Teori Bilangan Elementer Bagian 2

$\gcd$ dan lcm – Kongruensi Linier dan Ring $\mathbb{Z}_m$

MZI

Fakultas Informatika
Telkom University

FIF Tel-U

Juni 2023

Acknowledgements

Slide ini disusun berdasarkan materi yang terdapat pada sumber-sumber berikut:

1. *Discrete Mathematics and Its Applications*, Edisi 8, 2019, oleh K. H. Rosen (acuan utama).
2. *Discrete Mathematics with Applications*, Edisi 5, 2018, oleh S. S. Epp.
3. *Mathematics for Computer Science*. MIT, 2010, oleh E. Lehman, F. T. Leighton, A. R. Meyer.
4. *Slide* kuliah Matematika Diskret 2 (2012) di Fasilkom UI oleh B. H. Widjaja.
5. Slide kuliah Matematika Diskret 1 di Fasilkom UI oleh A. A. Krisnadhi.
6. *Slide* kuliah Matematika Diskrit di Telkom University oleh B. Purnama.

Beberapa gambar dapat diambil dari sumber-sumber di atas. *Slide* ini ditujukan untuk keperluan akademis di lingkungan FIF Telkom University. Jika Anda memiliki saran/ pendapat/ pertanyaan terkait materi dalam *slide* ini, silakan kirim email ke `<pleasedontspam>@telkomuniversity.ac.id`.

Bahasan

1. $\gcd$, lcm, dan Algoritma Euclid (Euclidean Algorithm)
   - $\gcd$
   - lcm
   - Algoritma Euclid (Euclidean Algorithm)
   - $\gcd$ Sebagai Kombinasi Linier
   - Beberapa Teorema Penting dan Challenging Problems
2. Aritmetika Modular dan Ring $\mathbb{Z}_m$
3. Kongruensi Linier dan Solusinya
4. Kongruensi Linier dan Ring $\mathbb{Z}_m$

Bahasan

Bahasan

FPB (*Greatest Common Divisor*, gcd)

Bilangan bulat terbesar yang membagi dua bilangan (tak keduanya nol) dinamakan sebagai faktor persekutuan terbesar dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}$ dan tidak keduanya nol. Bilangan bulat terbesar d yang memenuhi $d|a$ dan $d|b$ dinamakan sebagai faktor persekutuan terbesar (*greatest common divisor*) dari a dan b. Dalam hal ini, kita dapat menuliskan d sebagai $\text{FPB}(a, b)$ atau $\gcd(a, b)$.

Kita memiliki sifat bahwa d adalah $\gcd(a, b)$ apabila memenuhi kedua syarat berikut:

FPB (*Greatest Common Divisor*, gcd)

Bilangan bulat terbesar yang membagi dua bilangan (tak keduanya nol) dinamakan sebagai faktor persekutuan terbesar dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}$ dan tidak keduanya nol. Bilangan bulat terbesar d yang memenuhi $d|a$ dan $d|b$ dinamakan sebagai faktor persekutuan terbesar (*greatest common divisor*) dari a dan b. Dalam hal ini, kita dapat menuliskan d sebagai $\text{FPB}(a, b)$ atau $\gcd(a, b)$.

Kita memiliki sifat bahwa d adalah $\gcd(a, b)$ apabila memenuhi kedua syarat berikut:

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

FPB (*Greatest Common Divisor*, gcd)

Bilangan bulat terbesar yang membagi dua bilangan (tak keduanya nol) dinamakan sebagai faktor persekutuan terbesar dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}$ dan tidak keduanya nol. Bilangan bulat terbesar d yang memenuhi $d|a$ dan $d|b$ dinamakan sebagai faktor persekutuan terbesar (*greatest common divisor*) dari a dan b. Dalam hal ini, kita dapat menuliskan d sebagai $\text{FPB}(a, b)$ atau $\gcd(a, b)$.

Kita memiliki sifat bahwa d adalah $\gcd(a, b)$ apabila memenuhi kedua syarat berikut:

1. $d|a$ dan $d|b$,
2. jika terdapat $c \in \mathbb{Z}$ dengan sifat $c|a$ dan $c|b$, maka $c|d$.

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah ± 1, ± 3, dan ± 9, akibatnya $\gcd(-3, -9) =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah ± 1, ± 3, dan ± 9, akibatnya $\gcd(-3, -9) = 3$.

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah ± 1, ± 3, dan ± 9, akibatnya $\gcd(-3, -9) = 3$.
5. Bilangan yang dapat membagi -3 adalah

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah ± 1, ± 3, dan ± 9, akibatnya $\gcd(-3, -9) = 3$.
5. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian karena 0 habis dibagi 3, maka $\gcd(-3, 0) =$

Latihan

Tentukan $\gcd$ dari

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

Solusi: Perhatikan bahwa

1. Pembagi positif dari 24 adalah $1, 2, 3, 4, 6, 8, 12, 24$, kemudian pembagi positif dari 36 adalah $1, 2, 3, 4, 6, 9, 12, 18, 36$. Akibatnya $\gcd(24, 36) = 12$.
2. Pembagi positif dari 17 adalah 1 dan 17, pembagi positif dari 22 adalah $1, 2, 11, 22$. Akibatnya $\gcd(17, 22) = 1$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5^1 = 20$.
4. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian bilangan yang dapat membagi -9 adalah ± 1, ± 3, dan ± 9, akibatnya $\gcd(-3, -9) = 3$.
5. Bilangan yang dapat membagi -3 adalah ± 1 dan ± 3, kemudian karena 0 habis dibagi 3, maka $\gcd(-3, 0) = 3$.

Teorema

Apabila a dan b keduanya bilangan bulat tidak nol dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)}$. Notasi $\min(a, b)$ berarti bilangan terkecil diantara a dan b.

Contoh

Untuk menghitung $\gcd(36, 45)$, kita memiliki $36 =$

Teorema

Apabila a dan b keduanya bilangan bulat tidak nol dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)}$. Notasi $\min(a, b)$ berarti bilangan terkecil diantara a dan b.

Contoh

Untuk menghitung $\gcd(36, 45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 =$

Teorema

Apabila a dan b keduanya bilangan bulat tidak nol dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)}$. Notasi $\min(a, b)$ berarti bilangan terkecil diantara a dan b.

Contoh

Untuk menghitung $\gcd(36, 45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 = 3^2 \cdot 5$, akibatnya

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

sehingga $\gcd(36, 45) =$

Teorema

Apabila a dan b keduanya bilangan bulat tidak nol dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)}$. Notasi $\min(a, b)$ berarti bilangan terkecil diantara a dan b.

Contoh

Untuk menghitung $\gcd(36, 45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 = 3^2 \cdot 5$, akibatnya

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

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

Relatif Prima dan Relatif Prima Sepasang-sepasang

Definisi

Dua bilangan bulat a dan b dikatakan relatif prima apabila $\gcd(a, b) = 1$.

Definisi

Sekelompok bilangan bulat $a_1, a_2, \ldots, a_n$ dikatakan relatif prima sepasang-sepasang (*pairwise relatively prime*) apabila $\gcd(a_i, a_j) = 1$ untuk setiap $i \neq j$, $i, j \in \{1, 2, \ldots, n\}$.

Latihan

Periksa apakah sekelompok bilangan bulat berikut relatif prima sepasang-sepasang atau tidak

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

Perhatikan bahwa:

Latihan

Periksa apakah sekelompok bilangan bulat berikut relatif prima sepasang-sepasang atau tidak

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

Perhatikan bahwa:

1. $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, $\gcd(17, 21) = 1$; akibatnya 10, 17, dan 21 relatif prima sepasang-sepasang;

Latihan

Periksa apakah sekelompok bilangan bulat berikut relatif prima sepasang-sepasang atau tidak

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

Perhatikan bahwa:

1. $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, $\gcd(17, 21) = 1$; akibatnya 10, 17, dan 21 relatif prima sepasang-sepasang;
2. $\gcd(10, 19) = 1$, $\gcd(10, 24) = 2$, $\gcd(19, 24) = 1$; akibatnya 10, 19, dan 24 tidak relatif prima sepasang-sepasang.

Teorema Penting Terkait gcd

Beberapa sifat terkait gcd dijelaskan pada teorema berikut.

Teorema

Misalkan a dan b adalah dua bilangan bulat yang tak keduanya nol, maka

1. setiap faktor bersama dari a dan b membagi $\gcd(a, b)$;
2. untuk setiap $k > 0$ berlaku $\gcd(ka, kb) = k \cdot \gcd(a, b)$;
3. jika $\gcd(a, b) = 1$ dan $\gcd(a, c) = 1$, maka $\gcd(a, bc) = 1$;
4. jika $a|bc$ dan $\gcd(a, b) = 1$, maka $a|c$;
5. $\gcd(a, b) = \gcd(b, a \bmod b)$.

Untuk mencari gcd dari tiga bilangan, misalkan a, b, dan c, kita dapat memakai teorema berikut.

Teorema

Jika a, b, dan c adalah tiga bilangan yang tidak semuanya nol, maka

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

Sehingga gcd dari tiga bilangan a, b, dan c dapat ditulis sebagwherai $\gcd(a, b, c)$.

Bahasan

KPK (*Least Common Multiple*, lcm)

Bilangan bulat terkecil yang merupakan kelipatan dari dua bilangan positif dinamakan sebagai kelipatan persekutuan terkecil dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}^+$. Bilangan bulat terkecil c yang merupakan kelipatan terkecil dari a dan b dinamakan sebagai kelipatan persekutuan terkecil (*least common multiple*) dari a dan b. Dalam hal ini, kita dapat menuliskan c sebagai $\mathrm{KPK}\,(a, b)$ atau $\mathrm{lcm}\,(a, b)$.

Kita memiliki sifat bahwa c adalah $\mathrm{lcm}\,(a, b)$ apabila memenuhi kedua syarat berikut:

KPK (*Least Common Multiple*, lcm)

Bilangan bulat terkecil yang merupakan kelipatan dari dua bilangan positif dinamakan sebagai kelipatan persekutuan terkecil dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}^+$. Bilangan bulat terkecil c yang merupakan kelipatan terkecil dari a dan b dinamakan sebagai kelipatan persekutuan terkecil (*least common multiple*) dari a dan b. Dalam hal ini, kita dapat menuliskan c sebagai $\text{KPK}\,(a, b)$ atau $\text{lcm}\,(a, b)$.

Kita memiliki sifat bahwa c adalah $\text{lcm}\,(a, b)$ apabila memenuhi kedua syarat berikut:

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

KPK (*Least Common Multiple*, lcm)

Bilangan bulat terkecil yang merupakan kelipatan dari dua bilangan positif dinamakan sebagai kelipatan persekutuan terkecil dari kedua bilangan tersebut.

Definisi

Misalkan $a, b \in \mathbb{Z}^+$. Bilangan bulat terkecil c yang merupakan kelipatan terkecil dari a dan b dinamakan sebagai kelipatan persekutuan terkecil (*least common multiple*) dari a dan b. Dalam hal ini, kita dapat menuliskan c sebagai $\mathrm{KPK}\,(a, b)$ atau $\mathrm{lcm}\,(a, b)$.

Kita memiliki sifat bahwa c adalah $\mathrm{lcm}\,(a, b)$ apabila memenuhi kedua syarat berikut:

1. $a|c$ dan $b|c$,
2. jika terdapat $d \in \mathbb{Z}$ dengan sifat $a|d$ dan $b|d$, maka $c|d$.

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) =$

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\text{lcm}\,(24, 36) = 72$.

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\text{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(7, 3) =$

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(7, 3) = 21$.

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(7, 3) = 21$.
3. Kita memiliki $120 =$

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(7, 3) = 21$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 =$

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\mathrm{lcm}\,(7, 3) = 21$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\mathrm{lcm}\,(120, 500) =$

Latihan

Tentukan lcm dari

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

Solusi: Perhatikan bahwa

1. Kelipatan dari 24 adalah $24, 48, 72, 96, \ldots$, kelipatan dari 36 adalah $36, 72, 108, \ldots$, akibatnya diperoleh $\text{lcm}\,(24, 36) = 72$.
2. Kelipatan dari 7 adalah $7, 14, 21, \ldots$, kelipatan dari 3 adalah $3, 9, 12, 15, 18, 21, \ldots$, akibatnya diperoleh $\text{lcm}\,(7, 3) = 21$.
3. Kita memiliki $120 = 2^3 \cdot 3 \cdot 5$ dan $500 = 2^2 \cdot 5^3$, jadi $\text{lcm}\,(120, 500) = 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)} = 2^3 \cdot 3 \cdot 5^3 = 3000$.

Teorema

Apabila a dan b keduanya bilangan bulat positif dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \cdots \cdot p_n^{\max(a_n, b_n)}$. Notasi $\max(a, b)$ berarti bilangan terbesar diantara a dan b.

Contoh

Untuk menghitung $\operatorname{lcm}(36, 45)$, kita memiliki $36 =$

Teorema

Apabila a dan b keduanya bilangan bulat positif dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \cdots \cdot p_n^{\max(a_n, b_n)}$. Notasi $\max(a, b)$ berarti bilangan terbesar diantara a dan b.

Contoh

Untuk menghitung $\operatorname{lcm}(36, 45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 =$

Teorema

Apabila a dan b keduanya bilangan bulat positif dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_n^{\max(a_n,b_n)}$. Notasi $\max(a,b)$ berarti bilangan terbesar diantara a dan b.

Contoh

Untuk menghitung $\operatorname{lcm}(36,45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 = 3^2 \cdot 5$, akibatnya

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

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

Teorema

Apabila a dan b keduanya bilangan bulat positif dengan faktorisasi prima

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

dengan p_i adalah bilangan prima (positif) serta a_i dan b_i *bilangan bulat tak negatif* untuk setiap $i = 1, 2, \ldots, n$, maka $\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_n^{\max(a_n,b_n)}$. Notasi $\max(a,b)$ berarti bilangan terbesar diantara a dan b.

Contoh

Untuk menghitung $\operatorname{lcm}(36,45)$, kita memiliki $36 = 2^2 \cdot 3^2$ dan $45 = 3^2 \cdot 5$, akibatnya

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

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

Bahasan

Algoritma Euclid – Motivasi

Untuk mencari $\gcd$ dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
$\gcd$ dari 91 dan 287 dengan langkah-langkah berikut:

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

Algoritma Euclid – Motivasi

Untuk mencari $\gcd$ dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
$\gcd$ dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$ | pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$

Algoritma Euclid – Motivasi

Untuk mencari $\gcd$ dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
$\gcd$ dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$
	pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$
	pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$ pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	mencari $\gcd(14, 91)$ direduksi menjadi mencari $\gcd(7, 14)$

Karena $14 = 7 \cdot 2$, maka $\gcd(14, 7) =$

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$
	pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	mencari $\gcd(14, 91)$ direduksi menjadi mencari $\gcd(7, 14)$

Karena $14 = 7 \cdot 2$, maka $\gcd(14, 7) = 7$. Kemudian, karena
$\gcd(287, 91) =$

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$
	pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	mencari $\gcd(14, 91)$ direduksi menjadi mencari $\gcd(7, 14)$

Karena $14 = 7 \cdot 2$, maka $\gcd(14, 7) = 7$. Kemudian, karena
$\gcd(287, 91) = \gcd(91, 14) =$

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$
	pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	mencari $\gcd(14, 91)$ direduksi menjadi mencari $\gcd(7, 14)$

Karena $14 = 7 \cdot 2$, maka $\gcd(14, 7) = 7$. Kemudian, karena
$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) =$

Algoritma Euclid – Motivasi

Untuk mencari gcd dari dua bilangan yang cukup besar, kita dapat menggunakan algoritma Euclid (*Euclidean algorithm*).
gcd dari 91 dan 287 dengan langkah-langkah berikut:

$287 = 91 \cdot 3 + 14$	pembagi 91 dan 287 juga pembagi dari $287 - 91 \cdot 3 = 14$ pembagi 91 dan 14 juga pembagi dari $91 \cdot 3 + 14 = 287$
$91 = 14 \cdot 6 + 7$	mencari $\gcd(91, 287)$ direduksi menjadi mencari $\gcd(14, 91)$
$14 = 7 \cdot 2 + 0$	mencari $\gcd(14, 91)$ direduksi menjadi mencari $\gcd(7, 14)$

Karena $14 = 7 \cdot 2$, maka $\gcd(14, 7) = 7$. Kemudian, karena $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$, maka pencarian gcd dari 91 dan 287 telah selesai dilakukan dan kita memiliki $\gcd(287, 91) = 7$.

Algoritma Euclid – Teorema

Teorema

Apabila $a = bq + r$ dengan $a, b, q, r \in \mathbb{Z}$, maka $\gcd(a, b) = \gcd(b, r)$.

Teorema

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

Bukti dapat dilihat pada buku teks.

Algoritma Euclid – Versi Iteratif

Algoritma Euclid – Versi Iteratif

```
     function gcd (a, b)          // a, b ∈ ℤ⁺
1        x := a
2        y := b
3        while y ≠ 0
4            r := x mod y
5            x := y
6            y := r
7        return x                 // gcd (a, b) = x
```

Algoritma Euclid – Versi Rekursif

Algoritma Euclid - Versi Rekursif

```
    function gcd (a, b)                          // a, b ∈ ℤ⁺
1       if b = 0
2           return a
3       else
4           return gcd (b, a mod b)
            // gcd (a, b) = gcd (b, a mod b)
```

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

$$662 \quad =$$

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Jadi $\gcd(414, 662) =$

Latihan

Tentukan $\gcd$ dari 414 dan 662 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan gcd dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Latihan

Tentukan $\gcd$ dari 1147 dan 899 dengan algoritma Euclid.

Solusi: Perhatikan bahwa

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

Bahasan

gcd Sebagai Kombinasi Linier – Teorema Bézout

Jika $a, b \in \mathbb{Z}$ tidak keduanya nol, maka $\gcd(a,b) \mid a$ dan $\gcd(a,b) \mid b$. Lebih lanjut, kita memiliki $\gcd(a,b) \mid sa + tb$, untuk setiap $s, t \in \mathbb{Z}$.

Teorema (Teorema Bézout)

Apabila $a, b \in \mathbb{Z}$, maka terdapat $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a,b) = sa + tb$.

Pada Teorema di atas, persamaan $\gcd(a,b) = sa + tb$ dinamakan sebagai identitas Bézout, bilangan s dan t dinamakan sebagai koefisien Bézout. Sebagai contoh kita memiliki $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Koefisien Bézout tidak unik, sebagai contoh kita memiliki

$$\vdots$$

$$\gcd(6,14) = 2 \quad =$$

gcd Sebagai Kombinasi Linier – Teorema Bézout

Jika $a, b \in \mathbb{Z}$ tidak keduanya nol, maka $\gcd(a,b) \mid a$ dan $\gcd(a,b) \mid b$. Lebih lanjut, kita memiliki $\gcd(a,b) \mid sa + tb$, untuk setiap $s, t \in \mathbb{Z}$.

Teorema (Teorema Bézout)

Apabila $a, b \in \mathbb{Z}$, maka terdapat $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a,b) = sa + tb$.

Pada Teorema di atas, persamaan $\gcd(a,b) = sa + tb$ dinamakan sebagai identitas Bézout, bilangan s dan t dinamakan sebagai koefisien Bézout. Sebagai contoh kita memiliki $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Koefisien Bézout tidak unik, sebagai contoh kita memiliki

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

gcd Sebagai Kombinasi Linier – Teorema Bézout

Jika $a, b \in \mathbb{Z}$ tidak keduanya nol, maka $\gcd(a,b) \mid a$ dan $\gcd(a,b) \mid b$. Lebih lanjut, kita memiliki $\gcd(a,b) \mid sa + tb$, untuk setiap $s, t \in \mathbb{Z}$.

Teorema (Teorema Bézout)

Apabila $a, b \in \mathbb{Z}$, maka terdapat $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a,b) = sa + tb$.

Pada Teorema di atas, persamaan $\gcd(a,b) = sa + tb$ dinamakan sebagai identitas Bézout, bilangan s dan t dinamakan sebagai koefisien Bézout. Sebagai contoh kita memiliki $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Koefisien Bézout tidak unik, sebagai contoh kita memiliki

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

gcd Sebagai Kombinasi Linier – Teorema Bézout

Jika $a, b \in \mathbb{Z}$ tidak keduanya nol, maka $\gcd(a,b) \mid a$ dan $\gcd(a,b) \mid b$. Lebih lanjut, kita memiliki $\gcd(a,b) \mid sa + tb$, untuk setiap $s, t \in \mathbb{Z}$.

Teorema (Teorema Bézout)

Apabila $a, b \in \mathbb{Z}$, maka terdapat $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a,b) = sa + tb$.

Pada Teorema di atas, persamaan $\gcd(a,b) = sa + tb$ dinamakan sebagai identitas Bézout, bilangan s dan t dinamakan sebagai koefisien Bézout. Sebagai contoh kita memiliki $\gcd(6,14) = 2 = (-2) \cdot 6 + (1) \cdot 14$. Koefisien Bézout tidak unik, sebagai contoh kita memiliki

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

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

$$252 \quad =$$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

$$252 = 1 \cdot 198 + 54 \quad (1)$$

$$198 =$$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

$$252 = 1 \cdot 198 + 54 \quad (1)$$

$$198 = 3 \cdot 54 + 36 \quad (2)$$

$$54 =$$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

$$252 = 1 \cdot 198 + 54 \quad (1)$$
$$198 = 3 \cdot 54 + 36 \quad (2)$$
$$54 = 1 \cdot 36 + 18 \quad (3)$$
$$36 =$$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

$$252 = 1 \cdot 198 + 54 \quad (1)$$
$$198 = 3 \cdot 54 + 36 \quad (2)$$
$$54 = 1 \cdot 36 + 18 \quad (3)$$
$$36 = 2 \cdot 18 + 0, \quad (4)$$

akibatnya $\gcd(252, 198) =$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

$$18 =$$

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

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

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

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

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

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

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

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

Untuk mencari $s, t \in \mathbb{Z}$ yang memenuhi $\gcd(a, b) = sa + tb$, kita dapat melakukan langkah-langkah yang serupa dengan yang terdapat dalam algoritma Euclid.

Latihan

Nyatakan $\gcd(252, 198)$ sebagai kombinasi linier dari 252 dan 198.

Solusi: Pertama akan dicari $\gcd(252, 198)$ melalui algoritma Euclid

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

akibatnya $\gcd(252, 198) = 18$. Dengan melakukan 'proses yang dibalik', perhatikan bahwa

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

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

$$312 \quad =$$

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

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

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

$$312 = 4 \cdot 70 + 32 \quad (5)$$

$$70 = 2 \cdot 32 + 6 \quad (6)$$

$$32 =$$

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

$$312 = 4 \cdot 70 + 32 \quad (5)$$
$$70 = 2 \cdot 32 + 6 \quad (6)$$
$$32 = 5 \cdot 6 + 2 \quad (7)$$
$$6 =$$

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

$$312 = 4 \cdot 70 + 32 \quad (5)$$
$$70 = 2 \cdot 32 + 6 \quad (6)$$
$$32 = 5 \cdot 6 + 2 \quad (7)$$
$$6 = 3 \cdot 2 + 0 \quad (8)$$

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

$$2 =$$

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

$$312 = 4 \cdot 70 + 32 \quad (5)$$
$$70 = 2 \cdot 32 + 6 \quad (6)$$
$$32 = 5 \cdot 6 + 2 \quad (7)$$
$$6 = 3 \cdot 2 + 0 \quad (8)$$

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

$$2 = 32 - 5 \cdot 6 \text{ (dari (7))}$$
$$=$$

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

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

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

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

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

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

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

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

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

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

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

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

Latihan

Nyatakan $\gcd(312, 70)$ sebagai kombinasi linier dari 312 dan 70.

Solusi: Pertama akan dicari $\gcd(312, 70)$ melalui algoritma Euclid

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

Jadi $\gcd(312, 70) = 2$ dan kita juga memiliki

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

Bahasan

Teorema Penting Terkait gcd dan lcm

Teorema

Jika a dan b adalah dua bilangan bulat positif, maka berlaku

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

Bukti

Dijadikan salah satu *challenging problems*.

Teorema

Jika a, b, dan c adalah tiga bilangan bulat positif, maka

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

Sehingga lcm dari tiga bilangan a, b, dan c dapat ditulis sebagai $\operatorname{lcm}(a, b, c)$.

CP 1

CP 1

Alice dan Bob masing-masing memiliki sebuah toko roti. Toko roti Alice menghasilkan A potong roti coklat per hari sedangkan toko roti Bob menghasilkan B potong roti keju per hari. Untuk efisiensi penjualan, mereka berencana menjual roti coklat dan keju yang diproduksi dalam kemasan yang sama. Tugas Anda adalah menentukan banyaknya kemasan maksimal yang mungkin dengan syarat semua roti harus dimasukkan ke dalam kemasan. Banyaknya roti coklat dan keju dalam satu kemasan boleh berbeda, namun banyaknya roti coklat maupun keju antara kemasan satu dan yang lain harus sama.

Tugas Anda adalah membuat program dalam C, C++, Java, atau Python untuk menyelesaikan masalah ini. Misalkan A dan B berturut-turut adalah banyaknya roti coklat dan keju yang diproduksi, N adalah banyak maksimal kemasan yang mungkin, serta C dan K berturut-turut adalah banyaknya roti coklat dan keju per kemasan. Sebagai contoh:

- Misalkan $A = 720$, $B = 900$ (roti yang diproduksi).
- Maka haruslah $N = 180$ (banyak maksimal kemasan yang mungkin).
- Akibatnya $C = 4$ dan $K = 5$ (4 roti coklat dan 5 roti keju per kemasan).

CP 1 – I/O

CP 1

Format *input* dan *output* program yang Anda buat adalah sebagai berikut.
input: nilai A dan B
output: nilai N, C, dan K

Contoh:

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

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

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

Catatan: nilai A dan B memenuhi $1 \leq A, B \leq 10^4$.

CP 2

CP 2

Alice dan Bob masing-masing memiliki sebuah toko roti. Setiap beberapa hari sekali toko mereka masing-masing ditutup untuk pemeliharaan alat-alat dapur. Toko milik Alice tutup setiap A hari sekali, sedangkan toko milik Bob tutup setiap B hari sekali. Ketika toko Alice dan Bob keduanya tutup, kedai kopi milik Carlos, keponakan mereka, akan menjual roti yang biasanya diproduksi oleh Alice dan Bob.

Tugas Anda adalah menentukan periode (siklus) ketika toko milik Alice dan Bob keduanya tutup. Hal ini diperlukan Carlos untuk menyiapkan penjualan roti yang dilakukannya.

Tugas Anda adalah membuat program dalam C, C++, Java, atau Python untuk menyelesaikan masalah ini. Misalkan A dan B berturut-turut adalah periode ketika toko milik Alice dan Bob tutup dan P adalah periode ketika kedua toko mereka tutup bersama.

- Misalkan $A = 14$, $B = 21$ (toko Alice tutup setiap 14 hari sekali, toko Bob tutup setiap 21 hari sekali).
- Maka haruslah $P = 42$ (kedua toko tersebut tutup setiap 42 hari sekali).

CP 2 – I/O

CP 2

Format *input* dan *output* program yang Anda buat adalah sebagai berikut.
input: nilai A dan B
output: nilai P

Contoh:

```
input:  14, 21
output:  42

input:  30, 10
output:  30

input:  7, 15
output:  105
```

Catatan: nilai A dan B memenuhi $1 \leq A, B \leq 365$.

Bahasan

Definisi Kongruensi Modulo m

Ingat kembali bahwa jika $a \in \mathbb{Z}$ dan $m \in \mathbb{Z}^+$, maka $a \bmod m$ adalah sisa pembagian dari a terhadap m.

Nilai $a \bmod m$ berada pada himpunan $\{0, 1, 2, \ldots, m-1\}$. Selanjutnya nilai m pada ekspresi $a \bmod m$ juga dikatakan sebagai modulus.

Definisi

Apabila $a, b \in \mathbb{Z}$ dan $m \in \mathbb{Z}^+$, maka a kongruen b modulo m (atau a kongruen dengan b dalam modulo m), ditulis $a \equiv b \pmod m$, jikka $m|a-b$. Selanjutnya notasi $a \not\equiv b \pmod m$ menyatakan bahwa a tidak kongruen dengan b modulo m.

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

1. $6|17 - 5$ (karena $6|12$), akibatnya $17 \equiv 5 \pmod 6$,

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

1. $6|17-5$ (karena $6|12$), akibatnya $17 \equiv 5 \pmod 6$,
2. $6 \nmid -17-5$ (karena $6 \nmid -22$), akibatnya $-17 \not\equiv 5 \pmod 6$.

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

1. $6|17-5$ (karena $6|12$), akibatnya $17 \equiv 5 \pmod 6$,
2. $6 \nmid -17-5$ (karena $6 \nmid -22$), akibatnya $-17 \not\equiv 5 \pmod 6$.
3. $7 \nmid 17-2$ (karena $7 \nmid 15$), akibatnya $17 \not\equiv 2 \pmod 7$.

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

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

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

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

Latihan

Periksa apakah

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. $-8 \equiv 4 \pmod 4$

Solusi: Tinjau bahwa

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

Teorema

Apabila $m \in \mathbb{Z}^+$, maka $a \equiv b \pmod{m}$ jikka terdapat $k \in \mathbb{Z}$ yang memenuhi $a = b + km$.

Bukti

Teorema

Apabila $m \in \mathbb{Z}^+$, maka $a \equiv b \pmod{m}$ jikka terdapat $k \in \mathbb{Z}$ yang memenuhi $a = b + km$.

Bukti

Perhatikan bahwa $a \equiv b \pmod{m} \Leftrightarrow$

Teorema

Apabila $m \in \mathbb{Z}^+$, maka $a \equiv b \pmod{m}$ jikka terdapat $k \in \mathbb{Z}$ yang memenuhi $a = b + km$.

Bukti

Perhatikan bahwa $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \Leftrightarrow$

Teorema

Apabila $m \in \mathbb{Z}^+$, maka $a \equiv b \pmod{m}$ jikka terdapat $k \in \mathbb{Z}$ yang memenuhi $a = b + km$.

Bukti

Perhatikan bahwa $a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b) \Leftrightarrow km = a - b$ untuk suatu $k \in \mathbb{Z}$. □

Teorema

Apabila $a, b \in \mathbb{Z}$ dan $m \in \mathbb{Z}^+$, maka

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

Contoh

Kita memiliki:

1. $23 \bmod 5 =$

Contoh

Kita memiliki:

1. $23 \bmod 5 = 3 \bmod 5 = 3$, akibatnya $23 \equiv 3 \pmod 5$,
2. $27 \bmod 3 =$

Contoh

Kita memiliki:

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

Contoh

Kita memiliki:

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

Contoh

Kita memiliki:

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

Contoh

Kita memiliki:

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

Contoh

Kita memiliki:

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

Teorema Aritmetika Modular (*Challenging Problems*)

Teorema

Misalkan $m \in \mathbb{Z}^+$. Apabila $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ untuk setiap bilangan bulat tak negatif r

Bukti

Dijadikan sebagai *challenging problems* untuk pembaca.

Contoh

Kita memiliki $7 \equiv 2 \pmod{5}$ dan $11 \equiv 1 \pmod{5}$, akibatnya diperoleh

1. $(7 + 11) \equiv$

Teorema Aritmetika Modular (*Challenging Problems*)

Teorema

Misalkan $m \in \mathbb{Z}^+$. Apabila $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ untuk setiap bilangan bulat tak negatif r

Bukti

Dijadikan sebagai *challenging problems* untuk pembaca.

Contoh

Kita memiliki $7 \equiv 2 \pmod{5}$ dan $11 \equiv 1 \pmod{5}$, akibatnya diperoleh

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

Teorema Aritmetika Modular (*Challenging Problems*)

Teorema

Misalkan $m \in \mathbb{Z}^+$. Apabila $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ untuk setiap bilangan bulat tak negatif r

Bukti

Dijadikan sebagai *challenging problems* untuk pembaca.

Contoh

Kita memiliki $7 \equiv 2 \pmod{5}$ dan $11 \equiv 1 \pmod{5}$, akibatnya diperoleh

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

Teorema Aritmetika Modular (*Challenging Problems*)

Teorema

Misalkan $m \in \mathbb{Z}^+$. Apabila $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

1. $a + c \equiv b + d \pmod{m}$
2. $ac \equiv bd \pmod{m}$
3. $a^r \equiv b^r \pmod{m}$ untuk setiap bilangan bulat tak negatif r

Bukti

Dijadikan sebagai *challenging problems* untuk pembaca.

Contoh

Kita memiliki $7 \equiv 2 \pmod{5}$ dan $11 \equiv 1 \pmod{5}$, akibatnya diperoleh

1. $(7 + 11) \equiv 2 + 1 \pmod{5}$, atau $18 \equiv 3 \pmod{5}$;
2. $(7 \cdot 11) \equiv 2 \cdot 1 \pmod{5}$, atau $77 \equiv 2 \pmod{5}$;
3. $7^r \equiv 2^r \pmod{5}$ dan $11^r \equiv 1^r \pmod{5} \equiv 1 \pmod{5}$, untuk setiap bilangan bulat tak negatif r.

Aritmetika pada $\mathbb{Z}_m$

- Kita notasikan himpunan seluruh bilangan bulat nonnegatif yang kurang dari m dengan $\mathbb{Z}_m$, yaitu $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- Kita definisikan operasi $+_m$ dan $\cdot_m$ berturut-turut sebagai operasi penjumlahan dan perkalian pada $\mathbb{Z}_m$ yang didefinisikan sebagai berikut: untuk setiap $a, b \in \mathbb{Z}_m$, maka

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

Jika m sudah jelas, maka subskrip m dapat dihilangkan.

Latihan

Tentukan $7 +_{11} 9$ dan $7 \cdot_{11} 9$.

Solusi: Perhatikan bahwa

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

Aritmetika pada $\mathbb{Z}_m$

- Kita notasikan himpunan seluruh bilangan bulat nonnegatif yang kurang dari m dengan $\mathbb{Z}_m$, yaitu $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- Kita definisikan operasi $+_m$ dan $\cdot_m$ berturut-turut sebagai operasi penjumlahan dan perkalian pada $\mathbb{Z}_m$ yang didefinisikan sebagai berikut: untuk setiap $a, b \in \mathbb{Z}_m$, maka

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

Jika m sudah jelas, maka subskrip m dapat dihilangkan.

Latihan

Tentukan $7 +_{11} 9$ dan $7 \cdot_{11} 9$.

Solusi: Perhatikan bahwa

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

Aritmetika pada $\mathbb{Z}_m$

- Kita notasikan himpunan seluruh bilangan bulat nonnegatif yang kurang dari m dengan $\mathbb{Z}_m$, yaitu $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
- Kita definisikan operasi $+_m$ dan $\cdot_m$ berturut-turut sebagai operasi penjumlahan dan perkalian pada $\mathbb{Z}_m$ yang didefinisikan sebagai berikut: untuk setiap $a, b \in \mathbb{Z}_m$, maka

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

Jika m sudah jelas, maka subskrip m dapat dihilangkan.

Latihan

Tentukan $7 +_{11} 9$ dan $7 \cdot_{11} 9$.

Solusi: Perhatikan bahwa

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

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Komutatif Untuk setiap $a, b \in \mathbb{Z}_m$ berlaku

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Komutatif Untuk setiap $a, b \in \mathbb{Z}_m$ berlaku $a +_m b = b +_m a$ dan $a \cdot_m b = b \cdot_m a$

Eksistensi 0 Terdapat $0 \in \mathbb{Z}_m$ dengan sifat

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Komutatif Untuk setiap $a, b \in \mathbb{Z}_m$ berlaku $a +_m b = b +_m a$ dan $a \cdot_m b = b \cdot_m a$

Eksistensi 0 Terdapat $0 \in \mathbb{Z}_m$ dengan sifat $a +_m 0 = 0 +_m a = a$ untuk setiap $a \in \mathbb{Z}_m$.

Eksistensi 1 Terdapat $1 \in \mathbb{Z}_m$ dengan sifat

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Komutatif Untuk setiap $a, b \in \mathbb{Z}_m$ berlaku $a +_m b = b +_m a$ dan $a \cdot_m b = b \cdot_m a$

Eksistensi 0 Terdapat $0 \in \mathbb{Z}_m$ dengan sifat $a +_m 0 = 0 +_m a = a$ untuk setiap $a \in \mathbb{Z}_m$.

Eksistensi 1 Terdapat $1 \in \mathbb{Z}_m$ dengan sifat $a \cdot_m 1 = 1 \cdot_m a = a$ untuk setiap $a \in \mathbb{Z}_m$.

Invers aditif Untuk setiap $a \in \mathbb{Z}_m$, terdapat

Ring $\mathbb{Z}_m$

Ring $\mathbb{Z}_m$

Untuk setiap himpunan $\mathbb{Z}_m$ dengan $m \geq 2$, operasi $+_m$ dan $\cdot_m$ memenuhi sifat-sifat berikut:

Tertutup (*closure*) Untuk setiap $a, b \in \mathbb{Z}_m$, maka $a +_m b \in \mathbb{Z}_m$ dan $a \cdot_m b \in \mathbb{Z}_m$.

Asosiatif Untuk setiap $a, b, c \in \mathbb{Z}_m$ berlaku $(a +_m b) +_m c = a +_m (b +_m c)$ dan $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Komutatif Untuk setiap $a, b \in \mathbb{Z}_m$ berlaku $a +_m b = b +_m a$ dan $a \cdot_m b = b \cdot_m a$

Eksistensi 0 Terdapat $0 \in \mathbb{Z}_m$ dengan sifat $a +_m 0 = 0 +_m a = a$ untuk setiap $a \in \mathbb{Z}_m$.

Eksistensi 1 Terdapat $1 \in \mathbb{Z}_m$ dengan sifat $a \cdot_m 1 = 1 \cdot_m a = a$ untuk setiap $a \in \mathbb{Z}_m$.

Invers aditif Untuk setiap $a \in \mathbb{Z}_m$, terdapat $(m - a) \in \mathbb{Z}_m$ dengan sifat $a +_m (m - a) = (m - a) +_m a = 0$.

Kita dapat mengkonstruksi tabel penjumlahan dan perkalian pada $\mathbb{Z}_m$. Untuk $\mathbb{Z}_2$ kedua tabel tersebut adalah dijelaskan sebagai berikut:

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

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

Latihan

Buatlah tabel penjumlahan dan perkalian untuk:

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

Untuk $\mathbb{Z}_3$ kita memiliki tabel berikut:

$+_3$	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

Kemudian untuk $\mathbb{Z}_4$ kita memiliki tabel berikut:

$+_4$	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

Bahasan

Definisi Kongruensi Linier

Kita akan membahas kongruensi linier satu variabel dan solusinya.

Definisi (Kongruensi linier satu variabel)

Misalkan $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, dan x adalah suatu variabel. Suatu kongruensi linier (satu variabel) adalah kongruensi yang berbentuk $ax \equiv b \pmod{m}$.

Contoh

Contoh-contoh kongruensi linier adalah $3x \equiv 9 \pmod{7}$, $2x \equiv 1 \pmod{4}$, dan $5x \equiv 0 \pmod{7}$.

Permasalahan

Diberikan suatu kongruensi linier $ax \equiv b \pmod{m}$. Syarat apa yang diperlukan untuk memperoleh nilai x (bilangan bulat) yang memenuhi kongruensi linier ini?

Permasalahan

Diberikan suatu kongruensi linier $ax \equiv b \pmod{m}$. Syarat apa yang diperlukan untuk memperoleh nilai x (bilangan bulat) yang memenuhi kongruensi linier ini?

Pencarian solusi dari $ax \equiv b \pmod{m}$ dapat dilakukan dengan cara *brute-force/ exhaustive search*. Karena nilai x berada di himpunan $\{0, 1, \ldots, m-1\}$, maka kita dapat mencari solusi $ax \equiv b \pmod{m}$ dengan mensubstitusikan nilai $x = 0, 1, \ldots, m-1$. Namun cara ini tidak efisien.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Versi analitis:

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Versi analitis:

1. Andaikan $2x \equiv 1 \pmod 4$ memiliki solusi, maka diperoleh $4 \mid (2x - 1)$, atau $4k = 2x - 1$, untuk suatu $k \in \mathbb{Z}$.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Versi analitis:

1. Andaikan $2x \equiv 1 \pmod 4$ memiliki solusi, maka diperoleh $4 \mid (2x - 1)$, atau $4k = 2x - 1$, untuk suatu $k \in \mathbb{Z}$.
2. Akibatnya $2x = 4k + 1$, untuk suatu $k \in \mathbb{Z}$.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Versi analitis:

1. Andaikan $2x \equiv 1 \pmod 4$ memiliki solusi, maka diperoleh $4 \mid (2x - 1)$, atau $4k = 2x - 1$, untuk suatu $k \in \mathbb{Z}$.
2. Akibatnya $2x = 4k + 1$, untuk suatu $k \in \mathbb{Z}$.
3. Hal ini memberikan $x = \frac{(4k+1)}{2}$, tetapi karena $4k + 1$ selalu ganjil untuk setiap $k \in \mathbb{Z}$, maka $x = \frac{(4k+1)}{2} \notin \mathbb{Z}$.

Latihan

Periksa apakah terdapat nilai x sehingga $2x \equiv 1 \pmod 4$

Solusi:

Versi *brute-force*.
Nilai x yang mungkin adalah $x = 0, 1, 2, 3$. Tinjau bahwa $2 \cdot 0 \equiv 0 \pmod 4$, $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, $2 \cdot 3 \equiv 2 \pmod 4$. Jadi tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$.

Versi analitis:

1. Andaikan $2x \equiv 1 \pmod 4$ memiliki solusi, maka diperoleh $4 \mid (2x - 1)$, atau $4k = 2x - 1$, untuk suatu $k \in \mathbb{Z}$.
2. Akibatnya $2x = 4k + 1$, untuk suatu $k \in \mathbb{Z}$.
3. Hal ini memberikan $x = \frac{(4k+1)}{2}$, tetapi karena $4k + 1$ selalu ganjil untuk setiap $k \in \mathbb{Z}$, maka $x = \frac{(4k+1)}{2} \notin \mathbb{Z}$.
4. Jadi tidak mungkin ada nilai x yang memenuhi.

Invers Perkalian Modulo m

Di sekolah menengah, kita telah belajar cara mencari solusi $ax = b$ untuk $a \neq 0$, solusi dari $ax = b$ dapat diperoleh dengan langkah-langkah berikut

$$\begin{aligned} ax &= b \end{aligned}$$

Invers Perkalian Modulo m

Di sekolah menengah, kita telah belajar cara mencari solusi $ax = b$ untuk $a \neq 0$, solusi dari $ax = b$ dapat diperoleh dengan langkah-langkah berikut

$$\begin{aligned} ax &= b \\ a^{-1} \cdot ax &= a^{-1} \cdot b \text{ (kalikan kedua ruas dengan } a^{-1}) \\ x &= a^{-1}b. \end{aligned}$$

Untuk mencari solusi kongruensi modular di $\mathbb{Z}_m$ pertama kita perlu mendefinisikan *invers perkalian* di $\mathbb{Z}_m$.

Definisi

Invers Perkalian Modulo m

Di sekolah menengah, kita telah belajar cara mencari solusi $ax = b$ untuk $a \neq 0$, solusi dari $ax = b$ dapat diperoleh dengan langkah-langkah berikut

$$\begin{aligned} ax &= b \\ a^{-1} \cdot ax &= a^{-1} \cdot b \text{ (kalikan kedua ruas dengan } a^{-1}) \\ x &= a^{-1}b. \end{aligned}$$

Untuk mencari solusi kongruensi modular di $\mathbb{Z}_m$ pertama kita perlu mendefinisikan *invers perkalian* di $\mathbb{Z}_m$.

Definisi

Misalkan $a \in \mathbb{Z}$, bilangan $a^{-1} \in \mathbb{Z}$ dikatakan sebagai invers dari a modulo m (atau invers dari a dalam modulo m) apabila $a^{-1} \cdot a = a \cdot a^{-1} \equiv 1 \pmod{m}$.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.
4. 3 tidak memiliki invers dalam modulo 6, karena tidak ada x yang memenuhi $3x \equiv 1 \pmod 6$. Tinjau argumen berikut:

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.
4. 3 tidak memiliki invers dalam modulo 6, karena tidak ada x yang memenuhi $3x \equiv 1 \pmod 6$. Tinjau argumen berikut:
   - Jika $3x \equiv 1 \pmod 6$, maka nilai x yang mungkin adalah $x = 0, 1, 2, 3, 4, 5$.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.
4. 3 tidak memiliki invers dalam modulo 6, karena tidak ada x yang memenuhi $3x \equiv 1 \pmod 6$. Tinjau argumen berikut:
   - Jika $3x \equiv 1 \pmod 6$, maka nilai x yang mungkin adalah $x = 0, 1, 2, 3, 4, 5$.
   - Jika $x = 0$, 2, 4, maka diperoleh $3x \equiv 0 \pmod 6$.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.
4. 3 tidak memiliki invers dalam modulo 6, karena tidak ada x yang memenuhi $3x \equiv 1 \pmod 6$. Tinjau argumen berikut:
   - Jika $3x \equiv 1 \pmod 6$, maka nilai x yang mungkin adalah $x = 0, 1, 2, 3, 4, 5$.
   - Jika $x = 0$, 2, 4, maka diperoleh $3x \equiv 0 \pmod 6$.
   - Jika $x = 1, 3, 5$, maka diperoleh $3x \equiv 3 \pmod 6$.

Latihan

Periksa apakah

1. 2 memiliki invers dalam modulo 4, jika ya tentukan invers tersebut,
2. 2 memiliki invers dalam modulo 5, jika ya tentukan invers tersebut,
3. 3 memiliki invers dalam modulo 7, jika ya tentukan invers tersebut.
4. 3 memiliki invers dalam modulo 6, jika ya tentukan invers tersebut,
5. 5 memiliki invers dalam modulo 8, jika ya tentukan invers tersebut.

Solusi:

1. 2 tidak memiliki invers dalam modulo 4, karena tidak ada x yang memenuhi $2x \equiv 1 \pmod 4$, hal ini telah dijelaskan pada argumen sebelumnya,
2. $2 \cdot 3 \equiv 1 \pmod 5$, akibatnya 3 adalah invers dari 2 dalam modulo 5.
3. $3 \cdot 5 \equiv 1 \pmod 7$, akibatnya 5 adalah invers dari 3 dalam modulo 7.
4. 3 tidak memiliki invers dalam modulo 6, karena tidak ada x yang memenuhi $3x \equiv 1 \pmod 6$. Tinjau argumen berikut:
   - Jika $3x \equiv 1 \pmod 6$, maka nilai x yang mungkin adalah $x = 0, 1, 2, 3, 4, 5$.
   - Jika $x = 0$, 2, 4, maka diperoleh $3x \equiv 0 \pmod 6$.
   - Jika $x = 1, 3, 5$, maka diperoleh $3x \equiv 3 \pmod 6$.
5. $5 \cdot 5 \equiv 1 \pmod 8$, akibatnya 5 adalah invers dari 5 dalam modulo 8.

Metode Sistematis Pencarian Invers

Kita telah melihat bahwa cara menentukan a^{-1} pada $\mathbb{Z}_m$ dapat ditentukan dengan cara *brute-force*, namun cara ini tidak efisien. Untuk mencari cara yang efisien, terlebih dulu tinjau teorema berikut.

Teorema

Misalkan $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, maka a^{-1} ada di $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Bukti (a^{-1} ada $\Rightarrow \gcd(a, m) = 1$)

Metode Sistematis Pencarian Invers

Kita telah melihat bahwa cara menentukan a^{-1} pada $\mathbb{Z}_m$ dapat ditentukan dengan cara *brute-force*, namun cara ini tidak efisien. Untuk mencari cara yang efisien, terlebih dulu tinjau teorema berikut.

Teorema

Misalkan $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, maka a^{-1} ada di $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Bukti (Bukti a^{-1} ada $\Rightarrow \gcd(a, m) = 1$)

1. Karena a^{-1} ada, maka $a \cdot a^{-1} \equiv 1 \pmod{m}$. Untuk mempermudah kita akan menulis $a^{-1} = t$.

Metode Sistematis Pencarian Invers

Kita telah melihat bahwa cara menentukan a^{-1} pada $\mathbb{Z}_m$ dapat ditentukan dengan cara *brute-force*, namun cara ini tidak efisien. Untuk mencari cara yang efisien, terlebih dulu tinjau teorema berikut.

Teorema

Misalkan $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, maka a^{-1} ada di $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Bukti (Bukti a^{-1} ada $\Rightarrow \gcd(a, m) = 1$)

1. Karena a^{-1} ada, maka $a \cdot a^{-1} \equiv 1 \pmod{m}$. Untuk mempermudah kita akan menulis $a^{-1} = t$.
2. Karena $at \equiv 1 \pmod{m}$, maka $m | at - 1$, akibatnya $km = at - 1$ untuk suatu $k \in \mathbb{Z}$. Sehingga $at - km = 1$.

Metode Sistematis Pencarian Invers

Kita telah melihat bahwa cara menentukan a^{-1} pada $\mathbb{Z}_m$ dapat ditentukan dengan cara *brute-force*, namun cara ini tidak efisien. Untuk mencari cara yang efisien, terlebih dulu tinjau teorema berikut.

Teorema

Misalkan $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, maka a^{-1} ada di $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Bukti (Bukti a^{-1} ada $\Rightarrow \gcd(a, m) = 1$)

1. Karena a^{-1} ada, maka $a \cdot a^{-1} \equiv 1 \pmod{m}$. Untuk mempermudah kita akan menulis $a^{-1} = t$.
2. Karena $at \equiv 1 \pmod{m}$, maka $m | at - 1$, akibatnya $km = at - 1$ untuk suatu $k \in \mathbb{Z}$. Sehingga $at - km = 1$.
3. Karena $\gcd(a, m) | a$ dan $\gcd(a, m) | m$, maka $\gcd(a, m) | at - km$, akibatnya $\gcd(a, m) | 1$.

Metode Sistematis Pencarian Invers

Kita telah melihat bahwa cara menentukan a^{-1} pada $\mathbb{Z}_m$ dapat ditentukan dengan cara *brute-force*, namun cara ini tidak efisien. Untuk mencari cara yang efisien, terlebih dulu tinjau teorema berikut.

Teorema

Misalkan $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, maka a^{-1} ada di $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$.

Bukti (Bukti a^{-1} ada $\Rightarrow \gcd(a, m) = 1$)

1. Karena a^{-1} ada, maka $a \cdot a^{-1} \equiv 1 \pmod{m}$. Untuk mempermudah kita akan menulis $a^{-1} = t$.
2. Karena $at \equiv 1 \pmod{m}$, maka $m | at - 1$, akibatnya $km = at - 1$ untuk suatu $k \in \mathbb{Z}$. Sehingga $at - km = 1$.
3. Karena $\gcd(a, m) | a$ dan $\gcd(a, m) | m$, maka $\gcd(a, m) | at - km$, akibatnya $\gcd(a, m) | 1$.
4. Karena bilangan bulat yang dapat membagi 1 hanya -1 dan 1, maka diperoleh $\gcd(a, m) = 1$.

□

Bukti (Bukti $\gcd(a, m) = 1 \Rightarrow a^{-1}$ ada)

Bukti (Bukti $\gcd(a, m) = 1 \Rightarrow a^{-1}$ ada)

1. Karena $\gcd(a, m) = 1$, berdasarkan Teorema Bézout $1 = sa + tm = as + mt$.

Bukti (Bukti $\gcd(a, m) = 1 \Rightarrow a^{-1}$ ada)

1. Karena $\gcd(a, m) = 1$, berdasarkan Teorema Bézout $1 = sa + tm = as + mt$.
2. Akibatnya $m(-t) = as - 1$, ini berarti $m|as - 1$.

Bukti (Bukti $\gcd(a, m) = 1 \Rightarrow a^{-1}$ ada)

1. Karena $\gcd(a, m) = 1$, berdasarkan Teorema Bézout $1 = sa + tm = as + mt$.
2. Akibatnya $m(-t) = as - 1$, ini berarti $m | as - 1$.
3. Akibatnya $as \equiv 1 \pmod{m}$, sehingga kita memiliki $s = a^{-1}$. □

Bukti teorema juga menyatakan bahwa invers perkalian dapat dicari dengan bantuan Algoritma Euclid.

Latihan

Tentukan (jika ada) invers dari

1. 3 dalam modulo 7, atau solusi dari $3x \equiv 1 \pmod 7$
2. 4 dalam modulo 8, atau solusi dari $4x \equiv 1 \pmod 8$
3. 4 dalam modulo 9, atau solusi dari $4x \equiv 1 \pmod 9$
4. 7 dalam modulo 17, atau solusi dari $7x \equiv 1 \pmod{17}$

Solusi soal 1:

Cara 1: versi *brute-force*
Karena $\gcd(3, 7) = 1$, maka 3^{-1} ada dalam modulo 7. Dengan mencoba nilai x pada himpunan $\{0, 1, 2, \ldots, 6\}$, diperoleh $3 \cdot 5 = 15 \equiv 1 \pmod 7$. Akibatnya $3^{-1} \equiv 5 \pmod 7$.

Cara 2: versi Algoritma Euclid
Tinjau bahwa

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

akibatnya $1 =$

Solusi soal 1:

Cara 1: versi *brute-force*
Karena $\gcd(3,7) = 1$, maka 3^{-1} ada dalam modulo 7. Dengan mencoba nilai x pada himpunan $\{0,1,2,\ldots,6\}$, diperoleh $3 \cdot 5 = 15 \equiv 1 \pmod 7$. Akibatnya $3^{-1} \equiv 5 \pmod 7$.

Cara 2: versi Algoritma Euclid
Tinjau bahwa

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

akibatnya $1 = 3(-2) + 7$. Hal ini memberikan fakta bahwa -2 adalah invers dari 3 dalam modulo 7. Karena $-2 \equiv 5 \pmod 7$, maka diperoleh $3^{-1} \equiv 5 \pmod 7$.

Solusi soal 2: Karena $\gcd(4, 8) = 4 \neq 1$, maka tidak ada nilai x yang memenuhi $4x \equiv 1 \pmod 8$.

Solusi soal 2: Karena $\gcd(4, 8) = 4 \neq 1$, maka tidak ada nilai x yang memenuhi $4x \equiv 1 \pmod 8$.

Solusi soal 3:

Versi *brute-force*:
Karena $\gcd(4, 9) = 1$, maka 4^{-1} ada dalam modulo 9. Dengan mencoba nilai x pada himpunan $\{0, 1, 2, \ldots, 8\}$ diperoleh $4 \cdot 7 = 28 \equiv 1 \pmod 9$. Akibatnya $4^{-1} \equiv 7 \pmod 9$.

Versi algoritma Euclid:
Tinjau bahwa

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

akibatnya $1 =$

Solusi soal 2: Karena $\gcd(4, 8) = 4 \neq 1$, maka tidak ada nilai x yang memenuhi $4x \equiv 1 \pmod 8$.

Solusi soal 3:

Versi *brute-force*:
Karena $\gcd(4, 9) = 1$, maka 4^{-1} ada dalam modulo 9. Dengan mencoba nilai x pada himpunan $\{0, 1, 2, \ldots, 8\}$ diperoleh $4 \cdot 7 = 28 \equiv 1 \pmod 9$. Akibatnya $4^{-1} \equiv 7 \pmod 9$.

Versi algoritma Euclid:
Tinjau bahwa

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

akibatnya $1 = 4(-2) + 9$. Hal ini memberikan fakta bahwa -2 adalah invers dari 4 dalam modulo 9. Karena $-2 \equiv 7 \pmod 9$, maka diperoleh $4^{-1} \equiv 7 \pmod 9$.

Solusi soal 4:

Cara 1: versi *brute-force*
Karena $\gcd(7, 17) = 1$, maka 7^{-1} ada dalam modulo 17. Dengan mencoba nilai x pada himpunan $\{0, 1, 2, \ldots, 16\}$, diperoleh $7 \cdot 5 = 35 \equiv 1 \pmod{17}$. Akibatnya $7^{-1} \equiv 5 \pmod{17}$.

Cara 2: versi Algoritma Euclid
Tinjau bahwa

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

akibatnya

Solusi soal 4:

Cara 1: versi *brute-force*
Karena $\gcd(7, 17) = 1$, maka 7^{-1} ada dalam modulo 17. Dengan mencoba nilai x pada himpunan $\{0, 1, 2, \ldots, 16\}$, diperoleh $7 \cdot 5 = 35 \equiv 1 \pmod{17}$. Akibatnya $7^{-1} \equiv 5 \pmod{17}$.

Cara 2: versi Algoritma Euclid
Tinjau bahwa

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

akibatnya

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

Hal ini memberikan hasil bahwa 5 adalah invers dari 7 dalam modulo 17. Maka diperoleh $7^{-1} \equiv 5 \pmod{17}$.

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x - 1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x - 1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x =$

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x - 1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x = \frac{1}{4} \notin \mathbb{Z}$
  2. bila $k = 1$, maka $x =$

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x-1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x = \frac{1}{4} \notin \mathbb{Z}$
  2. bila $k = 1$, maka $x = \frac{10}{4} \notin \mathbb{Z}$
  3. bila $k = 2$, maka $x =$

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x-1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x = \frac{1}{4} \notin \mathbb{Z}$
  2. bila $k = 1$, maka $x = \frac{10}{4} \notin \mathbb{Z}$
  3. bila $k = 2$, maka $x = \frac{19}{4} \notin \mathbb{Z}$
  4. bila $k = 3$, maka $x =$

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x-1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x = \frac{1}{4} \notin \mathbb{Z}$
  2. bila $k = 1$, maka $x = \frac{10}{4} \notin \mathbb{Z}$
  3. bila $k = 2$, maka $x = \frac{19}{4} \notin \mathbb{Z}$
  4. bila $k = 3$, maka $x = \frac{28}{4} = 7 \in \mathbb{Z}$.

Penentuan Invers – Metode Lain

Untuk mencari invers dari 4 dalam modulo 9, yaitu nilai x yang memenuhi $4x \equiv 1 \pmod 9$, kita dapat melakukannya dengan cara berikut.

- Tinjau bahwa bila $4x \equiv 1 \pmod 9$, maka $9|4x-1$, sehingga $9k = 4x - 1$ untuk suatu $k \in \mathbb{Z}$.
- Akibatnya $x = \frac{9k+1}{4}$, dengan $k \in \mathbb{Z}$. Nilai x juga harus bilangan bulat.
- Kita akan mencari nilai x dengan mensubstitusikan nilai $k = 0, 1, 2, \ldots$.
  1. bila $k = 0$, maka $x = \frac{1}{4} \notin \mathbb{Z}$
  2. bila $k = 1$, maka $x = \frac{10}{4} \notin \mathbb{Z}$
  3. bila $k = 2$, maka $x = \frac{19}{4} \notin \mathbb{Z}$
  4. bila $k = 3$, maka $x = \frac{28}{4} = 7 \in \mathbb{Z}$.
- Jadi diperoleh $4^{-1} = x \equiv 7 \pmod 9$.

Latihan: Mencari Solusi Kongruensi Linier

Latihan

Tentukan solusi dari kongruensi linier

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

Solusi Soal 1:

Sebelumnya kita memiliki $3^{-1} \equiv 5 \pmod 7$ karena $3 \cdot 5 \equiv 1 \pmod 7$. Selanjutnya perhatikan bahwa

$$\begin{aligned} 3x &\equiv 4 \pmod 7, \text{ dengan mengalikan kedua ruas dengan } 5, \text{ diperoleh} \\ x &\equiv 20 \pmod 7, \text{ karena } 6 \equiv 20 \pmod 7, \text{ maka diperoleh} \\ x &\equiv 6 \pmod 7. \end{aligned}$$

Jadi solusi dari kongruensi linier $3x \equiv 4 \pmod 7$ adalah $x \equiv 6 \pmod 7$.

Solusi Soal 2:
Dari $12x \equiv 3 \pmod{15}$ diperoleh $15 \mid (12x - 3)$, atau $15k = 12x - 3$, untuk suatu $k \in \mathbb{Z}$. Perhatikan bahwa

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

sehingga diperoleh $5 \mid (4x - 1)$, atau kongruensi linier $4x \equiv 1 \pmod{5}$. Kita memiliki $4^{-1} \equiv 4 \pmod{5}$ karena $4 \cdot 4 \equiv 1 \pmod{5}$, akibatnya $x \equiv 4 \pmod{5}$. Karena kongruensi awal mensyaratkan dalam modulo 15, maka nilai x yang memenuhi adalah

Solusi Soal 2:
Dari $12x \equiv 3 \pmod{15}$ diperoleh $15 \mid (12x - 3)$, atau $15k = 12x - 3$, untuk suatu $k \in \mathbb{Z}$. Perhatikan bahwa

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

sehingga diperoleh $5 \mid (4x - 1)$, atau kongruensi linier $4x \equiv 1 \pmod{5}$. Kita memiliki $4^{-1} \equiv 4 \pmod{5}$ karena $4 \cdot 4 \equiv 1 \pmod{5}$, akibatnya $x \equiv 4 \pmod{5}$. Karena kongruensi awal mensyaratkan dalam modulo 15, maka nilai x yang memenuhi adalah

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

Tinjau bahwa

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

Jadi solusi dari kongruensi linier $12x \equiv 3 \pmod{15}$ adalah semua bilangan bulat x yang memenuhi salah satu dari kongruensi berikut

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

Bahasan

Kongruensi Linier dan Ring $\mathbb{Z}_m$

Suatu kongruensi linier dapat dipandang sebagai persamaan linier yang solusinya dicari pada ring $\mathbb{Z}_m$. Tinjau beberapa kongruensi linier berikut.

Latihan

Tentukan nilai x (jika ada) yang memenuhi kongruensi-kongruensi linier berikut:

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

Untuk mencari x yang merupakan solusi dari kongruensi-kongruensi tersebut, kita dapat membuat tabel penjumlahan dan perkalian untuk $\mathbb{Z}_4$ terlebih dulu.

Kongruensi Linier dan Ring $\mathbb{Z}_m$

Suatu kongruensi linier dapat dipandang sebagai persamaan linier yang solusinya dicari pada ring $\mathbb{Z}_m$. Tinjau beberapa kongruensi linier berikut.

Latihan

Tentukan nilai x (jika ada) yang memenuhi kongruensi-kongruensi linier berikut:

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

Untuk mencari x yang merupakan solusi dari kongruensi-kongruensi tersebut, kita dapat membuat tabel penjumlahan dan perkalian untuk $\mathbb{Z}_4$ terlebih dulu.

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

Kongruensi Linier dan Ring $\mathbb{Z}_m$

Suatu kongruensi linier dapat dipandang sebagai persamaan linier yang solusinya dicari pada ring $\mathbb{Z}_m$. Tinjau beberapa kongruensi linier berikut.

Latihan

Tentukan nilai x (jika ada) yang memenuhi kongruensi-kongruensi linier berikut:

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

Untuk mencari x yang merupakan solusi dari kongruensi-kongruensi tersebut, kita dapat membuat tabel penjumlahan dan perkalian untuk $\mathbb{Z}_4$ terlebih dulu.

$+_4$	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

Selanjutnya kita akan mencari nilai x dengan aturan aritmetika untuk $\mathbb{Z}_4$.

Solusi soal 1:

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

Solusi soal 1:

$$\begin{aligned} 3x &\equiv 2 \pmod 4 \\ 3^{-1} \cdot 3x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Kalikan kedua ruas dengan } 3^{-1}\text{]} \\ x &\equiv 3 \cdot 2 \pmod 4 \text{ [Karena } 3^{-1} = 3 \text{ di } \mathbb{Z}_4\text{]} \\ x &\equiv 6 \pmod 4 \equiv 2 \pmod 4 \end{aligned}$$

Solusi soal 2:

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

Solusi soal 1:

$$\begin{aligned} 3x &\equiv 2 \pmod 4 \\ 3^{-1} \cdot 3x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Kalikan kedua ruas dengan } 3^{-1}\text{]} \\ x &\equiv 3 \cdot 2 \pmod 4 \text{ [Karena } 3^{-1} = 3 \text{ di } \mathbb{Z}_4\text{]} \\ x &\equiv 6 \pmod 4 \equiv 2 \pmod 4 \end{aligned}$$

Solusi soal 2:

$$\begin{aligned} x + 2 &\equiv 1 \pmod 4 \\ x + 2 - 2 &\equiv (1 - 2) \pmod 4 \text{ [Tambah kedua ruas dengan } -2\text{]} \\ x + 0 &\equiv -1 \pmod 4 \\ x &\equiv 3 \pmod 4 \text{ [Karena } -1 = 3 \text{ di } \mathbb{Z}_4\text{]} \end{aligned}$$

Solusi soal 3:

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

Solusi soal 3:

$$
\begin{aligned}
3x+3 &\equiv 1 \pmod 4 \\
3x &\equiv -2 \pmod 4 \text{ [Tambah kedua ruas dengan } -3\text{]} \\
3x &\equiv 2 \pmod 4 \text{ [Karena } -2 = 2 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Kalikan kedua ruas dengan } 3^{-1}\text{]} \\
x &\equiv 3 \cdot 2 \pmod 4 \equiv 6 \pmod 4 \text{ [Karena } 3^{-1} = 3 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 2 \pmod 4 .
\end{aligned}
$$

Solusi soal 4:

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

Solusi soal 3:

$$\begin{aligned}
3x+3 &\equiv 1 \pmod 4 \\
3x &\equiv -2 \pmod 4 \text{ [Tambah kedua ruas dengan } -3\text{]} \\
3x &\equiv 2 \pmod 4 \text{ [Karena } -2 = 2 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Kalikan kedua ruas dengan } 3^{-1}\text{]} \\
x &\equiv 3 \cdot 2 \pmod 4 \equiv 6 \pmod 4 \text{ [Karena } 3^{-1} = 3 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 2 \pmod 4 .
\end{aligned}$$

Solusi soal 4:

$$\begin{aligned}
2x+3 &\equiv 2 \pmod 4 \\
2x &\equiv -1 \pmod 4 \text{ [Tambah kedua ruas dengan } -3\text{]} \\
2x &\equiv 3 \pmod 4 \text{ [Karena } -1 = 3 \text{ di } \mathbb{Z}_4\text{]}
\end{aligned}$$

Dari tabel perkalian,

Solusi soal 3:

$$\begin{aligned}
3x+3 &\equiv 1 \pmod 4 \\
3x &\equiv -2 \pmod 4 \text{ [Tambah kedua ruas dengan } -3\text{]} \\
3x &\equiv 2 \pmod 4 \text{ [Karena } -2 = 2 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 3^{-1} \cdot 2 \pmod 4 \text{ [Kalikan kedua ruas dengan } 3^{-1}\text{]} \\
x &\equiv 3 \cdot 2 \pmod 4 \equiv 6 \pmod 4 \text{ [Karena } 3^{-1} = 3 \text{ di } \mathbb{Z}_4\text{]} \\
x &\equiv 2 \pmod 4 .
\end{aligned}$$

Solusi soal 4:

$$\begin{aligned}
2x+3 &\equiv 2 \pmod 4 \\
2x &\equiv -1 \pmod 4 \text{ [Tambah kedua ruas dengan } -3\text{]} \\
2x &\equiv 3 \pmod 4 \text{ [Karena } -1 = 3 \text{ di } \mathbb{Z}_4\text{]}
\end{aligned}$$

Dari tabel perkalian, 2 tidak memiliki invers perkalian di $\mathbb{Z}_4$, akibatnya 2^{-1} tidak ada di $\mathbb{Z}_4$, sehingga $2x \equiv 3 \pmod 4$ tidak memiliki solusi (lebih jauh, $\gcd(2,4) = 2 \neq 1$).