# Euclid’s algorithm

# Euclid's algorithm

Suppose we have $a, b \in \mathbb{N}$, and we want to find $\gcd(a, b)$.

# Euclid's algorithm

Suppose we have $a, b \in \mathbb{N}$, and we want to find $\gcd(a, b)$.

(Can assume $a \geqslant b$.)

# Euclid's algorithm

Suppose we have $a, b \in \mathbb{N}$, and we want to find $\gcd(a, b)$.

(Can assume $a \geqslant b$.)

- If $b \mid a$, then $\gcd(a, b) = b$, and we can stop.

# Euclid's algorithm

Suppose we have $a, b \in \mathbb{N}$, and we want to find $\gcd(a, b)$.

(Can assume $a \geqslant b$.)

- If $b \mid a$, then $\gcd(a, b) = b$, and we can stop.
- Otherwise, find $q, r$ with $0 < r < b$ such that $a = qb + r$.

# Euclid's algorithm

Suppose we have $a, b \in \mathbb{N}$, and we want to find $\gcd(a, b)$.

(Can assume $a \geqslant b$.)

- If $b \mid a$, then $\gcd(a, b) = b$, and we can stop.
- Otherwise, find $q, r$ with $0 < r < b$ such that $a = qb + r$. Then $\gcd(a, b) = \gcd(b, r)$, so we can replace $a, b$ with the smaller numbers $b, r$, and repeat.

# Example

# Example

Want $\gcd(110, 32)$.

# Example

Want $\gcd(110, 32)$.

$110 = 3 \times 32 + 14$ so $\gcd(110, 32) = \gcd(32, 14)$.

# Example

Want $\gcd(110, 32)$.

$110 = 3 \times 32 + 14$ so $\gcd(110, 32) = \gcd(32, 14)$.

$32 = 2 \times 14 + 4$ so $\gcd(32, 14) = \gcd(14, 4)$.

# Example

Want $\gcd(110, 32)$.

$110 = 3 \times 32 + 14$ so $\gcd(110, 32) = \gcd(32, 14)$.

$32 = 2 \times 14 + 4$ so $\gcd(32, 14) = \gcd(14, 4)$.

$14 = 3 \times 4 + 2$ so $\gcd(14, 4) = \gcd(4, 2)$.

# Example

Want $\gcd(110, 32)$.

$110 = 3 \times 32 + 14$ so $\gcd(110, 32) = \gcd(32, 14)$.

$32 = 2 \times 14 + 4$ so $\gcd(32, 14) = \gcd(14, 4)$.

$14 = 3 \times 4 + 2$ so $\gcd(14, 4) = \gcd(4, 2)$.

$2 \mid 4$, so $\gcd(4, 2) = 2$.

# Lowest common multiple

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) =$

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) =$

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.
- $\operatorname{lcm}(99, 100) =$

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.
- $\operatorname{lcm}(99, 100) = 9900$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.
- $\operatorname{lcm}(99, 100) = 9900$.
- $\operatorname{lcm}(1, b) =$

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.
- $\operatorname{lcm}(99, 100) = 9900$.
- $\operatorname{lcm}(1, b) = b$.

# Lowest common multiple

$a, b \in \mathbb{N}$. The lowest common multiple of $a$ and $b$ is the smallest $m \in \mathbb{N}$ such that $a \mid m$ and $b \mid m$.

Write $\operatorname{lcm}(a, b)$.

**Examples**

- $\operatorname{lcm}(6, 10) = 30$.
- $\operatorname{lcm}(9, 12) = 36$.
- $\operatorname{lcm}(99, 100) = 9900$.
- $\operatorname{lcm}(1, b) = b$.

How do we find $\operatorname{lcm}(a, b)$ quickly?

# Lowest common multiple

# Lowest common multiple

**Lemma 4.7:** Let $m = \operatorname{lcm}(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots .$$

# Lowest common multiple

**Lemma 4.7:** Let $m = \operatorname{lcm}(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots .$$

**Example:**

# Lowest common multiple

**Lemma 4.7:** Let $m = \operatorname{lcm}(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots.$$

**Example:** $\operatorname{lcm}(6, 10) = 30$.

# Lowest common multiple

**Lemma 4.7:** Let $m = \operatorname{lcm}(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots .$$

**Example:** $\operatorname{lcm}(6, 10) = 30$.

Multiples of 6:

$$6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, \ldots$$

# Lowest common multiple

**Lemma 4.7:** Let $m = \text{lcm}\,(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots.$$

**Example:** $\text{lcm}\,(6, 10) = 30$.

Multiples of 6:

$$6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, \ldots$$

Multiples of 10:

$$10, 20, 30, 40, 50, 60, 70, 80, 90, \ldots$$

# Lowest common multiple

**Lemma 4.7:** Let $m = \operatorname{lcm}(a, b)$. Then the common multiples of $a$ and $b$ are

$$m, 2m, 3m, \ldots .$$

**Example:** $\operatorname{lcm}(6, 10) = 30$.

Multiples of 6:

$$6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, \ldots$$

Multiples of 10:

$$10, 20, 30, 40, 50, 60, 70, 80, 90, \ldots$$

So the common multiples of 6 and 10 are the multiples of 30.

# Finding the lcm

# Finding the lcm

**Theorem 4.8:** Suppose $a, b \in \mathbb{N}$. Then $\operatorname{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$.