Number Theory: The Euclidean Algorithm

Ian Ludden

Learning Objectives

By the end of this lesson, you will be able to:

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definitions of gcd and lcm.

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.

Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.
- Apply the Euclidean algorithm to compute the gcd of two larger integers.

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and

"divides"

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

- $\gcd(8, 12) = 4$

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

- $\gcd(8, 12) = 4$
- $\gcd(-35, 20) = 5$

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

- $\gcd(8, 12) = 4$
- $\gcd(-35, 20) = 5$
- $\gcd(a, b) = \gcd(b, a)$

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

- $\gcd(8, 12) = 4$
- $\gcd(-35, 20) = 5$
- $\gcd(a, b) = \gcd(b, a)$
- For any integer $a \neq 0$, $\gcd(a, 0) = |a|$

$\forall n \in \mathbb{Z}, \ n \mid 0.$

$0 = n \cdot 0.$

Greatest Common Divisor

Definition

For any integers a and b, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a ***greatest common divisor*** (gcd) of a and b if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
2. for every common divisor d of a and b, $d \mid c$.

Examples

- $\gcd(8, 12) = 4$
- $\gcd(-35, 20) = 5$
- $\gcd(a, b) = \gcd(b, a)$
- For any integer $a \neq 0$, $\gcd(a, 0) = |a|$
- $\gcd(0, 0)$ is undefined

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
2. for every positive common multiple d of a and b, $c \leq d$.

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
2. for every positive common multiple d of a and b, $c \leq d$.

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
2. for every positive common multiple d of a and b, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
2. for every positive common multiple d of a and b, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

Examples

- $a = 4$, $b = 7$

gcd(4,7) = 1 "relatively prime"
lcm(4,7) = $\frac{4 \cdot 7}{1}$ = 28

Least Common Multiple

Definition

For any *positive* integers a and b, $c \in \mathbb{Z}^+$ is called a ***least common multiple*** (lcm) of a and b if

1. $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
2. for every positive common multiple d of a and b, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

Examples

- $a = 4$, $b = 7$
- $a = 20$, $b = 12$

$gcd(20,12) = 4$

$lcm(20,12) = \frac{20 \cdot 12}{4} = 60.$

Computing gcd

- By comparing prime factorizations (slow)

$a = 168, \quad b = 228$

$a = 2^3 \cdot 3^1 \cdot 7^1 \cdot 19^0$

$b = 2^2 \cdot 3^1 \cdot 7^0 \cdot 19^1$

$\gcd(a,b) = 2^2 \cdot 3^1 \cdot 7^0 \cdot 19^0$

$= 12$

Computing gcd

- By comparing prime factorizations (slow)
- By the Euclidean algorithm (fast, easy to do by hand)

The Division Algorithm, Revisited

Theorem

For any integers a *and* b*, where* $b > 0$*, there exist a unique quotient* $q \in \mathbb{Z}$ *and remainder* $r \in \mathbb{Z}$ *such that*

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

The Division Algorithm, Revisited

Theorem

For any integers a and b, where $b > 0$, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

Claim

For any integers a, b, q, and r, with b positive, if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

The Division Algorithm, Revisited

Theorem

For any integers a and b, where $b > 0$, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

Claim

For any integers a, b, q, and r, with b positive, if $a = bq + r$, then $gcd(a, b) = gcd(b, r)$.

See textbook, Section 4.6, for proof of claim

$n \mid a$ and $n \mid b \Rightarrow n \mid (bq) \Rightarrow n \mid (a - bq) \Rightarrow n \mid r$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

"function"

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

recursion

a % b

$a = bq + r$

$a = bq + 0$

$\gcd(a,b) \leq a$

$\gcd(a,b) \leq b$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168$, $b = 456$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168$, $b = 456$

$$168 = 456 \cdot 0 + 168$$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168,\ b = 456$

$168 = 456 \cdot 0 + 168$

a b q r

$456 = 168 \cdot 2 + 120$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168,\ b = 456$

$168 = 456 \cdot 0 + 168$

$456 = 168 \cdot 2 + 120$

$168 = 120 \cdot 1 + 48$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168$, $b = 456$

$168 = 456 \cdot 0 + 168$

$456 = 168 \cdot 2 + 120$

$168 = 120 \cdot 1 + 48$

$120 = 48 \cdot 2 + 24$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

```
procedure gcd(a, b)
    r := remainder(a, b)
    if r == 0
        return b
    else
        return gcd(b, r)
```

Example

$a = 168$, $b = 456$

$168 = 456 \cdot 0 + 168$

$456 = 168 \cdot 2 + 120$

$168 = 120 \cdot 1 + 48$

$120 = 48 \cdot 2 + 24$

$48 = 24 \cdot 2 + 0$

Recap: Learning Objectives

By the end of this lesson, you will be able to:

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.
- Apply the Euclidean algorithm to compute the gcd of two larger integers.