

$$a = \underbrace{q}_{\text{quotient}} b + \underbrace{r}_{\text{remainder}}$$

we have $q, r \in \mathbb{Z}$ such that

$$a = qd + r, r \in [0, d)$$

- Then

$$\begin{aligned} r &= a - qd \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \\ &\in \mathbb{Z}\{a, b\} \end{aligned}$$

- If $r > 0$ then $r \in S$ which contradicts $r \in [0, d) \cap d = \min S$.
- Thus $r = 0$
- Hence,

$$a = qd$$

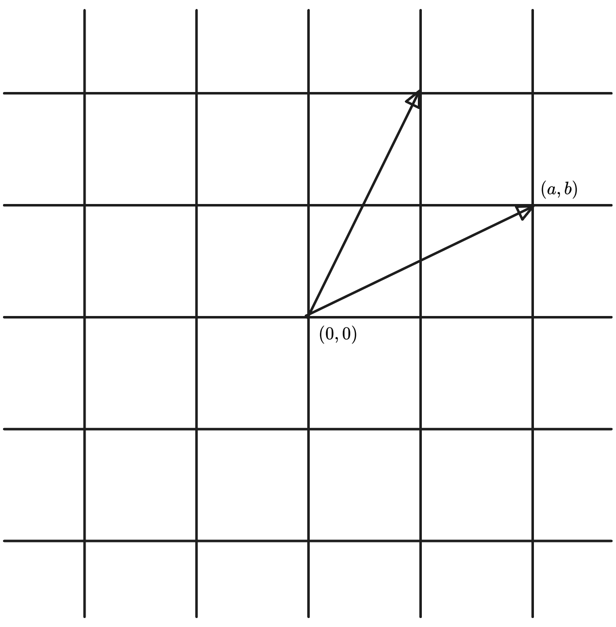
and similarly $b = q'd$ so d is a common divisor of a, b

$$a, b \in d\mathbb{Z}$$

- Let c be another common divisor

$$\begin{aligned} & a, b \in c\mathbb{Z} \\ \implies & d = ax + by \in c\mathbb{Z} \\ \implies & \frac{d}{c} = \left|\frac{d}{c}\right| \in \mathbb{Z} \\ \implies & d \geq c \end{aligned}$$

- Thus d is the greatest among all common divisors of d.



$(x, y) \mapsto ax + by$

https://www.desmos.com/calculator/ipp1prje1z

Let $a, b \in \mathbb{Z}$, not both zero. Then

$$\mathbb{Z}\{a, b\} = \gcd(a, b)\mathbb{Z}$$

- As

$$\begin{aligned} a, b &\in \gcd(a,b)\mathbb{Z} \\ \implies ax + by &\in \gcd(a,b)\mathbb{Z} \end{aligned}$$

  we have

$$\mathbb{Z}\{a,b\} \subseteq \gcd(a,b)\mathbb{Z}$$

- Now, because

$$\gcd(a,b) \in \mathbb{Z}\{a,b\}$$

  by

  > Let $a, b \in \mathbb{Z}$, not both zero. Then
  >
  > $$\gcd(a,b) = \min \mathbb{Z}\{a,b\} \cap \mathbb{Z}_{>0}$$

  we have

$$\gcd(a,b)\mathbb{Z} \subseteq \mathbb{Z}\{a,b\}$$

Let $a, b \in \mathbb{Z}$, not both zero. Then

$$\gcd(a,b) = 1 \iff 1 \in \mathbb{Z}\{a,b\} \iff \mathbb{Z}\{a,b\} = \mathbb{Z}$$

(Euclid's lemma)

$$\gcd(a,b) = 1, bc \in a\mathbb{Z} \implies c \in a\mathbb{Z}$$

Current note has 0 direct children and 0 total descendants.

- stretchy
  - $\mathbb{Z}$
    - gcd of integers

And it has 6 siblings.

- stretchy
  - $\mathbb{Z}$
    - Division in $\mathbb{Z}$
    - Euler totient function
    - gcd of integers
    - Primes in $\mathbb{N}$
    - Partitions of naturals
    - Prime-representing function