Euclidean Algorithm

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

Today's Objectives

- Modular Arithmetics

Today's Objectives

- Modular Arithmetics
- Euclidean Algorithm

Today's Objectives

- Modular Arithmetics
- Euclidean Algorithm

Modular Arithmetics

Set of Integers

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Modular Arithmetics

Set of Integers

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Modular Arithmetics

Set of Integers

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Definition

We say that $a(\neq 0)$ divides b, written as $a|b$, if there is an integer k with $b = ka$

Modular Arithmetics

Set of Integers

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Note: Integer by integer is not always integer

Example

There is no integer n such that $1/2 = n$

Definition

We say that $a(\neq 0)$ divides b, written as $a|b$, if there is an integer k with $b = ka$

- Examples: $2|4$, $(-7)|7$, and $6|0$

Basic Properties of Divisibility

- If $a|b$, then $a|bc$ for any c
- If $a|b$ and $b|c$, then $a|c$
- If $a|b$ and $a|c$, then $a|(xb + yc)$ for any x and y
- If $a|b$ and $b|a$, then $a = \pm b$
- If $a|b$, and $a, b > 0$, then $a \leq b$
- For any $m \neq 0$, $a|b$ is equivalent to $(ma)|(mb)$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$
- Positive divisors of 42 are $1, 2, 3, 6, 7, 14, 21, 42$

Greatest Common Divisor (GCD)

Quotient With Remainder

If $a, b > 0$ integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r \leq b - 1$.

- Furthermore, $r = 0$ if and only if $b|a$

Definition (Common Divisor)

If $d|a$ and $d|b$, then d is a common divisor of a and b

- Largest one is called greatest common divisor

Example

- Positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$
- Positive divisors of 42 are $1, 2, 3, 6, 7, 14, 21, 42$
- Common (positive) divisors are $1, 2, 3, 6$
- $GCD(30, 42) = 6$

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime
- But, 8 and 32 are not relatively prime

Relatively Prime

If $GCD(a, b) = 1$, we say a and b are relatively prime

Example

- 7 and 12 are relatively prime
- But, 8 and 32 are not relatively prime
- 11 and 13 are relatively prime

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$
- If $d > 0$ divides both a and b, then $GCD(a/d, b/d) = GCD(a, b)/d$

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$
- If $d > 0$ divides both a and b, then $GCD(a/d, b/d) = GCD(a, b)/d$
- If both a and b relatively prime to m, then so is ab

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$
- If $d > 0$ divides both a and b, then $GCD(a/d, b/d) = GCD(a, b)/d$
- If both a and b relatively prime to m, then so is ab
- For any integer x, $GCD(a, b) = GCD(a, b + ax)$

Basic facts about greatest common divisors

- If $m > 0$, then $GCD(ma, mb) = m \times GCD(a, b)$
- If $d > 0$ divides both a and b, then $GCD(a/d, b/d) = GCD(a, b)/d$
- If both a and b relatively prime to m, then so is ab
- For any integer x, $GCD(a, b) = GCD(a, b + ax)$
- If $c|ab$ and b, c are relatively prime, then $c|a$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$a = q_1 b + r_1$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \end{aligned}$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \end{aligned}$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$
\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-1} &= q_k r_k + r_k + 1
\end{aligned}
$$

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-1} &= q_k r_k + r_k + 1 \\
r_k &= q_{k+1} r_{k+1}
\end{aligned}$$

Then $d = GCD(a, b)$ is equal to the last nonzero remainder, r_{k+1}

Euclidean Algorithm

Given integers $0 < b < a$,

- repeatedly apply the division algorithm
- until a remainder of zero is obtained

Algorithm (q_i - quotient and r_i - remainder)

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{k-1} &= q_k r_k + r_k + 1 \\
r_k &= q_{k+1} r_{k+1}
\end{aligned}$$

Then $d = GCD(a, b)$ is equal to the last nonzero remainder, r_{k+1}

- **Linear Combination**: There exist integers x and y such that $d = ax + by$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$
$$30 = 2 \times 12 + 6$$
$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$
$$30 = 2 \times 12 + 6$$
$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$
$$30 = 2 \times 12 + 6$$
$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$
$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

We have to find x and y such that $6 = 30x + 42y$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$
$$30 = 2 \times 12 + 6$$
$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$
$$6 = 30 - 2 \times 12$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

Hence, $6 = 30 \times 3 - 42 \times 2$

Euclidean Algorithm - Linear Combination

Find linear combination of 30 and 42 using Euclidean Algorithm

Find the GCD of 30 and 42

$$42 = 1 \times 30 + 12$$

$$30 = 2 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Thus, GCD(42, 36) = 6

Linear Combination of (30, 42)

$$12 = 42 - 1 \times 30$$

$$6 = 30 - 2 \times 12$$

We have to find x and y such that $6 = 30x + 42y$

$$6 = 30 - 2 \times 12$$

$$6 = 30 - 2 \times (42 - 1 \times 30)$$

Hence, $6 = 30 \times 3 - 42 \times 2$

That is, $x = 3$ and $y = -2$

Thank You