Elementary Number Theory Part 2

$\gcd$ and lcm – Linear Congruence and The Ring $\mathbb{Z}_m$

MZI

School of Computing
Telkom University

SoC Tel-U

June 2023

Acknowledgements

This slide is composed based on the following materials:

1. *Discrete Mathematics and Its Applications*, 8th Edition, 2019, by K. H. Rosen (main).
2. *Discrete Mathematics with Applications*, 5th Edition, 2018, by S. S. Epp.
3. *Mathematics for Computer Science*. MIT, 2010, by E. Lehman, F. T. Leighton, A. R. Meyer.
4. Slide for Matematika Diskret 2 (2012). Fasilkom UI, by B. H. Widjaja.
5. Slide for Matematika Diskret 2 at Fasilkom UI by Team of Lecturers.
6. Slide for Matematika Diskret. Telkom University, by B. Purnama.

Some of the pictures are taken from the above resources. This slide is intended for academic purpose at FIF Telkom University. If you have any suggestions/comments/questions related to the material on this slide, send an email to `<pleasedontspam>@telkomuniversity.ac.id`.

Contents

Contents

1. $\gcd$, lcm, and Euclidean Algorithm
   - $\gcd$
   - lcm
   - Euclidean Algorithm
   - $\gcd$ as Linear Combination
   - Some Important Theorems and Challenging Problems
2. Modular Arithmetic and the Ring $\mathbb{Z}_m$
3. Linear Congruence and Its Solution
4. Linear Congruence and Ring $\mathbb{Z}_m$

Contents

1 gcd, lcm, and Euclidean Algorithm

- gcd
- lcm
- Euclidean Algorithm
- gcd as Linear Combination
- Some Important Theorems and Challenging Problems

Greatest Common Divisor, gcd

The greatest integer that divides two numbers (not both zero) is called as the greatest common divisor of these two numbers.

Definition

Suppose $a, b \in \mathbb{Z}$ and not both of them are zero. The greatest integer d that satisfies $d|a$ and $d|b$ is called as the greatest common divisor of a and b. Here, we can write d as $\gcd(a, b)$.

We have a property that d is equal to $\gcd(a, b)$ if it satisfies the two following requirements:

Greatest Common Divisor, gcd

The greatest integer that divides two numbers (not both zero) is called as the greatest common divisor of these two numbers.

Definition

Suppose $a, b \in \mathbb{Z}$ and not both of them are zero. The greatest integer d that satisfies $d|a$ and $d|b$ is called as the greatest common divisor of a and b. Here, we can write d as $\gcd(a, b)$.

We have a property that d is equal to $\gcd(a, b)$ if it satisfies the two following requirements:

1. $d|a$ and $d|b$,

Greatest Common Divisor, gcd

The greatest integer that divides two numbers (not both zero) is called as the greatest common divisor of these two numbers.

Definition

Suppose $a, b \in \mathbb{Z}$ and not both of them are zero. The greatest integer d that satisfies $d|a$ and $d|b$ is called as the greatest common divisor of a and b. Here, we can write d as $\gcd(a, b)$.

We have a property that d is equal to $\gcd(a, b)$ if it satisfies the two following requirements:

1. $d|a$ and $d|b$,
2. if there is $c \in \mathbb{Z}$ with properties $c|a$ and $c|b$, then $c|d$.

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so
$\gcd(120, 500) =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.

Exercise

Determine the gcd of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are ± 1, ± 3, and ± 9, therefore $\gcd(-3, -9) =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are ± 1, ± 3, and ± 9, therefore $\gcd(-3, -9) = 3$.

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are ± 1, ± 3, and ± 9, therefore $\gcd(-3, -9) = 3$.
5. The numbers that divides -3 are

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are ± 1, ± 3, and ± 9, therefore $\gcd(-3, -9) = 3$.
5. The numbers that divides -3 are ± 1 and ± 3, then because 0 is divisible by 3, then $\gcd(-3, 0) =$

Exercise

Determine the $\gcd$ of

1. 24 and 36
2. 17 and 22
3. 120 and 500
4. -3 and -9
5. -3 and 0

Solution: Notice that

1. Positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, then positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Therefore, $\gcd(24, 36) = 12$.
2. Positive divisors of 17 are 1 and 17, positive divisors of 22 are $1, 2, 11, 22$. Therefore $\gcd(17, 22) = 1$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, so $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. The numbers that divides -3 are ± 1 and ± 3, the numbers that divides -9 are ± 1, ± 3, and ± 9, therefore $\gcd(-3, -9) = 3$.
5. The numbers that divides -3 are ± 1 and ± 3, then because 0 is divisible by 3, then $\gcd(-3, 0) = 3$.

Theorem

If a and b are nonzero integers, with the following prime factorization

$$\begin{aligned} a &= (\pm 1)\cdot p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdot p_n^{a_n} \text{ and} \\ b &= (\pm 1)\cdot p_1^{b_1}\cdot p_2^{b_2}\cdot\cdots\cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\gcd(a,b) = p_1^{\min(a_1,b_1)}\cdot p_2^{\min(a_2,b_2)}\cdot\cdots\cdot p_n^{\min(a_n,b_n)}$. The notation $\min(a,b)$ means the minimum number between a and b.

Example

To calculate $\gcd(36, 45)$, we have $36 =$

Theorem

If a and b are nonzero integers, with the following prime factorization

$$\begin{aligned} a &= (\pm 1) \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= (\pm 1) \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_n^{\min(a_n,b_n)}$. The notation $\min(a,b)$ means the minimum number between a and b.

Example

To calculate $\gcd(36,45)$, we have $36 = 2^2 \cdot 3^2$ and $45 =$

Theorem

If a and b are nonzero integers, with the following prime factorization

$$\begin{aligned} a &= (\pm 1) \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= (\pm 1) \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_n^{\min(a_n,b_n)}$. The notation $\min(a,b)$ means the minimum number between a and b.

Example

To calculate $\gcd(36,45)$, we have $36 = 2^2 \cdot 3^2$ and $45 = 3^2 \cdot 5$, so

$$36 = 2^2 \cdot 3^2 \cdot 5^0 \text{ and } 45 = 2^0 \cdot 3^2 \cdot 5^1,$$

hence $\gcd(36,45) =$

Theorem

If a and b are nonzero integers, with the following prime factorization

$$\begin{aligned} a &= (\pm 1) \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= (\pm 1) \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_n^{\min(a_n,b_n)}$. The notation $\min(a,b)$ means the minimum number between a and b.

Example

To calculate $\gcd(36,45)$, we have $36 = 2^2 \cdot 3^2$ and $45 = 3^2 \cdot 5$, so

$$36 = 2^2 \cdot 3^2 \cdot 5^0 \text{ and } 45 = 2^0 \cdot 3^2 \cdot 5^1,$$

hence $\gcd(36,45) = 2^{\min(2,0)} \cdot 3^{\min(2,2)} \cdot 5^{\min(0,1)} = 2^0 \cdot 3^2 \cdot 5^0 = 9$.

Relatively Prime and Pairwise Relatively Prime

Definition

Two integers a and b are called relatively prime if $\gcd(a, b) = 1$.

Definition

Integers $a_1, a_2, \ldots, a_n$ are called pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for every $i \neq j$, $i, j \in \{1, 2, \ldots, n\}$.

Exercise

Check whether the following integers are pairwise relatively prime.

1. $10, 17, 21$
2. $10, 19, 24$

Notice that:

Exercise

Check whether the following integers are pairwise relatively prime.

1. $10,\ 17,\ 21$
2. $10,\ 19,\ 24$

Notice that:

1. $\gcd(10,17)=1$, $\gcd(10,21)=1$, $\gcd(17,21)=1$; therefore 10, 17, and 21 are pairwise relatively prime;

Exercise

Check whether the following integers are pairwise relatively prime.

1. $10,\ 17,\ 21$
2. $10,\ 19,\ 24$

Notice that:

1. $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, $\gcd(17, 21) = 1$; therefore 10, 17, and 21 are pairwise relatively prime;
2. $\gcd(10, 19) = 1$, $\gcd(10, 24) = 2$, $\gcd(19, 24) = 1$; therefore 10, 19, and 24 are not pairwise relatively prime.

Important Theorem on $\gcd$

Some properties of $\gcd$ are explained in the following theorems.

Theorem

Suppose a and b are two integers, not both zero, then

1. each common factor of a and b divides $\gcd(a, b)$;
2. for every $k > 0$ we have $\gcd(ka, kb) = k \cdot \gcd(a, b)$;
3. if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$;
4. if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$;
5. $\gcd(a, b) = \gcd(b, a \bmod b)$.

To find $\gcd$ from three numbers, e.g.: a, b, and c, we can use the following theorem.

Theorem

If a, b, and c are three numbers, not all of them are zero, then

$$\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b).$$

Thus, the $\gcd$ of the three numbers a, b, and c can be written as $\gcd(a, b, c)$.

Contents

1 gcd, lcm, and Euclidean Algorithm

- gcd
- lcm
- Euclidean Algorithm
- gcd as Linear Combination
- Some Important Theorems and Challenging Problems

Least Common Multiple, lcm

The smallest integer that is a multiple of two positive numbers is called as the least common multiple of the two numbers.

Definition

Suppose $a, b \in \mathbb{Z}^+$. The smallest integer c that is the smallest multiple of a and b is called as the least common multiple of a and b. Here, we can write c as $\mathrm{lcm}\,(a, b)$.

We have properties that c is equal to $\mathrm{lcm}\,(a, b)$ if it satisfies the two following requirements:

Least Common Multiple, lcm

The smallest integer that is a multiple of two positive numbers is called as the least common multiple of the two numbers.

Definition

Suppose $a, b \in \mathbb{Z}^+$. The smallest integer c that is the smallest multiple of a and b is called as the least common multiple of a and b. Here, we can write c as $\mathrm{lcm}\,(a, b)$.

We have properties that c is equal to $\mathrm{lcm}\,(a, b)$ if it satisfies the two following requirements:

1. $a|c$ and $b|c$,

Least Common Multiple, lcm

The smallest integer that is a multiple of two positive numbers is called as the least common multiple of the two numbers.

Definition

Suppose $a, b \in \mathbb{Z}^+$. The smallest integer c that is the smallest multiple of a and b is called as the least common multiple of a and b. Here, we can write c as $\mathrm{lcm}\,(a, b)$.

We have properties that c is equal to $\mathrm{lcm}\,(a, b)$ if it satisfies the two following requirements:

1. $a|c$ and $b|c$,
2. if there is $d \in \mathbb{Z}$ with properties $a|d$ and $b|d$, then $c|d$.

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\operatorname{lcm}(24, 36) =$

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.
2. Multiples of 7 are

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\mathrm{lcm}\,(7, 3) =$

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\operatorname{lcm}(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\operatorname{lcm}(7, 3) = 21$.

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\mathrm{lcm}\,(7, 3) = 21$.
3. We have $120 =$

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\operatorname{lcm}(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\operatorname{lcm}(7, 3) = 21$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 =$

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\mathrm{lcm}\,(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\mathrm{lcm}\,(7, 3) = 21$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, hence $\mathrm{lcm}\,(120, 500) =$

Exercise

Determine the lcm of

1. 24 and 36,
2. 7 and 3,
3. 120 and 500,

Solution: Notice that

1. Multiples of 24 are $24, 48, 72, 96, \ldots$, multiples of 36 are $36, 72, 108, \ldots$, therefore we obtain $\operatorname{lcm}(24, 36) = 72$.
2. Multiples of 7 are $7, 14, 21, \ldots$, multiples of 3 are $3, 9, 12, 15, 18, 21, \ldots$, therefore we obtain $\operatorname{lcm}(7, 3) = 21$.
3. We have $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, hence $\operatorname{lcm}(120, 500) = 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)} = 2^3 \cdot 3 \cdot 5^3 = 3000$.

Theorem

If a and b are positive integers with the following prime factorization

$$\begin{aligned} a &= p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_n^{\max(a_n,b_n)}$. The notation $\max(a, b)$ means the maximum number between a and b.

Example

To calculate $\operatorname{lcm}(36, 45)$, we have $36 =$

Theorem

If a and b are positive integers with the following prime factorization

$$\begin{aligned} a &= p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_n^{\max(a_n,b_n)}$. The notation $\max(a,b)$ means the maximum number between a and b.

Example

To calculate $\operatorname{lcm}(36, 45)$, we have $36 = 2^2 \cdot 3^2$ and $45 =$

Theorem

If a and b are positive integers with the following prime factorization

$$\begin{aligned} a &= p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_n^{\max(a_n,b_n)}$. The notation $\max(a, b)$ means the maximum number between a and b.

Example

To calculate $\operatorname{lcm}(36, 45)$, we have $36 = 2^2 \cdot 3^2$ and $45 = 3^2 \cdot 5$, so

$$36 = 2^2 \cdot 3^2 \cdot 5^0 \text{ and } 45 = 2^0 \cdot 3^2 \cdot 5^1,$$

hence $\operatorname{lcm}(36, 45) =$

Theorem

If a and b are positive integers with the following prime factorization

$$\begin{aligned} a &= p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \text{ and} \\ b &= p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}, \end{aligned}$$

where p_i is a (positive) prime number, a_i and b_i are *nonnegative integers* for every $i = 1, 2, \ldots, n$, then $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \cdots \cdot p_n^{\max(a_n, b_n)}$. The notation $\max(a, b)$ means the maximum number between a and b.

Example

To calculate $\operatorname{lcm}(36, 45)$, we have $36 = 2^2 \cdot 3^2$ and $45 = 3^2 \cdot 5$, so

$$36 = 2^2 \cdot 3^2 \cdot 5^0 \text{ and } 45 = 2^0 \cdot 3^2 \cdot 5^1,$$

hence $\operatorname{lcm}(36, 45) = 2^{\max(2,0)} \cdot 3^{\max(2,2)} \cdot 5^{\max(0,1)} = 2^2 \cdot 3^2 \cdot 5^1 = 180$.

Contents

1. gcd, lcm, and Euclidean Algorithm
    - gcd
    - lcm
    - Euclidean Algorithm
    - gcd as Linear Combination
    - Some Important Theorems and Challenging Problems

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm. The $\gcd$ of 91 and 287 can be obtained using the following steps:

$$287 = 91 \cdot 3 + 14 \quad \Big|$$

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm.
The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$ | a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$

Euclid's Algorithm – Motivation

To find the gcd from two large numbers, we can use Euclidean algorithm. The gcd of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$ a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	

Euclid's Algorithm – Motivation

To find the gcd from two large numbers, we can use Euclidean algorithm. The gcd of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\mathrm{gcd}\,(91, 287)$ is reduced into finding $\mathrm{gcd}\,(14, 91)$
$14 = 7 \cdot 2 + 0$	

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm.
The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\gcd(91, 287)$ is reduced into finding $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	finding $\gcd(14, 91)$ is reduced into finding $\gcd(7, 14)$

Since $14 = 7 \cdot 2$, then $\gcd(14, 7) =$

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm. The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\gcd(91, 287)$ is reduced into finding $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	finding $\gcd(14, 91)$ is reduced into finding $\gcd(7, 14)$

Since $14 = 7 \cdot 2$, then $\gcd(14, 7) = 7$. Consequently, since $\gcd(287, 91) =$

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm. The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\gcd(91, 287)$ is reduced into finding $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	finding $\gcd(14, 91)$ is reduced into finding $\gcd(7, 14)$

Since $14 = 7 \cdot 2$, then $\gcd(14, 7) = 7$. Consequently, since $\gcd(287, 91) = \gcd(91, 14) =$

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm. The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\gcd(91, 287)$ is reduced into finding $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	finding $\gcd(14, 91)$ is reduced into finding $\gcd(7, 14)$

Since $14 = 7 \cdot 2$, then $\gcd(14, 7) = 7$. Consequently, since $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) =$

Euclid's Algorithm – Motivation

To find the $\gcd$ from two large numbers, we can use Euclidean algorithm. The $\gcd$ of 91 and 287 can be obtained using the following steps:

$287 = 91 \cdot 3 + 14$	a divisor of 91 and 287 is also a divisor of $287 - 91 \cdot 3 = 14$
	a divisor of 91 and 14 is also a divisor of $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	finding $\gcd(91, 287)$ is reduced into finding $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	finding $\gcd(14, 91)$ is reduced into finding $\gcd(7, 14)$

Since $14 = 7 \cdot 2$, then $\gcd(14, 7) = 7$. Consequently, since $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$, then our search for the $\gcd$ of 91 and 287 has finished and we have $\gcd(287, 91) = 7$.

Euclid's Algorithm – Theorem

Theorem

If $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem

For $a, b \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, a \bmod b)$.

The proof can be read on the textbook.

Euclid's Algorithm – Iterative Version

Euclid's Algorithm – Iterative Version

```
function $\gcd(a, b)$          // $a, b \in \mathbb{Z}^+$
    $x := a$
    $y := b$
    while $y \neq 0$
        $r := x \bmod y$
        $x := y$
        $y := r$
    return $x$                 // $\gcd(a, b) = x$
```

Euclid's Algorithm – Recursive Version

Euclid's Algorithm – Recursive Version

```
function $\gcd(a, b)$                          // $a, b \in \mathbb{Z}^{+}$
    if $b = 0$
        return $a$
    else
        return $\gcd(b, a \bmod b)$
        // $\gcd(a, b) = \gcd(b, a \bmod b)$
```

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$662 =$$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= \end{aligned}$$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= \end{aligned}$$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &=
\end{aligned}$$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= \end{aligned}$$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Therefore, $\gcd(414, 662) =$

Exercise

Determine the $\gcd$ of 414 and 662 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Therefore, $\gcd(414, 662) = 2$.

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\gcd(1147, 899) \quad =$$

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned} \gcd(1147, 899) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\ &= \end{aligned}$$

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}\gcd(1147, 899) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\ &= \gcd(248, \underbrace{899 \bmod 248}_{155}) \\ &= \end{aligned}$$

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}
\gcd(1147, 899) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\
&= \gcd(248, \underbrace{899 \bmod 248}_{155}) \\
&= \gcd(155, \underbrace{248 \bmod 155}_{93}) \\
&=
\end{aligned}$$

Exercise

Determine the gcd of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}
\gcd(1147, 899) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\
&= \gcd(248, \underbrace{899 \bmod 248}_{155}) \\
&= \gcd(155, \underbrace{248 \bmod 155}_{93}) \\
&= \gcd(93, \underbrace{155 \bmod 93}_{62}) \\
&=
\end{aligned}$$

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}
\gcd\left(1147, 899\right) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\
&= \gcd(248, \underbrace{899 \bmod 248}_{155}) \\
&= \gcd(155, \underbrace{248 \bmod 155}_{93}) \\
&= \gcd(93, \underbrace{155 \bmod 93}_{62}) \\
&= \gcd(62, \underbrace{93 \bmod 62}_{31}) \\
&=
\end{aligned}$$

Exercise

Determine the $\gcd$ of 1147 and 899 using Euclid's algorithm.

Solution: Notice that

$$\begin{aligned}
\gcd(1147, 899) &= \gcd(899, \underbrace{1147 \bmod 899}_{=248}) \\
&= \gcd(248, \underbrace{899 \bmod 248}_{155}) \\
&= \gcd(155, \underbrace{248 \bmod 155}_{93}) \\
&= \gcd(93, \underbrace{155 \bmod 93}_{62}) \\
&= \gcd(62, \underbrace{93 \bmod 62}_{31}) \\
&= \gcd(31, \underbrace{62 \bmod 31}_{=0}) = \gcd(31, 0) = 31.
\end{aligned}$$

Contents

1 gcd, lcm, and Euclidean Algorithm
- gcd
- lcm
- Euclidean Algorithm
- gcd as Linear Combination
- Some Important Theorems and Challenging Problems

gcd as Linear Combinations – Bézout's Theorem

If $a, b \in \mathbb{Z}$ are not both zero, then $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Furthermore, we have $\gcd(a,b) \mid sa + tb$, for every $s, t \in \mathbb{Z}$.

Theorem (Bézout's Theorem)

If $a, b \in \mathbb{Z}$, then there are $s, t \in \mathbb{Z}$ that satisfy $\gcd(a,b) = sa + tb$.

On the above theorem, the equation $\gcd(a,b) = sa + tb$ is called as Bézout's identity, the numbers s and t are called Bézout's coefficients. For example, we have $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Bézout's coefficient is not unique, for example, we have

$$\begin{aligned} & \vdots \\ \gcd(6,14) = 2 \quad & = \end{aligned}$$

gcd as Linear Combinations – Bézout's Theorem

If $a, b \in \mathbb{Z}$ are not both zero, then $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Furthermore, we have $\gcd(a,b) \mid sa + tb$, for every $s, t \in \mathbb{Z}$.

Theorem (Bézout's Theorem)

If $a, b \in \mathbb{Z}$, then there are $s, t \in \mathbb{Z}$ that satisfy $\gcd(a,b) = sa + tb$.

On the above theorem, the equation $\gcd(a,b) = sa + tb$ is called as Bézout's identity, the numbers s and t are called Bézout's coefficients. For example, we have $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Bézout's coefficient is not unique, for example, we have

$$\begin{aligned} & \vdots \\ \gcd(6,14) = 2 &= (-2) \cdot 6 + (1) \cdot 14 \\ &= \end{aligned}$$

gcd as Linear Combinations – Bézout's Theorem

If $a, b \in \mathbb{Z}$ are not both zero, then $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Furthermore, we have $\gcd(a,b) \mid sa + tb$, for every $s, t \in \mathbb{Z}$.

Theorem (Bézout's Theorem)

If $a, b \in \mathbb{Z}$, then there are $s, t \in \mathbb{Z}$ that satisfy $\gcd(a,b) = sa + tb$.

On the above theorem, the equation $\gcd(a,b) = sa + tb$ is called as Bézout's identity, the numbers s and t are called Bézout's coefficients. For example, we have $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Bézout's coefficient is not unique, for example, we have

$$\begin{aligned} & \vdots \\ \gcd(6,14) = 2 &= (-2) \cdot 6 + (1) \cdot 14 \\ &= (5) \cdot 6 + (-2) \cdot 14 \\ &= \end{aligned}$$

gcd as Linear Combinations – Bézout's Theorem

If $a, b \in \mathbb{Z}$ are not both zero, then $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. Furthermore, we have $\gcd(a,b) \mid sa + tb$, for every $s, t \in \mathbb{Z}$.

Theorem (Bézout's Theorem)

If $a, b \in \mathbb{Z}$, then there are $s, t \in \mathbb{Z}$ that satisfy $\gcd(a,b) = sa + tb$.

On the above theorem, the equation $\gcd(a,b) = sa + tb$ is called as Bézout's identity, the numbers s and t are called Bézout's coefficients. For example, we have $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Bézout's coefficient is not unique, for example, we have

$$\begin{aligned} & && \vdots \\ \gcd(6,14) = 2 &= && (-2) \cdot 6 + (1) \cdot 14 \\ &= && (5) \cdot 6 + (-2) \cdot 14 \\ &= && (12) \cdot 6 + (-5) \cdot 14 \\ & && \vdots \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$252 \quad =$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \qquad (1) \\ 198 &= \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= 1 \cdot 36 + 18 && (3) \\ 36 &= \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$
\begin{aligned}
252 &= 1 \cdot 198 + 54 && (1)\\
198 &= 3 \cdot 54 + 36 && (2)\\
54 &= 1 \cdot 36 + 18 && (3)\\
36 &= 2 \cdot 18 + 0, && (4)
\end{aligned}
$$

therefore $\gcd(252, 198) =$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= 1 \cdot 36 + 18 && (3) \\ 36 &= 2 \cdot 18 + 0, && (4) \end{aligned}$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$18 =$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$
\begin{aligned}
252 &= 1 \cdot 198 + 54 && (1)\\
198 &= 3 \cdot 54 + 36 && (2)\\
54 &= 1 \cdot 36 + 18 && (3)\\
36 &= 2 \cdot 18 + 0, && (4)
\end{aligned}
$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$
\begin{aligned}
18 &= 54 - 1 \cdot 36 \text{ (from (3))}\\
&=
\end{aligned}
$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$
\begin{aligned}
252 &= 1 \cdot 198 + 54 && (1)\\
198 &= 3 \cdot 54 + 36 && (2)\\
54 &= 1 \cdot 36 + 18 && (3)\\
36 &= 2 \cdot 18 + 0, && (4)
\end{aligned}
$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$
\begin{aligned}
18 &= 54 - 1 \cdot 36 \text{ (from (3))}\\
&= 54 - 1 \cdot (198 - 3 \cdot 54) = 54 - 1 \cdot 198 + 3 \cdot 54 \text{ (from (2))}\\
&=
\end{aligned}
$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= 1 \cdot 36 + 18 && (3) \\ 36 &= 2 \cdot 18 + 0, && (4) \end{aligned}$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \text{ (from (3))} \\ &= 54 - 1 \cdot (198 - 3 \cdot 54) = 54 - 1 \cdot 198 + 3 \cdot 54 \text{ (from (2))} \\ &= 4 \cdot 54 - 1 \cdot 198 \\ &= \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= 1 \cdot 36 + 18 && (3) \\ 36 &= 2 \cdot 18 + 0, && (4) \end{aligned}$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \text{ (from (3))} \\ &= 54 - 1 \cdot (198 - 3 \cdot 54) = 54 - 1 \cdot 198 + 3 \cdot 54 \text{ (from (2))} \\ &= 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 4 \cdot 198 - 1 \cdot 198 \text{ (from (1))} \\ &= \end{aligned}$$

To find $s, t \in \mathbb{Z}$ that satisfy $\gcd(a, b) = sa + tb$, we can exploit the steps in Euclid's algorithm.

Exercise

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.

Solution: Firstly, we will find $\gcd(252, 198)$ through Euclid's algorithm

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 && (1) \\ 198 &= 3 \cdot 54 + 36 && (2) \\ 54 &= 1 \cdot 36 + 18 && (3) \\ 36 &= 2 \cdot 18 + 0, && (4) \end{aligned}$$

therefore $\gcd(252, 198) = 18$. By doing the "reverse process", observe that

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \text{ (from (3))} \\ &= 54 - 1 \cdot (198 - 3 \cdot 54) = 54 - 1 \cdot 198 + 3 \cdot 54 \text{ (from (2))} \\ &= 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 4 \cdot 198 - 1 \cdot 198 \text{ (from (1))} \\ &= 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$312 \quad =$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 \qquad (5) \\ 70 &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= 3 \cdot 2 + 0 && (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$2 \quad =$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= 3 \cdot 2 + 0 && (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$\begin{aligned} 2 &= 32 - 5 \cdot 6 \text{ (from (7))} \\ &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= 3 \cdot 2 + 0 && (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$\begin{aligned} 2 &= 32 - 5 \cdot 6 \text{ (from (7))} \\ &= 32 - 5 \cdot (70 - 2 \cdot 32) = 32 - 5 \cdot 70 + 10 \cdot 32 \text{ (from (6))} \\ &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 &\quad (5)\\ 70 &= 2 \cdot 32 + 6 &\quad (6)\\ 32 &= 5 \cdot 6 + 2 &\quad (7)\\ 6 &= 3 \cdot 2 + 0 &\quad (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$\begin{aligned} 2 &= 32 - 5 \cdot 6 \text{ (from (7))}\\ &= 32 - 5 \cdot (70 - 2 \cdot 32) = 32 - 5 \cdot 70 + 10 \cdot 32 \text{ (from (6))}\\ &= 11 \cdot 32 - 5 \cdot 70\\ &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= 3 \cdot 2 + 0 && (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$\begin{aligned} 2 &= 32 - 5 \cdot 6 \text{ (from (7))} \\ &= 32 - 5 \cdot (70 - 2 \cdot 32) = 32 - 5 \cdot 70 + 10 \cdot 32 \text{ (from (6))} \\ &= 11 \cdot 32 - 5 \cdot 70 \\ &= 11 \cdot (312 - 4 \cdot 70) - 5 \cdot 70 = 11 \cdot 312 - 44 \cdot 70 - 5 \cdot 70 \text{ (from (5))} \\ &= \end{aligned}$$

Exercise

Express $\gcd(312, 70)$ as a linear combination of 312 and 70.

Solution: Firstly, we will find $\gcd(312, 70)$ through Euclid's algorithm

$$\begin{aligned} 312 &= 4 \cdot 70 + 32 && (5) \\ 70 &= 2 \cdot 32 + 6 && (6) \\ 32 &= 5 \cdot 6 + 2 && (7) \\ 6 &= 3 \cdot 2 + 0 && (8) \end{aligned}$$

Thus, $\gcd(312, 70) = 2$ and we also have

$$\begin{aligned} 2 &= 32 - 5 \cdot 6 \text{ (from (7))} \\ &= 32 - 5 \cdot (70 - 2 \cdot 32) = 32 - 5 \cdot 70 + 10 \cdot 32 \text{ (from (6))} \\ &= 11 \cdot 32 - 5 \cdot 70 \\ &= 11 \cdot (312 - 4 \cdot 70) - 5 \cdot 70 = 11 \cdot 312 - 44 \cdot 70 - 5 \cdot 70 \text{ (from (5))} \\ &= 11 \cdot 312 - 49 \cdot 70. \end{aligned}$$

Contents

1. gcd, lcm, and Euclidean Algorithm
   - gcd
   - lcm
   - Euclidean Algorithm
   - gcd as Linear Combination
   - Some Important Theorems and Challenging Problems

Important Theorems Pertaining to $\gcd$ and lcm

Theorem

If a and b are two positive integers, then we have

$$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

Proof

The proof is left to the reader as one of the *challenging problems*.

Theorem

If a, b, and c are three positive numbers, then

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

Consequently the lcm of the three numbers a, b, and c can be written as $\operatorname{lcm}(a, b, c)$.

CP 1

CP 1

Alice and Bob are sibling and each of them have a bakery. Alice's bakery produces A pieces of chocolate breads a day while Bob's bakery yields B pieces of cheese breads a day. To make an efficient selling, they plan to sell the chocolate and cheese breads within the same packages. Your task is to determine the maximum number of possible packages with the requirement: all of bread must be in the packages. The number of chocolate breads and cheese breads can be different in one package. However, the number of chocolate breads as well as cheese breads between one package to another must be the same.

Your task is to develop a program in C, C++, Java, or Python to solve this problem. Suppose A and B are the number of chocolate breads and cheese breads that have been produced, respectively, N is the maximum number of possible packages, while C and K are the number of chocolate breads and cheese breads per package, respectively. For example:

- Suppose $A = 720$, $B = 900$ (the amount of breads produced).
- Then we have $N = 180$ (the possible maximum number of packages).
- Hence, $C = 4$ and $K = 5$ (4 chocolate breads and 5 cheese breads per package).

CP 1 – I/O

CP 1

input and output format of your program are as follows.
input: the value of A and B
output: the value of N, C, and K

Example:

```
input:  720, 900
output:  180, 4, 5

input:  30, 120
output:  30, 1, 4

input:  31, 33
output:  1, 31, 33
```

Notes: the value of A and B satisfy $1 \leq A, B \leq 10^4$.

CP 2

CP 2

Alice and Bob are sibling and each of them have a bakery. Once every several days they are closed to maintain the kitchen tools. Alice's bakery is closed every A days, while Bob's is closed every B days. When both of Alice's and Bob's bakery are closed at the same day, the coffee shop owned by Carlos, their nephew, will sell the bread that usually produced by them.

Your task is to determine the period (cycle) when both of Alice's and Bob's bakery are closed. This is needed by Carlos to prepare the bread selling.

Your task is to develop a program in C, C++, Java, or Python to solve this problem. Suppose A and B are the period when Alice's and Bob's bakery are closed, respectively and P is the period when both of the store are closed.

- Suppose $A = 14$, $B = 21$ (Alice's bakery closed every 14 days, Bob's bakery closed every 21 days).
- Then we have $P = 42$ (both bakeries are closed at the same time every 42 days).

CP 2 – I/O

CP 2

input and output format of your program are as follows.
input: the value of A and B
output: the value of P

Example:

```
input:  14, 21
output:  42

input:  30, 10
output:  30

input:  7, 15
output:  105
```

Notes: the value of A and B satisfy $1 \leq A, B \leq 365$.

Contents

1. gcd, lcm, and Euclidean Algorithm
   - gcd
   - lcm
   - Euclidean Algorithm
   - gcd as Linear Combination
   - Some Important Theorems and Challenging Problems

2. Modular Arithmetic and the Ring $\mathbb{Z}_m$

3. Linear Congruence and Its Solution

4. Linear Congruence and Ring $\mathbb{Z}_m$

Congruence Modulo m

Remember that if $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \bmod m$ is the remainder of a divided by m.

The value of $a \bmod m$ is in the set $\{0, 1, 2, \ldots, m-1\}$. Furthermore, the value of m in the expression $a \bmod m$ is called modulus.

Definition

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is congruent to b modulo m , denoted as $a \equiv b \pmod{m}$, iff $m | a - b$. Then the notation $a \not\equiv b \pmod{m}$ denotes a is not congruent to b modulo m.

Exercise

Check whether

1. $17 \equiv 5 \pmod 6$
2. $-17 \equiv 5 \pmod 6$
3. $17 \equiv 2 \pmod 7$
4. $-17 \equiv 2 \pmod 7$
5. $8 \equiv 4 \pmod 4$
6. $-8 \equiv 4 \pmod 4$

Solution: Notice that

Exercise

Check whether

1. $17 \equiv 5 \pmod{6}$
2. $-17 \equiv 5 \pmod{6}$
3. $17 \equiv 2 \pmod{7}$
4. $-17 \equiv 2 \pmod{7}$
5. $8 \equiv 4 \pmod{4}$
6. $-8 \equiv 4 \pmod{4}$

Solution: Notice that

1. $6|17-5$ (because $6|12$), therefore $17 \equiv 5 \pmod{6}$,

Exercise

Check whether

1. $17 \equiv 5 \pmod{6}$
2. $-17 \equiv 5 \pmod{6}$
3. $17 \equiv 2 \pmod{7}$
4. $-17 \equiv 2 \pmod{7}$
5. $8 \equiv 4 \pmod{4}$
6. $-8 \equiv 4 \pmod{4}$

Solution: Notice that

1. $6|17-5$ (because $6|12$), therefore $17 \equiv 5 \pmod{6}$,
2. $6 \nmid -17-5$ (because $6 \nmid -22$), therefore $-17 \not\equiv 5 \pmod{6}$.

Exercise

Check whether

1. $17 \equiv 5 \pmod{6}$
2. $-17 \equiv 5 \pmod{6}$
3. $17 \equiv 2 \pmod{7}$
4. $-17 \equiv 2 \pmod{7}$
5. $8 \equiv 4 \pmod{4}$
6. $-8 \equiv 4 \pmod{4}$

Solution: Notice that

1. $6|17-5$ (because $6|12$), therefore $17 \equiv 5 \pmod{6}$,
2. $6 \nmid -17-5$ (because $6 \nmid -22$), therefore $-17 \not\equiv 5 \pmod{6}$.
3. $7 \nmid 17-2$ (because $7 \nmid 15$), therefore $17 \not\equiv 2 \pmod{7}$.

Exercise

Check whether

1. $17 \equiv 5 \pmod 6$
2. $-17 \equiv 5 \pmod 6$
3. $17 \equiv 2 \pmod 7$
4. $-17 \equiv 2 \pmod 7$
5. $8 \equiv 4 \pmod 4$
6. $-8 \equiv 4 \pmod 4$

Solution: Notice that

1. $6|17-5$ (because $6|12$), therefore $17 \equiv 5 \pmod 6$,
2. $6 \nmid -17-5$ (because $6 \nmid -22$), therefore $-17 \not\equiv 5 \pmod 6$.
3. $7 \nmid 17-2$ (because $7 \nmid 15$), therefore $17 \not\equiv 2 \pmod 7$.
4. $7 \nmid -17-2$ (because $7 \nmid -19$), therefore $-17 \not\equiv 2 \pmod 7$,

Exercise

Check whether

1. $17 \equiv 5 \pmod 6$
2. $-17 \equiv 5 \pmod 6$
3. $17 \equiv 2 \pmod 7$
4. $-17 \equiv 2 \pmod 7$
5. $8 \equiv 4 \pmod 4$
6. $-8 \equiv 4 \pmod 4$

Solution: Notice that

1. $6|17-5$ (because $6|12$), therefore $17 \equiv 5 \pmod 6$,
2. $6 \nmid -17-5$ (because $6 \nmid -22$), therefore $-17 \not\equiv 5 \pmod 6$.
3. $7 \nmid 17-2$ (because $7 \nmid 15$), therefore $17 \not\equiv 2 \pmod 7$.
4. $7 \nmid -17-2$ (because $7 \nmid -19$), therefore $-17 \not\equiv 2 \pmod 7$,
5. $4|8-4$ (because $4|4$), therefore $8 \equiv 4 \pmod 4$,

Exercise

Check whether

1. $17 \equiv 5 \pmod 6$
2. $-17 \equiv 5 \pmod 6$
3. $17 \equiv 2 \pmod 7$
4. $-17 \equiv 2 \pmod 7$
5. $8 \equiv 4 \pmod 4$
6. $-8 \equiv 4 \pmod 4$

Solution: Notice that

1. $6 | 17 - 5$ (because $6|12$), therefore $17 \equiv 5 \pmod 6$,
2. $6 \nmid -17 - 5$ (because $6 \nmid -22$), therefore $-17 \not\equiv 5 \pmod 6$.
3. $7 \nmid 17 - 2$ (because $7 \nmid 15$), therefore $17 \not\equiv 2 \pmod 7$.
4. $7 \nmid -17 - 2$ (because $7 \nmid -19$), therefore $-17 \not\equiv 2 \pmod 7$,
5. $4 | 8 - 4$ (because $4|4$), therefore $8 \equiv 4 \pmod 4$,
6. $4| - 8 - 4$ (because $4| - 12$), therefore $-8 \equiv 4 \pmod 4$.

Theorem

If $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff there is $k \in \mathbb{Z}$ that satisfies $a = b + km$.

Proof

Theorem

If $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff there is $k \in \mathbb{Z}$ that satisfies $a = b + km$.

Proof

Notice that $a \equiv b \pmod{m} \Leftrightarrow$

Theorem

If $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff there is $k \in \mathbb{Z}$ that satisfies $a = b + km$.

Proof

Notice that $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \Leftrightarrow$

Theorem

If $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff there is $k \in \mathbb{Z}$ that satisfies $a = b + km$.

Proof

Notice that $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \Leftrightarrow km = a - b$ for a $k \in \mathbb{Z}$. □

Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then

$$a \equiv b \pmod{m} \text{ iff } a \bmod m = b \bmod m.$$

Example

We have:

1. $23 \bmod 5 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod{5}$,
2. $27 \bmod 3 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod{5}$,
2. $27 \bmod 3 = 3 \bmod 3 = 0$, therefore $27 \equiv 3 \pmod{3}$,
3. $6 \bmod 8 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod 5$,
2. $27 \bmod 3 = 3 \bmod 3 = 0$, therefore $27 \equiv 3 \pmod 3$,
3. $6 \bmod 8 = 6$, therefore $6 \equiv 6 \pmod 8$,
4. $0 \bmod 12 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod 5$,
2. $27 \bmod 3 = 3 \bmod 3 = 0$, therefore $27 \equiv 3 \pmod 3$,
3. $6 \bmod 8 = 6$, therefore $6 \equiv 6 \pmod 8$,
4. $0 \bmod 12 = 0$, therefore $0 \equiv 0 \pmod{12}$,
5. $-41 \bmod 9 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod{5}$,
2. $27 \bmod 3 = 3 \bmod 3 = 0$, therefore $27 \equiv 3 \pmod{3}$,
3. $6 \bmod 8 = 6$, therefore $6 \equiv 6 \pmod{8}$,
4. $0 \bmod 12 = 0$, therefore $0 \equiv 0 \pmod{12}$,
5. $-41 \bmod 9 = 4 \bmod 9 = 4$, therefore $-41 \equiv 4 \pmod{9}$,
6. $-39 \bmod 13 =$

Example

We have:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, therefore $23 \equiv 3 \pmod 5$,
2. $27 \bmod 3 = 3 \bmod 3 = 0$, therefore $27 \equiv 3 \pmod 3$,
3. $6 \bmod 8 = 6$, therefore $6 \equiv 6 \pmod 8$,
4. $0 \bmod 12 = 0$, therefore $0 \equiv 0 \pmod{12}$,
5. $-41 \bmod 9 = 4 \bmod 9 = 4$, therefore $-41 \equiv 4 \pmod 9$,
6. $-39 \bmod 13 = 0 \bmod 13 = 0$, therefore $-39 \equiv 0 \pmod{13}$.

Theorems about Modular Arithmetic (*Challenging Problems*)

Theorem

Suppose $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ for every nonnegative integer r

Proof

The proof of the theorem is left as *challenging problems* for the reader.

Example

We have $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, therefore, we obtain

1. $(7 + 11) \equiv$

Theorems about Modular Arithmetic (*Challenging Problems*)

Theorem

Suppose $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ for every nonnegative integer r

Proof

The proof of the theorem is left as *challenging problems* for the reader.

Example

We have $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, therefore, we obtain

1. $(7 + 11) \equiv 2 + 1 \pmod{5}$, or $18 \equiv 3 \pmod{5}$;
2. $(7 \cdot 11) \equiv$

Theorems about Modular Arithmetic (*Challenging Problems*)

Theorem

Suppose $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ for every nonnegative integer r

Proof

The proof of the theorem is left as *challenging problems* for the reader.

Example

We have $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, therefore, we obtain

1. $(7 + 11) \equiv 2 + 1 \pmod{5}$, or $18 \equiv 3 \pmod{5}$;
2. $(7 \cdot 11) \equiv 2 \cdot 1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$;

Theorems about Modular Arithmetic (*Challenging Problems*)

Theorem

Suppose $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ for every nonnegative integer r

Proof

The proof of the theorem is left as *challenging problems* for the reader.

Example

We have $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, therefore, we obtain

1. $(7 + 11) \equiv 2 + 1 \pmod{5}$, or $18 \equiv 3 \pmod{5}$;
2. $(7 \cdot 11) \equiv 2 \cdot 1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$;
3. $7^r \equiv 2^r \pmod{5}$ and $11^r \equiv 1^r \pmod{5} \equiv 1 \pmod{5}$, for every nonnegative integer r.

Arithmetic on $\mathbb{Z}_m$

- We denote a set of all nonnegative integers that is less than m using $\mathbb{Z}_m$, namely $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- We respectively denote the operators $+_m$ and $\cdot_m$ as addition and multiplication operators on $\mathbb{Z}_m$ that are defined as follows: for every $a, b \in \mathbb{Z}_m$, then

$$\begin{aligned} a +_m b &= (a+b) \bmod m, \\ a \cdot_m b &= (ab) \bmod m. \end{aligned}$$

If m is obvious, then the subscript m can be omitted.

Exercise

Determine $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Notice that

1. $7 +_{11} 9 =$

Arithmetic on $\mathbb{Z}_m$

- We denote a set of all nonnegative integers that is less than m using $\mathbb{Z}_m$, namely $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- We respectively denote the operators $+_m$ and $\cdot_m$ as addition and multiplication operators on $\mathbb{Z}_m$ that are defined as follows: for every $a, b \in \mathbb{Z}_m$, then

$$\begin{aligned} a +_m b &= (a+b) \bmod m, \\ a \cdot_m b &= (ab) \bmod m. \end{aligned}$$

If m is obvious, then the subscript m can be omitted.

Exercise

Determine $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Notice that

1. $7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5$.
2. $7 \cdot_{11} 9 =$

Arithmetic on $\mathbb{Z}_m$

- We denote a set of all nonnegative integers that is less than m using $\mathbb{Z}_m$, namely $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- We respectively denote the operators $+_m$ and $\cdot_m$ as addition and multiplication operators on $\mathbb{Z}_m$ that are defined as follows: for every $a, b \in \mathbb{Z}_m$, then

$$\begin{aligned} a +_m b &= (a+b) \bmod m, \\ a \cdot_m b &= (ab) \bmod m. \end{aligned}$$

If m is obvious, then the subscript m can be omitted.

Exercise

Determine $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Notice that

1. $7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5.$
2. $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutative For every $a, b \in \mathbb{Z}_m$ we have

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutative For every $a, b \in \mathbb{Z}_m$ we have $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Existence of 0 There is $0 \in \mathbb{Z}_m$ with the property

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutative For every $a, b \in \mathbb{Z}_m$ we have $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Existence of 0 There is $0 \in \mathbb{Z}_m$ with the property $a +_m 0 = 0 +_m a = a$ for every $a \in \mathbb{Z}_m$.

Existence of 1 There is $1 \in \mathbb{Z}_m$ with the property

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutative For every $a, b \in \mathbb{Z}_m$ we have $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Existence of 0 There is $0 \in \mathbb{Z}_m$ with the property $a +_m 0 = 0 +_m a = a$ for every $a \in \mathbb{Z}_m$.

Existence of 1 There is $1 \in \mathbb{Z}_m$ with the property $a \cdot_m 1 = 1 \cdot_m a = a$ for every $a \in \mathbb{Z}_m$.

Additive Inverse For every $a \in \mathbb{Z}_m$, there is

The Ring $\mathbb{Z}_m$

The Ring $\mathbb{Z}_m$

For every set $\mathbb{Z}_m$ with $m \geq 2$, operators $+_m$ and $\cdot_m$ satisfy the following properties:

Closure For every $a, b \in \mathbb{Z}_m$, then $a +_m b \in \mathbb{Z}_m$ and $a \cdot_m b \in \mathbb{Z}_m$.

Associative For every $a, b, c \in \mathbb{Z}_m$ we have $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutative For every $a, b \in \mathbb{Z}_m$ we have $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Existence of 0 There is $0 \in \mathbb{Z}_m$ with the property $a +_m 0 = 0 +_m a = a$ for every $a \in \mathbb{Z}_m$.

Existence of 1 There is $1 \in \mathbb{Z}_m$ with the property $a \cdot_m 1 = 1 \cdot_m a = a$ for every $a \in \mathbb{Z}_m$.

Additive Inverse For every $a \in \mathbb{Z}_m$, there is $(m - a) \in \mathbb{Z}_m$ with properties $a +_m (m - a) = (m - a) +_m a = 0$.

We can construct the addition and multiplication table on $\mathbb{Z}_m$. For $\mathbb{Z}_2$ both tables are explained as follows:

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Exercise

Construct the addition and multiplication tables for:

1. $\mathbb{Z}_3$
2. $\mathbb{Z}_4$

For $\mathbb{Z}_3$ we have the following tables:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Then for $\mathbb{Z}_4$ we have the following tables:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Contents

Linear Congruence

We discuss linear congruence of one variable and its solution.

Definition (linear congruence of one variable)

Suppose $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, and x is a variable. A linear congruence (of one variable) is an expression of the form $ax \equiv b \pmod{m}$.

Example

The examples of linear congruence are $3x \equiv 9 \pmod{7}$, $2x \equiv 1 \pmod{4}$, and $5x \equiv 0 \pmod{7}$.

Problem

Given a linear congruence $ax \equiv b \pmod{m}$. What are the requirements to obtain the value of x (integer) that satisfies this linear congruence?

Problem

Given a linear congruence $ax \equiv b \pmod{m}$. What are the requirements to obtain the value of x (integer) that satisfies this linear congruence?

Finding the solution of $ax \equiv b \pmod{m}$ can be done using *brute-force/ exhaustive search*. Since the value of x is in the set $\{0, 1, \ldots, m-1\}$, then we can find the solution to $ax \equiv b \pmod{m}$ by substituting the value of $x = 0, 1, \ldots, m-1$. However, this is not an efficient way.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod{4}$

Solution:

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod{4}$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod 4$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. So there is no x that satisfies $2x \equiv 1 \pmod 4$.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod{4}$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod{4}$, $2 \cdot 1 \equiv 2 \pmod{4}$, $2 \cdot 2 = 0 \pmod{4}$, $2 \cdot 3 \equiv 2 \pmod{4}$. So there is no x that satisfies $2x \equiv 1 \pmod{4}$.

Analytical version:

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod 4$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. So there is no x that satisfies $2x \equiv 1 \pmod 4$.

Analytical version:

1. Suppose $2x \equiv 1 \pmod 4$ has a solution, then we obtain $4 \mid (2x - 1)$, or $4k = 2x - 1$, for a $k \in \mathbb{Z}$.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod 4$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. So there is no x that satisfies $2x \equiv 1 \pmod 4$.

Analytical version:

1. Suppose $2x \equiv 1 \pmod 4$ has a solution, then we obtain $4 | (2x - 1)$, or $4k = 2x - 1$, for a $k \in \mathbb{Z}$.
2. Therefore, $2x = 4k + 1$, for a $k \in \mathbb{Z}$.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod 4$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. So there is no x that satisfies $2x \equiv 1 \pmod 4$.

Analytical version:

1. Suppose $2x \equiv 1 \pmod 4$ has a solution, then we obtain $4 | (2x - 1)$, or $4k = 2x - 1$, for a $k \in \mathbb{Z}$.
2. Therefore, $2x = 4k + 1$, for a $k \in \mathbb{Z}$.
3. This gives $x = \frac{(4k+1)}{2}$, but since $4k + 1$ is always odd for every $k \in \mathbb{Z}$, then $x = \frac{(4k+1)}{2} \notin \mathbb{Z}$.

Exercise

Check whether there is the value of x such that $2x \equiv 1 \pmod{4}$

Solution:

Brute-force version.
The possible value of x is $x = 0, 1, 2, 3$. Notice that $2 \cdot 0 \equiv 0 \pmod{4}$, $2 \cdot 1 \equiv 2 \pmod{4}$, $2 \cdot 2 = 0 \pmod{4}$, $2 \cdot 3 \equiv 2 \pmod{4}$. So there is no x that satisfies $2x \equiv 1 \pmod{4}$.

Analytical version:

1. Suppose $2x \equiv 1 \pmod{4}$ has a solution, then we obtain $4 \mid (2x - 1)$, or $4k = 2x - 1$, for a $k \in \mathbb{Z}$.
2. Therefore, $2x = 4k + 1$, for a $k \in \mathbb{Z}$.
3. This gives $x = \frac{(4k+1)}{2}$, but since $4k + 1$ is always odd for every $k \in \mathbb{Z}$, then $x = \frac{(4k+1)}{2} \notin \mathbb{Z}$.
4. So, it is impossible to have a value x that satisfies the requirement.

Multiplicative Inverse Modulo m

In high school, we have learned the way to find a solution of $ax = b$ for $a \neq 0$, the solution of $ax = b$ can be obtained using the following steps

$$ax = b$$

Multiplicative Inverse Modulo m

In high school, we have learned the way to find a solution of $ax = b$ for $a \neq 0$, the solution of $ax = b$ can be obtained using the following steps

$$\begin{aligned} ax &= b \\ a^{-1} \cdot ax &= a^{-1} \cdot b \text{ (multiplying both sides by } a^{-1}\text{)} \\ x &= a^{-1}b. \end{aligned}$$

To find a solution of a modular congruence in $\mathbb{Z}_m$ firstly we need to define the *multiplicative inverse* in $\mathbb{Z}_m$.

Definition

Multiplicative Inverse Modulo m

In high school, we have learned the way to find a solution of $ax = b$ for $a \neq 0$, the solution of $ax = b$ can be obtained using the following steps

$$\begin{aligned} ax &= b \\ a^{-1} \cdot ax &= a^{-1} \cdot b \text{ (multiplying both sides by } a^{-1}\text{)} \\ x &= a^{-1}b. \end{aligned}$$

To find a solution of a modular congruence in $\mathbb{Z}_m$ firstly we need to define the *multiplicative inverse* in $\mathbb{Z}_m$.

Definition

Suppose $a \in \mathbb{Z}$, the number $a^{-1} \in \mathbb{Z}$ is called as inverse of a modulo m (or inverse of a in modulo m) if $a^{-1} \cdot a = a \cdot a^{-1} \equiv 1 \pmod{m}$.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod 4$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod 5$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, therefore, 5 is the inverse of 3 in modulo 7.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod{7}$, therefore, 5 is the inverse of 3 in modulo 7.
4. 3 has no inverse in modulo 6, because there is no x that satisfies $3x \equiv 1 \pmod{6}$. Notice the following argument:

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod{7}$, therefore, 5 is the inverse of 3 in modulo 7.
4. 3 has no inverse in modulo 6, because there is no x that satisfies $3x \equiv 1 \pmod{6}$. Notice the following argument:
    - If $3x \equiv 1 \pmod{6}$, then the possible value of x is $x = 0, 1, 2, 3, 4, 5$.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod{7}$, therefore, 5 is the inverse of 3 in modulo 7.
4. 3 has no inverse in modulo 6, because there is no x that satisfies $3x \equiv 1 \pmod{6}$. Notice the following argument:
    - If $3x \equiv 1 \pmod{6}$, then the possible value of x is $x = 0, 1, 2, 3, 4, 5$.
    - If $x = 0$, 2, 4, then we obtain $3x \equiv 0 \pmod{6}$.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod{7}$, therefore, 5 is the inverse of 3 in modulo 7.
4. 3 has no inverse in modulo 6, because there is no x that satisfies $3x \equiv 1 \pmod{6}$. Notice the following argument:
   - If $3x \equiv 1 \pmod{6}$, then the possible value of x is $x = 0, 1, 2, 3, 4, 5$.
   - If $x = 0,\ 2,\ 4$, then we obtain $3x \equiv 0 \pmod{6}$.
   - If $x = 1, 3, 5$, then we obtain $3x \equiv 3 \pmod{6}$.

Exercise

Check whether

1. 2 has an inverse in modulo 4, if yes then determine the inverse,
2. 2 has an inverse in modulo 5, if yes then determine the inverse,
3. 3 has an inverse in modulo 7, if yes then determine the inverse,
4. 3 has an inverse in modulo 6, if yes then determine the inverse,
5. 5 has an inverse in modulo 8, if yes then determine the inverse.

Solution:

1. 2 has no inverse in modulo 4, because there is no x that satisfies $2x \equiv 1 \pmod{4}$, this has been explained in the previous argument,
2. $2 \cdot 3 \equiv 1 \pmod{5}$, therefore, 3 is the inverse of 2 in modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod{7}$, therefore, 5 is the inverse of 3 in modulo 7.
4. 3 has no inverse in modulo 6, because there is no x that satisfies $3x \equiv 1 \pmod{6}$. Notice the following argument:
    - If $3x \equiv 1 \pmod{6}$, then the possible value of x is $x = 0, 1, 2, 3, 4, 5$.
    - If $x = 0,\ 2,\ 4$, then we obtain $3x \equiv 0 \pmod{6}$.
    - If $x = 1, 3, 5$, then we obtain $3x \equiv 3 \pmod{6}$.
5. $5 \cdot 5 \equiv 1 \pmod{8}$, therefore, 5 is an inverse of 5 in modulo 8.

A Systematic Methods to Find Multiplicative Inverse

We have already seen that the way to determine a^{-1} in $\mathbb{Z}_m$ can be determined using the *brute-force* way, however, this way is not efficient. To find the efficient way, first we need to see the following theorem.

Theorem

Suppose $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a^{-1} exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Proof (Proof of a^{-1} exists $\Rightarrow \gcd(a, m) = 1$)

A Systematic Methods to Find Multiplicative Inverse

We have already seen that the way to determine a^{-1} in $\mathbb{Z}_m$ can be determined using the *brute-force* way, however, this way is not efficient. To find the efficient way, first we need to see the following theorem.

Theorem

Suppose $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a^{-1} exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Proof (Proof of a^{-1} exists $\Rightarrow \gcd(a, m) = 1$)

1. Since a^{-1} exist, then $a \cdot a^{-1} \equiv 1 \pmod{m}$. To make it easier, we write $a^{-1} = t$.

A Systematic Methods to Find Multiplicative Inverse

We have already seen that the way to determine a^{-1} in $\mathbb{Z}_m$ can be determined using the *brute-force* way, however, this way is not efficient. To find the efficient way, first we need to see the following theorem.

Theorem

Suppose $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a^{-1} exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Proof (Proof of a^{-1} exists $\Rightarrow \gcd(a, m) = 1$)

1. Since a^{-1} exist, then $a \cdot a^{-1} \equiv 1 \pmod{m}$. To make it easier, we write $a^{-1} = t$.
2. Since $at \equiv 1 \pmod{m}$, then $m | at - 1$, therefore, $km = at - 1$ for a $k \in \mathbb{Z}$. Hence $at - km = 1$.

A Systematic Methods to Find Multiplicative Inverse

We have already seen that the way to determine a^{-1} in $\mathbb{Z}_m$ can be determined using the *brute-force* way, however, this way is not efficient. To find the efficient way, first we need to see the following theorem.

Theorem

Suppose $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a^{-1} exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Proof (Proof of a^{-1} exists $\Rightarrow \gcd(a, m) = 1$)

1. Since a^{-1} exist, then $a \cdot a^{-1} \equiv 1 \pmod{m}$. To make it easier, we write $a^{-1} = t$.
2. Since $at \equiv 1 \pmod{m}$, then $m | at - 1$, therefore, $km = at - 1$ for a $k \in \mathbb{Z}$. Hence $at - km = 1$.
3. Since $\gcd(a, m) | a$ and $\gcd(a, m) | m$, then $\gcd(a, m) | at - km$, therefore, $\gcd(a, m) | 1$.

A Systematic Methods to Find Multiplicative Inverse

We have already seen that the way to determine a^{-1} in $\mathbb{Z}_m$ can be determined using the *brute-force* way, however, this way is not efficient. To find the efficient way, first we need to see the following theorem.

Theorem

Suppose $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, then a^{-1} exists in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Proof (Proof of a^{-1} exists $\Rightarrow \gcd(a, m) = 1$)

1. Since a^{-1} exist, then $a \cdot a^{-1} \equiv 1 \pmod{m}$. To make it easier, we write $a^{-1} = t$.
2. Since $at \equiv 1 \pmod{m}$, then $m | at - 1$, therefore, $km = at - 1$ for a $k \in \mathbb{Z}$. Hence $at - km = 1$.
3. Since $\gcd(a, m) | a$ and $\gcd(a, m) | m$, then $\gcd(a, m) | at - km$, therefore, $\gcd(a, m) | 1$.
4. Since an integer that can divide 1 are only -1 and 1, then we obtain $\gcd(a, m) = 1$.

□

Proof (Proof of $\gcd(a, m) = 1 \Rightarrow a^{-1}$ exists)

Proof (Proof of $\gcd(a, m) = 1 \Rightarrow a^{-1}$ exists)

1. Since $\gcd(a, m) = 1$, based on Bézout's theorem $1 = sa + tm = as + mt$.

Proof (Proof of $\gcd(a,m) = 1 \Rightarrow a^{-1}$ exists)

1. Since $\gcd(a,m) = 1$, based on Bézout's theorem $1 = sa + tm = as + mt$.
2. Therefore, $m(-t) = as - 1$, this means $m|as - 1$.

Proof (Proof of $\gcd(a,m)=1 \Rightarrow a^{-1}$ exists)

1. Since $\gcd(a,m)=1$, based on Bézout's theorem $1=sa+tm=as+mt$.
2. Therefore, $m(-t)=as-1$, this means $m|as-1$.
3. Thus, $as\equiv 1\,(\mathrm{mod}\,m)$, so we have $s=a^{-1}$. □

Proof of the theorem also say that the multiplicative inverse can be found using Euclid's Algorithm.

Exercise

Determine (if any) the inverse of

1. 3 in modulo 7, or a solution to $3x \equiv 1 \pmod{7}$
2. 4 in modulo 8, or a solution to $4x \equiv 1 \pmod{8}$
3. 4 in modulo 9, or a solution to $4x \equiv 1 \pmod{9}$
4. 7 in modulo 17, or a solution to $7x \equiv 1 \pmod{17}$

Solution no. 1:

Approach 1: *brute-force* version
Since $\gcd(3,7)=1$, then 3^{-1} exists in modulo 7. By trying the value of x in set $\{0,1,2,\ldots,6\}$, we obtain $3\cdot 5=15\equiv 1 \pmod{7}$. Therefore, $3^{-1}\equiv 5 \pmod{7}$.

Approach 2: Euclid's algorithm version
Notice that

$$\begin{aligned} 7 &= 2\cdot 3+1, \text{ so } 1=7-2\cdot 3 \\ 3 &= 1\cdot 3+0, \end{aligned}$$

therefore, $1=$

Solution no. 1:

Approach 1: *brute-force* version
Since $\gcd(3,7)=1$, then 3^{-1} exists in modulo 7. By trying the value of x in set $\{0,1,2,\ldots,6\}$, we obtain $3\cdot 5=15\equiv 1\pmod 7$. Therefore, $3^{-1}\equiv 5\pmod 7$.

Approach 2: Euclid's algorithm version
Notice that

$$\begin{aligned} 7 &= 2\cdot 3+1, \text{ so } 1=7-2\cdot 3 \\ 3 &= 1\cdot 3+0, \end{aligned}$$

therefore, $1=3(-2)+7$. This gives the fact that -2 is an inverse of 3 in modulo 7. Since $-2\equiv 5\pmod 7$, then we obtain $3^{-1}\equiv 5\pmod 7$.

Solution no. 2: Since $\gcd(4, 8) = 4 \neq 1$, then there is no value of x that satisfies $4x \equiv 1 \pmod{8}$.

Solution no. 2: Since $\gcd(4,8) = 4 \neq 1$, then there is no value of x that satisfies $4x \equiv 1 \pmod{8}$.

Solution no. 3:

brute-force version:
Since $\gcd(4,9) = 1$, then 4^{-1} exist in modulo 9. By trying the value of x in set $\{0,1,2,\ldots,8\}$ we obtain $4 \cdot 7 = 28 \equiv 1 \pmod{9}$. Therefore, $4^{-1} \equiv 7 \pmod{9}$.

Euclid's algorithm version:
Notice that

$$\begin{aligned} 9 &= 2 \cdot 4 + 1, \text{ so } 1 = 9 - 2 \cdot 4 \\ 4 &= 4 \cdot 1 + 0, \end{aligned}$$

therefore, $1 =$

Solution no. 2: Since $\gcd(4,8) = 4 \neq 1$, then there is no value of x that satisfies $4x \equiv 1 \pmod 8$.

Solution no. 3:

brute-force version:
Since $\gcd(4,9) = 1$, then 4^{-1} exist in modulo 9. By trying the value of x in set $\{0,1,2,\ldots,8\}$ we obtain $4 \cdot 7 = 28 \equiv 1 \pmod 9$. Therefore, $4^{-1} \equiv 7 \pmod 9$.

Euclid's algorithm version:
Notice that

$$\begin{aligned} 9 &= 2 \cdot 4 + 1, \text{ so } 1 = 9 - 2 \cdot 4 \\ 4 &= 4 \cdot 1 + 0, \end{aligned}$$

therefore, $1 = 4(-2) + 9$. This gives the fact that -2 is an inverse of 4 in modulo 9. Since $-2 \equiv 7 \pmod 9$, then we obtain $4^{-1} \equiv 7 \pmod 9$.

Solution no. 4:

Approach 1: *brute-force* version
Since $\gcd(7,17)=1$, then 7^{-1} exist in modulo 17. By trying the value of x in set $\{0,1,2,\ldots,16\}$, we obtain $7\cdot 5=35\equiv 1 \pmod{17}$. Therefore, $7^{-1}\equiv 5 \pmod{17}$.

Approach 2: Euclid's algorithm version
Notice that

$$\begin{aligned} 17 &= 2\cdot 7+3, \text{ so } 3=17-2\cdot 7 \\ 7 &= 2\cdot 3+1, \text{ so } 1=7-2\cdot 3 \\ 3 &= 3\cdot 1+0, \end{aligned}$$

therefore,

Solution no. 4:

Approach 1: *brute-force* version
Since $\gcd(7,17)=1$, then 7^{-1} exist in modulo 17. By trying the value of x in set $\{0,1,2,\ldots,16\}$, we obtain $7\cdot 5=35\equiv 1 \pmod{17}$. Therefore, $7^{-1}\equiv 5 \pmod{17}$.

Approach 2: Euclid's algorithm version
Notice that

$$\begin{aligned}
17 &= 2\cdot 7+3, \text{ so } 3=17-2\cdot 7\\
7 &= 2\cdot 3+1, \text{ so } 1=7-2\cdot 3\\
3 &= 3\cdot 1+0,
\end{aligned}$$

therefore,

$$\begin{aligned}
1 &= 7-2\cdot 3\\
&= 7-2\cdot(17-2\cdot 7)=7-2\cdot 17+4\cdot 7\\
&= 5\cdot 7-2\cdot 17
\end{aligned}$$

This gives the result that 5 is an inverse of 7 in modulo 17. Then we obtain $7^{-1}\equiv 5 \pmod{17}$.

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod 9$, we can do the following steps.

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod{9}$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod{9}$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod 9$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod 9$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
  1. if $k = 0$, then $x =$

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod{9}$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod{9}$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
    1. if $k = 0$, then $x = \frac{1}{4} \notin \mathbb{Z}$
    2. if $k = 1$, then $x =$

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod 9$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod 9$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
  1. if $k = 0$, then $x = \frac{1}{4} \notin \mathbb{Z}$
  2. if $k = 1$, then $x = \frac{10}{4} \notin \mathbb{Z}$
  3. if $k = 2$, then $x =$

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod{9}$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod{9}$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
  1. if $k = 0$, then $x = \frac{1}{4} \notin \mathbb{Z}$
  2. if $k = 1$, then $x = \frac{10}{4} \notin \mathbb{Z}$
  3. if $k = 2$, then $x = \frac{19}{4} \notin \mathbb{Z}$
  4. if $k = 3$, then $x =$

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod{9}$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod{9}$, then $9|4x-1$, such that $9k = 4x-1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
    1. if $k = 0$, then $x = \frac{1}{4} \notin \mathbb{Z}$
    2. if $k = 1$, then $x = \frac{10}{4} \notin \mathbb{Z}$
    3. if $k = 2$, then $x = \frac{19}{4} \notin \mathbb{Z}$
    4. if $k = 3$, then $x = \frac{28}{4} = 7 \in \mathbb{Z}$.

Determining Inverse – Another Method

To find the inverse of 4 in modulo 9, i.e., the value of x that satisfies $4x \equiv 1 \pmod{9}$, we can do the following steps.

- Notice that if $4x \equiv 1 \pmod{9}$, then $9 | 4x - 1$, such that $9k = 4x - 1$ for a $k \in \mathbb{Z}$.
- Therefore, $x = \frac{9k+1}{4}$, with $k \in \mathbb{Z}$. The value of x must be an integer as well.
- We will find the value of x by substitute the value of $k = 0, 1, 2 \ldots$.
  1. if $k = 0$, then $x = \frac{1}{4} \notin \mathbb{Z}$
  2. if $k = 1$, then $x = \frac{10}{4} \notin \mathbb{Z}$
  3. if $k = 2$, then $x = \frac{19}{4} \notin \mathbb{Z}$
  4. if $k = 3$, then $x = \frac{28}{4} = 7 \in \mathbb{Z}$.
- So we obtain $4^{-1} = x \equiv 7 \pmod{9}$.

Exercise: Finding The Solution of Linear Congruence

Exercise

Determine the solution of linear congruence

1. $3x \equiv 4 \pmod{7}$.
2. $12x \equiv 3 \pmod{15}$.

Solution no. 1:

Initially we have $3^{-1} \equiv 5 \pmod{7}$ because $3 \cdot 5 \equiv 1 \pmod{7}$. Then notice that

$$\begin{aligned} 3x &\equiv 4 \pmod{7}\text{, by multiplying both of sides with } 5\text{, we obtain} \\ x &\equiv 20 \pmod{7}\text{, because } 6 \equiv 20 \pmod{7}\text{, then we obtain} \\ x &\equiv 6 \pmod{7}. \end{aligned}$$

So the solution of linear congruence $3x \equiv 4 \pmod{7}$ is $x \equiv 6 \pmod{7}$.

Solution no. 2:
From $12x \equiv 3 \pmod{15}$ we obtain $15 \mid (12x - 3)$, or $15k = 12x - 3$, for a $k \in \mathbb{Z}$. Notice that

$$15k = 12x - 3 \text{ iff } 5k = 4x - 1,$$

so we obtain $5 \mid (4x - 1)$, or the linear congruence $4x \equiv 1 \pmod{5}$. We have $4^{-1} \equiv 4 \pmod{5}$ because $4 \cdot 4 \equiv 1 \pmod{5}$, therefore, $x \equiv 4 \pmod{5}$. Since the initial congruence requires in modulo 15, then the value of x must satisfy

Solution no. 2:
From $12x \equiv 3 \pmod{15}$ we obtain $15 | (12x - 3)$, or $15k = 12x - 3$, for a $k \in \mathbb{Z}$. Notice that

$$15k = 12x - 3 \text{ iff } 5k = 4x - 1,$$

so we obtain $5 | (4x - 1)$, or the linear congruence $4x \equiv 1 \pmod{5}$. We have $4^{-1} \equiv 4 \pmod{5}$ because $4 \cdot 4 \equiv 1 \pmod{5}$, therefore, $x \equiv 4 \pmod{5}$. Since the initial congruence requires in modulo 15, then the value of x must satisfy

$$x \equiv 4 \pmod{15}, \; x \equiv 9 \pmod{15}, \text{ and } x \equiv 14 \pmod{15}.$$

Observe that

$$\begin{array}{ccccc} 12 \cdot 4 & = & 48 & \equiv & 3 \pmod{15} \\ 12 \cdot 9 & = & 108 & \equiv & 3 \pmod{15} \\ 12 \cdot 14 & = & 158 & \equiv & 3 \pmod{15} \end{array}$$

So the solution of the linear congruence $12x \equiv 3 \pmod{15}$ is any integer x that satisfies one of the following congruence

$$x \equiv 4 \pmod{15}, \; x \equiv 9 \pmod{15}, \; x \equiv 14 \pmod{15}.$$

Contents

1. gcd, lcm, and Euclidean Algorithm
   - gcd
   - lcm
   - Euclidean Algorithm
   - gcd as Linear Combination
   - Some Important Theorems and Challenging Problems
2. Modular Arithmetic and the Ring $\mathbb{Z}_m$
3. Linear Congruence and Its Solution
4. Linear Congruence and Ring $\mathbb{Z}_m$

Linear Congruence and The Ring $\mathbb{Z}_m$

A linear congruence can be viewed as a linear equation whose solution is in the ring $\mathbb{Z}_m$. Notice some of the following linear congruence.

Exercise

Determine the value of x (if any) that satisfies the following linear congruences:

1. $3x \equiv 2 \pmod 4$
2. $x + 2 \equiv 1 \pmod 4$
3. $3x + 3 \equiv 1 \pmod 4$
4. $2x + 3 \equiv 2 \pmod 4$

To find x that is a solution of the congruences, we can create addition and multiplication table for $\mathbb{Z}_4$ first.

Linear Congruence and The Ring $\mathbb{Z}_m$

A linear congruence can be viewed as a linear equation whose solution is in the ring $\mathbb{Z}_m$. Notice some of the following linear congruence.

Exercise

Determine the value of x (if any) that satisfies the following linear congruences:

1. $3x \equiv 2 \pmod 4$
2. $x + 2 \equiv 1 \pmod 4$
3. $3x + 3 \equiv 1 \pmod 4$
4. $2x + 3 \equiv 2 \pmod 4$

To find x that is a solution of the congruences, we can create addition and multiplication table for $\mathbb{Z}_4$ first.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Linear Congruence and The Ring $\mathbb{Z}_m$

A linear congruence can be viewed as a linear equation whose solution is in the ring $\mathbb{Z}_m$. Notice some of the following linear congruence.

Exercise

Determine the value of x (if any) that satisfies the following linear congruences:

1. $3x \equiv 2 \pmod{4}$
2. $x + 2 \equiv 1 \pmod{4}$
3. $3x + 3 \equiv 1 \pmod{4}$
4. $2x + 3 \equiv 2 \pmod{4}$

To find x that is a solution of the congruences, we can create addition and multiplication table for $\mathbb{Z}_4$ first.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Afterwards, we will find the value of x by arithmetic rule for $\mathbb{Z}_4$.

Solution no. 1:

$$3x \equiv 2 \pmod{4}$$

Solution no. 1:

$$\begin{aligned} 3x &\equiv 2 \pmod{4} \\ 3^{-1}\cdot 3x &\equiv 3^{-1}\cdot 2 \pmod{4} \;\; \text{[Multiplying both sides by } 3^{-1}\text{]} \\ x &\equiv 3\cdot 2 \pmod{4} \;\; \text{[Since } 3^{-1}=3 \text{ in } \mathbb{Z}_4\text{]} \\ x &\equiv 6 \pmod{4} \equiv 2 \pmod{4} \end{aligned}$$

Solution no. 2:

$$x+2 \equiv 1 \pmod{4}$$

Solution no. 1:

$$\begin{aligned}
3x &\equiv 2 \pmod 4 \\
3^{-1} \cdot 3x &\equiv 3^{-1} \cdot 2 \pmod 4 \;\; [\text{Multiplying both sides by } 3^{-1}] \\
x &\equiv 3 \cdot 2 \pmod 4 \;\; [\text{Since } 3^{-1} = 3 \text{ in } \mathbb{Z}_4] \\
x &\equiv 6 \pmod 4 \equiv 2 \pmod 4
\end{aligned}$$

Solution no. 2:

$$\begin{aligned}
x + 2 &\equiv 1 \pmod 4 \\
x + 2 - 2 &\equiv (1 - 2) \pmod 4 \;\; [\text{Adding both sides with } -2] \\
x + 0 &\equiv -1 \pmod 4 \\
x &\equiv 3 \pmod 4 \;\; [\text{Because } -1 = 3 \text{ in } \mathbb{Z}_4]
\end{aligned}$$

Solution no. 3:

$$3x + 3 \equiv 1 \pmod{4}$$

Solution no. 3:

$$\begin{aligned}
3x+3 &\equiv 1 \pmod 4 \\
3x &\equiv -2 \pmod 4 \ \text{[Adding both of sides by } -3\text{]} \\
3x &\equiv 2 \pmod 4 \ \text{[Because } -2=2 \text{ in } \mathbb{Z}_4\text{]} \\
x &\equiv 3^{-1}\cdot 2 \pmod 4 \ \text{[Multiplying both of sides by } 3^{-1}\text{]} \\
x &\equiv 3\cdot 2 \pmod 4 \equiv 6 \pmod 4 \ \text{[Because } 3^{-1}=3 \text{ in } \mathbb{Z}_4\text{]} \\
x &\equiv 2 \pmod 4 .
\end{aligned}$$

Solution no. 4:

$$2x+3 \equiv 2 \pmod 4$$

Solution no. 3:

$$\begin{aligned}
3x+3 &\equiv 1 \pmod 4 \\
3x &\equiv -2 \pmod 4 \text{ [Adding both of sides by } -3] \\
3x &\equiv 2 \pmod 4 \text{ [Because } -2 = 2 \text{ in } \mathbb{Z}_4] \\
x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Multiplying both of sides by } 3^{-1}] \\
x &\equiv 3 \cdot 2 \pmod 4 \equiv 6 \pmod 4 \text{ [Because } 3^{-1} = 3 \text{ in } \mathbb{Z}_4] \\
x &\equiv 2 \pmod 4 .
\end{aligned}$$

Solution no. 4:

$$\begin{aligned}
2x+3 &\equiv 2 \pmod 4 \\
2x &\equiv -1 \pmod 4 \text{ [Adding both of sides by } -3] \\
2x &\equiv 3 \pmod 4 \text{ [Because } -1 = 3 \text{ in } \mathbb{Z}_4]
\end{aligned}$$

From the multiplication table,

Solution no. 3:

$$\begin{aligned}
3x+3 &\equiv 1 \pmod{4}\\
3x &\equiv -2 \pmod{4} \text{ [Adding both of sides by } -3]\\
3x &\equiv 2 \pmod{4} \text{ [Because } -2 = 2 \text{ in } \mathbb{Z}_4]\\
x &\equiv 3^{-1} \cdot 2 \pmod{4} \text{ [Multiplying both of sides by } 3^{-1}]\\
x &\equiv 3 \cdot 2 \pmod{4} \equiv 6 \pmod{4} \text{ [Because } 3^{-1} = 3 \text{ in } \mathbb{Z}_4]\\
x &\equiv 2 \pmod{4}.
\end{aligned}$$

Solution no. 4:

$$\begin{aligned}
2x+3 &\equiv 2 \pmod{4}\\
2x &\equiv -1 \pmod{4} \text{ [Adding both of sides by } -3]\\
2x &\equiv 3 \pmod{4} \text{ [Because } -1 = 3 \text{ in } \mathbb{Z}_4]
\end{aligned}$$

From the multiplication table, 2 has no multiplicative inverse in $\mathbb{Z}_4$, therefore, 2^{-1} does not exist in $\mathbb{Z}_4$, and so $2x \equiv 3 \pmod{4}$ has no solution (furthermore, $\gcd(2,4) = 2 \neq 1$).