# PENGANTAR TEORI BILANGAN

Margaretha Madha Melissa
Cyrenia Novella Krisnamurti

# PENGANTAR TEORI BILANGAN

**Penulis**
Margaretha Madha Melissa
Cyrenia Novella Krisnamurti

PASCAL BOOKS
Pascal Books

2022

# PENGANTAR TEORI BILANGAN

**Penulis**

Margaretha Madha Melissa

Cyrenia Novella Krisnamurti

**ISBN**

978-623-5312-62-0

**Layouter**

Della Anastiya Putri

**ANGGOTA IKAPI**

062/BANTEN/2021

**Penerbit**

Pascal Books

**Redaksi**

Jl Garuda B 30 Rt 1 Rw 12 Cipayung, Kec. Ciputat, Kota Tangerang Selatan Tangerang Selatan

penerbitpascalbooks@gmail.com

# KATA PENGANTAR

Puji dan syukur kami panjatkan kepada Tuhan Yang Maha Esa, karena dengan rahmat-Nya kami dapat menyelesaikan buku Pengantar Teori Bilangan ini. Kami juga ingin mengucapkan terima kasih kepada semua pihak yang telah membantu sehinga buku ini dapat terselesaikan dan diterbitkan.

Buku ini dibagi ke dalam lima bab, yaitu (1) sistem bilangan, induksi matematik, dan teorema binomial, (2) keterbagian dan faktorisasi prima (3) kekongruenan dan persamaan diophantine, (4) sistem nurmerik dan fungsi tangga, dan (5) kriptologi. Selain itu, dalam buku ini dilengkapi dengan materi ajar, contoh-contoh soal, dan penyelesaiannya dengan maksud agar pembaca dapat lebih memahami materi. Dengan adanya soal evaluasi disertai dengan kunci jawaban, diharapkan juga dapat membantu pembaca dalam memperkaya jenis-jenis permasalahan-permasalahan terkait materi dalam teori bilangan dan diharapkan pembaca dapat belajar secara mandiri melalui buku ajar ini.

Yogyakarta, Mei 2022
Tim Penulis

# DAFTAR ISI

# BAB I
# SISTEM BILANGAN, INDUKSI MATEMATIK, DAN TEOREMA BINOMIAL

## I. Tujuan instruksional

Pada bab ini, mahasiswa diharapkan mampu: 1) menjelaskan definisi dan sifat-sifat himpunan bilangan asli, cacah, bula, rasonal, real, kompleks; 2) mampu mengidentifikasi hubungan antar himpunan bilangan; 3) mampu membuktikan suatu pernyataan dengan menggunakan induksi matematika dan teorema binomial.

## II. Uraian Materi

### A. Sistem Bilangan

Bilangan adalah ide yang bersifat abstrak mengenai banyaknya kumpulan benda. Bilangan juga bisa diartikan sebagai konsep matematika yang digunakan untuk pencacahan dan pengukuran. Simbol ataupun lambang yang digunakan untuk mewakili suatu bilangan disebut sebagai angka atau lambang bilangan.

Bilangan terdiri dari beberapa jenis, yaitu:

1. **Bilangan Asli**

   Bilangan asli atau disebut juga *natural number* adalah himpunan bilangan positif yang dimulai dari bilangan satu.

   Jika bilangan asli dituliskan dalam simbol notasi himpunan yaitu $\mathbb{N} = \{1,2,3,4,5,\dots\}$.

Bilangan asli mempunyai **sifat tertutup** pada operasi **penjumlahan** dan **perkalian**. Artinya setiap bilangan asli, jika dijumlahkan dengan bilangan asli maka hasilnya merupakan bilangan asli. Demikian juga setiap bilangan asli jika dikalikan dengan bilangan asli hasilnya merupakan bilangan asli.

2. **Bilangan Cacah**

   Bilangan cacah atau disebut *whole number* adalah himpunan bilangan positif dan nol.

   Jika bilangan cacah dituliskan dalam simbol notasi himpunan yaitu $\mathbb{N} \cup \{0\} = \{0.1,2,3,4,5, \dots\}$..

   Bilangan cacah mempunyai sifat tertutup pada operasi penjumlahan dan perkalian.

3. **Bilangan Bulat**

   Bilangan bulat atau disebut *integer* terdiri dari himpunan bilangan bulat negatif, bilangan nol, dan bilangan bulat positif.

   Jika bilangan bulat dituliskan dalam simbol notasi himpunan yaitu $\mathbb{Z} = \{\dots, -3, -2, -1,0,1,2,3, \dots\}$.

   Bilangan bulat mempunyai sifat tertutup pada operasi penjumlahan, pengurangan, dan perkalian.

4. **Bilangan rasional**

   Bilangan rasional adalah bilangan yang dapat dinyatakan sebagai pecahan $\frac{a}{b}, a, b \in Z, b \neq 0$.

   Bilangan rasional terdiri dari bilangan bulat dan pecahan. Dilambangkan dengan $\mathbb{Q}$.

   Jika bilangan rasional dituliskan dalam simbol notasi himpunan yaitu $\mathbb{Q} = \left\{\frac{1}{2}, \frac{1}{5}, 0,1, \frac{5}{4}, 2, \dots\right\}$.

   Operasi apa saja yang mempunyai sifat tertutup pada bilangan rasional? Silahkan dijawab sebagai latihan.

5. **Bilangan irrasional**

Bilangan irrasional adalah bilangan yang tidak dapat dinyatakan sebagai pecahan $\frac{a}{b}, b \neq 0$.

Bilangan irrasional dilambangkan dengan $\mathbb{Q}^{c}$

Jika bilangan irrasional dituliskan dalam simbol notasi himpunan yaitu $\mathbb{Q}^{C} = \{\sqrt{2}, \sqrt{3}, \pi, e, \dots\}$

Operasi apa saja yang mempunyai sifat tertutup pada bilangan irrasional? Silahkan dijawab sebagai latihan.

6. **Bilangan Real**

Bilangan real adalah bilangan yang merupakan gabungan dari bilangan rasional dan bilangan irrasional. Dilabangkan dengan $\mathbb{R}$.

Bilangan real dapat digambarkan dengan garis bilangan.

$\mathbb{R}$

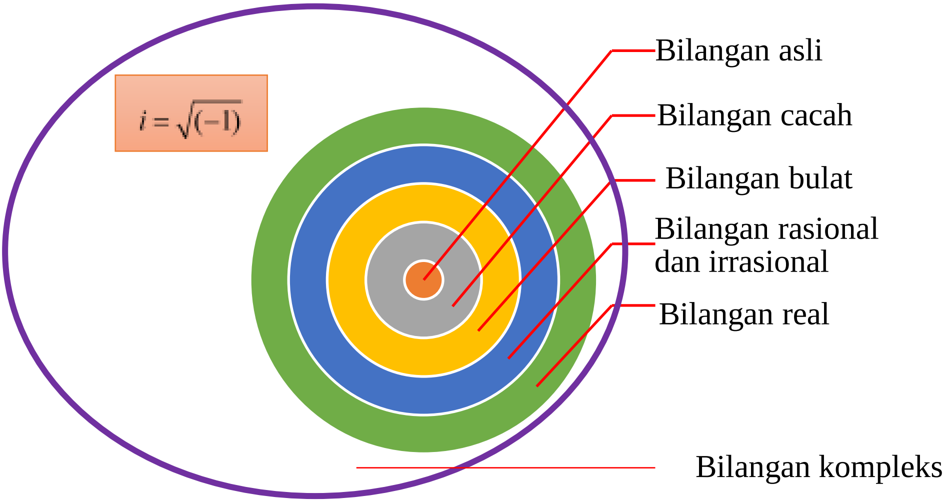
Operasi apa saja yang mempunyai sifat tertutup pada bilangan real? Silahkan dijawab sebagai latihan.

7. **Bilangan Kompleks**

Bilangan kompleks terdiri dari bilangan real dan bilangan imaginer. Bilangan imaginer dilambangkan dengan *i*, dengan $i = \sqrt{(-1)}$. Bilangan kompleks dilambangkan dengan $\mathbb{C}$.

Jika bilangan kompleks dituliskan dalam simbol notasi himpunan yaitu $\mathbb{C} = \{x | x = a + bi\ , a, b \in \mathbb{Z}, i = \sqrt{(-1)}\}$

Berikut ini adalah system bilangan yang disajikan dalam bentuk diagram.




## B. Induksi Matematik

Induksi matematik merupakan salah satu metode atau cara pembuktian yang absah dalam matematika. Meskipun namanya induksi matematik, namun metode ini merupakan penalaran deduktif. Pembuktian dengan induksi matematik berkenaan dengan pembuktian pada pernyataan-pernyataan yang semestanya adalah himpunan bilangan bulat atau lebih khusus himpunan semua bilangan asli.

Misalkan $p(n)$ adalah suatu pernyataan yang berlaku untuk setiap bilangan asli n. Pembuktian kebenaran dari pernyataan ini dengan menggunakan induksi matematik mengikuti langkah-langkah sebagai berikut.

Langkah (1) : Ditunjukkan bahwa $p(1)$ benar.

Langkah (2) : Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli $k > 1$, dan ditunjukkan bahwa $p(k+1)$ benar.

Apabila kedua langkah tersebut berhasil, maka kita dapat menyimpulkan bahwa $p(n)$ benar untuk setiap bilangan asli $n$. Langkah (1) disebut *basis (dasar)* induksi dan langkah (2) disebut *langkah induksi.*

Basis induksi tidak mesti diambil $n = 1$, tetapi diambil sesuai dengan permasalahan yang dihadapi atau pernyataan yang ingin dibuktikan. Misalkan akan dibuktikan bahwa $p(n)$ berlaku untuk setiap bilangan asli $n \geq t$. Maka langkah-langkah pembuktiannya dengan induksi matematik sebagai berikut.

Langkah (1) : Ditunjukkan bahwa $p(t)$ benar.

Langkah (2) : Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli $k \geq t$, dan ditunjukkan bahwa $p(k + 1)$ benar.

Apabila kedua langkah ini berhasil, maka kita dapat menyimpulkan bahwa $p(n)$ benar untuk setiap bilangan asli $n \geq t$.

Dalam pembuktian dengan induksi matematik, kita tidak boleh mengabaikan langkah (1), yaitu basis induksi, sebab ada kemungkinan kita mendapatkan kesimpulan yang salah.

## Latihan

1. $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1)$, untuk setiap bilangan asli $n$.
2. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$, untuk setiap bilangan asli $n$.
3. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, untuk setiap bilangan asli $n$.
4. $4 + 10 + 16 + \cdots + (6n - 2) = n(3n + 1)$ untuk setiap bilangan asli $n$.

## Kunci Jawaban

1. Jawab

   Bukti :

   a. Ditunjukkan bahwa $n = 1$ benar.

   $$1 = \frac{1}{2}n(n+1)$$
   $$= \frac{1}{2}1(1+1)$$
   $$= 1$$

   b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $1 + 2 + 3 + \cdots + k = \frac{1}{2}k(k+1)$

   Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

   $$1 + 2 + 3 + \cdots + k + (k+1)$$
   $$= (1 + 2 + 3 + \cdots + k) + (k+1)$$
   $$= \frac{1}{2}k(k+1) + (k+1)$$
   $$= \left(\frac{1}{2}k + 1\right)(k+1)$$
   $$= \frac{1}{2}(k+1)(k+2)$$
   $$= \frac{1}{2}(k+1)\big((k+1)+1\big)$$

Jadi, $1 + 2 + 3 + \cdots + k + (k+1) = \frac{1}{2}(k+1)\big((k+1)+1\big)$ berarti $n = k + 1$ benar. Sehingga $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$ benar untuk setiap bilangan asli $n$.

2. Jawab

   Bukti :

   a. Ditunjukkan bahwa $n = 1$ benar.

   $$1 = n^2$$
   $$= 1^2$$
   $$= 1$$

   b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $1 + 3 + 5 + \cdots + (2k-1) = k^2$

Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

$1 + 3 + 5 + \cdots + 2(k-1) + (2(k+1) - 1)$

$= \big(1 + 3 + 5 + \cdots + 2(k-1)\big) + (2(k+1) - 1) = k^2 + (2(k+1) - 1)$

$= k^2 + (2k + 2 - 1) = k^2 + (2k+1) = (k+1)^2$

*Jadi*, $1 + 3 + 5 + \cdots + 2(k-1) + (2(k+1) - 1) = (k+1)^2$ berarti $n = k + 1$ benar.

Sehingga $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ benar untuk setiap bilangan asli $n$.

3. Jawab

Bukti :

a. Ditunjukkan bahwa $n = 1$ benar.

$$1^2 = \frac{n(n+1)(2n+1)}{6}$$
$$1 = \frac{1(1+1)(2(1)+1)}{6}$$
$$= \frac{2\times 3}{6}$$
$$= \frac{6}{6} = 1$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$

Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2$

$= (1^2 + 2^2 + 3^2 + \cdots + k^2) + (k+1)^2$

$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right)$

$= (k+1)\left(\frac{k(2k+1)+6(k+1)}{6}\right)$

$= (k+1)\left(\frac{2k^2+k+6k+6)}{6}\right)$

$= (k+1)\left(\frac{2k^2+7k+6)}{6}\right)$
$= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right)$
$= \frac{(k+1)(k+2)(2k+3)}{6}$
$= \frac{(k+1)\left((k+1)+1\right)(2(k+1)+1)}{6}$

Jadi, $1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)\left((k+1)+1\right)(2(k+1)+1)}{6}$ berarti $n = k+1$ benar.

Sehingga $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ benar untuk setiap bilangan asli $n$.

4. Jawab

Bukti :

a. Ditunjukkan bahwa $n = 1$ benar.

$$(6n-2) = n(3n+1)$$
$$(6(1)-2) = 1(3(1)+1)$$
$$4 = 1(4)$$
$$4 = 4$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $4 + 10 + 16 + \cdots + (6k-2) = k(3k+1)$

Selanjutnya ditunjukkan bahwa $n = k+1$ benar, yaitu:

$4 + 10 + 16 + \cdots + (6k-2) + (6(k+1)-2)$
$= \left(4 + 10 + 16 + \cdots + (6k-2)\right) + (6(k+1) - 2)$
$= k(3k+1) + (6k+4)$
$= 3k^2 + k + 6k + 4$
$= 3k^2 + 7k + 4$
$= (k+1)(3k+4)$
$= (k+1)(3k+3+1)$
$= (k+1)(3(k+1)+1)$

Jadi, $4 + 10 + 16 + \cdots + (6k - 2) + (6(k + 1) - 2) = (k + 1)(3(k + 1) + 1)$ berarti $n = k + 1$ benar.
Sehingga $4 + 10 + 16 + \cdots + (6n - 2) = n(3n + 1)$ benar untuk setiap bilangan asli $n$.

## C. Teorema Binomial

Banyaknya kombinasi dari sejumlah $r$ objek yang diambil dari $n$ objek $(r \leq n)$adalah

$$\boldsymbol{C(n, r) = \binom{n}{r} = \frac{n!}{(n-r)!\,r!}}$$

**Teorema 1.1**
**Jika $(\boldsymbol{r \leq n})$, maka**

$$\boldsymbol{\binom{n}{r} = \binom{n}{n-r}}$$

Teorema ini sering disebut sifat simetrik dari koefisien binomial.
Bukti :

$$\begin{aligned}\binom{n}{r} &= \frac{n!}{(n-r)!r!}\\ &= \frac{n!}{(n-r)!(n-n+r)!}\\ &= \frac{n!}{(n-r)!\big(n-(n-r)\big)!}\\ &= \frac{n!}{\big(n-(n-r)\big)!(n-r)!}\\ &= \binom{n}{n-r}\end{aligned}$$

**Teorema 1.2**
**Jika $\boldsymbol{k}$ dan $\boldsymbol{r}$ bilangan-bilangan asli dengan $\boldsymbol{k > r}$, maka**

$$\boldsymbol{\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}}$$

Bukti :

$$\binom{k}{r-1} + \binom{k}{r} = \frac{k!}{\big(k-(r-1)\big)!(r-1)!} + \frac{k!}{(k-r)!r!}$$

$$= \frac{k!}{(k-(r-1))!(r-1)!} + \frac{k!}{(k-r)!r!}$$
$$= \frac{k!(k-r)!r! + k!(k-(r-1))!(r-1)!}{(k-(r-1))!(r-1)!(k-r)!r!}$$
$$= \frac{k!(k-r)!r! + k!(k-r+1)!(r-1)!}{(k-r+1)!(r-1)!(k-r)!r!}$$
$$= \frac{k!r + k!(k-r+1)}{(k-r+1)(k-r)!r!}$$
$$= \frac{k!(r+(k-r+1))}{(k-r+1)!r!}$$
$$= \frac{k!(k+1)}{(k+1-r)!r!}$$
$$= \frac{(k+1)!}{((k+1)-r)!r!}$$
$$= \binom{k+1}{r}$$

**Teorema 1.3 (Teorema Binomial)**

$\boldsymbol{(1+a)^n = \binom{n}{0} + \binom{n}{1} a + \binom{n}{2} a^2 + \binom{n}{3} a^3 + \cdots + \binom{n}{k} a^k + \cdots + \binom{n}{n} a^n}$ **untuk setiap bilangan asli $\boldsymbol{n}$.**

Bukti:

Kita buktikan dengan induksi matematik.

1. Untuk $n = 1$, maka

   $(1+a)^1 = \binom{1}{0} + \binom{1}{1} a$

   $1 + a = 1 + 1.a$

   $1 + a = 1 + a$, benar

2. Diasumsikan bahwa pernyataan benar untuk suatu bilangan asli $k$, yaitu: $(1+a)^k = \binom{k}{0} + \binom{k}{1} a + \binom{k}{2} a^2 + \binom{k}{3} a^3 + \cdots + \binom{k}{r} a^r + \cdots + \binom{k}{k} a^k$

   Selanjutnya akan ditunjukkan benar untuk bilangan asli $k + 1$,

   $(1+a)^{k+1} = (1+a)^k(1+a)$

$= \left[\binom{k}{0} + \binom{k}{1} a + \binom{k}{2} a^2 + \binom{k}{3} a^3 + \cdots + \binom{k}{r} a^r + \right.$

$\left. \cdots + \binom{k}{k} a^k \right] (1 + a)$

$= \binom{k}{0} + \left[\binom{k}{0} + \binom{k}{1}\right] a + \left[\binom{k}{2} + \binom{k}{3}\right] a^2 + \cdots +$

$\left[\binom{k}{k-1} + \binom{k}{k}\right] a^k + \binom{k}{k} a^{k+1}$

$= \binom{k+1}{0} + \binom{k+1}{1} a + \binom{k+1}{2} a^2 + \cdots +$

$\binom{k+1}{k} a^k + \binom{k+1}{k+1} a^k$

Jadi $(1 + a)^{k+1} = \binom{k+1}{0} + \binom{k+1}{1} a + \binom{k+1}{2} a^2 + \cdots + \binom{k+1}{k} a^k + \binom{k+1}{k+1} a^k$ benar, sehingga $(1 + a)^n = \binom{n}{0} + \binom{n}{1} a + \binom{n}{2} a^2 + \binom{n}{3} a^3 + \cdots + \binom{n}{k} a^k + \cdots + \binom{n}{n} a^n$ benar untuk setiap bilangan asli $n$.

**Teorema 1.4**

**Jika n suatu bilangan asli, maka**

$$\boldsymbol{\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n}$$

Bukti:

Kita buktikan dengan induksi matematik.

1. Untuk $n = 1$, maka

   $\binom{1}{0} + \binom{1}{1} = 2^1$

   $1 + 1 = 2$

   $2 = 2$

2. Diasumsikan bahwa pernyataan benar untuk suatu bilangan asli $k$, yaitu:

   $$\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \binom{k}{3} + \cdots + \binom{k}{r} + \cdots + \binom{k}{k} = 2^k$$

Selanjutnya akan ditunjukkan benar untuk bilangan asli $k+1$,

$$\binom{k+1}{0}+\binom{k+1}{1}+\binom{k+1}{2}+\cdots+\binom{k+1}{r}+\cdots+$$
$$\binom{k+1}{k}+\binom{k+1}{k+1}$$
$$=\binom{k}{0}+\left[\binom{k}{0}+\binom{k}{1}\right]+\left[\binom{k}{1}+\binom{k}{2}\right]+\cdots+$$
$$\left[\binom{k}{k-1}+\binom{k}{k}\right]+\binom{k}{k}$$
$$=\left[\binom{k}{0}+\binom{k}{1}+\binom{k}{2}+\binom{k}{3}+\cdots+\binom{k}{r}+\cdots+\right.$$
$$\left.\binom{k}{k}\right](1+1)$$
$$=(1+1)^k(1+1)$$
$$=2^k 2$$
$$=2^{k+1}$$

Jadi $\binom{k+1}{0}+\binom{k+1}{1}+\binom{k+1}{2}+\cdots+\binom{k+1}{r}+\cdots+\binom{k+1}{k}+\binom{k+1}{k+1}=2^{k+1}$ benar, sehingga $\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{k}+\cdots+\binom{n}{n}=2^n$ benar untuk setiap bilangan asli $n$.

**Teorema 1.5**

**Jika $\boldsymbol{n}$, $\boldsymbol{m}$ dan $\boldsymbol{k}$ adalah bilangan-bilangan asli dengan $\boldsymbol{n>k>m}$, maka**

$$\boldsymbol{\binom{n}{k}\binom{k}{m}=\binom{n}{m}\binom{n-m}{k-m}}$$

Bukti :

$$\binom{n}{k}\binom{k}{m}=\frac{n!}{(n-k)!k!}\times\frac{k!}{(k-m)!m!}$$
$$=\frac{n!k!}{(n-k)!k!(k-m)!m!}$$
$$=\frac{n!}{(n-k)!(k-m)!m!}$$

$$= \frac{n!(n-m)!}{(n-m)!(n-k)!(k-m)!m!}$$
$$= \frac{n!}{(n-m)!m!} \times \frac{(n-m)!}{(n-k)!(k-m)!}$$
$$= \frac{n!}{(n-m)!m!} \times \frac{(n-m)!}{(n-m+m-k)!(k-m)!}$$
$$= \frac{n!}{(n-m)!m!} \times \frac{(n-m)!}{\big((n-m)-(k-m)\big)!(k-m)!}$$
$$= \binom{n}{m}\binom{n-m}{k-m}$$

Terbukti.

**Teorema 6**

**Jika n dan k bilangan-bilangan asli dengan $\boldsymbol{n \geq k}$, maka**

$$\boldsymbol{k\binom{n}{k} = n\binom{n-1}{k-1}}$$

Bukti :

$$k\binom{n}{k} = k\frac{n!}{(n-k)!k!}$$
$$= \frac{kn!}{(n-k)!k!}$$
$$= \frac{n!}{(n-k)!(k-1)!}$$
$$= \frac{n!(n-k+1)}{(n-k+1)!(k-1)!}$$
$$= \frac{n!\big(n-(k-1)\big)}{\big(n-(k-1)\big)!(k-1)!}$$
$$= \frac{n!}{(n-(k-1)-1)!(k-1)!}$$
$$= \frac{n(n-1)!}{\big((n-1)-(k-1)\big)!(k-1)!}$$
$$= n\frac{(n-1)!}{\big((n-1)-(k-1)\big)!(k-1)!}$$
$$= n\binom{n-1}{k-1}$$

Terbukti

**Teorema 7**

**Jika $\boldsymbol{k}$ dan $\boldsymbol{r}$ bilangan-bilangan asli dengan $\boldsymbol{k \geq r}$, maka**

a. $\boldsymbol{\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+r}{r} = \binom{k+r+1}{r}}$

Bukti:

Kita buktikan dengan induksi matematik.

a. Untuk $r = 1$, maka

$$\binom{k}{0} + \binom{k+1}{1} = \binom{k+r+1}{r}$$

$$\binom{k}{0} + \binom{k+1}{1} = \binom{k+1+1}{1}$$

$$\frac{k!}{k!0!} + \frac{(k+1)!}{k!1!} = \frac{(k+2)!}{(k+1)!1!}$$

$$\frac{k!}{k!} + \frac{(k+1)!}{k!} = \frac{(k+2)!}{(k+1)!}$$

$$1 + (k+1) = (k+2)$$

$$k + 2 = k + 2$$

b. Diasumsikan bahwa pernyataan benar untuk suatu bilangan asli $n$, yaitu:

$$\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+n}{n} = \binom{k+n+1}{n}$$

Selanjutnya akan ditunjukkan benar untuk bilangan asli $n + 1$,

$$\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+n}{n} + \binom{k+n+1}{n+1}$$

$$= \left[\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+n}{n}\right] + \binom{k+n+1}{n+1}$$

$$= \binom{k+n+1}{n} + \binom{k+n+1}{n+1}$$

$= \binom{k+n+1+1}{n+1}$ **Teorema 2**

$= \binom{k+(n+1)+1}{(n+1)}$

Jadi $\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+n}{n} + \binom{k+n+1}{n+1} = \binom{k+(n+1)+1}{(n+1)}$ benar, sehingga $\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+r}{r} = \binom{k+r+1}{r}$ benar untuk setiap bilangan asli $k \geq r$.

b. $\boldsymbol{\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} = \binom{k+r+1}{k+1}}$

Bukti:

Kita buktikan dengan induksi matematik.

a. Untuk $r = 1$, maka

$$\binom{k}{k} + \binom{k+1}{k} = \binom{k+r+1}{k+1}$$

$$\binom{k}{k} + \binom{k+1}{k} = \binom{k+1+1}{k+1}$$

$$\frac{k!}{0!k!} + \frac{(k+1)!}{1!k!} = \frac{(k+2)!}{1!(k+1)!}$$

$$\frac{k!}{k!} + \frac{(k+1)!}{k!} = \frac{(k+2)!}{(k+1)!}$$

$$1 + (k+1) = (k+2)$$

$$k+2 = k+2$$

b. Diasumsikan bahwa pernyataan benar untuk suatu bilangan asli $n$, yaitu:

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+n}{k} = \binom{k+n+1}{k+1}$$

Selanjutnya akan ditunjukkan benar untuk bilangan asli $n+1$,

$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots +$
$\binom{k+n}{k} + \binom{k+n+1}{k}$
$= \left[\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots +\right.$
$\left.\binom{k+n}{k}\right] + \binom{k+n+1}{k}$
$= \binom{k+n+1}{k+1} + \binom{k+n+1}{k}$
$= \binom{k+n+1+1}{k+1}$ **Teorema 2**
$= \binom{k+(n+1)+1}{(k+1)}$

Jadi $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+n}{k} + \binom{k+n+1}{k} = \binom{k+(n+1)+1}{(n+1)}$ benar, sehingga $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} = \binom{k+r+1}{k+1}$ benar untuk setiap bilangan asli $k \geq r$.

## Latihan

1. Tunjukkan bahwa $1 + 2 + 3 + 4 + \cdots + n = \binom{n+1}{2}$.

2. Buktikanlah bahwa $n \geq 1$, berlaku $\binom{n}{k} = \binom{n}{k+1}$ bila dan hanya bila $n$ suatu bilangan ganjil dan $k = \frac{1}{2}(n-1)$.

3. Buktikan bahwa $\binom{2n}{n} + \binom{2n}{n-1} = \frac{1}{2}\binom{2n+2}{n+1}$.

## Kunci Jawaban

1. Bukti:
   a. Untuk $n = 1$, maka
   $1 = \binom{1+1}{2}$
   $1 = \frac{2!}{2!}$
   $1 = 1$
   b. Diasumsikan bahwa pernyataan benar untuk suatu bilangan asli $k$, yaitu: $1 + 2 + 3 + 4 + \cdots + k = \binom{k+1}{2}$.
   Selanjutnya akan ditunjukkan benar untuk bilangan asli $k + 1$,
   $1 + 2 + 3 + 4 + \cdots + k + (k+1) \ = (1 + 2 + 3 + 4 + \cdots + k) + (k+1)$
   $= \binom{k+1}{2} + (k+1)$
   $= \frac{(k+1)!}{(k-1)!2!} + (k+1)$
   $= \frac{(k+1)!}{(k-1)!2!} + \frac{(k-1)!2(k+1)}{(k-1)!2!}$
   $= \frac{(k-1)!\left((k+1)k+2(k+1)\right)}{(k-1)!2!}$
   $= \frac{(k-1)!\left(k^2+k+2k+2\right)}{(k-1)!2!}$

$$= \frac{(k-1)!\left(k^2+3k+2\right)}{(k-1)!2!}$$
$$= \frac{(k-1)!(k+1)(k+2)}{(k-1)!2!}$$
$$= \frac{(k+2)!}{k(k-1)!2!}$$
$$= \frac{(k+2)!}{k!2!}$$
$$= \frac{(k+2)!}{(k+2-2)!2!}$$
$$= \frac{\left((k+1)+1\right)!}{\left((k+1)+1-2\right)!2!}$$
$$= \binom{(k+1)+1}{2}$$

Jadi $1 + 2 + 3 + 4 + \cdots + k + (k+1) = \binom{(k+1)+1}{2}$ benar, sehingga $1 + 2 + 3 + 4 + \cdots + n = \binom{n+1}{2}$ benar untuk setiap bilangan asli $n$.

**2.** Bukti

$$\binom{n}{k} = \binom{n}{k+1}$$
$$\frac{n!}{(n-k)!k!} = \frac{n!}{\left(n-(k+1)\right)!(k+1)!}$$
$$n!\left(n-(k+1)\right)!\,(k+1)! = n!\,(n-k)!\,k!$$
$$\left(n-(k+1)\right)!\,(k+1)! = (n-k)!\,k!$$
$$(n-k-1)!\,(k+1)k! = (n-k)!\,k!$$
$$(n-k-1)!\,(k+1)k! = (n-k)(n-k-1)!\,k!$$
$$k+1 = n-k$$
$$-n = -2k-1$$
$$n = 2k+1$$

terbukti bahwa $n$ adalah bilangan ganjil dimana $k$ adalah anggota bilangan bulat.

$$n = 2k+1$$
$$2k = n-1$$

$k = \frac{1}{2}(n-1)$

Terbukti $n \geq 1$, berlaku $\binom{n}{k} = \binom{n}{k+1}$ bila dan hanya bila $n$ suatu bilangan ganjil dan $k = \frac{1}{2}(n-1)$.

3. Bukti:

$$\binom{2n}{n} + \binom{2n}{n-1} = \frac{(2n)!}{(2n-n)!n!} + \frac{(2n)!}{(2n-(n-1))!(n-1)!}$$
$$= \frac{(2n)!}{n!n!} + \frac{(2n)!}{(n+1)!(n-1)!}$$
$$= \frac{(2n)!(n+1)+(2n)!n}{n!(n+1)!}$$
$$= \frac{(2n)!\big((n+1)+n\big)}{n!(n+1)!}$$
$$= \frac{(2n)!(2n+1)}{n!(n+1)!}$$
$$= \frac{(2n+1)!}{n!(n+1)!}$$
$$= \frac{(2n+2)!}{(2n+2)n!(n+1)!}$$
$$= \frac{(2n+2)!}{2(n+1)n!(n+1)!}$$
$$= \frac{(2n+2)!}{2(n+1)!(n+1)!}$$
$$= \frac{1}{2} \times \frac{(2n+2)!}{(2n-n+2-1)!(n+1)!}$$
$$= \frac{1}{2} \times \frac{(2n+2)!}{\big((2n+2)-(n+1)\big)!(n+1)!}$$
$$= \frac{1}{2}\binom{2n+2}{n+1}$$

Terbukti $\binom{2n}{n} + \binom{2n}{n-1} = \frac{1}{2}\binom{2n+2}{n+1}$.

## III. RANGKUMAN

1. Sistem bilangan kompleks terdiri dari bilangan real, bilangan rasional dan irrasional, bilangan bulat, bilangan cacah, dan bilangan asli.
2. Langkah pembuktian dalam induksi matematika adalah:

Langkah (1) : Ditunjukkan bahwa $p(1)$ benar.

Langkah (2) : Diasumsikan bahwa $p(k)$ benar untuk suatu bilangan asli $k > 1$, dan ditunjukkan bahwa $p(k+1)$ benar.

3. Banyaknya kombinasi dari sejumlah $r$ objek yang diambil dari $n$ objek $(r \leq n)$adalah

$$C(n,r) = \binom{n}{r} = \frac{n!}{(n-r)!\,r!}$$

4. Jika $(r \leq n)$, maka

$$\binom{n}{r} = \binom{n}{n-r}$$

Teorema ini sering disebut sifat simetrik dari koefisien binomial.

5. Jika $k$ dan $r$ bilangan-bilangan asli dengan $k > r$, maka

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}$$

6. Teorema Binomial

$(1+a)^n = \binom{n}{0} + \binom{n}{1}a + \binom{n}{2}a^2 + \binom{n}{3}a^3 + \cdots +$
$\binom{n}{k}a^k + \cdots + \binom{n}{n}a^n$ untuk setiap bilangan asli $n$.

7. Jika n suatu bilangan asli, maka

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{k} + \cdots + \binom{n}{n} = 2^n$$

8. Jika $n$, $m$ dan $k$ adalah bilangan-bilangan asli dengan $n > k > m$, maka

$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$$

9. Jika n dan k bilangan-bilangan asli dengan $n \geq k$, maka

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

10. Jika $k$ dan $r$ bilangan-bilangan asli dengan $k \geq r$, maka

a. $\binom{k}{0} + \binom{k+1}{1} + \binom{k+2}{2} + \binom{k+3}{3} + \cdots + \binom{k+r}{r} =$
$\binom{k+r+1}{r}$

b. $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \binom{k+3}{k} + \cdots + \binom{k+r}{k} =$
$\binom{k+r+1}{k+1}$

## IV. LATIHAN SOAL

1. $1.2 + 2.3 + 3.4 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$ untuk setiap bilangan asli $n$.
2. $1^2 + 2^2 + 3^2 + \cdots + (2n-1)^2 = \frac{1}{3}n(4n^2-1)$ untuk setiap bilangan asli $n$.
3. $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ untuk setiap bilangan asli $n$.
4. $\sum_{n=1}^{k} cn = c\sum_{n=1}^{k} n$ untuk setiap bilangan asli $n$.
5. $\sum_{n=1}^{k}(3n-2) = \frac{1}{2}(3k^2-k)$ untuk setiap bilangan asli $n$.
6. $\frac{1}{1.3} + \frac{1}{3.5} + \frac{1}{5.7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$ untuk setiap bilangan asli $n$.
7. Buktikan bahwa $n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$.
8. Buktikanlah bahwa $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = 3^n$

**Kunci Jawaban**

1. Bukti :
   a. Ditunjukkan bahwa $n = 1$ benar.

$$n(n+1) = \frac{1}{3}n(n+1)(n+2)$$
$$1(1+1) = \frac{1}{3}1(1+1)(1+2)$$
$$1(2) = \frac{1}{3}1(2)(3)$$
$$2 = \frac{1}{3}6$$
$$2 = 2$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $1.2 + 2.3 + 3.4 + \cdots + k(k+1) = \frac{1}{3}k(k+1)(k+2)$

Selanjutnya dintunjukkan bahwa $n = k + 1$ benar, yaitu:

$1.2 + 2.3 + 3.4 + \cdots + k(k+1) + (k+1)\big((k+1)+1\big)$

$= \big(1.2 + 2.3 + 3.4 + \cdots + k(k+1)\big) + (k+1)\big((k+1) + 1\big)$

$= \frac{1}{3}k(k+1)(k+2) + (k+1)\big((k+1)+1\big)$

$= \frac{1}{3}k(k+1)(k+2) + (k+1)(k+2)$

$= \frac{1}{3}(k+1)\big(k(k+2) + 3(k+2)\big)$

$= \frac{1}{3}(k+1)(k+2)(k+3)$

$= \frac{1}{3}(k+1)\big((k+1)+1\big)\big((k+1)+2\big)$

Jadi, $1.2 + 2.3 + 3.4 + \cdots + k(k+1) + (k+1)\big((k+1)+1\big) = \frac{1}{3}(k+1)\big((k+1)+1\big)\big((k+1)+2\big)$ berarti $n = k+1$ benar. Sehingga $1.2 + 2.3 + 3.4 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$ benar untuk setiap bilangan asli $n$.

2. Bukti :

a. Ditunjukkan bahwa $n = 1$ benar.

$$(2n-1)^2 = \frac{1}{3}n(4n^2-1)$$
$$(2(1)-1)^2 = \frac{1}{3}(1)(4(1)^2-1)$$
$$(2-1)^2 = \frac{1}{3}(4-1)$$
$$(1)^2 = \frac{1}{3}(3)$$
$$1 = 1$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu

$1^2 + 2^2 + 3^2 + \cdots + (2k-1)^2 = \frac{1}{3}k(4k^2 - 1)$

Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

$1^2 + 2^2 + 3^2 + \cdots + (2k-1)^2 + (2(k+1)-1)^2$

$= (1^2 + 2^2 + 3^2 + \cdots + (2k-1)^2) + (2(k+1)-1)^2$

$= \frac{1}{3}k(4k^2 - 1) + (2(k+1)-1)^2$

$= \frac{1}{3}k(4k^2 - 1) + (2k+1)^2$

$= \frac{1}{3}k(2k-1)(2k+1) + (2k+1)^2$

$= (2k+1)\left(\frac{1}{3}k(2k-1) + (2k+1)\right)$

$= (2k+1)\left(\frac{2}{3}k^2 - \frac{1}{3}k + 2k + 1\right)$

$= (2k+1)\left(\frac{2}{3}k^2 + \frac{5}{3}k + 1\right)$

$= \frac{1}{3}(2k+1)(2k^2 + 5k + 3)$

$= \frac{1}{3}(2k+1)(2k+3)(k+1)$

$= \frac{1}{3}(k+1)(4k^2 + 8k + 3)$

$= \frac{1}{3}(k+1)(4(k^2 + 2k + 1) - 1)$

$= \frac{1}{3}(k+1)(4(k+1)^2 - 1)$

Jadi, $1^2 + 2^2 + 3^2 + \cdots + (2k-1)^2 + (2(k+1)-1)^2 = \frac{1}{3}(k+1)(4(k+1)^2 - 1)$ berarti $n = k + 1$ benar. Sehingga $1^2 + 2^2 + 3^2 + \cdots + (2n-1)^2 = \frac{1}{3}n(4n^2 - 1)$ benar untuk setiap bilangan asli $n$.

3. Bukti :

   a. Ditunjukkan bahwa $n = 1$ benar.

$$\frac{1}{1.2} = \frac{n}{n+1}$$

$$\frac{1}{2} = \frac{1}{1+1}$$

$$\frac{1}{2} = \frac{1}{2}$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$

Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)((k+1)+1)}$

$= \left(\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{k(k+1)}\right) + \frac{1}{(k+1)(k+2)}$

$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}$

$= \frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)}$

$= \frac{k(k+2)+1}{(k+1)(k+2)}$

$= \frac{k^2+2k+1}{(k+1)(k+2)}$

$= \frac{(k+1)^2}{(k+1)(k+2)}$

$= \frac{(k+1)}{(k+2)}$

$= \frac{(k+1)}{(k+1)+1}$

Jadi, $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)((k+1)+1)} = \frac{(k+1)}{(k+1)+1}$ berarti $n = k + 1$ benar. Sehingga $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ benar untuk setiap bilangan asli $n$.

4. Bukti :

a. Ditunjukkan bahwa $n = 1$ benar.

$$\sum_{n=1}^{1} cn = c \sum_{n=1}^{1} n$$
$$cn = c(n)$$
$$c1 = c(1)$$
$$1c = 1c$$

b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $\sum_{n=1}^{k} cn = c \sum_{n=1}^{k} n$

Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:

$\sum_{n=1}^{k+1} cn = 1c + 2c + 3c + \cdots + kc + (k+1)c$
$= c\big(1 + 2 + 3 + \cdots + k + (k+1)\big)$
$= c\sum_{n=1}^{k+1} n$
Jadi, $\sum_{n=1}^{k+1} cn = c\sum_{n=1}^{k+1} n$ berarti $n = k + 1$ benar. Sehingga $\sum_{n=1}^{k} cn = c\sum_{n=1}^{k} n$ benar untuk setiap bilangan asli $n$.

5. Bukti :
   a. Ditunjukkan bahwa $n = 1$ benar.

$$\sum_{n=1}^{1}(3n-2) = \frac{1}{2}(3(1)^2 - 1)$$
$$(3-2) = \frac{1}{2}(3-1)$$
$$1 = \frac{1}{2}(2)$$
$$1 = 1$$

   b. Diasumsikan bahwa $n = k$ benar untuk suatu bilangan asli $k$, yaitu $\sum_{n=1}^{k}(3n-2) = \frac{1}{2}(3k^2 - k)$
   Selanjutnya ditunjukkan bahwa $n = k + 1$ benar, yaitu:
   $$\sum_{n=1}^{k+1}(3n-2)$$
   $= \sum_{n=1}^{k}(3n-2) + (3(k+1)-2)$
   $= \frac{1}{2}(3k^2 - k) + (3(k+1)-2)$
   $= \frac{1}{2}(3k^2 - k) + (3k+1)$
   $= \frac{1}{2}(3k^2 - k) + \frac{1}{2}(6k+2)$
   $= \frac{1}{2}(3k^2 - k + 6k + 2)$
   $= \frac{1}{2}\big(3k^2 - k + 7k + 3 - (k+1)\big)$
   $= \frac{1}{2}\big(3k^2 + 6k + 3 + (k+1)\big)$
   $= \frac{1}{2}\big(3(k^2 + 2k + 1) + (k+1)\big)$
   $= \frac{1}{2}\big(3(k+1)^2 + (k+1)\big)$

Jadi, $\sum_{n=1}^{k+1}(3n-2)=\frac{1}{2}\left(3(k+1)^2+(k+1)\right)$ berarti $n=k+1$ benar. Sehingga $\sum_{n=1}^{k}(3n-2)=\frac{1}{2}(3k^2-k)$ benar untuk setiap bilangan asli $n$.

6. Bukti :

a. Ditunjukkan bahwa $n=1$ benar.

$$\frac{1}{1.3}=\frac{1}{2(1)+1}$$
$$\frac{1}{3}=\frac{1}{2+1}$$
$$\frac{1}{3}=\frac{1}{3}$$

b. Diasumsikan bahwa $n=k$ benar untuk suatu bilangan asli $k$, yaitu $\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\cdots+\frac{1}{(2k-1)(2k+1)}=\frac{k}{2k+1}$

Selanjutnya ditunjukkan bahwa $n=k+1$ benar, yaitu:

$$\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\cdots+\frac{1}{(2k-1)(2k+1)}+\frac{1}{(2(k+1)-1)(2(k+1)+1)}$$
$$=\left(\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\cdots+\frac{1}{(2k-1)(2k+1)}\right)+\frac{1}{(2k+1)(2k+3)}$$
$$=\frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)}$$
$$=\frac{k(2k+3)+1}{(2k+1)(2k+3)}$$
$$=\frac{2k^2+3k+1}{(2k+1)(2k+3)}$$
$$=\frac{(2k+1)(k+1)}{(2k+1)(2k+3)}$$
$$=\frac{(k+1)}{(2(k+1)+1)}$$

Jadi,

$$\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\cdots+\frac{1}{(2k-1)(2k+1)}+\frac{1}{(2(k+1)-1)(2(k+1)+1)}=\frac{(k+1)}{(2(k+1)+1)}$$

berarti $n=k+1$ benar. Sehingga $\frac{1}{1.3}+\frac{1}{3.5}+\frac{1}{5.7}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}$ benar untuk setiap bilangan asli $n$.

7. Pembuktian

$$
\begin{aligned}
n\binom{n-1}{k} &= n\frac{(n-1)!}{(n-1-k)!k!} \\
&= \frac{n!}{(n-1-k)!k!} \\
&= \frac{n!(k+1)}{(n-1-k)!(k+1)k!} \\
&= \frac{n!(k+1)}{\big(n-(k+1)\big)!(k+1)!} \\
&= (k+1)\frac{n!}{\big(n-(k+1)\big)!(k+1)!} \\
&= (k+1)\binom{n}{k+1}
\end{aligned}
$$

Terbukti.

8. Pembuktian:

$$\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n} = (1+2)^n$$

Teorema 3

$$= 3^n$$

Terbukti.

**Refleksi :)**

1. Hal menarik apa saja yang kamu pelajari pada bab ini?
2. Pembuktian menggunakan induksi matematika merupakan suatu langkah seperti pada permainan, coba tebak permainan apakah itu?

# BAB II
# KETERBAGIAN DAN FAKTORISASI PRIMA

## I. Tujuan Instruksional

Pada bab ini mahasiswa diharapkan: 1) mampu menyebutkan sifat-sifat keterbagian bilangan bulat; 2) mampu menjelaskan pengertian KPK dan FPB; 3) mampu menjelaskan pengertian bilangan prima; 4) mampu menentukan faktor prima dari suatu bilangan; 5) mampu menentukan apakah suatu bilangan merupakan bilangan prima atau bukan.

## II. Uraian Materi

### A. Keterbagian

**Definisi 2.1**

Jika $a$ dan b adalah bilangan bulat dengan $a \neq 0$, dikatakan $a$ membagi $b$ jika terdapat sebuah bilangan bulat $c$ sehingga $b = ac$. Jika $a$ membagi $b$, dikatakan juga bahwa $a$ adalah pembagi atau faktor dari $b$ dan bahwa $b$ adalah perkalian dari $a$.

Jika $a$ membagi $b$ dilambangkan dengan $a \mid b$ sedangkan jika $a$ tidak membagi $b$ maka dilambangkan dengan $a \nmid b$.

Contoh penyataan yang menggambarkan konsep keterbagian bilangn bulat adalah $13 \mid 182, -5 \mid 30, 17 \mid 289$, $6 \nmid 44$ dan $7 \nmid 50$.

**Teorema 2.1**

Jika $a$, $b$ dan $c$ adalah bilangan bulat dengan $a \mid b$ dan $b \mid c$, maka $a \mid c$.

***Bukti***

Karena $a$ / $b$ dan $b$ / $c$, ada bilangan bulat $e$ dan $f$ sedemikian hingga $ae = b$ dan $bf = c$.

Oleh karena itu

$$c = bf$$
$$= (ae)f$$
$$= a(ef)$$

Dan dapat disimpulkan bahwa $a$ / $c$.

**Contoh:**

Karena 11 | 66 dan 66 | 198, maka 11 | 198

**Teorema 2.2**

Jika $a$, $b$, $m$ dan $n$ adalah bilangan bulat dan jika $c \mid a$ dan $c \mid b$ maka $c \mid (ma + nb)$

***Bukti***

Karena $c$ / $a$ dan $c$ / $b$, ada bilang bulat $e$ dan $f$ sedemikian hingga $a = ce$ dan $b = cf$.

Karena itu,

$$ma + nb = mce + ncf$$
$$= c\,(me + nf)$$

Konsenkuansinya, terlihat bahwa $c$ / $(ma + nb)$.

**Contoh**

Ketika 3 | 21 dan 3 | 33, maka

3 membagi $5 \cdot 21 - 3 \cdot 33 = 105 - 99 = 6$

**Teorema 2.3 Algoritma Pembagian**

Jika $a$ dan $b$ adalah bilangan bulat sehingga $b > 0$ maka terdapat bilangan bulat unik $q$ dan $r$ sehingga $a = bq + r$ dengan $0 \leq r < b$

Dalam Algoritma Pembagian, $q$ disebut hasil bagi (*quotient*) dan $r$ di sebut sisa (*remainder*). Dan juga $a$ disebut bilangan yang dibagi (*devidend*) dan $b$ pembagi (*divisor*).

***Bukti***

Mengingat bahwa himpunan seluruh bilangn bulat S dengan bentuk $a - bk$ dimana $k$ adalah sebuah bilangan bulat, yang mana, $S = \{a - bk \mid k \in \square\}$. Misalkan T adalah himpunan bilangan bulat bukan negatif dalam S. T bukan himpunan kosong, karenan $a - bk$ adalah positif apapun nilai bilangan bulat $k$ dengan $k < \frac{a}{b}$.

Dengan ini, T setidaknya mempunyai sebuah element $r = a - bq$ (terdapat nilai $q$ dan $r$ secera spesifik dalam teorema). Dengan kontradiksi diketahui bahwa $r \geq 0$ dan dengan mudah terlihat bahwa $r < b$. Jika $r \geq b$, kemudian $r > r - b = a - bq = a - b(q + 1) \geq 0$, hal ini kontradiksi dengan pemisalan $r = a - bq$ sebagai bilangan bulat non negatif dengan bentuk $a - bk$. Oleh karena itu, $0 \leq r < b$.

Untuk menunjukkan bahwa nilai $q$ dan $r$ adalah unik, asumsikan bahwa terdapat dua persamaan $a = bq_1 + r_1$ dan $a = bq_2 + r_2$, dengan $0 \leq r_1 < b$ dan $0 \leq r_2 < b$. Dengan pengurangan persamaan pertama dengan persamaan kedua, dapat ditemukan bahwa

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

Oleh karena itu, terlihat bahwa

$$r_1 - r_2 = b(q_1 - q_2)$$

hal ini menyatakan bahwa b membagi $r_1 - r_2$. Karena $0 \leq r_1 < b$ dan $0 \leq r_2 < b$, kita mempunya $-b < r_2 - r_1 < b$. Oleh karena itu, b dapat membagi $r_2 - r_1$ jika dan hanya jika $r_2 - r_1 = 0$ atau, dengan kata lain, jika $r_1 = r_2$. Karena $bq_1 + r_1 = bq_2 + r_2$ dan $r_1 = r_2$, terlihat juga $q_1 = q_2$. Ini menunjukkan bahwa $q$ hasil bagi dan $r$ sisa adalah unik.

**Contoh**

Jika $a = 133$ dan $b = 21$, maka $q = 6$ dan $r = 7$, karena $133 = 21 \cdot 6 + 7$ dan $0 \leq 7 < 21$.

**Latihan**

1. **Tunjukan bahwa 33|99, 5|145, 7|343, dan 888|0.**

Jawaban

$3|99$ karena $99 = 3 \times 33$

$5|145$ karena $145 = 5 \times 29$

$7|343$ karena $343 = 7 \times 49$

$888|0$ karena $0 = 888 \times 0$

2. **Tunjukan bahwa 1001 dapat di bagi oleh 7, 11, 13.**

   Jawaban

   $7|1001$ karena $1001 = 7 \times 143$

   $11|1001$ karena $1001 = 11 \times 91$

   $13|1001$ karena $1001 = 13 \times 77$

3. **Apakah bilangan bulat 0, 444, 1.716, 192.554, -32.516, -195.518 dapat dibagi oleh 22?**

   Jawaban

   a. Ya $22|0$ terbagi habis karena $0 = 22 \times 0$
   b. Tidak $444 = 20 \times 22 + 4$ karena sisanya tidak nol maka $22 \nmid 444$
   c. Ya karena $1716 = 22 \times 78$
   d. Ya karena $192.554 = 22 \times 8752$
   e. Ya karena $-32.516 = 22 \times -1478$
   f. Tidak karena $-195.518 = -8888 \times 22 + 18$ karena sisanya tidak nol maka $22 \nmid -195518$

## B. Bilangan Prima

### Definisi 2.2 Bilangan Prima

Bilangan prima adalah sebuah bilangan bulat yang lebih besar dari 1 yang tidak dapat dibagi oleh bilangan positif selain dari 1 dan bilangan itu sendiri.

**Contoh :**

1. Bilangan bulat 2, 3, 5, 13, 101, 103, 107, dan 113 adalah bilangan prima.
2. Temukan semua bilangan prima dari selisih pangkat empat dari dua bilangan bulat !

   Jawab :

   Misalkan :$n = x^4 - y^4$

   $n = (x + y)(x - y)(x^2 + y^2)$,dimana$x > y$

   Bilangan bulat $n$ tidak dapat menjadi bilangan prima karena dapat dibagi oleh $x + y$ yang bukan merupakan 1 atau $n$.

**Definisi 2.3 Bilangan Komposit**

Sebuah bilangan bulat yang lebih besar dari 1 yang bukan bilangan prima disebut **bilangan komposit** atau **bilangan campuran.**

**Contoh** :

Bilangan bulat 4 = 2.2, 8 = 4.2, 33 = 3.11, 111 = 3.37 adalah bilangan komposit atau bilangan campuran.

Bilangan komposit dapat dinyatakan sebagai faktorisasi bilangan bulat atau hasil perkalian dua bilangan prima atau lebih.

**Lemma 2.1**

Setiap bilangan bulat positif yang lebih besar dari 1 mempunyai suatu pembagi prima.

**Bukti**

Ambil sebarang bilangan bulat positif $n > 1$. Apabila n suatu bilangan prima, maka n|n, berarti teorema terbukti. Apabila $n$ suatu bilangan komposit, maka n mempunyai faktor bulat positif selain 1 dan $n$ sendiri, misalnya $d_1$, yaitu $d_2/n$. Sehingga ada bilangan bulat positif $n_1$ sedemikian sehingga $n = d_1n_1$ dengan $1 < n_1 < n$.

Jika $n_1$ suatu bilangan prima, maka $n_1/n$, sehingga teorema terbukti. Tetapi jika $n_1$ suatu bilangan komposit, maka $n_1$ mempunyai faktor bulat positif selain 1 dan $n_1$, misalnya $d_2/n_1$. Sehingga ada bilangan bulat positif $n_2$ sedemikian hingga $n_1 = d_2n_2$ dengan $1 < n_2 < n$.

Jika $n_2$ suatu bilangan prima, maka $n_2/n_1$. Dan karena $n_1/n$ maka $n_2/n$. Jadi n terbagi bilangan prima $n_2$, berarti teorema terbukti. Tetapi jika $n_2$ suatu bilangan komposit, maka $n_2$ mempunyai faktor bulat positif selain 1 dan $n_2$, misalnya $d_3$, yaitu $d_3/n_2$. Ini berarti ada bilangan positif $n_3$ sedemikian hingga $n_2 = d_3n_3$ dengan $1 < n_3 < n_3$.
Jika $n_3$ suatu bilangan prima, maka $n_3|n_2$. Dan karena $n_2|n_1$ dan $n_1|n$, maka $n_3|n$. Jadi n terbagi bilangan prima $n_3$, berarti teorema terbukti. Tetapi jika $n_3$ suatu bilangan komposit, maka proses seperti di atas dapat dilanjutkan sedemikian hingga diperoleh suatu barisan n, $n_1$, $n_2$, $n_3$, ... dengan $n > n_1 > n_2 > n_3 > ... > 1$.
Penguraian atas faktor-faktor komposit ini tentu berakhir pada suatu faktor prima, karena faktor-faktor tersebut selalu lebih kecil dari bilangan yang difaktorkan dan selalu lebih besar dari 1. Misalkan pemfaktoran tersebut berakhir pada faktor prima $n_k$, maka $n_k|n_{k+1}$, $n_{k+1}|n_{k+2}$, ..., $n_2|n_1$ dan $n_1|n$ , sehingga $n_k|n$.

**Contoh :**
12 bukan bilangan prima.
12 = 6.2, 6 bukan prima, namun 6 mempunyai pembagi prima yaitu 2 dan 3. Karena 2|6, 6|12 maka 2|12 demikian juga dengan 3 yaitu 3|6, 6|12 maka 3|12. Sehingga 12 mempunyai pembagi prima 2 dan 3.

**Teorema 2.4**
Banyaknya bilangan prima adalah tak berhingga.
**Bukti** :
Andaikan ada bilangan prima yang banyaknya terhingga, yaitu $p_1, p_2, ..., p_n$, dimana $n$ adalah bilangan bulat positif. Diberikan bilangan bulat $Q_n$ yang diperoleh dari perkalian semua bilangan prima dan ditambah 1, maka : $Q_n = p_1 p_2 ... p_n + 1$
Berdasarkan **Lemma 2.1** $Q_n$ mempunyai paling sedikit satu pembagi prima, misalkan $q = p_j$ untuk suatu $j$ bilangan bulat dengan $1 \leq j \leq n$, maka $Q_n - p_1 p_2 ... p_n = 1$, dan $q$ membagi kedua ruas.

Pembagian kedua ruas kiri dijelaskan oleh **Teorema 2.2**, itu menunjukkan bahwa $q|1$. Ini tidak mungkin karena, tidak ada bilangan prima yang membagi 1. Kontradiksi ini menunjukkan bahwa banyaknya bilangan prima adalah tak berhingga.

## Menemukan Bilangan Prima

**Teorema 2.5**

Jika $n$ adalah bilangan komposit, maka $n$ mempunyai suatu faktor prima yang tidak lebih dari $\sqrt{n}$.

**Bukti :**

Karena $n$ adalah bilangan komposit, maka dapat ditulis $n = ab$, dimana $a$ dan$b$ adalah bilangan bulat dengan $1 < a \leq b < n$. Diperoleh $a \leq \sqrt{n}$, dengan kata lain $b \geq a > \sqrt{n}$ dan $ab > \sqrt{n}\,.\sqrt{n} = n$. Berdasarkan Lemma 2.1 dan Teorema 2.1, $a$ harus mempunyai suatu pembagi prima dan merupakan suatu pembagi dari $n$. Jadi, jelas bahwa kurang dari atau sama dengan $\sqrt{n}$.

Aplikasi **Teorema 2.2** digunakan untuk menemukan semua bilangan prima yang kurang dari atau sama dengan $n$. Prosedur ini disebut dengan **saringan *Eratosthenes***. Saringan Erasthotenes merupakan prosedur yang salah satunya digunakan untuk mencari bilangan prima kurang dari 100. Seperti pada **Teorema 2.2**, setiap bilangan bulat komposit kurang dari 100 harus mempunyai faktor prima kurang dari $\sqrt{100} = 10$. Karena bilangan prima yang kurang dari 10 hanya 2, 3, 5, dan 7, maka perlu ditunjukkan bahwa setiap bilangan komposit yang kurang dari 100 dapat dibagi oleh bilangan prima tersebut.

Langkah-langkah untuk menemukan bilangan prima dengan prosedur saringan Eratoshenes:

1. Buat daftar dari semua bilangan tersebut, yaitu 1, 2, 3, ... , 100. Daftar tersebut dapat dibuat sedemikian rupa sehingga menghemat tempat, misalkan dibuat dalam bentuk persegi.
2. Coret dengan garis horisontal ( - ) bilangan kelipatan 2, kecuali bilangan 2 itu sendiri yaitu 4, 6, 8, ...

3. Coret dengan *slash* (/) bilangan kelipatan 3, kecuali bilangan 3 itu sendiri.
4. Coret dengan *backslash* ( \ ) bilangan kelipatan 5, kecuali bilangan 5 itu sendiri.
5. Coret dengan garis vertikal ( | ) bilangan kelipatan 7, kecuali bilangan 7 itu sendiri.
6. Bilangan yang tidak dicoret merupakan bilangan prima, kecuali 1 coret dengan x.

Berikut ilustrasi dari saringan Erastothenes :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~1~~ | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ |
| 11 | ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ |
| ~~21~~ | ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ |
| 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ |
| 41 | ~~42~~ | 43 | ~~44~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ | ~~49~~ | ~~50~~ |
| ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |
| 61 | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | 67 | ~~68~~ | ~~69~~ | ~~70~~ |
| 71 | ~~72~~ | 73 | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | 79 | ~~80~~ |
| ~~81~~ | ~~82~~ | 83 | ~~84~~ | ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | 89 | ~~90~~ |
| ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ | 97 | ~~98~~ | ~~99~~ | ~~100~~ |

Prosedur saringan Erastothenes tidak efisien jika digunakan untuk mencari bilangan yang cukup besar.

**Contoh:**

Temukan bilangan prima terkecil dari barisan aritmatika $an+b$, untuk nilai $a$ dan $b$ berikut :

1. $a = 3$ dan $b = 1$
2. $a = 5$ dan $b = 4$
3. $a = 11$ dan $b = 16$

Jawab :

1. $an+b = 3n + 1$

untuk $n = 0$ maka, $3\ (0) + 1 = 1$
untuk $n = 1$ maka, $3\ (1) + 1 = 4$
untuk $n = 2$ maka, $3(2) + 1 = 7$
untuk $n = 3$ maka, $3\ (3) + 1 = 10$
dan seterusnya
Bilangan prima terkecil adalah 7

2. $an+b = 5n + 4$
untuk $n = 0$ maka, $5\ (0) + 4 = 4$
untuk $n = 1$ maka, $5\ (1) + 4 = 9$
untuk $n = 2$ maka, $5(2) + 4 = 14$
untuk $n = 3$ maka, $5\ (3) + 4 = 19$
dan seterusnya
Bilangan prima terkecil adalah 19

3. $an+b = 11n + 16$
untuk $n = 0$ maka, $11\ (0) + 16 = 16$
untuk $n = 1$ maka, $11\ (1) + 16 = 27$
untuk $n = 2$ maka, $11(2) + 16 = 38$
untuk $n = 3$ maka, $11\ (3) + 16 = 49$
untuk $n = 4$ maka, $11\ (4) + 16 = 60$
untuk $n = 5$ maka, $11\ (5) + 16 = 71$
dan seterusnya
Bilangan prima terkecil adalah 71

## C. Faktor Persekutuan Terbesar (FPB)

**Definisi 2.4**

Jika $a$ dan $b$ adalah bilangan-bilangan bulat, maka suatu bilangan bulat $d$ disebut **faktor persekutuan** dari $a$ dan $b$ jika $d/a$ dan $d/b$.

Karena 1 adalah pembagi (factor) dari setiap bilangan bulat, maka 1 adalah factor persekutuan dari dua bilangan bulat *a* dan *b*, sehingga himpunan factor persekutuan dari *a* dan *b* tidak pernah kosong.

**Definisi 2.5**

Jika *a* dan *b* bilangan bulat yang sekurang-kurangnya satu diantaranya tidak sama dengan nol, maka **Faktor Persekutuan Terbesar (FPB)** dari *a* dan *b* diberi symbol *"(a,b)"* adalah suatu bilangan bulat positif, misalnya *d* yang memenuhi:

i. $d/a$ dan $d/b$, serta

ii. Jika $e/a$ dan $e/b$, maka $e \leq d$.

**Teorema 2.6**

Jika $(a,b) = d$, maka $(a:d, b:d) = 1$.

Apabila ***a*** dan ***b*** dua bilangan bulat positif dengan $(a,b)=1$, maka dikatakan bahwa ***a* dan *b* saling prima** atau ***a*** prima relative terhadap ***b***.

**Contoh:**

- (30, 105) = 15
- (30:15, 105:15) = (2, 7) = 1
- Artinya 2 dan 7 saling prima.

**Akibat 2.1 Akibat Algorimat Pembagian**

Jika *a* dan *b* bilangan-bilangan bulat dengan $b \neq 0$, maka ada dengan tunggal pasangan bilangan-bilangan bulat *q* dan *r* sedemikian sehingga $b = qa + r$, dengan $0 \leq r < /a/$

**Bukti**

Untuk membuktikanya kita cukup memperhatikan untuk a yang negative, maka $/a/ > 0$, sehingga dengan Teorema 2.3 menghasilkan pasangan bilangan-bilangan bulat yang tunggal *q* dan *r* yang memenuhi

$$b = aq' + r \text{ dengan } a \leq r < /a/$$

Perhatikan bahwa |a| = a dan mengambil q = q' untuk mendapatkan

$$b = aq + r \text{ dengan } a \leq r < /a/$$

**Teorema 2.7**
Jika $b = aq + r$, maka $(b, a) = (a, r)$
**Bukti**
Misalkan $(b,a) = d$ dan $(a,r) = c$, kita akan menunjukkan bahwa $c = d$.
Karena $(b,a) = d$, maka $d \mid b$ dan $d \mid a$, dan karena $b = aq + r$, maka $d \mid r$.
$d \mid a$ dan $d \mid r$, maka d adalah factor persekutuan dari $a$ dan $r$. akan tetapi karena $(a,r) = c$, maka $d \leq c$.
Karena $(a,r) = c$, maka $c \mid a$ dan $c \mid r$ dan karena $b = aq + r$, maka $c \mid b$.
$c \mid a$ dan $c \mid b$, maka $c$ adalah factor persekutuan dari $a$ dan $b$. tetapi $(b,a) = d$, maka $d \geq c$.
$d \leq c$ dan $d \geq c$, maka c = d, yaitu $(b,a) = (a,r)$.

**Akibat 2.2**
Jika $a$ dan $b$ suatu bilangan bulat, maka
$(a, b) = (a, b-a) = (b, a-b)$

**Contoh**
Tentukn FPB (252, 198).
Dengan memanfaatkan teorema 2.7, maka

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

**Teorema 2.8**
Apabila $a$ dan $b$ bilangan-bilangan bulat tidak nol, maka ada bilangan-bilangan bulat $x$ dan $y$ sedemikian sehingga
$ax + by = (a,b)$

Dengan kata lain FPB dapat dinyatakan sebagai kombinasi linier.
**Contoh**

Nyatakan 18 sebagai kombinasi linier dari 252 dan 198.

Jawab

Tentukan bilangan bulat $m$ dan $n$ yang memenuhi

$252m + 198n = (252, 198)$

Jawab:

$18 = 54 - 36$

$= 54 - (198 - 54.3)$

$= 54.\ 4 - 198$

$= (252 - 198).4 - 198$

$= 252.4 + 198(-5)$

Jadi, $m = 4$ dan $n = -5$

Nilai $m$ dan $n$ tidak tunggal, ada bilangan lain yaitu

$m = 4 - 198t$ dan

$n = -5 + 252t$ untuk setiap bilangan bulat $t$.

## D. Kelipatan Persekutuan Terkecil (KPK)

**Definisi 2.6**

Misalkan $a$ dan $b$ merupakan bilangan bulat. Bilangan bulat $m$ adalah kelipatan persekutuan dari $a$ dan $b$ jika dan hanya jika $a/m$ dan $b/m$.

**Definisi 2.7**

Kelipatan persekutuan terkecil (KPK) dari dua bilangan bulat tidak nol $a$ dan $b$ adalah suatu bilangan bulat positif $m$ ditulis $[a,b] = m$, apabila memenuhi

i. $a/m$ dan $b/m$

ii. Jika $a/c$ dan $b/c$, maka $m \leq c$.

**Contoh**

[6, 8] = 24, maka $6|24$ dan $8|24$

Kelipatan persekutuan yang lain misalnya 48, 72, 96, ...

Masing-masing lebih dari 24.

**Teorema 2.9**

Jika *c* adalah suatu kelipatan persekutuan dari dua bilangan bulat tidak nol *a* dan *b*, maka KPK dari *a* dan *b* membagi *c*, yaitu $[a,b] \mid c$ .

**Bukti**

Misalkan $[a,b] = m$ , maka harus ditunjukkan bahwa $m \mid c$ .

Andaikan $m \nmid c$, maka menurut algoritma pembagian ada bilangan bulat *q* dan *r* sedemikian sehingga

$c = qm + r$ dengan $0 < r < m$

Karena *c* adalah kelipatan persekutuan dari *a* dan *b*, maka $a/c$ dan $b/c$.

Karena $[a,b] = m$ , maka $a \mid m$ dan $b \mid m$

Karena $a \mid m$, maka $a \mid qm$ dan karena $a \mid c$ maka $a \mid (c - qm)$ . Berarti $a \mid r$ .

Demikian pula $b \mid m$, maka $b \mid qm$ dan karena $b \mid c$ , maka $b \mid (c - qm)$ . Berarti $b \mid r$ .

Karena $a \mid r$ dan $b \mid r$ , maka r adalah kelipatan persekutuan dari a dan b.

Tetapi karena $[a,b] = m$ dan $0 < r < m$, maka hal tersebut tidak mungkin (kontrakdiksi). Jadi pengandaian di atas salah, berarti $m \mid c$ atau $[a,b] \mid c$

**Teorema 2.10**

Jika $c > 0$, maka $[ca, cb] = c[a,b]$

**Bukti**

Misalkan $[a,b] = d$ , maka $a \mid d$ dan $b \mid d$ , sehingga $ac \mid dc$ dan $bc \mid dc$ . Hal tersebut berarti dc adalah kelipatan persekutuan dari ac dan bc.

Menurut teorema 2.9, maka $[ac,bc] \mid dc$. Karena $[ac,bc]$ adalah suatu kelipatan dari c.

Misalkan $[ac,bc] = mc$ maka $mc \mid dc$ sehingga $m \mid d$.

Karena $[ac,bc] = mc$ maka $ac \mid mc$ dan $bc \mid mc$, sehingga $a \mid m$ dan $b \mid m$ dan menurut teorema 2.9 maka $[a,b] \mid m$, yaitu $d \mid m$ dan $m \mid d$, maka $m = d$. Sehingga $dc = mc$, yaitu $c[a,b] = [ac,bc]$.

**Teorema 2.11**

Jika *a* dan *b* bilangan-bilangan bulat yang keduanya positif, maka $(a,b)[a,b] = ab$

**Contoh**

Karena $(16,20) = 4$ dan $[16,20] = 80$, terdapat hubungan $(16,20)[16,20] = 4 \times 80 = 320 = 16 \times 20$

## III. Rangkuman

1. Jika *a* dan b adalah bilangan bulat dengan $a \neq 0$, dikatakan *a* membagi *b* jika terdapat sebuah bilangan bulat *c* sehingga $b = ac$. Jika *a* membagi *b*, dikatakan juga bahwa *a* adalah embagi atau faktor dari *b* dan bahwa *b* adalah perkalian dari *a.* Jika *a* membagi *b* dilambangkan dengan $a \mid b$ sedangkan jika *a* tidak membagi *b* maka dilambangkan dengan $a \nmid b$.
2. Jika *a, b* dan *c* adalah bilangan bulat dengan $a \mid b$ dan $b \mid c$, maka $a \mid c$.
3. Jika *a, b, m* dan *n* adalah bilangan bulat dan jika $c \mid a$ dan $c \mid b$ maka $c \mid (ma + nb)$

4. Algoritma Pembagian. Jika $a$ dan $b$ adalah bilangan bulat sehingga $b > 0$ maka terdapat bilangan bulat unik $q$ dan $r$ sehingga $a = bq + r$ dengan $0 \leq r < b$
5. Bilangan prima adalah sebuah bilangan bulat yang lebih besar dari 1 yang tidak dapat dibagi oleh bilangan positif selain dari 1 dan bilangan itu sendiri.
6. Sebuah bilangan bulat yang lebih besar dari 1 yang bukan bilangan prima disebut **bilangan komposit** atau **bilangan campuran.**
7. Setiap bilangan bulat positif yang lebih besar dari 1 mempunyai suatu pembagi prima.
8. Banyaknya bilangan prima adalah tak berhingga.
9. Jika $n$ adalah bilangan komposit, maka $n$ mempunyai suatu faktor prima yang tidak lebih dari $\sqrt{n}$.
10. Jika $a$ dan $b$ adalah bilangan-bilangan bulat, maka suatu bilangan bulat $d$ disebut **faktor persekutuan** dari $a$ dan $b$ jika $d/a$ dan $d/b$.
11. Jika $a$ dan $b$ bilangan bulat yang sekurang-kurangnya satu diantaranya tidak sama dengan nol, maka **Faktor Persekutuan Terbesar (FPB)** dari $a$ dan $b$ diberi symbol *"(a,b)"* adalah suatu bilangan bulat positif, misalnya $d$ yang memenuhi:
    i. $d/a$ dan $d/b$, serta
    ii. Jika $e/a$ dan $e/b$, maka $e \leq d$.
    iii.Jika $(a,b) = d$, maka $(a:d, b:d) = 1$.
12. Apabila ***a*** dan ***b*** dua bilangan bulat positif dengan $(a,b)=1$, maka dikatakan bahwa ***a* dan *b* saling prima** atau ***a*** prima relative terhadap ***b.***
13. **Akibat Algorimat Pembagian**
    Jika $a$ dan $b$ bilangan-bilangan bulat dengan $b \neq 0$, maka ada dengan tunggal pasangan bilangan-bilangan bulat $q$ dan $r$ sedemikian sehingga $b = qa + r$ , dengan $0 \leq r < |a|$
14. Jika $b = aq + r$, maka $(b, a) = (a, r)$
15. Jika $a$ dan $b$ suatu bilangan bulat, maka
    $(a, b) = (a, b-a) = (b, a-b)$

16. Apabila $a$ dan $b$ bilangan-bilangan bulat tidak nol, maka ada bilangan-bilangan bulat $x$ dan $y$ sedemikian sehingga $ax + by = (a,b)$
17. Misalkan $a$ dan $b$ merupakan bilangan bulat. Bilangan bulat $m$ adalah kelipatan persekutuan dari $a$ dan $b$ jika dan hanya jika $a/m$ dan $b/m$.
18. Kelipatan persekutuan terkecil (KPK) dari dua bilangan bulat tidak nol $a$ dan $b$ adalah suatu bilangan bulat positif $m$ ditulis $[a,b] = m$, apabila memenuhi
    i. $a/m$ dan $b/m$
    ii. Jika $a/c$ dan $b/c$, maka $m \leq c$.
19. Jika $c$ adalah suatu kelipatan persekutuan dari dua bilangan bulat tidak nol $a$ dan $b$, maka KPK dari $a$ dan $b$ membagi $c$, yaitu $[a,b] \mid c$.
20. Jika $c > 0$, maka $[ca,cb] = c[a,b]$
21. Jika $a$ dan $b$ bilangan-bilangan bulat yang keduanya positif, maka $(a,b)[a,b] = ab$

## IV. Latihan Soal

1. Buktikan jika a|b, maka (-a)|b.
2. Tentukan hasil dari:
    a. (12,18)
    b. (12, 25)
    c. (11,19)
    d. (-15,25)
    e. (3,0)
    f. (15,-25)
    g. (-15,-25)
    h. (204,276)
    i. (252,198)
3. Nyatakan FPB bilangan bulat berikut sebagai kombinasi linear.
    a. (51,87)
    b. (105, 300)
4. Tentukan FPB dari setiap bilangan bulat dibawah ini:

a. 15, 35, 90

b. 300, 2160, 5040

5. Jika a and b adalah bilangan bulat dengan *(a, b) = 1*, tunjukan bahwa *(a+ b, a - b) = 1* atau 2 .
6. Tunjukan bahwa KPK dari dua bilangan genap adalah bilangan genap.

**Kunci Jawaban:**

1. Bukti:

a|b maka ada bilangan bulat k sedemikian sehingga

b = ka

b = (-1.m)a , (dengan k = -1.m)

b = m (-a)

Maka (-a)|b

2. Diserahkan kepada pembaca
3. Diserahkan kepada pembaca
4. Diserahkan kepada pembaca
5. Misalkan bahwa $d|(a + b)$ dan $d|(a - b)$ maka, $d|((a + b) + (a - b))$ $= 2a$ dan $d|((a + b) - (a - b)) = 2b$. Dari latihan 5, diperoleh $(2a,2b) = 2\ (a,b) = 2$. Karena $d$ adalah pembagi besar dari $2a$ dan $2b$ maka $d/2$. Oleh karena itu, $d = 1$ atau $d = 2$. Selain itu, jika $a$ dan $b$ genap maka, $a + b$ dan $a - b$ adalah ganjil jadi $(a+b, a-b) =$ 1. Jika $a$ dan $b$ adalah ganjil maka $a + b$ dan $a - b$ adalah genap jadi $(a+b, a-b) = 2$.
6. Misalkan $a$ genap dan $b$ ganjil maka, $d = (a,b)$ genap. Ketika $d =$ $2k$, untuk bilangan bulat $k$ dan $d|b$. Ketika $dn = b$ untuk bilangan bulat $n$ dan $2kn = b$, sehingga $2|b$ yang menyatakan bahwa $b$ adalah genap. Ini merupakan kontradiksi dari pemisalan di atas. Jadi $d$ harus ganjil.

## Refleksi :)

1. Apa yang kamu dapatkan dari pembelajaran pada bab ini?

2.Coba cari tahu berapa bilangan prima terbesar yang telah ditemukan sampai saat ini.

# BAB III
# KEKONGRUENAN DAN PERSAMAAN DIOPHANTINE

## I. Tujuan Instruksional

Pada bab ini mahasiswa diharapkan mampu: 1) Mampu menyebutkan definisi “kongruen modulo”; 2) Mampu menyebutkan sifat-sifat dasar kongruensi; 3) Mampu menentukan penyelesaian suatu kongruensi linier; 4) Mampu menyelesaikan masalah dengan persamaan Diophantine

## II. Uraian Materi

## A. Definisi dan Sifat Kekongruenan

Kekongruenan (kongruensi) merupakan cara lain dalam membahas relasi keterbagian. Konsep dan sifat-sifat keterbagian itu dapat dipelajari lebih mendalam lagi dengan menggunakan konsep kekongruenan.

**Definisi 1**

Jika m suatu bilangan bulat positif, maka $a$ kongruen dengan $b$ modulo $m$ (ditulis $a \equiv b(mod\ m)$) bila dan hanya bila $m$ membagi $(a-b)$. Jika $m$ tidak membagi $(a-b)$ maka dikatakan bahwa $a$ tidak kongruen dengan $b$ modulo $m$ (ditulis $a \not\equiv b(mod\ m)$).

Definisi 1 tersebut dapat ditulis: Jika $m > 0$, maka $m|(a-b)$ bila dan hanya bila $a \equiv b(mod\, m)$. Jika $m|(a-b)$, maka ada bilangan bulat $k$ sehingga $(a-b) = mk$. Sehingga $a \equiv b(mod\, m)$ bila dan hanya bila $(a-b) = mk$ untuk suatu bilangan bulat $k$. Tetapi, karena $(a-b) = mk$ sama artinya dengan $a = mk + b$, maka $a \equiv b(mod\, m)$ bila dan hanya bila $a = mk + b$.

**Teorema 1**

$a \equiv b(mod\, m)$ bila dan hanya bila ada bilangan bulat $k$ sehingga $a = mk + b$.

**Bukti:**

1. Jika $a \equiv b(mod\, m)$ maka ada bilangan bulat $k$ sehingga $a = mk + b$.
   Ambil sembarang $a, b, m \in \boldsymbol{Z}$ dan $m > 0$.
   Diketahui $a \equiv b(mod\, m)$
   Akan dibuktikan $a = mk + b$ untuk suatu $k \in \boldsymbol{Z}$
   $a \equiv b(mod\, m)$ menurut algoritma pembagian maka sama artinya dengan $m|(a-b)$.
   $a - b = mk$
   $a = mk + b$ untuk suatu $k \in \boldsymbol{Z}$
2. Jika $a = mk + b$ dan ada bilangan bulat $k$ maka $a \equiv b(mod\, m)$.
   Ambil sembarang $a, b, m \in \boldsymbol{Z}$ dan $m > 0$.
   Diketahui $a = mk + b$ untuk suatu $k \in \boldsymbol{Z}$
   Akan dibuktikan $a \equiv b(mod\, m)$
   $a = mk + b$
   $a - b = mk$ memiliki arti yang sama dengan algoritma $m|(a-b)$.
   $m|(a-b)$ dapat dinyatakan dengan $a \equiv b(mod\, m)$.

Terbukti.

**Teorema 2**

Setiap bilangan buat kongruen modulo $m$ dengan tepat satu di antara $0,1,2,3,\ldots,(m-1)$.

**Definisi 2**

Jika $a \equiv b(mod\ m)$ dengan $0 \leq r < m$, maka $r$ disebut residu terkecil dari $a$ modulo $m$. Untuk kekongruenan modulo $m$ ini, $\{0,1,2,3,\ldots,(m-1)\}$ disebut himpunan residu terkecil modulo $m$.

**Teorema 3**

$a \equiv b(mod\ m)$ bila dan hanya bila $a$ dan $b$ memiliki sisa yang sama jika dibagi $m$.

**Definisi 3**

Himpunan bilangan bulat $\{r_1, r_2, r_3, \ldots, r_m\}$ disebut sistem residu lengkap modulo $m$ bila dan hanya bila setiap elemennya kongruen modulo $m$ dengan satu dan hanya satu dari $0,1,2,3,\ldots,(m-1)$.

Jika $m$, $a$, $b$, dan $c$ adalah bilangan-bilangan bulat dengan $m$ positif, maka

1. $\boldsymbol{a \equiv a(mod\ m)}$**, sifat refleksi**

   Bukti:

   Ambil sembarang $a, m \in \boldsymbol{Z}$ dan $m > 0$.

   Akan dibuktikan $a \equiv a(mod\ m)$ berarti $a = a + km$, untuk suatu $k \in \boldsymbol{Z}$

   $$a = a + km$$
   $$a - a = km$$
   $$0 = km$$
   $$k = \frac{0}{m}$$
   $k = 0$, ada bilangan bulat yang memenuhi

Sehingga $m|(a-b)$ maka terbukti $a \equiv a(mod\ m)$.

2. **Jika $a \equiv b(mod\ m)$ maka $b \equiv a(mod\ m)$, sifat simetris**

   Bukti:

   Ambil sembarang $a, b, m \in \boldsymbol{Z}$ dan $m > 0$.

   Diketahui $a \equiv b(mod\ m)$ berarti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$

   Akan dibuktikan $b \equiv a(mod\ m)$ berarti $b = a + km$, untuk suatu $l \in \boldsymbol{Z}$

   $$a = b + km$$
   $$a - b = km$$
   $$-b = -a + km$$
   $$b = a - km$$
   $$b = a + (-k)m, \text{ misalkan } (-k) = l$$
   $$b = a + lm$$
   $$b \equiv a(mod\ m)$$

   Terbukti.

3. **Jika $a \equiv b(mod\ m)$ dan $b \equiv c(mod\ m)$ maka $a \equiv c(mod\ m)$, sifat transitif**

   Bukti:

   Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.

   Diketahui:

   $a \equiv b(mod\ m)$ berarti $a = b + km$ ... pers 1, untuk suatu $k \in \boldsymbol{Z}$

   $b \equiv c(mod\ m)$ berarti $b = c + lm$ ... pers 2, untuk suatu $l \in \boldsymbol{Z}$

   Akan dibuktikan $a \equiv c(mod\ m)$ berarti $a = c + nm$, untuk suatu $n \in \boldsymbol{Z}$

   Substitusi pers 2 ke pers 1

   $$a = b + km$$
   $$a = (c + lm) + km$$
   $$a = c + (lm + km)$$

$a = c + (l + k)m$, misalkan $l + k = n$

$a = c + nm$

$a \equiv c(mod\ m)$

Terbukti.

Karena relasi "≡" (kekongruenan) pada himpunan bilangan bulat memenuhi tiga sifat tersebut, maka relasi kekongruenan pada himpunan semua bilangan bulat merupakan relasi ekuivalen. Akibatnya himpunan bilangan bulat terpartisi dalam himpunan-himpunan bagian yang setiap himpunan bagian disebut kelas.

$$[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$$

Misalnya kita memperhatikan himpunan bilangan bulat dengan relasi kekongruenan modulo 5, maka dengan relasi ini himpunan bilangan bulat terpartisi (terbagi-bagi menjadi himpunan bagian-himpunan bagian yang saling asing dan gabungannya sama dengan himpunan bilangan bulat) menjadi 5 kelas yaitu:

1. $[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$
   $[0]_5 = \{b \in \boldsymbol{Z} | (b, 0) \in \equiv (mod\ 5), 0 \in \boldsymbol{Z}\}$
   $[0]_5 = \{b \in \boldsymbol{Z} | b - 0 = 5k, k \in \boldsymbol{Z}\}$
   $[0]_5 = \{b \in \boldsymbol{Z} | b = 5k, k \in \boldsymbol{Z}\}$
   $[0]_5 = \{\dots, -10, -5, 0, 5, 10, \dots\}$
   $[0]_5 = [-10]_5 = [-5]_5 = [5]_5 = [10]_5 = \cdots$
2. $[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$
   $[1]_5 = \{b \in \boldsymbol{Z} | (b, 1) \in \equiv (mod\ 5), 1 \in \boldsymbol{Z}\}$
   $[1]_5 = \{b \in \boldsymbol{Z} | b - 1 = 5k, k \in \boldsymbol{Z}\}$
   $[1]_5 = \{b \in \boldsymbol{Z} | b = 5k + 1, k \in \boldsymbol{Z}\}$
   $[1]_5 = \{\dots, -9, -4, 1, 6, 11, \dots\}$
   $[1]_5 = [-9]_5 = [-4]_5 = [6]_5 = [11]_5 = \cdots$
3. $[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$
   $[2]_5 = \{b \in \boldsymbol{Z} | (b, 2) \in \equiv (mod\ 5), 2 \in \boldsymbol{Z}\}$
   $[2]_5 = \{b \in \boldsymbol{Z} | b - 2 = 5k, k \in \boldsymbol{Z}\}$

$[2]_5 = \{b \in \boldsymbol{Z} | b = 5k + 2, k \in \boldsymbol{Z}\}$

$[2]_5 = \{\dots, -8, -3, 2, 7, 12, \dots\}$

$[2]_5 = [-8]_5 = [-3]_5 = [7]_5 = [12]_5 = \cdots$

4. $[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$

   $[3]_5 = \{b \in \boldsymbol{Z} | (b, 3) \in \equiv (mod\ 5), 3 \in \boldsymbol{Z}\}$

   $[3]_5 = \{b \in \boldsymbol{Z} | b - 3 = 5k, k \in \boldsymbol{Z}\}$

   $[3]_5 = \{b \in \boldsymbol{Z} | b = 5k + 3, k \in \boldsymbol{Z}\}$

   $[3]_5 = \{\dots, -7, -2, 3, 8, 13, \dots\}$

   $[3]_5 = [-7]_5 = [-2]_5 = [8]_5 = [13]_5 = \cdots$

5. $[a]_m = \{b \in \boldsymbol{Z} | (b, a) \in \equiv (mod\ m), a \in \boldsymbol{Z}\}$

   $[4]_5 = \{b \in \boldsymbol{Z} | (b, 4) \in \equiv (mod\ 5), 4 \in \boldsymbol{Z}\}$

   $[4]_5 = \{b \in \boldsymbol{Z} | b - 4 = 5k, k \in \boldsymbol{Z}\}$

   $[4]_5 = \{b \in \boldsymbol{Z} | b = 5k + 4, k \in \boldsymbol{Z}\}$

   $[4]_5 = \{\dots, -6, -1, 4, 9, 14, \dots\}$

   $[4]_5 = [-6]_5 = [-1]_5 = [9]_5 = [14]_5 = \cdots$

Relasi kekongruenan mempunyai kemiripan sifat dengan sifat persamaan, sebab relasi kekongruenan dapat dinyatakan sebagai persamaan, yaitu $a \equiv b(mod\ m)$ sama artinya dengan $a = b + km$, untuk suatu bilangan bulat $k$.

**Jika $\boldsymbol{a \equiv b(mod\ m)}$ dan $\boldsymbol{c \in Z}$ maka:**

1. $\boldsymbol{(a + c) \equiv (b + c)\ (mod\ m)}$
2. $\boldsymbol{(a - c) \equiv (b - c)\ (mod\ m)}$
3. $\boldsymbol{ac \equiv bc\ (mod\ m)}$
4. $\boldsymbol{a^2 \equiv b^2 (mod\ m)}$

Berikut adalah pembuktiannya:

1. Jika $a \equiv b(mod\ m)$, maka $(a + c) \equiv (b + c)\ (mod\ m)$ untuk setiap bilangan bulat $c$.

   Bukti:

   Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.

Diketahui $a \equiv b(mod\ m)$ berarti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$

Akan dibuktikan $(a + c) \equiv (b + c)\ (mod\ m)$

$a = b + km$

$a + c = b + km + c$, kedua ruas ditambah $c$

$a + c = b + c + km$

$a + c = (b + c) + km$

$a + c \equiv (b + c)\ (mod\ m)$

Terbukti.

2. Jika $a \equiv b(mod\ m)$, maka $(a - c) \equiv (b - c)\ (mod\ m)$ untuk setiap bilangan bulat $c$.

   Bukti:

   Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.

   Dikrtahui $a \equiv b(mod\ m)$ berarti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$

   Akan dibuktikan $(a - c) \equiv (b - c)\ (mod\ m)$

   $a = b + km$

   $a - c = b + km - c$, kedua ruas dikurangi $c$

   $a - c = b - c + km$

   $a - c = (b - c) + km$

   $a - c \equiv (b - c)\ (mod\ m)$

   Terbukti.

3. Jika $a \equiv b(mod\ m)$, maka $ac \equiv bc\ (mod\ m)$ untuk setiap bilangan bulat $c$.

   Bukti:

   Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.

   Diketahui $a \equiv b(mod\ m)$ berarti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$

   Akan dibuktikan $ac \equiv bc\ (mod\ m)$

   $a = b + km$

   $ac = (b + km)c$, kedua ruas dikalikan $c$

   $ac = bc + kmc$

$ac = bc + kcm$
$ac = bc + (kc)m$
$ac \equiv (bc)\ (mod\ m)$
Terbukti.

4. Jika $a \equiv b(mod\ m)$, maka $a^2 \equiv b^2(mod\ m)$.
Bukti:
Ambil sembarang $a, b, m \in \boldsymbol{Z}$ dan $m > 0$.
Diketahui $a \equiv b(mod\ m)$ berarti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$
Akan dibuktikan $a^2 \equiv b^2(mod\ m)$
$a = b + km$
$a^2 = (b + km)^2$, kedua ruas dikuadratkan
$a^2 = b^2 + 2bkm + (km)^2$
$a^2 = b^2 + (2bk + k^2m)m$
$a^2 \equiv b^2(mod\ m)$
Terbukti.

**Teorema 4**
Jika $a \equiv b(mod\ m)$, maka $a^n \equiv b^n(mod\ m)$
**Bukti:**
Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.
$a \equiv b(mod\ m)$ bearti $a = b + km$, untuk suatu $k \in \boldsymbol{Z}$
Akan dibuktikan $a^n \equiv b^n(mod\ m)$
$a = b + km$
$a^n = (b + km)^n$
$a^n = \binom{n}{0} b^n + \binom{n}{1} b^{n-1}(km) + \cdots + \binom{n}{n-1} b(km)^{n-1} + \binom{n}{n}(km)^n$
$a^n = \binom{n}{0} b^n + \left[\binom{n}{1} b^{n-1}k + \cdots + \binom{n}{n-1} bk^{n-1}m^{n-2} + \binom{n}{n} k^n m^{n-1}\right] m$

kombinasi akan selalu menghasilkan suatu nilai bilangan bulat sehingga $\binom{n}{1} b^{n-1}k + \cdots + \binom{n}{n-1} bk^{n-1}m^{n-2} + \binom{n}{n} k^n m^{n-1}$ akan menghasilkan bilangan bulat.

$a^n = 1b^n + \left[\binom{n}{1} b^{n-1}k + \cdots + \binom{n}{n-1} bk^{n-1}m^{n-2} + \binom{n}{n} k^n m^{n-1}\right] m$

$a^n = b^n + \left[\binom{n}{1} b^{n-1}k + \cdots + \binom{n}{n-1} bk^{n-1}m^{n-2} + \binom{n}{n} k^n m^{n-1}\right] m$

$a^n \equiv b^n (mod\ m)$

Terbukti.

**Teorema 5**

Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka

1. $a + c \equiv b + d\ (mod\ m)$
2. $a - c \equiv b - d\ (mod\ m)$
3. $ac \equiv bd\ (mod\ m)$

**Berikut adalah pembuktiannya:**

1. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka $a + c \equiv b + d\ (mod\ m)$

   Bukti:

   Ambil sembarang $a, b, c, d, m \in \boldsymbol{Z}$ dan $m > 0$.

   Diketahui

   $a \equiv b(mod\ m)$ berarti $a = b + km$ ... pers 1, untuk suatu $k \in \boldsymbol{Z}$

   $c \equiv d(mod\ m)$ berarti $c = d + lm$ ... pers 2, untuk suatu $l \in \boldsymbol{Z}$

   Akan dibuktikan $a + c \equiv b + d\ (mod\ m)$

   Eliminasi pers 1 dan 2

   $a = b + km$

   $c = d + lm \quad +$

$a + c = (b + km) + (d + lm)$
$a + c = b + km + d + lm$
$a + c = b + d + km + lm$
$a + c = b + d + (k + l)m$
$a + c \equiv b + d \ (mod\ m)$
Terbukti.

2. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka $a - c \equiv b - d \ (mod\ m)$
   Bukti:
   Ambil sembarang $a, b, c, d, m \in \boldsymbol{Z}$ dan $m > 0$.
   Diketahui
   $a \equiv b(mod\ m)$ berarti $a = b + km$ ... pers 1, untuk suatu $k \in \boldsymbol{Z}$
   $c \equiv d(mod\ m)$ berarti $c = d + lm$ ... pers 2, untuk suatu $l \in \boldsymbol{Z}$
   Akan dibuktikan $a - c \equiv b - d \ (mod\ m)$
   Eliminasi pers 1 dan 2
   $a = b + km$
   $c = d + lm \quad -$
   $a - c = (b + km) - (d + lm)$
   $a - c = b + km - d - lm$
   $a - c = b - d + km - lm$
   $a - c = b - d + (k - l)m$
   $a - c \equiv b - d \ (mod\ m)$
   Terbukti.
3. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka $ac \equiv bd \ (mod\ m)$
   Bukti:
   Ambil sembarang $a, b, c, d, m \in \boldsymbol{Z}$ dan $m > 0$.
   Diketahui
   $a \equiv b(mod\ m)$ berarti $a = b + km$ ... pers 1, untuk suatu $k \in \boldsymbol{Z}$

$c \equiv d(mod\ m)$ berarti $c = d + lm$ ... pers 2, untuk suatu $l \in \boldsymbol{Z}$

Akan dibuktikan $ac \equiv bd\ (mod\ m)$

Persamaan 1 dikali dengan persamaan 2

$ac = (b + km)(d + lm)$

$ac = bd + blm + dkm + klm^2$

$ac = bd + (bl + dk + klm)m$

$ac \equiv bd\ (mod\ m)$

Terbukti.

**Teorema 6**

Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka $ax + cy \equiv bx + dy\ (mod\ m)$ untuk setiap bilangan bulat $x$ dan $y$.

**Bukti:**

Ambil sembarang $a, b, c, d, m, x, y \in \boldsymbol{Z}$ dan $m > 0$.

Diketahui

$a \equiv b(mod\ m)$ berarti $a = b + km$ ... pers 1, untuk suatu $k \in \boldsymbol{Z}$

$c \equiv d(mod\ m)$ berarti $c = d + lm$ ... pers 2, untuk suatu $l \in \boldsymbol{Z}$

Akan dibuktikan $ax + cy \equiv bx + dy\ (mod\ m)$

Kalikan kedia ruas dengan $x$ pada pers 1

$ax = bx + kxm$ ... pers 3

Kalikan kedia ruas dengan $y$ pada pers 2

$cy = dy + lym$ ... pers 4

Eliminasi pers 3 dan 4

$ax = bx + kxm$

$\underline{cy = dy + lym}\quad +$

$ax + cy = (bx + kxm) + (dy + lym)$

$ax + cy = bx + kxm + dy + lym$

$ax + cy = bx + dy + kxm + lym$

$ax + cy = bx + dy + (kx + ly)m$

$ax + cy \equiv bx + dy (mod\ m)$
Terbukti.

**Teorema 7**
Jika $ac \equiv bc(mod\ m)$ dengan $(c, m) = 1$, maka $a \equiv b(mod\ m)$
**Bukti:**
Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.
Diketahui
$ac \equiv bc(mod\ m)$ berarti $ac = bc + km$ untuk suatu $k \in \boldsymbol{Z}$
$(c, m) = 1$ berarti FPB dari $m$ dan $c$ adalah 1
Akan dibuktikan $a \equiv b(mod\ m)$

$$ac = bc + km$$
$$ac - bc = km$$

$(a - b)c = km$, dalam keterbagian dapat ditulis dengan $m|(a - b)c$.
Berdasarkan **Teorema (Lemma Euclid)** jika $a|bc$ dan $(a, b) = 1$, maka $a|c$. Sehingga karena $m|(a - b)c$ dan $(c, m) = 1$ maka $m|(a - b)$.
$m|(a - b)$ sama arti dengan
$a - b = lm$, untuk suatu $l \in \boldsymbol{Z}$

$$a = b + lm$$
$$a \equiv b(mod\ m)$$

Terbukti.

**Teorema 8**
Jika $ac \equiv bc(mod\ m)$ dengan $(c, m) = d$, maka $a \equiv b\left(mod\ \frac{m}{d}\right)$
**Bukti:**
Ambil sembarang $a, b, c, m \in \boldsymbol{Z}$ dan $m > 0$.
Diketahui
$ac \equiv bc(mod\ m)$ berarti $ac = bc + km$ untuk suatu $k \in \boldsymbol{Z}$

$(c, m) = d$ berarti FPB dari $m$ dan $c$ adalah $d$

Akan dibuktikan $a \equiv b \left(mod\ \frac{m}{d}\right)$

$$ac = bc + km$$
$$ac - bc = km$$
$$(a - b)c = km$$
$$\frac{(a-b)c}{d} = \frac{km}{d}$$
$$(a - b)\frac{c}{d} = k\frac{m}{d}$$
$$\frac{m}{d} | (a - b)\frac{c}{d}$$

Karena $d$ adalah FPB dari $m$ dan $c$ maka $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$.

Karena $\frac{m}{d} | (a - b)\frac{c}{d}$ dan $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ maka $\frac{m}{d} | (a - b)$ berdasarkan **Teorema (Lemma Euclid)**.

$\frac{m}{d} | (a - b)$ artinya $a - b = l\frac{m}{d}$ untuk suatu $l \in \boldsymbol{Z}$

$$a - b = l\frac{m}{d}$$
$$a = b + l\frac{m}{d}$$
$$a \equiv b \left(mod\ \frac{m}{d}\right)$$

Terbukti.

## Latihan

1. Tentukan bilangan-bilangan bulat positif $m$, agar kekongruenan berikut ini benar!
   a. $27 \equiv 5(mod\ m)$
   b. $1000 \equiv 1(mod\ m)$
   c. $1331 \equiv 0(mod\ m)$
2. Tunjukkanlah bahwa jika $a$ suatu bilangan bulat yang genap, maka $a^2 \equiv 0(mod\ 4)$, dan jika $a$ suatu bilangan bulat yang ganjil, maka $a^2 \equiv 1(mod\ 4)$.
3. Tentukanlah sisanya apabila $2^{55}$ dibagi dengan 7.

## Kunci Jawaban

1a. Jawab:

$27 \equiv 5(mod\ m)$ berarti $27 = 5 + mk$ untuk suatu $k \in \boldsymbol{Z}$

$27 - 5 = mk$

$22 = mk$

1) $22 \times 1 = 22$
2) $11 \times 2 = 22$

22, 11, 2, 1 adalah bilangan yang habis membagi 22, karena $27 \equiv 5(mod\ m)$ memiliki residu terkecil 5 maka pilih bilangan bulat yang lebih dari 5 dan habis membagi 22 yaitu 22 dan 11, sehingga diperoleh $27 \equiv 5(mod\ 22)$ dan $27 \equiv 5(mod\ 11)$.

1b. Jawab:

$1000 \equiv 1(mod\ m)$ berarti $1000 = 1 + mk$ untuk suatu $k \in \boldsymbol{Z}$

$1000 - 1 = mk$

$999 = mk$

1) $999 \times 1 = 999$
2) $333 \times 3 = 999$
3) $111 \times 9 = 999$
4) $37 \times 27 = 999$

999, 333, 111, 37, 27, 9, 3, 1 adalah bilangan yang habis membagi 999, karena $1000 \equiv 1(mod\ m)$ memiliki residu terkecil 1 maka pilih $m$ bilangan bulat yang lebih dari 1 dan habis membagi 999 yaitu 999, 333, 111, 37, 27, 9, dan 3.

1c. Jawab:

$1331 \equiv 0(mod\ m)$ berarti $1331 = 0 + mk$ untuk suatu $k \in \boldsymbol{Z}$

$1331 = mk$

1) $1331 \times 1 = 1331$
2) $121 \times 11 = 1331$

1331, 121, 11, 1 adalah bilangan yang habis membagi 1331, karena $1331 \equiv 0(mod\ m)$ memiliki residu terkecil 0 maka pilih $m$ bilangan bulat yang lebih dari 0 dan habis membagi 1331 yaitu 1331, 121, 11 dan 1.

2. Jawab:
   a. Jika $a$ suatu bilangan bulat yang genap, maka $a^2 \equiv 0(mod\ 4)$

$$a = 2b, \text{ untuk } b \in \boldsymbol{Z}$$
$$a^2 = (2b)^2$$
$$a^2 = 4b^2$$
$$a^2 = 0 + b^2(4)$$
$$a^2 \equiv 0(mod\ 4)$$

   b. Jika $a$ suatu bilangan bulat yang ganjil, maka $a^2 \equiv 1(mod\ 4)$

$$a = 2c + 1, \text{ untuk } c \in \boldsymbol{Z}$$
$$a^2 = (2c+1)^2$$
$$a^2 = 4c^2 + 4c + 1$$
$$a^2 = 1 + (c^2 + c)(4)$$
$$a^2 \equiv 1(mod\ 4)$$

   Terbukti.

3. Jawab:

$$2^2 \equiv \quad \equiv 4(mod\ 7)$$
$$2^4 \equiv 4^2 \equiv 2(mod\ 7)$$
$$2^8 \equiv 2^2 \equiv 4(mod\ 7)$$
$$2^{16} \equiv 4^2 \equiv 2(mod\ 7)$$
$$2^{32} \equiv 2^2 \equiv 4(mod\ 7)$$
$$2^{55} = 2^{32+16+4+2+1}$$
$$= 2^{32} \times 2^{16} \times 2^4 \times 2^2 \times 2$$
$$\equiv 4 \times 2 \times 2 \times 4 \times 2(mod\ 7)$$
$$\equiv 16 \times 8(mod\ 7)$$
$$\equiv 2 \times 1(mod\ 7)$$
$$\equiv 2(mod\ 7)$$

## B. Pengkongruenan Linear

$ax \equiv b(mod\ m)$ dengan $a,\ b,\ \ m \in \boldsymbol{Z}$ dan $m > 0$ berarti $ax = b + km$ untuk suatu $y \in \boldsymbol{Z}.$

$ax = b + km$

$x = \frac{b+km}{a}$, $x \in \boldsymbol{Z}$ merupakan penyelesaian dari persamaan kekongruenan linear $ax = b + km.$

Apabila $x$ dihubungkan dengan persamaan linear diophantus $ax + by = c$ dan gcd $(a,b)|c$ maka $x = x_o + \frac{b}{(a,b)}t$, untuk setiap $t \in \boldsymbol{Z}$ dan $y = y_o + \frac{a}{(a,b)}t$, untuk setiap $t \in \boldsymbol{Z}$.

**Teorema 9**

Persamaan linear kongruen $ax \equiv b(mod\ m)$ dapat diselesaikan jika dan hanya jika $d|b$ dimana $d = (a,m)$. Jika $d|b$ maka memiliki $d$ solusi.

**Bukti**

Ambil sembarang $a, b, c,\ m \in \boldsymbol{Z}$ dan $m > 0$

Diketahui

$ax \equiv b(mod\ m)$ berarti $ax = b + ym$ untuk suatu $y \in \boldsymbol{Z}$

$(a,m) = d$ berarti FPB dari $m$ dan $a$ adalah $d$

Akan dibuktikan persamaan linear kongruen $ax \equiv b(mod\ m)$ dapat diselesaikan jika dan hanya jika $d|b$ $ax \equiv b(mod\ m)$ dan memiliki $d$ solusi.

Jika $ax \equiv b(mod\ m)$ dapat dipecahkan maka $d|b$. Misalkan $x = \propto$ dan $y = \beta$ adalah solusi untuk $ax \equiv b(mod\ m)$ sehingga

$ax = b + ym$

$a \propto = b + \beta m$

$a \propto - \beta m = b$

Karena $d = (a,m)$ maka $d|a$, $d|m$ dan $d|a \propto - \beta m.$

Karena $a \propto - \beta m = b$ dan $d|a \propto - \beta m$ maka $d|b.$

Karena $d|b$ maka $ax = b + ym$ memiliki solusi atau dapat dipecahkan.

$d|b$ artinya $b = ld$ untuk suatu $l \in \boldsymbol{Z}$

$d = (a, m)$ maka ada bilangan $r$ dan $s \in \boldsymbol{Z}$ yang memenuhi

$d = ra + sm$

$de = rea + mes$

$de = rea - m(-es)$

$b = rea - m(-es)$

Oleh karena itu $x_0 = er$ dan $y_0 = -es$ adalah solusi dari persamaan $a \propto -\beta m = b.$ Sehingga terbukti persamaan linear kongruen $ax \equiv b(mod\ m)$ dapat diselesaikan jika dan hanya jika $d|b$ dimana $d = (a, m)$.

Selanjutnya kita akan memperlihatkan jika $d|b$ maka memiliki $d$ solusi.

Misalkan $x_1 = x_0 + \frac{m}{d}t_1$ dan $x_2 = x_0 + \frac{m}{d}t_2$ adalah solusi $ax - my = b.$

$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2\ (mod\ m)$

$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2\ (mod\ m)$

$t_1 \equiv t_2\ (mod\ m)$

$t_1 \equiv t_2\ (mod\ d)$ sebab $\frac{m}{d}|m$

Berdasarkan teorema 2 (Setiap bilangan buat kongruen modulo $m$ dengan tepat satu di antara $0,1,2,3, \dots, (m-1)$) $x_1 = x_0 + \frac{m}{d}t_1$ dimana $0 \leq t < d$ maka persamaan ini memiliki $d$ solusi.

Terbukti.

**Teorema 10**

Jika $(a, m) = 1$ maka perkongruenan linear $ax \equiv b(mod\ m)$ memiliki tepat 1 solusi.

**Bukti**

Ambil sembarang $a, b, c,\ m \in \boldsymbol{Z}$ dan $m > 0$
Diketahui
$ax \equiv b(mod\ m)$ berarti $ax = b + ym$ untuk suatu $y \in \boldsymbol{Z}$
$(a, m) = 1$ berarti FPB dari $m$ dan $a$ adalah 1
Akan dibuktikan persamaan linear kongruen $ax \equiv b(mod\ m)$ memiliki tepat satu solusi.
$(a, m) = 1$ artinya ada bilangan bulat $r$ dan $s$ sehingga

$$ar + ms = 1 \text{ untuk suatu } r, s \in \boldsymbol{Z}$$
$$arb + msb = b$$
$$arb - m(-sb) = b$$
$$arb = b + m(-sb)$$
$$arb \equiv b(mod\ m)$$

$ax \equiv b(mod\ m)$ dengan $x = rb$ maka $rb$ merupakan solusi
Andaikan solusi persamaan berikut tidak tunggal, misalkan $u$ dan $v \in \boldsymbol{Z}$ masing-masing solusinya maka.
$au \equiv b(mod\ m)$ berarti $au = b + km$ atau $au - mk = b$ untuk suatu $k \in \boldsymbol{Z}$
dan $av \equiv b(mod\ m)$ berarti $av = b + lm$ atau $av - ml = b$ untuk suatu $l \in \boldsymbol{Z}$.
Sehingga diperoleh
$au - mk = au - ml$
$au - av = mk - ml$
$a(u - v) = (k - l)m$ berarti $m|a(u - v)$
Karena $(a, m) = 1$ sehingga $m|a(u - v)$ menjadi $m|(u - v)$ berdasarkan **Teorema (Lemma Euclid)**.
Karena $u$ dan $v$ adalah solusi dari pengkongruenan itu maka $u$ dan $v$ masing-masing residu terkecil modulo $m$.
$0 \leq u < m$ dan $0 \leq v < m$
$0 \leq v < m$ dikali dengan $-1$ diperoleh $0 \geq -v > -m$ atau $-m < -v \leq 0$
$0 \leq u < m$

$$\begin{array}{r} -m < -v \leq 0 \quad + \\ \hline -m < u - v < m \end{array}$$

Tetapi karena $m|(u-v)$ maka $u-v=0$ (0 dipilih karena hanya 0 diantara $-m$ dan $m$ yang habis dibagi $m$) atau $u=v$. Ini berarti bahwa solusi dari pengkongruenan linear tersebut tunggal.

Terbukti.

## Latihan

1. Carilah penyelesaian dari $49x \equiv 94(mod\ 36)$.
   $49x \equiv 94(mod\ 36)$ artinya $49x - 36y = 94$, untuk suatu $y \in \boldsymbol{Z}$
2. Tentukan invers kongruensi berikut:
   a. $3(mod\ 5)$
   b. $12(mod\ 31)$
   c. $10(mod\ 12)$
   d. $4(mod\ 7)$

## Kunci Jawaban

1. $\gcd(49,36) = 1$ dan $1|94$ atau $(49,36)|94$ ini berarti persamaan $49x \equiv 94(mod\ 36)$ memiliki tepat satu solusi.

$$49 = 36 \times 1 + 13$$
$$36 = 13 \times 2 + 10$$
$$13 = 10 \times 1 + 3$$
$$10 = 3 \times 3 + 1$$
$$3 = 3 \times 1, 1 \text{ adalah } \gcd(49,36)$$
$$1 = 10 - 3 \times 3$$
$$1 = 10 - 3(13 - 10)$$
$$1 = 10(4) - 3(13)$$
$$1 = (36 - 13 \times 2)(4) - 3(13)$$

$$1 = (36)4 - 11(13)$$
$$1 = (36)4 - 11(49 - 36)$$
$$1 = (36)15 - 11(49)$$
$$1 = 49(-11) - 36(-15)$$
$$94 = 49(-1034) - 36(-1410)$$

Sehingga solusi dari $49x \equiv 94(mod\ 36)$ adalah $x = -1034$.

2a. Jawab:

$3(mod\ 5) \Leftrightarrow 3x \equiv 1(mod\ 5)$ dan gcd $(3,5) = 1$

$3x \equiv 1(mod\ 5)$ berarti $3x - 1 = 5k$ untuk suatu $k \in \boldsymbol{Z}$

$5 = 3.1 + 2$

$3 = 2.1 + 1$

$2 = 1.2$, 1 adalah gcd$(3,5)$

$1 = 3 - 2$

$1 = 3 - (5 - 3)$

$1 = 3.2 - 5$

$x_o = 2$

Invers dari $3(mod\ 5)$ adalah $2(mod\ 5)$.

2b. Jawab:

$12(mod\ 31) \Leftrightarrow 12x \equiv 1(mod\ 31)$ dan gcd $(12,31) = 1$

$12x \equiv 1(mod\ 31)$ berarti $12x - 1 = 31k$ untuk suatu $k \in \boldsymbol{Z}$

$31 = 12.2 + 7$

$12 = 7.1 + 5$

$7 = 5.1 + 2$

$5 = 2.2 + 1$

$2 = 1.2$, 1 adalah gcd$(12,31)$

$1 = 5 - 2.2$

$1 = 5 - 2(7 - 5)$

$1 = 5.3 - 2.7$

$1 = (12 - 7)3 - 2.7$

$1 = 12.3 - 7.5$

$1 = 12.3 - (31 - 12.2)5$

$1 = 12.13 - 31.5$

$x_o = 13$

Invers dari $12(mod\ 31)$ adalah $13(mod\ 31)$.

2c. Jawab:

$12(mod\ 31) \Leftrightarrow 12x \equiv 1(mod\ 31)$ dan gcd $(10,12) = 2$ karena gcd $(10,12) \neq 2$ maka $12(mod\ 31)$ tidak memiliki invers.

2d. Jawab:

$4(mod\ 7) \Leftrightarrow 4x \equiv 1(mod\ 7)$ dan gcd $(4,7) = 1$

$4x \equiv 1(mod\ 7)$ berarti $4x - 1 = 7k$ untuk suatu $k \in \boldsymbol{Z}$

$7 = 4.1 + 3$

$4 = 3.1 + 1$

$3 = 1.3$, 1 adalah gcd$(4,7)$

$1 = 4 - 3$

$1 = 4 - (7 - 4)$

$1 = 4.2 - 7$

$x_o = 2$

Invers dari $4(mod\ 7)$ adalah $2(mod\ 7)$.

## C. Teorema Sisa Cina

Hal ini yang berhubungan dengan perkongruenan linear, salah satu diantaranya adalah sistem perkongruenan linear. Masalah yang penyelesainnya menggunakan sistem perkongruenan ini telah muncul dalam suatu tulisan bangsa Cina kuno sebagai berikut.

**Contoh:**

1. Temukan kelipatan positif paling sedikit 7 yang meninggalkan sisa 2 ketika dibagi dengan 5, sisa 3 ketika dibagi 6 dan sisa 5 ketika dibagi 11.

   Jawab:

   $x \equiv 2(mod\ 5)$

   $x \equiv 3(mod\ 6)$

   $x \equiv 5(mod\ 11)$

Terlebih dahulu kita akan mencari gcd dari antar modulo perkongruenan tersebut.

gcd$(5,6) = 1$

gcd$(6,11) = 1$

gcd$(5,11) = 1$

karena diperoleh semua gcd bernilai 1 maka sistem kekongruenan memiliki solusi.

$M = m_1 m_2 m_3 = 5.6.11 = 330$

$M_1 = \frac{M}{m_1} = \frac{330}{5} = 66$

$M_2 = \frac{M}{m_2} = \frac{330}{6} = 55$

$M_3 = \frac{M}{m_3} = \frac{330}{11} = 30$

Mencari invers dari $M_n (mod\ m)$

- $66 (mod\ 5) \Leftrightarrow 66 y_1 \equiv 1 (mod\ 5)$ berarti
  $66 y_1 - 1 = 5a$ untuk suatu $a \in \boldsymbol{Z}$
  $66 = 13.5 + 1$
  $5 = 5.1$, gcd$(66,5) = 1$
  $1 = 66 - 5(13)$
  $y_1 = 1$
- $55 (mod\ 6) \Leftrightarrow 55 y_2 \equiv 1 (mod\ 6)$ berarti
  $55 y_2 - 1 = 6b$ untuk suatu $b \in \boldsymbol{Z}$
  $55 = 9.6 + 1$
  $6 = 6.1$, gcd$(55,6) = 1$
  $1 = 55 - 9(6)$
  $y_2 = 1$
- $30 (mod\ 11) \Leftrightarrow 30 y_3 \equiv 1 (mod\ 11)$ berarti
  $30 y_3 - 1 = 11c$ untuk suatu $c \in \boldsymbol{Z}$
  $30 = 2.11 + 8$
  $11 = 1.8 + 3$
  $8 = 2.3 + 2$
  $3 = 1.2 + 1$

$2 = 2.1$, gcd$(30,11) = 1$

$1 = 3 - 2$

$1 = 3 - (8 - 2.3)$

$1 = 3.3 - 8$

$1 = 3(11 - 8) - 8$

$1 = 3.11 - 4.8$

$1 = 3.11 - 4.(30 - 2.11)$

$1 = 30(-4) - 11(-11)$

$y_3 = -4$

Karena syarat $0 < y_3 < m$ maka kita akan mencari nilai $y_3$ pada kelas yang sama untuk memenuhi syarat.

$[-4]_{11} = \{b \in \boldsymbol{Z} | (b, -4) \in \equiv (mod\ 11), -4 \in \boldsymbol{Z}\}$

$[-4]_{11} = \{b \in \boldsymbol{Z} | b + 4 = 11k, k \in \boldsymbol{Z}\}$

$[-4]_{11} = \{b \in \boldsymbol{Z} | b = 11k - 4, k \in \boldsymbol{Z}\}$

$[-4]_{11} = \{\dots, -26, -15, -4, 7, 18, \dots\}$

$[-4]_{11} = [-26]_{11} = [-15]_{11} = [7]_{11} = [18]_{11} = \cdots$

$0 < 7 < 11, y_3 = 7$

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 (mod\ M)$

$x \equiv 2.66.1 + 3.55.1 + 5.30.7 (mod\ 330)$

$x \equiv 132 + 165 + 1050 (mod\ 330)$

$x \equiv 1347 (mod\ 330)$, $1347 = 330 \times 4 + 27$

$x \equiv 27 (mod\ 330)$ berarti $x = 330l + 27$ untuk setiap $l \in \boldsymbol{Z}$ merupakan penyelesaian.

Kelipatan positif yang memenuhi adalah:

a. $27$
b. $330 + 27 = 354$
c. $330 \times 2 + 27 = 687$
d. $330 \times 3 + 27 = 1017$
e. $330 \times 4 + 27 = 1347$

f. $330 \times 5 + 27 = 1677$

g. $330 \times 6 + 27 = 2007$

2. Carilah penyelesaian dari sistem perkongruenan linear berikut.

   $x \equiv 1(mod\ 2)$
   $x \equiv 2(mod\ 3)$
   $x \equiv 3(mod\ 5)$

   Jawab:

   Terlebih dahulu kita akan mencari GCD dari antar modulo perkongruenan tersebut.

   gcd$(2,3) = 1$
   gcd$(2,5) = 1$
   gcd$(3,5) = 1$

   karena diperoleh semua gcd bernilai 1 maka sistem kekongruenan memiliki solusi.

   $M = m_1 m_2 m_3 = 2.3.5 = 30$

   $M_1 = \frac{M}{m_1} = \frac{30}{2} = 15$

   $M_2 = \frac{M}{m_2} = \frac{30}{3} = 10$

   $M_3 = \frac{M}{m_3} = \frac{30}{5} = 6$

   Mencari invers dari $M_n(mod\ m)$

- $15(mod\ 2) \Leftrightarrow 15y_1 \equiv 1(mod\ 2)$ berarti
  $15y_1 - 2a = 1$ untuk suatu $a \in \boldsymbol{Z}$
  $15 = 2.7 + 1$
  $2 = 2.1$, gcd$(15,2) = 1$
  $1 = 15 - 2(7)$
  $y_1 = 1$
- $10(mod\ 3) \Leftrightarrow 10y_2 \equiv 1(mod\ 3)$ berarti
  $10y_2 - 3b = 1$ untuk suatu $b \in \boldsymbol{Z}$
  $10 = 3.3 + 1$
  $3 = 3.1$, gcd$(10,3) = 1$

$1 = 10 - 3(3)$

$y_2 = 1$

- $6(mod\ 5) \Leftrightarrow 6y_3 \equiv 1(mod\ 5)$ berarti

  $6y_3 - 5c = 1$ untuk suatu $c \in \boldsymbol{Z}$

  $6 = 1.5 + 1$

  $5 = 5.1$, gcd$(6,5) = 1$

  $1 = 6 - 5$

  $y_3 = 1$

$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3(mod\ M)$

$x \equiv 1.15.1 + 2.10.1 + 3.6.1(mod\ 30)$

$x \equiv 15 + 20 + 18(mod\ 30)$

$x \equiv 53(mod\ 30)$, $53 = 30 \times 1 + 23$

$x \equiv 23(mod\ 30)$ berarti $x = 30l + 23$ untuk setiap $l \in \boldsymbol{Z}$ merupakan penyelesaian.

3. Carilah penyelesaian dari sistem perkongruenan linear berikut.

   $x \equiv 2(mod\ 4)$

   $x \equiv 3(mod\ 5)$

   $x \equiv 4(mod\ 9)$

   $x \equiv 5(mod\ 13)$

   Terlebih dahulu kita akan mencari GCD dari antar modulo perkongruenan tersebut.

   gcd$(4,5) = 1$

   gcd$(4,9) = 1$

   gcd$(4,13) = 1$

   gcd$(5,9) = 1$

   gcd$(5,13) = 1$

   gcd$(9,13) = 1$

   karena diperoleh semua gcd bernilai 1 maka sistem kekongruenan memiliki solusi.

   $M = m_1m_2m_3m_4 = 4.5.9.13 = 2340$

$$M_1 = \frac{M}{m_1} = \frac{2340}{4} = 585$$
$$M_2 = \frac{M}{m_2} = \frac{2340}{5} = 468$$
$$M_3 = \frac{M}{m_3} = \frac{2340}{9} = 260$$
$$M_4 = \frac{M}{m_4} = \frac{2340}{13} = 180$$

Mencari invers dari $M_n(mod\ m)$

- $585(mod\ 4) \Leftrightarrow 585y_1 \equiv 1(mod\ 4)$ berarti $585y_1 - 4a = 1$ untuk suatu $a \in \boldsymbol{Z}$

$$585 = 146.4 + 1$$
$$4 = 4.1, \text{gcd}(585,4) = 1$$
$$1 = 585 - 4(146)$$
$$y_1 = 1$$

- $468(mod\ 5) \Leftrightarrow 468y_2 \equiv 1(mod\ 5)$ berarti $468y_2 - 5b = 1$ untuk suatu $b \in \boldsymbol{Z}$

$$468 = 93.5 + 3$$
$$5 = 1.3 + 2$$
$$3 = 1.2 + 1$$
$$2 = 2.1, \text{gcd}(468,5) = 1$$
$$1 = 3 - 2$$
$$1 = 3 - (5 - 3)$$
$$1 = 3.2 - 5$$
$$1 = (468 - 93 \times 5)2 - 5$$
$$1 = 468.2 - 5.94$$
$$y_2 = 2$$

- $260(mod\ 9) \Leftrightarrow 260y_3 \equiv 1(mod\ 9)$ berarti $260y_3 - 9c = 1$ untuk suatu $c \in \boldsymbol{Z}$

$$260 = 9.28 + 8$$
$$9 = 1.8 + 1$$
$$8 = 1.8, \text{gcd}(260,9) = 1$$
$$1 = 9 - 8$$
$$1 = 9 - (260 - 9.28)$$

$$1 = 9.29 - 260$$
$$1 = 260(-1) - 9(-29)$$
$$y_3 = -1$$

Karena syarat $0 < y_3 < m$ maka kita akan mencari nilai $y_3$ pada kelas yang sama untuk memenuhi syarat.

$[-1]_9 = \{b \in \boldsymbol{Z} | (b, -1) \in \equiv (mod\ 9), -1 \in \boldsymbol{Z}\}$
$[-1]_9 = \{b \in \boldsymbol{Z} | b + 1 = 9k, k \in \boldsymbol{Z}\}$
$[-1]_9 = \{b \in \boldsymbol{Z} | b = 9k - 1, k \in \boldsymbol{Z}\}$
$[-1]_9 = \{\dots, -19, -10, -1, 8, 17, \dots\}$
$[-1]_9 = [-19]_9 = [-10]_9 = [8]_9 = [17]_9 = \cdots$
$0 < 8 < 11, y_3 = 8$

- $180(mod\ 13) \Leftrightarrow 180y_4 \equiv 1(mod\ 13)$ berarti $180y_4 - 13d = 1$ untuk suatu $d \in \boldsymbol{Z}$

$$180 = 13.13 + 11$$
$$13 = 1.11 + 2$$
$$11 = 5.2 + 1$$
$$2 = 2.1, \gcd(180,13) = 1$$
$$1 = 11 - 5.2$$
$$1 = 11 - 5(13 - 11)$$
$$1 = 11.6 - 13.5$$
$$1 = (180 - 13 \times 13)6 - 13.5$$
$$1 = 180.6 - 13.83$$
$$y_4 = 6$$

$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4(mod\ M)$
$x \equiv$
$2.585.1 + 3.468.2 + 4.260.8 + 5.180.6(mod\ 2340)$
$x \equiv 1170 + 2808 + 8320 + 5400(mod\ 2340)$
$x \equiv 17698(mod\ 2340), 17698 = 2340 \times 7 + 1318$
$x \equiv 1318(mod\ 2340)$ berarti $x = 2340l + 1318$ untuk setiap $l \in \boldsymbol{Z}$ merupakan penyelesaian.

## D.Persamaan Linear Diophantine

**Definisi :**

Suatu persamaan linear $ax+by=c$ dengan $a,b,c\in\mathbb{Z}$, $a\neq 0$ dan $b\neq 0$ dikatakan sebagai **Persamaan Diophantine** jika hanya jika nilai-nilai penyelesaian dari persamaan tersebut adalah bilangan bulat. Suatu Persamaan Diophantine mempunyai penyelesaian jika hanya jika $\gcd(a,b)\mid c$.

**Teorema**

Terdapat suatu persamaan Diophantine $ax+by=c$. Jika $d=\gcd(a,b)$ dan $x_0$ dan $y_0$ adalah penyelesaian awal dari persamaan diophantie. Maka penyelesaian umum dari persamaan Diophantine adalah :

$x = x_0 + \left(\frac{b}{d}\cdot k\right)$ dan $y = y_0 - \left(\frac{a}{d}\cdot k\right)$ untuk setiap $k\in\mathbb{Z}$

**Bukti :**

suatu persamaan Diophantine $ax+by=c$. Misalkan $a=\gcd(a,b)\cdot a'$, $b=\gcd(a,b)\cdot b'$ dan $\gcd(a',b')=1$. Diketahui $(x_0,y_0)$ adalah penyelesaian bulat dari persamaan $ax+by=c$ sehingga diperoleh bahwa $ax_0+by_0=c$ ........(1). Ambil sebarang $(x,y)$ merupakan suatu penyelesain bulat dari $ax+by=c$ ...........(2). Dari(1) dan (2) diperoleh

$$ax+by=c$$

$$ax+by=ax_0+by_0$$

$$a(x-x_0)=b(y_0-y)$$

$$\gcd(a,b)\cdot a'(x-x_0)=\gcd(a,b)\cdot b'(y_0-y)$$

$$a'(x-x_0)=b'(y_0-y)$$

Sehingga diperoleh

$a' \mid a'(x - x_0)$ maka $a' \mid b'(y_0 - y)$

i. karena $\gcd(a', b') = 1$ maka $a' \mid (y_0 - y)$ artinya

$(y_0 - y) = a'.l$ dengan $l \in \mathbb{Z}$

$y = y_0 - a'.l$ dengan $l \in \mathbb{Z}$

ii. karena $\gcd(a', b') = 1$ maka $b' \mid (x_0 - x)$ artinya

$(x_0 - x) = b'.k$ dengan $k \in \mathbb{Z}$

$x = x_0 + b'.k$ dengan $k \in \mathbb{Z}$

Dari (i) dan (ii) diperoleh

$$a'((x_0 + b'k) - x_0) = b'(y_0 - (y_0 + a'l))$$

$$k = l$$

**Sehingga diperoleh bahwa penyelesaian umum dari persamaan Diophantine adalah**

$$x = x_0 + \left(\frac{b}{d} \cdot k\right) \text{ dan } y = y_0 - \left(\frac{a}{d} \cdot k\right)$$

Contoh :

Tentukan penyelesaian umum dari persamaan $738x + 621y = 45$

Penyelesaian :

$738 = 1.621 + 117$

$621 = 5.117 + 36$

$117 = 3.36 + 9$

$36 = 4.9 + 0$

Diperoleh $\gcd(738, 621) = 9$ dan $9 \mid 45$ maka persamaan $738x + 621y = 45$ mempunyai penyelesaian.

$$9 = 117 - 3 \cdot 36$$

$$9 = 117 - 3(621 - 5 \cdot 117)$$

$$9 = 117 - 3 \cdot 621 + 15 \cdot 117$$

Type equation here.

$$9 = 16 \cdot 117 - 3 \cdot 621$$

$$9 = 16(738 - 621) - 3 \cdot 621$$

$$9 = 16 \cdot 738 + (-19) \cdot 621$$

Sehingga diperoleh

$45 = 80 \cdot 738 + (-95) \cdot 621$ dengan $x_0 = 80$ dan $y_0 = -95$

Diperoleh penyelesaian umum dari $738x + 621y = 45$ adalah

$x = 80 + \left(\frac{621}{9} \cdot k\right)$ dan $y = (-95) - \left(\frac{738}{9} \cdot k\right)$

## Latihan

1. Selidiki apakah persamaan diophantus berikut mempunyai solusi.
   a. $17x + 13y = 100$
   b. $60x + 81y = 97$
   c. $1402x + 1969y = 1$
   d. $12x + 18y = 50$

## Kunci Jawaban

1.Jawab

a. $17x + 13y = 100$
   gcd $(17,13)$?
   $17 = 13.1 + 4$

$13 = 4.3 + 1$
$4 = 1.4$
Karena gcd $(17,13) = 1$ dan $1|100$ maka $17x + 13y = 100$ mempunyai solusi.

b. $60x + 81y = 97$
gcd $(60,81)$?
$81 = 60.1 + 21$
$60 = 21.2 + 18$
$21 = 18.1 + 3$
$18 = 3.6$
Karena gcd $(60,81) = 3$ dan $3|97$ maka $60x + 81y = 97$ mempunyai solusi.

c. $1402x + 1969y = 1$
gcd $(1402,1969)$?
$1969 = 1402.1 + 567$
$1402 = 567.2 + 268$
$567 = 268.2 + 31$
$268 = 31.8 + 20$
$31 = 20.1 + 11$
$20 = 11.1 + 9$
$11 = 9.1 + 2$
$9 = 2.4 + 1$
$2 = 1.2$
Karena gcd $(1402,1969) = 1$ dan $1|1$ maka $1402x + 1969y = 1$ mempunyai solusi.

d. $12x + 18y = 50$
gcd $(12,18)$?
$18 = 12.1 + 6$
$12 = 6.2$
Karena gcd $(12,18) = 6$ dan $6$ tidak habis membagi 50 maka $12x + 18y = 50$ tidak mempunyai solusi.

## D. Rangkuman

1. Jika m suatu bilangan bulat positif, maka $a$ kongruen dengan $b$ modulo $m$ (ditulis $a \equiv b(mod\ m)$) bila dan hanya bila $m$ membagi $(a - b)$. Jika $m$ tidak membagi $(a - b)$ maka dikatakan bahwa $a$ tidak kongruen dengan $b$ modulo $m$ (ditulis $a \not\equiv b(mod\ m)$).
2. $a \equiv b(mod\ m)$ bila dan hanya bila ada bilangan bulat $k$ sehingga $a = mk + b$.
3. Setiap bilangan buat kongruen modulo $m$ dengan tepat satu di antara $0,1,2,3, \dots, (m - 1)$.
4. Jika $a \equiv b(mod\ m)$ dengan $0 \le r < m$, maka $r$ disebut residu terkecil dari $a$ modulo $m$. Untuk kekongruenan modulo $m$ ini, $\{0,1,2,3, \dots, (m - 1)\}$ disebut himpunan residu terkecil modulo $m$.
5. $a \equiv b(mod\ m)$ bila dan hanya bila $a$ dan $b$ memiliki sisa yang sama jika dibagi $m$.
6. Himpunan bilangan bulat $\{r_1, r_2, r_3, \dots, r_m\}$ disebut sistem residu lengkap modulo $m$ bila dan hanya bila setiap elemennya kongruen modulo $m$ dengan satu dan hanya satu dari $0,1,2,3, \dots, (m - 1)$.
7. Jika $m$, $a$, $b$, dan $c$ adalah bilangan-bilangan bulat dengan $m$ positif, maka

   $a \equiv a(mod\ m)$, sifat refleksi

   Jika $a \equiv b(mod\ m)$ maka $b \equiv a(mod\ m)$, sifat simetris

   Jika $a \equiv b(mod\ m)$ dan $b \equiv c(mod\ m)$ maka $a \equiv c(mod\ m)$, sifat transitif
8. Jika $a \equiv b(mod\ m)$ dan $c \in Z$ maka:
   a. $(a + c) \equiv (b + c)\ (mod\ m)$
   b. $(a - c) \equiv (b - c)\ (mod\ m)$
   c. $ac \equiv bc\ (mod\ m)$
   d. $a^2 \equiv b^2(mod\ m)$

9. Jika $a \equiv b(mod\ m)$, maka $a^n \equiv b^n(mod\ m)$
10. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka
    a. $a + c \equiv b + d\ (mod\ m)$
    b. $a - c \equiv b - d\ (mod\ m)$
    c. $ac \equiv bd\ (mod\ m)$
11. Jika $a \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$ maka $ax + cy \equiv bx + dy\ (mod\ m)$ untuk setiap bilangan bulat $x$ dan $y$.
12. Jika $ac \equiv bc(mod\ m)$ dengan $(c, m) = 1$, maka $a \equiv b(mod\ m)$
13. Jika $ac \equiv bc(mod\ m)$ dengan $(c, m) = d$, maka $a \equiv b\left(mod\ \frac{m}{d}\right)$
14. Persamaan linear kongruen $ax \equiv b(mod\ m)$ dapat diselesaikan jika dan hanya jika $d|b$ dimana $d = (a, m)$. Jika $d|b$ maka memiliki $d$ solusi.
15. Jika $(a, m) = 1$ maka perkongruenan linear $ax \equiv b(mod\ m)$ memiliki tepat 1 solusi.
16. Suatu persamaan linear $ax + by = c$ dengan $a, b, c \in \mathbb{Z}$, $a \neq 0$ dan $b \neq 0$ dikatakan sebagai **Persamaan Diophantine** jika hanya jika nilai-nilai penyelesaian dari persamaan tersebut adalah bilangan bulat. Suatu Persamaan Diophantine mempunyai penyelesaian jika hanya jika $\gcd(a, b)|c$.
17. Terdapat suatu persamaan Diophantine $ax + by = c$. Jika $d = \gcd(a, b)$ dan $x_0$ dan $y_0$ adalah penyelesaian awal dari persamaan diophantie. Maka penyelesaian umum dari persamaan Diophantine adalah :

    $$x = x_0 + \left(\frac{b}{d} \cdot k\right) \text{ dan } y = y_0 - \left(\frac{a}{d} \cdot k\right) \text{ untuk setiap } k \in \mathbb{Z}$$

## E. Latihan Soal

1. Tentukanlah sisanya apabila $41^{75}$ dibagi dengan 7.
2. Tentukanlah sisanya apabila $3^{247}$ dibagi dengan 25.
3. Selidiki apakah persamaan diophantus berikut memiliki solusi.

   $25x + 95y = 970$

   $30x + 47y = -11$

   $102x + 1001y = 1$
4. Tentukan invers $7(mod\ 11)$
5. Tentukan invers $31(mod\ 43)$
6. Carilah penyelesaian dari sistem perkongruenan linear berikut.

   $x \equiv 3(mod\ 4)$

   $x \equiv 4(mod\ 5)$

   $x \equiv 4(mod\ 6)$

**Kunci Jawaban:**

1. Tentukanlah sisanya apabila $41^{75}$ dibagi dengan 7.

   Jawab:

   $41^2 \equiv \quad \equiv 1(mod\ 7)$

   $41^4 \equiv 1^2 \equiv 1(mod\ 7)$

   $41^8 \equiv 1^2 \equiv 1(mod\ 7)$

   $41^{16} \equiv 1^2 \equiv 1(mod\ 7)$

   $41^{32} \equiv 1^2 \equiv 1(mod\ 7)$

   $41^{64} \equiv 1^2 \equiv 1(mod\ 7)$

   $41^{75} = 41^{64+8+2+1}$

   $= 41^{64} \times 41^8 \times 41^2 \times 41$

   $\equiv 1 \times 1 \times 1 \times 41(mod\ 7)$

   $\equiv 41(mod\ 7)$

   $\equiv 6(mod\ 7)$

2. Tentukanlah sisanya apabila $3^{247}$ dibagi dengan 25.

   Jawab:

   $3^2 \equiv \quad \equiv 9(mod\ 25)$

   $3^4 \equiv 9^2 \equiv 6(mod\ 25)$

   $3^8 \equiv 6^2 \equiv 11(mod\ 25)$

   $3^{16} \equiv 11^2 \equiv 21(mod\ 25)$

$3^{32} \equiv 21^2 \equiv 16(mod\ 25)$
$3^{64} \equiv 16^2 \equiv 6(mod\ 25)$
$3^{128} \equiv 6^2 \equiv 11(mod\ 25)$
$3^{247} = 3^{128+64+32+16+4+2+1}$
$= 3^{128} \times 3^{64} \times 3^{32} \times 3^{16} \times 3^4 \times 3^2 \times 3$
$\equiv 11 \times 6 \times 16 \times 21 \times 6 \times 9 \times 3(mod\ 25)$
$\equiv 66 \times 16 \times 21 \times 54 \times 3(mod\ 25)$
$\equiv 16 \times 16 \times 21 \times 4 \times 3(mod\ 25)$
$\equiv 256 \times 21 \times 12(mod\ 25)$
$\equiv 6 \times 21 \times 12(mod\ 25)$
$\equiv 126 \times 12(mod\ 25)$
$\equiv 1 \times 12(mod\ 25)$
$\equiv 12(mod\ 25)$

3. Selidiki apakah persamaan diophantus berikut memiliki solusi.

a. $25x + 95y = 970$
gcd $(25,95)$?
$95 = 25.3 + 20$
$25 = 20.1 + 5$
$20 = 5.4$
Karena gcd $(25,95) = 5$ dan $5|970$ maka $25x + 95y = 970$ mempunyai solusi.

b. $30x + 47y = -11$
gcd $(30,47)$?
$47 = 30.1 + 17$
$30 = 17.1 + 13$
$17 = 13.1 + 4$
$13 = 4.3 + 1$
$4 = 1.4$

Karena gcd $(30,47) = 1$ dan $1| - 11$ maka $30x + 47y = -11$ mempunyai solusi.

c. $102x + 1001y = 1$

gcd $(102,1001)$?

$1001 = 102.9 + 83$

$102 = 83.1 + 19$

$83 = 19.4 + 7$

$19 = 7.2 + 5$

$7 = 5.1 + 2$

$5 = 2.2 + 1$

$2 = 1.2$

Karena gcd $(102,1001) = 1$ dan $1|1$ maka $102x + 1001y = 1$ mempunyai solusi.

Mencari invers kongruensi jika $ax \equiv 1(mod\ m)$, $a^{-1} > 0$ dan gcd $(a, m) = 1$ maka $x_o$ pada $x = x_o + \frac{m}{gcd(a,m)}t$ untuk setiap $t \in \boldsymbol{Z}$ adalah nilai inversnya.

4. Tentukan invers $7(mod\ 11)$

Jawab:

$7(mod\ 11) \Leftrightarrow 7x \equiv 1(mod\ 11)$ dan gcd $(7,11) = 1$

$7x \equiv 1(mod\ 11)$ berarti $7x - 1 = 11k$ untuk suatu $k \in \boldsymbol{Z}$

$11 = 7.1 + 4$

$7 = 4.1 + 3$

$4 = 3.1 + 1$

$3 = 1.3$, 1 adalah gcd$(7,11)$

$1 = 4 - 3$

$1 = 4 - (7 - 4)$

$1 = 4.2 - 7$

$1 = (11 - 7)2 - 7$

$1 = 11.2 - 7.3$

$1 = (-3)7 - (-2)11$

$x_o = -3$

Karena syarat $0 < x_o < m$ maka kita akan mencari nilai $x_o$ pada kelas yang sama untuk memenuhi syarat.

$[-3]_{11} = \{b \in \boldsymbol{Z} | (b, -3) \in \equiv (mod\ 11), -3 \in \boldsymbol{Z}\}$

$[-3]_{11} = \{b \in \boldsymbol{Z} | b + 3 = 11k, k \in \boldsymbol{Z}\}$

$[-3]_{11} = \{b \in \boldsymbol{Z} | b = 11k - 3, k \in \boldsymbol{Z}\}$

$[-3]_{11} = \{\dots, -25, -14, -3, 8, 19, \dots\}$

$[-3]_{11} = [-25]_{11} = [-14]_{11} = [8]_{11} = [19]_{11} = \cdots$

$$0 < 8 < 11$$

Invers dari $7(mod\ 11)$ adalah $8(mod\ 11)$.

5. Tentukan invers $31(mod\ 43)$

Jawab:

$31(mod\ 43) \Leftrightarrow 31x \equiv 1(mod\ 43)$ dan gcd $(31,43) = 1$

$31x \equiv 1(mod\ 43)$ berarti $31x - 1 = 43k$ untuk suatu $k \in \boldsymbol{Z}$

$43 = 31.1 + 12$

$31 = 12.2 + 7$

$12 = 7.1 + 5$

$7 = 5.1 + 2$

$5 = 2.2 + 1$

$2 = 1.2$, 1 adalah gcd$(31,43)$

$1 = 5 - 2.2$

$1 = 5 - 2(7 - 5)$

$1 = 3.5 - 2.7$

$1 = 3(12 - 7) - 2.7$

$1 = 3.12 - 5.7$

$1 = 3.12 - 5(31 - 12.2)$

$1 = 13.12 - 5.31$

$1 = 13(43 - 31) - 5.31$

$1 = 13.43 - 18.31$

$1 = (-18)31 - (-13)43$

$x_o = -18$

Karena syarat $0 < x_o < m$ maka kita akan mencari nilai $x_o$ pada kelas yang sama untuk memenuhi syarat.

$[-18]_{43} = \{b \in \boldsymbol{Z} | (b, -18) \in \equiv (mod\ 43), -18 \in \boldsymbol{Z}\}$

$[-18]_{43} = \{b \in \boldsymbol{Z} | b + 18 = 43k, k \in \boldsymbol{Z}\}$

$[-18]_{43} = \{b \in \boldsymbol{Z} | b = 43k - 18, k \in \boldsymbol{Z}\}$

$[-18]_{43} = \{\dots, -104, -61, -18, 25, 68, \dots\}$

$[-18]_{43} = [-104]_{43} = [-61]_{43} = [25]_{43} = [68]_{43} = \dots$

$$0 < 25 < 11$$

Invers dari $31(mod\ 43)$ adalah $25(mod\ 43)$.

6. Carilah penyelesaian dari sistem perkongruenan linear berikut.

   $x \equiv 3(mod\ 4)$

   $x \equiv 4(mod\ 5)$

   $x \equiv 4(mod\ 6)$

   Terlebih dahulu kita akan mencari gcd dari antar modulo perkongruenan tersebut.

   $\gcd(4,5) = 1$

   $\gcd(4,6) = 2$

   $\gcd(5,6) = 1$

   karena diperoleh tidak semua gcd bernilai 1 maka sistem kekongruenan tidak memiliki solusi.

**Refleksi :)**

1. Kesulitan apa yang kamu alami pada bab ini?
2. Buatlah soal kontekstual yang penyelesaianya menggunakan persamaan linear Diophantine.

# BAB IV
# SISTEM NUMERIK DAN FUNGSI TANGGA

## I. Tujuan instruksional

Pada bab ini mahasiswa diharapkan mampu: 1) mengubah suatu bilangan pada basis tertentu ke basis bilangan lain; 2) melakukan operasi pada basis bilangan; 3) menerapkan fungsi tangga dalam menyelesaikan masalah.

## II. Uraian Materi

## A. Sistem Numerik (Basis Bilangan)

**Teorema 4.1**

Misalkan $b$ suatu bilangan bulat positif yang lebih besar dari 1, maka setiap bilangan bulat positif $n$ dapat ditulis secara tunggal dalam bentuk

$$n = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \ldots + a_1 b + a_0$$

dengan $k$ suatu bilangan bulat tak negatif, $a_j$ suatu bilangan bulat dengan $0 \le a_j \le b-1$ untuk $j = 0, 1, 2, \ldots, k$ dengan

$a_k \neq 0$

**Bukti :**

Gunakanlah algoritma pembagian untuk memperoleh representasi dari *n* seperti yang diinginkan. Pertama, bagilah *n* dengan *b* sehingga :

$$n = bq_0 + a_0, \qquad 0 \le a_0 \le b-1$$

Jika $q_0 \neq 0$, bagilah $q_0$ dengan *b* dan diperoleh bahwa

$$q_0 = bq_1 + a_1, \qquad 0 \le a_1 \le b-1$$

$$q_1 = bq_2 + a_2, \qquad 0 \le a_2 \le b-1$$

dan seterusnya hingga

$$q_{k-2} = bq_{k-1} + a_{k-1}, \qquad 0 \le a_{k-1} \le b-1$$

$$q_{k-1} = b.0 + a_k, \qquad 0 \le a_k \le b-1$$

Langkah terakhir dari proses ini terjadi apabila kita memperoleh hasil bagi 0. Perhatikan bahwa dalam penerapan algoritma pembagian tersebut, kita memperoleh hasil bagi-hasil bagi yang memenuhi

$$n > q_0 > q_1 > q_2 > \ldots \ge 0$$

Karena barisan $q_0, q_1, q_2, \ldots$ adalah suatu barisan turun dari bilangan-bilangan bulat tak negatif, maka barisan ini akan berakhir pada suku 0. Selanjutnya dari persamaan pertama $q_0$ disubstitusi pada persamaan kedua diperoleh

$$n = bq_0 + a_0$$

$$n = b(bq_1 + a_1) + a_0 = b^2 q_1 + ba_1 + a_0$$

Proses substitusi dilanjutkan untuk $q_1, q_2, q_3, \ldots$ diperoleh

$$n = b^3 q_2 + b^2 a_2 + ba_1 + a_0$$

$$n = b^4 q_3 + b^3 a_3 + b^2 a_2 + ba_1 + a_0$$

dst hingga

$$n = b^{k-1} q_{k-2} + b^{k-2} a_{k-2} + \ldots. + b^2 a_2 + ba_1 + a_0$$

$$n = b^{k-1} q_{k-2} + b^{k-2} a_{k-2} + \ldots. + b^2 a_2 + ba_1 + a_0$$

$$n = b^k a_k + b^{k-1} a_{k-1} + \ldots. + b^2 a_2 + ba_1 + a_0$$

$$= a_k b^k + a_{k-1} b^{k-1} + \ldots. + a_2 b^2 + a_1 b + a_0$$

dimana $0 \le a_j \le b-1$ untuk $j = 0,1,2,...,k$ dan $a_k \ne 0$ karena $a_k = q_{k-1}$ adalah hasil bagi terakhir yang tidak sama dengan 0.

Representasi dari *n* seperti yang diinginkan telah diperoleh.
Selanjutnya, akan ditunjukkan bahwa representasi *n* tersebut tunggal.
Misalkan dipunyai dua representasi dari *n* yaitu :

dan

$$n = a_k b^k + a_{k-1} b^{k-1} + .... + a_2 b^2 + a_1 b + a_0, \qquad 0 \le a_j \le b-1$$

$$n = c_k b^k + c_{k-1} b^{k-1} + .... + c_2 b^2 + c_1 b + c_0, \qquad 0 \le c_j \le b-1$$

Jika kedua persamaan tersebut dikurangkan, maka diperoleh

$$(a_k - c_k) b^k + (a_{k-1} - b_{k-1}) b^{k-1} + .... + (a_1 - c_1) b + (a_0 - c_0) = 0$$

Jika dua representasi dari *n* tersebut berbeda, maka ada bilangan bulat terkecil *j*, $0 \le j \le k$, sedemikian sehingga $a_j \ne c_j$. Jadi

Sehingga

$$b^j \{(a_k - c_k) b^{k-j} + (a_{k-1} - b_{k-1}) b^{k-j-1} + .... + (a_{j+1} - c_{j+1}) b + (a_j - c_j)\} = 0$$

$$(a_k - c_k) b^{k-j} + (a_{k-1} - b_{k-1}) b^{k-j-1} + .... + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0$$

$$(a_j - c_j) = b\{(a_k - c_k) b^{k-j} + (a_{k-1} - b_{k-1}) b^{k-j-1} + .... + (a_{j+1} - c_{j+1})\}$$

Ini berarti bahwa *b* $(a_j \ne c_j)$

Tetapi karena $0 \le a_j < b$ dan $0 \le c_j < b$, yaitu $-b < a_j - c_j < b$, sehingga $a_j - c_j = 0$, yaitu $a_j = c_j$

Jadi, representasi dari n adalah tunggal. (terbukti)

**Akibat 4.1**

Setiap bilangan bulat positif dapat direpresentasikan dalam basis 2.

**Bukti :**

Misalkan *n* adalah bilangan bulat positif. Berdasarkan Teorema 2.1 dengan *b*= 2, diperoleh bahwa

$n = a_k 2^k + a_{k-1} 2^{k-1} + .... + a_1 2 + a_0$

dengan $a_j$ adalah 0 atau 1. Oleh karena itu, setiap bilangan bulat positif dapat direpresentasikan dalam basis 2 (terbukti).

Basis 10 disebut pula basis *desimal*. Basis 2 disebut *biner*, basis 4 disebut *quarter*, basis 8 disebut *oktal* dan basis 16 disebut *heksadesimal* atau secara singkat *heks*. Koefisien $a_j$ dalam ekspansi jumlahan itu disebut angka (digits). Angka biner biasa disebut dengan *bits*, yang merupakan singkatan dari *binary digits* yang merupakan istilah dalam komputer.

Untuk mengubah penulisan lambang bilangan dari basis desimal ke basis non desimal, gunakan proses algoritma pembagian secara berulang-ulang seperti pada proses pembuktian teorema diatas. Perhatikan contoh berikut ini.

**Contoh :**

1. Ubahlah $(1999)_{10}$ dari basis desimal menjadi notasi basis 7 dan $(6105)_7$ dari basis 7 menjadi notasi desimal.

Jawab :

- Untuk mengubah $(1999)_{10}$ dari basis desimal menjadi notasi basis 7, terapkanlah algoritma pembagian secara berulang-ulang, yaitu :

  $$\begin{aligned} 1999 &= 7.285 + 4 \\ 285 &= 7.40 + 5 \\ 40 &= 7.5 + 5 \\ 5 &= 7.0 + 5 \end{aligned} \Bigg\uparrow$$

  Jadi, $(1999)_{10} = (5554)_7$, yaitu dengan menuliskan sisa-sisa pembagian itu dengan urutan dari bawah ke atas seperti ditunjukkan anak panah.

- $(6105)_7$ ditulis dalam basis 7. Jika ingin mengubahnya menjadi basis desimal (sepuluh), maka yang harus dilakukan adalah tinggal menghitung jumlahan dari perpangkatan tujuh tersebut, yaitu :

$$\begin{aligned}(6105)_7 &= 6.7^3 + 1.7^2 + 0.7 + 5 \\ &= 6.343 + 49 + 0 + 5 = (2112)_{10}\end{aligned}$$

Jadi, $(6105)_7 = (2112)_{10}$

2. Ubahlah $(10101111)_2$ dari bentuk biner ke notasi desimal dan $(999)_{10}$ dari basis desimal ke notasi biner! (Rosen, 2011: 50, exercise 2.1, number 3).

Jawab :

- $(10101111)_2$ dirulis dalam basis 2. Jika ingin mengubahnya menjadi basis desimal (sepuluh), maka yang harus dilakukan adalah tinggal menghitung jumlahan dari perpangkatan dua tersebut, yaitu :

$$\begin{aligned}(10101111)_2 &= 1.2^7 + 0.2^6 + 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 1.2 + 1 \\ &= 128 + 0 + 32 + 0 + 8 + 4 + 2 + 1 = (175)_{10}\end{aligned}$$

Jadi, $(10101111)_2 = (175)_{10}$

- Untuk mengubah $(999)_{10}$ dari basis desimal menjadi notasi biner, terapkanlah algoritma pembagian secara berulang-ulang, yaitu :

$$\begin{aligned}999 &= 2.499 + 1 \\ 499 &= 2.249 + 1 \\ 249 &= 2.124 + 1 \\ 124 &= 2.62 + 0 \\ 62 &= 2.31 + 0 \\ 31 &= 2.15 + 0 \\ 15 &= 2.7 + 1\end{aligned}$$

$$7 = 2.3 + 1$$
$$3 = 2.1 + 1$$
$$1 = 2.0 + 1$$

Jadi, $(999)_{10} = (1111100111)_2$, yaitu dengan menuliskan sisa-sisa pembagian itu dengan urutan dari bawah ke atas seperti ditunjukkan anak panah.

3. Tentukanlah representasi desimal dari $(101001)_{-2}$ dan $(12012)_{-3}$.

   Jawab :

$$(101001)_{-2} = 1.(-2)^5 + 0.(-2)^4 + 1.(-2)^3 + 0.(-2)^2 + 0.(-2) + 1$$
$$= -32 + 0 - 8 + 0 + 0 + 1 = -39$$

$$(12012)_{-3} = 1.(-3)^4 + 2.(-3)^3 + 0.(-3)^2 + 1.(-3) + 2$$
$$= 81 - 54 + 0 - 3 + 2 = 26$$

4. Tentukanlah representasi basis -2 dari bilangan desimal -7, -17, dan 61.

   Jawab :

$$-7 = (-2).4 + 1$$
$$4 = (-2).(-2) + 0$$
$$-2 = (-2).1 + 0$$
$$1 = (-2).0 + 1$$

Jadi, $(-7)_{10} = (1001)_{-2}$.

$$-17 = (-2).9 + 1$$
$$9 = (-2).(-4) + 1$$
$$-4 = (-2).2 + 0$$
$$2 = (-2).(-1) + 0$$
$$-1 = (-2).1 + 1$$
$$1 = (-2).0 + 1$$

Jadi, $(-17)_{10} = (110011)_{-2}$.

$$61 = (-2).(-30) + 1$$
$$-30 = (-2).(15) + 0$$

$15 = (-2).(-7) + 1$

$-7 = (-2).(4) + 1$

$4 = (-2).(-2) + 0$

$-2 = (-2).(1) + 0$

$1 = (-2).0 + 1$

Jadi, $(61)_{10} = (1001101)_{-2}$.

Komputer, selain menggunakan basis 2, juga menggunakan basis 8 atau 16. Dalam heksadesimal (basis 16) mempunyai 16 lambang dasar yaitu :

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Huruf-huruf A, B, C, D, E, dan F digunakan untuk menyatakan angka-angka yang bersesuaian dengan 10, 11, 12, 13, 14, dan 15 (dalam basis desimal). Berikut ini tabel konversi penulisan lambang bilangan desimal, biner, quarter, oktal, dan heksadesimal.

**Tabel 4.1 Konversi Basis Bilangan**

| **Basis 10** | **Basis 2** | **Basis 4** | **Basis 8** | **Basis 16** |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 10 | 2 | 2 | 2 |
| 3 | 11 | 3 | 3 | 3 |
| 4 | 100 | 10 | 4 | 4 |
| 5 | 101 | 11 | 5 | 5 |
| 6 | 110 | 12 | 6 | 6 |
| 7 | 111 | 13 | 7 | 7 |
| 8 | 1000 | 20 | 10 | 8 |
| 9 | 1001 | 21 | 11 | 9 |
| 10 | 1010 | 22 | 12 | A |
| 11 | 1011 | 23 | 13 | B |
| 12 | 1100 | 30 | 14 | C |
| 13 | 1101 | 31 | 15 | D |
| 14 | 1110 | 32 | 16 | E |
| 15 | 1111 | 33 | 17 | F |

| | | | | |
|---|---|---|---|---|
| 16 | 10000 | 100 | 20 | 10 |

Pengubahan lambang bilangan dari basis 2 ke basis 8, maka lambang bilangan dalam basis 2 tersebut dikelompokkan tiga angka-tiga angka dari kanan. Selanjutnya, gantilah tiap kelompok tersebut dengan angka yang sesuai dengan angka pada basis 8. Untuk mengubah lambang bilangan dalam basis 8 ke basis 2, maka gantilah angka-angka pada lambang bilangan basis 8 dengan angka-angka yang sesuai dengan basis 2, dengan catatan tiap satu angka pada basis 8 disediakan tiga tempat pada basis 2.

**Contoh :**

1. $(1000010001)_2 = (1.000.010.001)_2 = (1021)_8$
2. $(7015)_8 = (111.000.001.101)_2 = (111000001101)_2$

Pengubahan lambang bilangan dalam basis 2 ke basis 4, kelompokkan dua angka-dua angka dari kanan pada lambang bilangan basis 2. Selanjutnya, ganti tiap kelompok dua angka itu dengan angka yang sesuai dengan angka pada basis 4. Untuk mengubah lambang bilangan dalam basis 4 ke basis 2, ganti tiap angka pada lambang bilangan basis 4 dengan angka yang sesuai dengan angka pada basis 2.

**Contoh :**

1. $(2013)_4 = (10.00.01.11)_2 = (100000111)_2$
2. $(101101001)_2 = (1.01.10.10.01)_2 = (11221)_4$

Bila menginginkan mengubah lambang bilangan dalam basis 2 ke basis 16 atau sebaliknya, dapat dilakukan dengan cara yang mirip dengan cara yang telah disebutkan diatas. Satu angka pada lambang bilangan basis 16 disediakan empat tempat pada lambang bilangan basis 2.

**Contoh :**

1. Ubahlah $(1000111101\,01)_2$ dan $(1110100111\,0)_2$ dari bentuk biner menjadi heksadesimal.

   Jawab :

   $(1000111101\,01)_2 = (1000.1111.0101)_2 = (8F5)_{16}$

   $(1110100111\,0)_2 = (111.0100.1110)_2 = (74E)_{16}$

2. Ubahlah $(ABCDEF)_{16}$, $(DEFACED)_{16}$, dan $(9A0B)_{16}$ dari heksadesimal menjadi biner.

   Jawab :

   $(ABCDEF)_{16} = (1010.1011.1100.1101.1110.1111)_2$
   $= (101010111100110111101111)_2$

   $(DEFACED)_{16}$
   $= (1101.1110.1111.1010.1100.1110.1101)_2$
   $= (1101111011111010110011101101)_2$

   $(9A0B)_{16} = (1001.1010.0000.1011)_2$
   $= (1001101000001011)_2$

Bila menginginkan mengubah digit dari basis 3 ke basis 9 maupun sebaliknya, perhatikan langkah berikut:

Setiap digit dari basis 9 berkorespondensi dengan dua buah digit basis 3. Korespondensinya adalah $(0)_9 = (00)_3$, $(1)_9 = (01)_3$, $(2)_9 = (02)_3$, $(3)_9 = (10)_3$, $(4)_9 = (11)_3$, $(5)_9 = (12)_3$, $(6)_9 = (20)_3$, $(7)_9 = (21)_3$, $(8)_9 = (22)_3$.

Untuk mengkonversi ekspansi basis 9 ke ekspansi basis 3, secara sederhana gantikan setiap digit basis 9 dengan dua buah digit basis 3 yang berkorespondensi. Untuk mengkonversi ekspansi basis 3 ke ekspansi basis 9, mulailah ekspansi dari sisi kanan dan gantikan dua buah digit basis 3 dengan digit pada basis 9 yang berkorespondensi, letakkan nilai awal nol pada blok terakhir dari sisi kiri jika hanya terdapat satu buah digit.

**Operasi pada basis biner**

**Penjumlahan**

Contoh

Jumlahkan $(101111011)_2$ dan $(1100111011)_2$.

Jawab :

$$
\begin{array}{r l}
\textit{1 \;\; 1\,1\,1\,1 \;\; 1\,1} & \\
1\;0\;1\;1\;1\;1\;0\;1\;1 & \\
1\;1\;0\;0\;1\;1\;1\;0\;1\;1 & + \\
\hline
1\;0\;0\;1\;0\;1\;1\;0\;1\;1\;0 &
\end{array}
$$

Perhitungan:

$1 + 1 \quad = 1.2 + 0$

$1 + 1 + 1 = 1.2 + 1$

$1 + 0 + 0 = 0.2 + 1$

$1 + 1 + 0 = 1.2 + 0$

$1 + 1 + 1 = 1.2 + 1$

$1 + 1 + 1 = 1.2 + 1$

$1 + 1 + 0 = 1.2 + 0$

$1 + 0 + 0 = 0.2 + 1$

$1 + 1 + 0 = 1.2 + 0$

$1 + 1 + 0 = 1.2 + 0$

Jadi, $(101111011)_2 + (1100111011)_2 = (10010110110)_2$

**Pengurangan**

**Contoh**

Kurangkan $(11010111)_2$ dari $(1111000011)_{2.}$

Jawab :

$$
\begin{array}{r l}
\textit{-1-1-1-1-1-1} \quad\quad\; & \\
1\;1\;1\;1\;0\;0\;0\;0\;1\;1 & \\
1\;1\;0\;1\;0\;1\;1\;1 & - \\
\hline
1\;0\;1\;1\;1\;0\;1\;1\;0\;0 &
\end{array}
$$

Perhitungan :

$1 - 1 \quad = 0.2 - 0$

$1 - 1 \quad = 0.2 - 0$

$0 - 1 \quad = (-1).2 + 1$

$0 - 0 - 1 \quad = (-1).2 + 1$

$0 - 1 - 1 \quad = (-1).2 + 0$

$0 - 0 - 1 \quad = (-1).2 + 1$

$1 - 1 - 1 \quad = (-1).2 + 1$

$1 - 1 - 1 \quad = (-1).2 + 1$

$1 - 1 \quad = 0.2 + 0$

$1 - 0 \quad = 0.2 + 1$

Jadi, $(1111000011)_2 - (11010111)_2 = (1011101100)_2$

**Perkalian**

**Contoh**

Kalikan $(11101)_2$ dan $(110001)_2$.

Jawab :

```
          1 1 0 0 0 1
            1 1 1 0 1   x
   ----------------------
          1 1 0 0 0 1
        0 0 0 0 0 0
      1 1 0 0 0 1
    1 1 0 0 0 1
  1 1 0 0 0 1         +
 ----------------------
1 0 1 1 0 0 0 1 1 0 1
```

Jadi, hasil kali dari $(11101)_2$ dan $(110001)_2$ adalah $(10110001101)_2$.

**Pembagian**

**Contoh**

Tentukanlah hasil bagi dan sisa bila $(110011111)_2$ dibagi dengan $(1101)_2$.

Jawab :

```
              1 1 1 1 1

1 1 0 1  /  1 1 0 0 1 1 1 1 1
              1 1 0 1          _
            0 1 1 0 0 1
                1 1 0 1        _
              0 1 1 0 0 1
                  1 1 0 1      _
                0 1 1 0 0 1
                        1 0 1  _
                  0 1 1 0 0 1
                      1 1 0 1  _
                    0 1 1 0 0
```

Diperoleh hasil bagi adalah $(11111)_2$ dan sisanya adalah $(1100)_2$.
Jadi, hasil bagi dari $(110011111)_2$ dibagi dengan $(1101)_2$ adalah $(11111)_2$ dan sisanya adalah $(1100)_2$

## B. Fungsi Tangga

**Definisi:**

Diberikan suatu bilangan real *a*, $[a]$ adalah suatu bilagan bulat yang kurang atau sama dengan *a*, yaitu $[a]$ adalah bilangan bulat tunggal yang memenuhi $a-1 \leq [a] \leq a$.

**Contoh :**

$\left[-3\frac{1}{2}\right] = -4$ dan $\left[7\frac{3}{5}\right] = 7$

**Teorema :**

Jika *n* adalah bilangan bulat positif dan *p* suatu bilangan prima maka eksponen tertinggi dari *p* yang membagi *n*! adalah $\sum_{k=1}^{\infty} \frac{n}{p^k}$

Bukti sebagai latihan.

$a_k \neq 0$

**Contoh :**

Berapa banyaknya angka nol dari representasi 50! ?

Penyelesaian

Eksponensial tertinggi adalah 2 dan 5 dalam faktorisasi prima 50! Dan memilih eksponennya yang terkecil.

Eksponen tertinggi dari 2 dalam 50! Adalah :

$$\sum_{k=1}^{5}\left(\frac{50}{2^k}\right)=\frac{50}{2^1}+\frac{50}{2^2}+\frac{50}{2^3}+\frac{50}{2^4}+\frac{50}{2^5}=47$$

Dan

$$\sum_{k=1}^{2}\left(\frac{50}{5^k}\right)=\frac{50}{5^1}+\frac{50}{5^2}=12$$

Jadi pangkat tertinggi dari 5 yang membagi 50! Adalh 12. Sehingg banyaknya angka nol dalam representasi decimal adalah 12

## III. Rangkuman

1. Misalkan *b* suatu bilangan bulat positif yang lebih besar dari 1, maka setiap bilangan bulat positif *n* dapat ditulis secara tunggal dalam bentuk

   $$n = a_k b^k + a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \ldots + a_1 b + a_0$$

   dengan *k* suatu bilangan bulat tak negatif, $a_j$ suatu bilangan bulat dengan $0 \le a_j \le b-1$ untuk $j$ = 0, 1, 2, . . ., *k* dengan $a_k \neq 0$
2. Setiap bilangan bulat positif dapat direpresentasikan dalam basis 2.
3. Diberikan suatu bilangan real *a*, $[a]$ adalah suatu bilagan bulat yang kurang atau sama dengan *a*, yaitu $[a]$ adalah bilangan bulat tunggal yang memenuhi $a-1 \le [a] \le a$ .

4. Jika $n$ adalah bilangan bulat positif dan $p$ suatu bilangan prima maka eksponen tertinggi dari $p$ yang membagi $n!$ adalah $\sum_{k=1}^{\infty} \frac{n}{p^k}$

## IV. Latihan Soal

1. Ubahlah bilangan berikut ini ke dalam basis tertentu.
   a. $2.020 = \ldots\ldots_2 = \ldots\ldots_4 = \ldots\ldots_8$
   b. $526 = \ldots\ldots_{16}$
   c. $1.254 = \ldots\ldots_3 = \ldots\ldots_9$
2. Hitunglah
   a. 1010111 + 110100
   b. 111000 – 10011
   c. 101010 × 101
   d. 100010 : 111

**Refleksi :)**

1. Hal apa yang berkesan pada bab ini?
2. **Tantangan.** Coba buatlah soal operasi pada basis lain selain basis 2 dan 10. Tukarkan soalmu dengan milik teman dan silahkan dikerjakan.

# BAB V
# KRIPTOLOGI

## V. Tujuan instruksional

Pada bab ini mahasiswa diharapkan mampu: 1) melakukan enkripsi dan dekripsi dari suatu teks; 2) melakukan enkripsi dan dekripsi menggunakan transformasi Caesar; 3) melakukan enkripsi dan dekripsi menggunakan transformasi Affine; 4) melakukan enkripsi dan dekripsi menggunakan transformasi RSA.

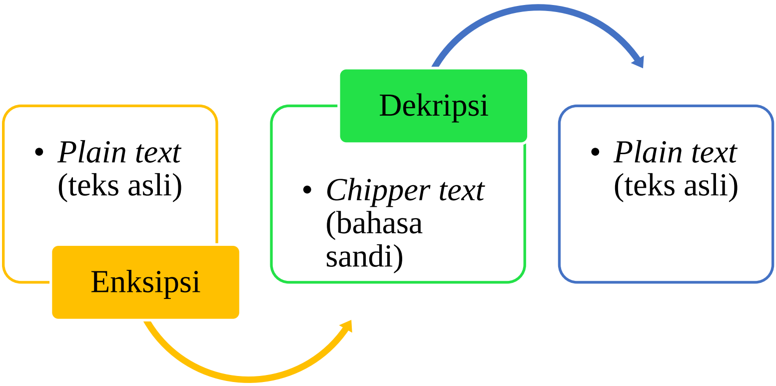
## VI. Uraian Materi

### A. Kriptografi

Dari zaman dahulu, orang-orang sudah mengirimkan pesan rahasia terutama saat terjadi perang atau penjajahan. Komunikasi rahasia ini dilakukan untuk menjaga kerahasiaan urusan diplomasi ataupun militer. Saat ini seiring kemajuan teknologi dan juga perkembangan zaman, pengiriman pesan kepada pihak lain menjadi lebih mudah dan cepat, akan tetapi membuka celah keamanan dalam pengiriman pesan tersebut. Untuk mengatasi masalah tersebut, maka salah satu cara yang dapat digunakan adalah kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan. Kriptografi adalah sebuah ilmu menyandikan dan mengacak suatu pesan untuk menjaga keamanan dari isi pesan tersebut. Kriptografi diperlukan untuk menghindari pihak yang tidak berhak mengetahui isi dari pesan yang dikirimkan tersebut. Dengan adanya kriptografi, isi dari pesan akan diacak sedemikian rupa menggunakan algoritma kriptografi tertentu sehingga akan menghasilkan sebuah pesan yang acak yang tidak dapat dibaca sebelum isi pesan yang sebenarnya kembali dimunculkan menggunakan algoritma kriptografi tersebut.

Pesan asli sebelum dienkripsi disebut *plain text*. Sedangkan pesan yang sudah diacak disebut *chipper text*. Proses pengubahan *plain text* menjadi *chipper text* disebut dengan enkripsi, sedangkan proses pengubahan *chipper text* kembali menjadi *plain text* disebut dengan dekripsi. Berikut ini disajikan bagan proses enkripsi dan dekripsi.




Gambar proses enkripsi dan dekripsi

Tujuan penggunaan kriptografi adalah dalam menjaga keamanan data dalam aspek- aspek berikut :

1. *Confidentiality* (kerahasiaan) : Menjaga isi informasi agar hanya dapat dilihat oleh pihak yang berhak.
2. *Data integrity* (integritas data) : Menjamin keaslian data selama pengiriman.
3. *Authentication* (otentikasi) : Mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4. *Non-repudiation* (penyangkalan): Mencegah entitas yang berkomunikasi melakukan penyangkalan, sehingga pengirim pesan tidak dapat menyangkal telah melakukan pengiriman pesan atau penerima pesan tidak dapat menyangkal telah menerima pesan.

Beberapa istilah dalam system sandi, yaitu:

1. Kriptologi adalah disiplin ilmu dalam sistem sandi.

2. Kriptografi adalah bagian dari kriptologi yang berhubungan dengan desain dan penerapan sandi rahasia.
3. Kriptanalisis dimaksudkan memecahkan sistem sandi.
4. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi.
5. Kunci menentukan sebuah transformasi khusus dari sekumpulan transformasi yang mungkin.

## B. Transformasi Caesar

Berikut ini akan dibahas sistem sandi rahasia berdasarkan aritmetika modular. Yang pertama berasal dari Julius Caesar. Dalam sistem ini, kita mulai dengan menerjemahkan huruf menjadi angka. Kita ambil huruf-huruf dalam alfabet standar dari huruf bahasa Inggris dan menerjemahkannya ke dalam bilangan bulat dari 0 sampai ke 25, seperti yang ditunjukkan pada Tabel 5.1 berikut.

Tabel 5.1 Konfersi huruf ke angka

| Huruf | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Angka | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Huruf | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Angka | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Sebuah *cipher*, yang digunakan oleh Julius Caesar, didasarkan pada substitusi di mana setiap huruf digantikan dengan huruf tiga bagian bawah abjad, dengan tiga huruf terakhir bergeser ke tiga huruf pertama dari alfabet. Untuk menggambarkan *cipher* ini menggunakan aritmetika modular, misalkan P sebagai bilangan yang ekuivalen dengan huruf dalam *plaintext* dan C sebagai bilangan yang ekuivalen dengan huruf pada *ciphertext*. Sehingga didapat :

$$C \equiv P + 3 \pmod{26}, 0 \leq C \leq 25$$

Berikut ini disajikan transformasi Caesar mengubah plain text menjadi chipper text pada tabel 5.2.

Tabel 5.2 enkripsi menggunakan transformasi Caesar

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Plaintext* | A | B | C | D | E | F | G | H | I | J | K | ... |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
| *Ciphertext* | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | ... |
| | D | E | F | G | H | I | J | K | L | M | N | ... |

**1. Proses enkripsi**

Untuk mengenkripsi sebuah pesan menggunakan transformasi Caesar, langkah-langkahnya sebagai berikut:

a. Mengelompokkan pesan menjadi 5 huruf.
b. Mengubah pesan menjadi bentuk angka dengan menggunakan tabel 5.1.
*c.* Menggunakan transformasi $C \equiv P + 3 \pmod{26}$ untuk memperoleh pesan *ciphertext*.
d. Setelah diperoleh hasil C, maka diterjemahkan kembali ke bentuk huruf.

**Contoh:**

Enkripsikan pesan : THIS MESSAGE IS TOP SECRET

**Jawab :**

Kita kelompokkan tiap blok berisi lima huruf, sehingga pesan akan berubah menjadi

THISM ESSAG EISTO PSECR ET

Mengubah huruf menjadi angka yang sesuai, kita peroleh

19 , 7 , 8 , 18, 12 4, 18, 18, 0, 6 4, 8, 18, 19, 14

15 , 18 , 4 , 2 , 17 4 , 19

Menggunakan transformasi Caesar $C \equiv P + 3\ (mod\ 26)$, angka-angka di atas berubah menjadi

22, 10, 11, 21, 15 7, 21, 21, 3, 9 7, 11, 21, 22, 17
18, 21, 7, 5, 20 7, 22

Menerjemahkan kembali ke huruf, kita diperoleh

WKLVP HVVDJ HLVWR SVHGU HW

Ini adalah pesan yang dikirim yang telah di enkripsi.

**2. Proses dekripsi**

Langkah- langkah untuk mendeskripsi pesan dari *cipher* Caesar sebagai berikut:

a. Mengelompokkan pesan menjadi 5 huruf.
b. Mengubah huruf menjadi bentuk angka (lihat tabel 5.1),
c. Menggunakan transformasi $P \equiv C - 3(Mod\,26)$ untuk memperoleh pesan *plaintext.*
d. Diperoleh *plaintext* dalam bentuk angka, kemudian angka diubah kembali menjadi huruf,
e. Susun huruf sehingga mempunyai arti.

**Contoh:**

Deskripsikan pesan:

WKLVL VKPZZ HGHFL SKHU

**Jawab :**

Untuk mendekripsikan pesan : WKLVL VKPZZ HGHFL SKHU

Pertama, kita ubah huruf menjadi angka yang sesuai, diperoleh

22, 10, 11, 21, 11 21, 10, 17, 25, 25 7, 6, 7, 5, 11
18, 10, 7, 20

Selanjutnya, melakukan transformasi $P \equiv C - 3(mod\,26)$ untuk mengubah menjadi *plaintext*, dan diperoleh

19, 7, 8, 18, 8     18, 7, 14, 22, 22     4, 3, 4, 2, 8   15, 7, 4 17

Lalu kita terjemahkan angka ini kembali ke huruf, dan diperoleh

THISI SHOWW EDECI PHER.

Dengan menggabungkan huruf-huruf menjadi kata yang sesuai, kita menemukan pesan yang dibaca sebagai berikut :

THIS IS HOW WE DECIPHER

## C.Transformasi Affine

*Cipher* Caesar adalah salah satu dari keluarga *cipher* serupa yang digambarkan oleh sifat transformasi pergeseran (*shift transformation).*

$$C \equiv P + k(mod\,26), 0 \leq C \leq 25$$

di mana *k* adalah kunci yang mewakili ukuran pergeseran huruf dalam alfabet. Ada 26 transformasi yang berbeda dari jenis ini, termasuk kasus *k = 0 (mod 26)*, di mana huruf tidak berubah, karena dalam hal ini $C \equiv P(mod\,26)$.

Secara umum dapat ditulis (5.1)

$$C \equiv aP + b(mod\,26), 0 \leq C \leq 25$$

dimana *k* menunjukkan seberapa banyak dilakukan pergeseran huruf dalam alfabet. Dimana *a* dan *b* adalah bilangan bulat dengan *(a, 26) = 1.* Ini disebut **Transformasi *Affine*.**

*Shift transformation* adalah transformasi *affine* dengan *a=1.* Mengharuskan *(a, 26) = 1,* sehingga *P* berjalan melalui sistem residu lengkap modulo 26, demikian juga dengan *C.* Ada $\Phi(26) = 12$ pilihan untuk *a,* dan 26 pilihan untuk *b,* sehingga totalnya ada $12 \times 26 = 312$ transformasi jenis ini.

1. **Proses enkripsi**

Langkah-langkah proses Transformasi Affine :

a. Mengelompokkan pesan menjadi 5 huruf.

b. Mengubah pesan menjadi bentuk angka dengan menggunakan tabel 5.1.
c. Menggunakan transformasi $C \equiv aP + b(mod 26), 0 \leq C \leq 25$
d. Setelah diperoleh hasil C, maka diterjemahkan kembali ke dalam bentuk huruf.

**2. Proses dekripsi**

Jika hubungan antara *plaintext* dan *ciphertext* dijelaskan oleh persamaan (5.1), maka invers dari hubungan tersebut adalah

$$P \equiv \bar{a}(C - b)(\text{mod } 26), 0 \leq P \leq 25$$

Dimana $\bar{a}$ merupakan invers dari *a (mod 26)* yang dapat ditemukan menggunakan konkruensi $\bar{a} \equiv a^{\phi(26)-1} = a^{11}(mod\ 26)$

Langkah-langkah dekripsi Transformasi Affine :

a. Mengelompokkan pesan menjadi 5 huruf.
b. Mengubah pesan menjadi bentuk angka dengan menggunakan tabel 5.1.
c. Menggunakan transformasi

$$P \equiv \bar{a}(C - b)(\text{mod } 26), 0 \leq P \leq 25$$

d. Setelah diperoleh hasil *P*, maka diterjemahkan kembali ke dalam bentuk huruf.

**Contoh:**

1. Misalkan *a=7* dan *b=10* dalam suatu *chiper affine* dengan $C \equiv aP + b(mod 26), 0 \leq C \leq 25$,

   Sehingga $C \equiv 7P + 10(mod 26)$

   Oleh karena itu, $P \equiv 15(C - 10) \equiv 15C + 6(mod 26)$.

   15 adalah invers dari 7 modulo 26.

Tabel 5.3. Transformasi affine $C \equiv 7P + 10 \pmod{26}$

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Plaintext* | A | B | C | D | E | F | G | H | I | J | K | ... |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
| *Ciphertext* | 10 | 17 | 24 | 5 | 12 | 19 | 0 | 7 | 14 | 21 | 2 | ... |
| | K | R | Y | F | M | T | A | H | O | V | C | ... |

Untuk menggambarkan bagaimana kita memperoleh hubungan tersebut, perhatikan bahwa huruf K pada *plaintext* setara dengan angka 10 yang kemudian dihubungkan sesuai dengan huruf C pada *ciphertext*, karena $7 \times 10 + 10 = 80 \equiv 2 \pmod{26}$ dan 2 adalah angka yang setara dengan huruf C.

2. Enkripsikan pesan:

PLEASE SEND MONEY

Kelompokkan pesan menjadi lima huruf, pesan menjadi
PLEAS ESEND MONEY
Mengubah huruf menjadi angka, selanjutnya menggunakan transformasi $C \equiv 7P + 10 \pmod{26}$, sehingga diperoleh
P = 15 maka C = 7. 15 + 10 = 115 ≡ 11 (mod 26 ), sehingga huruf P menjadi huruf L.
L = 11 maka C = 7. 11 + 10 = 87 ≡ 9 (mod 26), sehingga huruf L menjadi huruf J. Dan seterusnya dilakukan dengan cara yang sama. Sehingga di peroleh

LJMKG MGMXF QEXMW.

3. Dekripsikan pesan:

FEXEN ZMBMK JNHMG MYZMN

Menggunakan rumus P ≡ 15 C + 6 (mod 26 ) di peroleh
F = 5 maka P = 15. 5 + 6 = 81 ≡3 ( mod 26 ), sehingga huruf F menjadi huruf D.

$E = 4$ maka $P = 15.\ 4 + 6 = 66 \equiv 14 \pmod{26}$, sehingga huruf E menjadi huruf O. Dan seterusnya dilakukan dengan cara yang sama.

Menjadi

DONOT REVEA LTHES ECRET

atau pada *plaintext*

DO NOT REVEAL THE SECRET.

### 3. Teknik Langsung Transformasi *Affine*

Dalam upaya memecahkan *cipher* monografi, frekuensi huruf dalam *ciphertext* dibandingkan dengan frekuensi huruf pada teks berbahasa Inggris. Ini memberikan informasi mengenai kesesuaian antara huruf. Dalam perhitungan berbagai macam frekuensi pada teks *English*, salah satunya menemukan persentase yang terdapat dalam tabel 5.4 untuk kejadian ke-26 huruf.

Tabel 5.4 frekuensi kemunculan huruf dalam teks *English*

| Huruf | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Frekuensi(%) | 7 | 1 | 3 | 4 | 13 | 3 | 2 | 3 | 8 | <1 | <1 | 4 | 3 |
| Huruf | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Frekuensi(%) | 8 | 7 | 3 | <1 | 8 | 6 | 9 | 3 | 1 | 1 | <1 | 2 | <1 |

Dari tabel terlihat bahwa huruf yang paling sering muncul pada teks *English* adalah E, T, N, R, I, O dan A. Kita dapat menggunakan informasi ini untuk membedakan *chiper* yang mana pada sebuah transformasi *affine* yang telah digunakan untuk menulis pesan.

**Contoh :**

Misal telah kita ketahui sebuah pesan yang telah dienkripsikan. Tiap huruf telah ditransformasikan dengan korespondensi $C \equiv P + k\left(mod\, 26\right), 0 \leq C \leq 25$

Untuk mengkriptoanalisis *chiper*,

Dekripsikan pesan:

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDLR PD

Pertama-tama kita menghitung seberapa banyak huruf yang muncul dalam *chipertext*, yaitu:

| Huruf | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| frekuensi | 1 | 0 | 4 | 5 | 1 | 3 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| Huruf | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| frekuensi | 1 | 0 | 7 | 2 | 2 | 2 | 3 | 0 | 0 | 1 | 2 | 3 | 2 |

Dari tabel terlihat bahwa huruf yang paling sering muncul dalam *chipertext* adalah : P, C, D, F, T dan Y.

Huruf P menggambarkan huruf E karena berdasarkan Tabel 5.4, E adalah huruf yang paling sering muncul dalam teks *English*. Sehingga dapat ditulis :

Huruf P = 15 (*ciphertext*)

Huruf E = 4 (*plaintext*)

$C \equiv P + k \ (mod\ 26\ )$

$15 \equiv 4 + k(\text{mod } 26)$

$k \equiv 11 \ (\text{mod } 26).$

$C \equiv P + 11(\text{mod } 26)$

Dan $P \equiv C - 11(\text{mod } 26)$, maka didapatkan kesamaan

| *text per* | A | B | C | D | E | F | G | H | I | J | K | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *plaintext* | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | ... |
| | P | Q | R | S | T | U | V | W | X | Y | Z | ... |

Dari kesamaan ini maka:

YFXMP CESPZ CJTDF DPQFW QZCPY NTASP CTYRX PDDLR PD

sama dengan

NUMBE RTHEO RYISU SEFUL FOREN CIPHE RINGM ESSAG ES

atau

NUMBER THEORY IS USEFUL FOR ENCIPHERING MESSAGES.

Jika kita telah mencoba transformasi, namun menghasilkan bukan *plaintext* dan teks kacau, maka coba transformasi lain berdasarkan jumlah frekuensi huruf dalam *ciphertext*.

Transformasi *affine* dari bentuk $C \equiv aP + b(mod\ 26), 0 \leq C \leq 25$ digunakan dalam penerjemahan.

## VII. Rangkuman

1. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan.
2. Kriptografi adalah sebuah ilmu menyandikan dan mengacak suatu pesan untuk menjaga keamanan dari isi pesan tersebut.
3. Transformasi Caesar menggunakan transformasi $C \equiv P + 3(mod\,26)$ dan untuk memperoleh pesan *ciphertext* transformasi $P \equiv C - 3(Mod\,26)$ untuk memperoleh pesan *plaintext*.

4. Transformasi affine menggunakan rumus

$$C \equiv aP + b(mod\,26), 0 \leq C \leq 25$$

## VIII. Latihan Soal

1. Dekripsikan pesan *ciphertext* LFDPH LVDZL FRQTX HUHG yang telah dienkripsi menggunakan *cipher Caesar*.
2. Dekripsikan pesan RTOLK TOIK dengan menggunakan rumus $C \equiv 3P + 24\ (mod\ 26)$.

**Jawab:**

1. Dekripsikan LFDPH LVDZL FRQTX HUHG
   Mengubah huruf menjadi angka, kita memperoleh
   11 5 3 15 7 11 21 3 25 11 5 17 16 19 23
   7 20 7 6
   Menggunakan transformasi Caesar $P \equiv C - 3(mod\,26)$ ini menjadi
   8 2 0 12 4 8 18 0 22 8 2 14 13 16 20
   4 17 4 3
   Penerjemahan kembali ke huruf, diperoleh
   ICAME ISAWI CONQU ERED
   Atau
   I CAME I SAW I CONQUERED.
2. Mendekripsikan RTOLK TOIK
   Menggunakan rumus $C \equiv 3P + 24\ (mod\ 26)$
   Pertama, mengubah huruf menjadi angka, diperoleh
   17 19 14 11 10 19 14 8 10
   Selanjutnya, kita melakukan transformasi, untuk mengubah *plaintext*, dan diperoleh
   $C \equiv 3P + 24\ (mod\ 26)$
   Karena 9 adalah invers 3 modulo 26, maka
   $P \equiv 9(C - 24)\ (mod\ 26)$

$P \equiv 9C - 216 \ (\text{mod } 26)$

$P \equiv 9C + 18 \ (\text{mod } 26)$

Menggunakan transformasi $P \equiv 9C + 18 \ (\text{mod } 26)$ menjadi

Untuk 17

$P \equiv 9C + 18 \ (\text{mod } 26)$

$P \equiv 9(17) + 18 \ (\text{mod } 26)$

$P \equiv 171 \ (\text{mod } 26)$

$P \equiv 15 \ (\text{mod } 26)$

Jadi, 17= R setelah di transformasi menjadi 15 = P

Dengan cara yang sama, diperoleh

15 7 14 13 4     7 14 12 4

Menerjemahkan angka ini kembali ke huruf dan mengembalikan pesan *plaintext*, diperoleh

PHONE HOME

# DAFTAR PUSTAKA

Burton, D. M. 1980. Elementary Number Theory. Boston: Allyn and Bacon, Inc.

Koshy, Thomas. 2007. Elementary number theory with applications $2^{nd}$ ed. Burlington: Elsevier.

Rosen, K.H. 2011. Elementary Number Theory & its Application. 6th Ed. Boston: Pearson Education, Inc.

Sukirman. 2014. Teori Bilangan. Yogyakarta: FMIPA UNY

# BIOGRAFI PENULIS

**Margaretha Madha Melissa** lahir di Kulon Progo tanggal 15 Maret 1993. Penulis menyelesaikan studi Sarjana pada bidang Pendidikan Matematika di Universitas Negeri Yogyakarta tahun 2013, kemudian menyelesaikan studi program Pasca Sarjana di Universitas Negeri Yogyakarta pada bidang yang sama tahun 2015. Saat ini, penulis bekerja sebagai dosen tetap Program Studi Pendidikan Matematika di Universitas Sanata Dharma. Beberapa mata kuliah yang diampu yaitu Media dan Teknologi Pembelajaran Matematika, Psikologi Belajar dan Pembelajaran, Pembelajaran Matematika SMP, Pembelajaran Matematika SMA dan SMK, Desain Pembelajaran Matematika SMA dan SMK, dan Pengantar Teori Bilangan.

**Cyrenia Novella Krisnamurti** lahir di Yogyakarta, 1 November 1978. Lulus S1 Matematika Universitas Sanata Dharma, penulis melanjutkan studinya ke S2 Matematika Universitas Gadjah Mada bidang keahlian Aljabar. Banyak pengalaman kerja yang telah penulis alami antara lain Editor buku Matematika tingkat SMA/K. Data Analyst dan Auditor PT Gufo Garmen Indoneisa, Data Analyst PT. Citra Alda Mandiri , General Manager Area PT Elitestar Primajaya Gresik dan sebagai dosen tetap di Universitas Sanata Dharma.

# PENGANTAR TEORI BILANGAN

Buku ini dibagi ke dalam lima bab, yaitu (1) sistem bilangan, induksi matematik, dan teorema binomial, (2) keterbagian dan faktorisasi prima (3) kekongruenan dan persamaan diophantine, (4) sistem nurmerik dan fungsi tangga, dan (5) kriptologi. Selain itu, dalam buku ini dilengkapi dengan materi ajar, contoh-contoh soal, dan penyelesaiannya dengan maksud agar pembaca dapat lebih memahami materi. Dengan adanya soal evaluasi disertai dengan kunci jawaban, diharapkan juga dapat membantu pembaca dalam memperkaya jenis-jenis permasalahan-permasalahan terkait materi dalam teori bilangan dan diharapkan pembaca dapat belajar secara mandiri melalui buku ajar ini.

IKAPI
IKATAN PENERBIT INDONESIA
9 786235 312620