# KONSEP DASAR TEORI BILANGAN

Buku ini disusun bertujuan untuk memperluas ilmu pembaca tentang matematika abstrak khususnya konsep bilangan. Materi yang disajikan terdiri 10 BAB: Induksi Matematika Dan Binomial, Keterbagian, Basis Bilangan Bulat, Faktorisasi Bilangan Bulat, Kekongruenan, Teorema Fermat Dan Wilson Fungsi Aritmatik, Fungsi *Phi* Dan Teorema Euler, Akar Primitif Dan Indeks Residu Kuadratik. Semoga buku ini dapat memberikan wawasan yang lebih luas dan menjadi sumbangan pemikiran kepada pembaca khususnya. Pandangan dan saran juga diperlukan oleh penulis guna memperbaiki penulisan pada edisi selanjutnya agar buku ini dapat disempurnakan dengan baik dari waktu kewaktu.

INSIGHT MEDIATAMA

Zulkarnain

KONSEP DASAR TEORI BILANGAN

KONSEP DASAR TEORI BILANGAN

Zulkarnain


# KONSEP DASAR TEORI BILANGAN

Zulkarnain

# KONSEP DASAR TEORI BILANGAN

Penulis **: Zulkarnain**
Editor : **Misbahul Munir**
Desain Cover : **Muzammil Akbar**
Ilustrasi : **Freepik**

Ukuran: 21 x 29.7 cm; Hal: v + 164 (169)
Cetakan I, Agustus 2023
ISBN 978-623-8179-81-7

**Penerbit**
**Insight Mediatama**
Anggota IKAPI No. 338/JTI/2022
Watesnegoro No. 4 (61385) Mojokerto
Whatsapp 087762245559
www.insightmediatama.co.id

**© All Rights Reserved** Ketentuan Pidana Pasal 112-119 Undang-undang Nomor 28 Tahun 2014 Tentang Hak Cipta. Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit dan penulis.

# KATA PENGANTAR

Assallammualaikum wr.wb

Alhamdulillahhirrobilalamin, penulis panjatkan puja - puji syukur kehadirat Allah SWT, yang atas rahmat serta hidayah-Nya dapat menyelesaikan penyusunan buku "**Konsep Dasar Teori Bilangan**" ini dengan baik. Shalawat beriring salam semoga terlimpahkan kepada Nabi Muhammad SAW. Dalam penyusunan buku ini penulis menyampaikan ucapan terima kasih yang tidak terhingga, khususnya kepada kedua orang tua (Almarhum Fauzi Ismail dan Almarhummah Habiah Karim) dan Istri (Rusmiati) serta anak tercinta (Khaisan Hafiz Zulmi) yang tidak kenal lelah memberikan semangat dalam menyelesaikan buku ini.

Buku ini disusun bertujuan untuk memperluas ilmu pembaca tentang matematika abstrak khususnya konsep bilangan. Materi yang disajikan terdiri 10 BAB: Induksi Matematika Dan Binomial, Keterbagian, Basis Bilangan Bulat, Faktorisasi Bilangan Bulat, Kekongruenan, Teorema Fermat Dan Wilson Fungsi Aritmatik, Fungsi *Phi* Dan Teorema Euler, Akar Primitif Dan Indeks Residu Kuadratik. Semoga buku ini dapat memberikan wawasan yang lebih luas dan menjadi sumbangan pemikiran kepada pembaca khususnya. Pandangan dan saran juga diperlukan oleh penulis guna memperbaiki penulisan pada edisi selanjutnya agar buku ini dapat disempurnakan dengan baik dari waktu kewaktu.

Pontianak,  Agustus 2023

Zulkarnain

## DAFTAR ISI

**DAFTAR TABEL**

# BAB I

## INDUKSI MATEMATIKA DAN TEOREMA BINOMIAL

### A. Konsep Induksi Matematika

Induksi matematika merupakan materi yang menjadi perluasan dari logika matematika. Logika matematika sendiri mempelajari pernyataan yang bisa bernilai benar atau salah, ekuivalen atau ingkaran sebuah pernyataan, dan juga berisi penarikan kesimpulan. Induksi matematika menjadi sebuah metode pembuktian secara deduktif yang digunakan untuk membuktikan suatu pernyataan benar atau salah. Dimana merupakan suatu proses atau aktivitas berpikir untuk menarik kesimpulan berdasarkan pada kebenaran pernyataan yang berlaku secara umum sehingga pada pernyataan khusus atau tertentu juga bisa berlaku benar. Dalam induksi matematika, variabel dari suatu perumusan dibuktikan sebagai anggota dari himpunan bilangan asli. Dengan kata lain, induksi matematika hanya untuk membuktikan kebenaran suatu pernyataan matematika yang berhubungan, tidak untuk menemukan suatu rumus baru.

Induksi matematika adalah salah satu sifat penting dari bilangan bulat positif. Untuk memahami metode induksi matematika, simak pernyataan berikut ini: Misalkan $P(n)$ adalah sifat yang didefinisikan untuk suatu bilangan asli $n$, dan misalkan pula $a$ merupakan suatu bilangan asli tertentu. Jika terdapat dua pernyataan berikut bernilai benar, maka:

1. $P(a)$ bernilai benar.
2. Untuk sebarang bilangan asli $k \geq a$, apabila $P(k)$ bernilai benar, maka $P\ (k + 1)$ juga bernilai benar.

Jika bagian 1 dan bagian 2 terpenuhi pernyataan untuk sembarang bilangan asli $n \geq a$, $P(n)$ bernilai benar.

Secara ringkas Langkah - langkah metode induksi matematika sebagai berikut:

1. Membuktikan bahwa rumus atau pernyataan tersebut benar untuk n = 1.
2. Mengasumsikan bahwa rumus atau pernyataan tersebut benar untuk n = k.
3. Membuktikan bahwa rumus atau pernyataan tersebut benar untuk n = k + 1.

Untuk menerapkan induksi matematika, syaratnya harus bisa menyatakan pernyataan P (k + 1) ke dalam pernyataan P(k) yang diberikan. Untuk menyatakan persamaan P (k + 1), substitusikan kuantitas k + 1 kedalam pernyataan P(k).

## B. Jenis – Jenis Induksi Matematika

Ada berbagai macam permasalahan matematis yang dapat diselesaikan dengan menggunakan metode induksi matematika. Oleh sebab itulah, metode induksi matematika dibedakan menjadi tiga jenis di antara adalah deret, pembagian dan pertidaksamaan. Berikut penjelasannya.

### 1. Deret

Menurut KKBI Deret merupakan sususan yang teratur dalam bentuk garis lurus. Pada induksi matematika deret ditemui dalam bentuk penjumlahan yang beruntun. Untuk menyelesaikan persoalan induksi matematika berbentuk deret harus dibuktikan kebenarannya pada suku pertama, suku ke $k$ serta terakhir suku ke (k +1). Pada jenis deret, ada beberapa hal yang perlu diperhatikan dengan saksama. Antara lain adalah sebagai berikut:

Apabila

(i) $P(n) : u_1 + u_2 + u_3 + \cdots + u_n = S_n,$ Jika $n = 1$ maka $P(1) : u_1 = S_n$

(ii) $P(k) : u_1 + u_2 + u_3 + \cdots + u_k = S_k$

(iii) $P(k+1) : u_1 + u_2 + u_3 + \cdots + u_k + u_{k+1} = S_{k+1}$

**Contoh 1.1**

**Buktikan bahwa 1 + 2 + 3 + …+ $(2n - 1)$= $n^2$, untuk masing-masing dari $n$ bilangan asli.**

**Penyelesaian:**

1 + 2 + 3 + …+ …+ $(2n - 1)$= $n^2$

Langkah 1: tunjukkan n = 1 benar

$2n - 1 = n^2$

$2 (1) – 1 = 1^2$

1 = 1 (terbukti)

Langkah 2: asumsikan, n = k

$1 + 2 + 3 + … + (2k - 1) = k^2$

Langkah 3: asumsikan, n = k + 1

$1 + 2 + 3 + …+ (2n - 1) = n^2$

$1 + 2 + 3 +…+ (2k – 1) + 2 (k +1) – 1 = (k + 1)^2$

$1 + 2 + 3 + … + (2k – 1) + 2 k + 2 – 1 = (k + 1)^2$

$1 + 2 + 3 + … + (2k – 1) + 2 k + 1 = (k + 1)^2$

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

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

$(k + 1)^2 = (k + 1)^2$ **(terbukti)**

**Contoh 1.2**

**Buktikan bahwa $1^2+ 2^2+ \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ untuk masing-masing dari $n$ bilangan asli.**

**Penyelesaian:**

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

Langkah 1: tunjukkan n = 1 benar

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

$(1)^2 = \frac{1.(1+1)(2.1+1)}{6}$

$1 = \frac{1.2.3}{6}$

1 = 1 (terbukti)

Langkah 2: asumsikan, n = k

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

Langkah 3: asumsikan, n = k + 1

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

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

$1^2 + 2^2+ \dots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$

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

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

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

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

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

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

$\frac{(k+1)(k+2)(2k+3)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$ **(terbukti)**

**Contoh 1.3**

**Buktikan bahwa $1 + 2 + 3 + \dots + n = \frac{n}{2}(n+1)$ untuk masing-masing dari $n$ bilangan asli.**

**Penyelesaian:**

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

Langkah 1: tunjukkan n = 1 benar

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

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

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

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

1 = 1 (terbukti)

Langkah 2: asumsikan, n = k

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

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

Langkah 3: asumsikan, n = k + 1

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

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

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

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

$k^2 + k + 2k + 2 = k^2 + 3k + 2$

$k^2 + 3k + 2 = k^2 + 3k + 2$ **(terbukti)**

**Contoh 1.4**

**Buktikan bahwa 2 + 4 + 6 + … + 2n = n (n +1) untuk masing-masing dari *n* bilangan asli.**

**Penyelesaian:**

$2 + 4 + 6 + \ldots + 2n = n(n+1)$

Langkah 1: tunjukkan n = 1 benar

$2n = n(n+1)$

$2.1 = 1(1+1)$

$2 = 1.\ 2$

2 = 2 (terbukti)

Langkah 2: asumsikan, n = k

$2 + 4 + 6 + \ldots + 2n = n(n+1)$

$2 + 4 + 6 + \ldots + 2k = k(k+1)$

Langkah 3: asumsikan, n = k + 1

$2 + 4 + 6 + \ldots + 2n = n(n+1)$

$2 + 4 + 6 + \ldots + 2k + 2\ (k+1) = (k+1)\ ((k+1)+1)$

$2 + 4 + 6 + \ldots + 2k + 2k + 2 = (k+1)\ (k+2)$

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

$k^2 + k + 2k + 2 = k^2 + 3k + 2$

$k^2 + 3k + 2 = k^2 + 3k + 2$ **(terbukti)**

**Contoh 1.5**

**Buktikan bahwa $5 + 7 + 9 + \ldots + (2n+3) = n^2 + 4n$ untuk masing-masing dari $n$ bilangan asli.**

**Penyelesaian:**

$5 + 7 + 9 + \ldots + (2n+3) = n^2 + 4n$

Langkah 1: tunjukkan n = 1 benar

$2n + 3 = n^2 + 4n$

$2.1 + 3 = 1^2 + 4.\ 1$

5 = 5 (terbukti)

Langkah 2: asumsikan, n = k

$5 + 7 + 9 + \ldots + (2n+3) = n^2 + 4n$

$5 + 7 + 9 + \ldots + (2k+3) = k^2 + 4k$

Langkah 3: asumsikan, n = k + 1

$5 + 7 + 9 + \ldots + (2n+3) = n^2 + 4n$

$5 + 7 + 9 + \ldots + (2k+3) + (2\ (k+1) + 3) = (k+1)^2 + 4\ (k+1)$

$k^2 + 4k + 2k + 2 + 3 = k^2 + 2k + 1 + 4k + 4$

$k^2 + 6k + 5 = k^2 + 6k + 5$ **(terbukti)**

**Latihan 1.1**

a) Buktikan bahwa $4 + 6 + 8 + \ldots + (2n+2) = n^2 + 3n$ untuk masing-masing dari $n$ bilangan asli.

b) Buktikan bahwa $2 + 5 + 8 + \ldots + (3n-1) = \frac{n}{2}(3n+1)$ untuk masing-masing dari $n$ bilangan asli.

**2. Pembagi**

Jenis induksi matematika pembagian dapat dijumpai pada berbagai macam soal yang menggunakan kalimat yaitu: (1) A habis dibagi dengan B; (2) B faktor dari A; (3) B membagi A dan (4) A adalah kelipatan dari B. Keempat ciri tersebut, menjadi petunjuk bahwa pernyataan tersebut dapat diselesaikan dengan menggunakan induksi matematika jenis pembagian. Hal-hal yang perlu diingat ialah apabila bilangan A habis dibagi dengan B, maka A =B .M dengan

M adalah bilangan bulat Maka, jika p habis dibagi a serta q habis dibagi a, sehingga (p + q) juga akan habis dibagi a. Contohnya adalah, 4 habis dibagi 2 dan 6 habis dibagi 2, maka (4 + 6) pun akan habis dibagi dengan bilangan 2

**Contoh 1.6**

**Buktikan bahwa $7^n - 2^n$ terbagi habis oleh 5 untuk setiap bilagan asli n**

**Penyelesain:**

$7^n - 2^n$ terbagi habis oleh 5 untuk setiap bilagan asli n

Langkah 1: tunjukkan n = 1 benar

$7^n - 2^n = 7^1 - 2^1 = 5$ habis dibagi 5 (benar)

Langkah 2: asumsikan, n = k

$7^k - 2^k = 5p$ dengan p sebarang bilangan asli

Langkah 3: asumsikan, n = k + 1

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7^k.7^1 - 2^k .2^1 \\ &= 7^k.7^1 - 2^k .2^1 - 2^k .7^1 + 2^k .7^1 \\ &= 7^k.7^{\,1} - 2^k .7^1 - 2^k.2^1 + 2^k .7^1 \\ &= 7\,(7^k - 2^k) + 2^k\,(7 - 2) \\ &= 7.5P + 2^k\,(7 - 2) \\ &= 7.5P + 2^k.\,5 \end{aligned}$$

Karena 7.5P dan $2^k$. 5 habis terbagi 5 maka terbukti bahwa $7^n - 2^n$ terbagi habis oleh 5 untuk setiap bilangan asli n

**Contoh 1.7**

**Buktikan $11^n - 4^n$ terbagi habis oleh 7 untuk setiap bilagan asli n**

**Penyelesaian:**

Langkah 1: tunjukkan n = 1 benar

$11^n - 4^n = 11^1 - 4^1 = 7$ habis dibagi 7 (benar)

Langkah 2: asumsikan, n = k

$11^k - 4^k = 7p$ dengan p sebarang bilangan asli

Langkah 3: asumsikan, n = k + 1

$$\begin{aligned} 11^{k+1} - 4^{k+1} &= 11^k.11^1 - 4^k .4^1 \\ &= 11^k.11^1 - 4^k .4^1 + 4^k.11^1 - 4^k.11^1 \\ &= 11^k.11^1 - 4^k.11^1 + 4^k.\,11^1 - 4k\,.4^1 \\ &= 11\,(11^k - 4^k) + 4^k\,(11 - 4) \\ &= 11.\,7P + 4^k\,7 \end{aligned}$$

Karena 11.7 P dan $4^k$. 7 habis terbagi 7 maka terbukti bahwa $11^n - 4^n$ terbagi habis oleh 7 untuk setiap bilagan asli n

**a. Buktikan n (n + 1) habis dibagi 2?**

**Penyelesaian:**

Langkah 1: tunjukkan n = 1 benar

n (n + 1) = 1 (1 +1) = 1. 2 = 2, habis dibagi 2 (benar)

Langkah 2: asumsikan, n = k

n (n + 1) = k (k +1) = $k^2$ + k = 2p dengan p sebarang bilangan asli

Langkah 3: asumsikan, n = k + 1

n (n + 1) = (k+1) ((k+1) +1))

= (k+1) (k + 2)

= $k^2$ + 2k + k + 2

= $k^2$ + k + 2k + 2

= 2p + 2 (k + 1)

Karena 2P dan 2 (k + 1) masing – habis terbagi 2 maka terbukti bahwa n (n + 1) habis dibagi 2 untuk setiap bilangan asli n

**Contoh 1.8**

**Buktikan $5^{2n-1}$ habis dibagi 2**

**Penyelesaian:**

Langkah 1: tunjukkan n = 1 benar

$5^{2n-1} = 5^{2.1-1} = 5^1 = 5$, habis dibagi 5 (benar)

Langkah 2: asumsikan, n = k

$5^{2k-1}$ = 5p dengan p sebarang bilangan asli

Langkah 3: asumsikan, n = k + 1

$5^{2n-1} = 5^{2(k+1)-1}$

$= 5^{2k+2-1}$

$= 5^{2k} 5^1$

$= 5^{2k}. 5^1. 5^{-1} 5^1$

$= 5^{2k-1}. 5^2$

= 25(5p) habis terbagi 5

Karena 25(5p) terbagi 5 maka terbukti bahwa $5^{2n-1}$ habis dibagi 5 untuk setiap bilagan asli n

**Latihan 1.2**

a) Buktikan $6^n - 2^n$ terbagi habis oleh 4 untuk setiap bilangan asli n

b) Buktikan $5^n - 3^n$ terbagi habis oleh 2 untuk setiap bilangan asli n

c) Buktikan $11^n - 6$ terbagi habis oleh 5 untuk setiap bilangan asli n

d) Buktikan $2^{4n-1}$ terbagi habis oleh 8 untuk setiap bilangan asli n

e) Buktikan $n^3 + 2n$ terbagi habis oleh 3 untuk setiap bilangan asli n

**3. Pertidaksaman**

Selain menggunakan tiga (3) langkah metode induksi matematika yang telah dijelaskan sebelumnya. induksi matematika berbentuk pertidaksamaan menggunakan sifat transitif. Konsep transitit yang dimaksud jika a berhubungan dengan b, dan b berhubungan dengan c, maka a berhubungan dengan c secara langsung. Sebagai contoh, relasi dua transitif. Misalnya untuk 5, 6, dan 7, berlaku $5 < 6$, $6 < 7$, dan $5 < 7$. Untuk lebih jelas, perhatikan konsep berikut

a. $a > b > c$ maka $a > c$ atau

$a < b < c$ maka $a < c$ atau

b. $a < b$ dan $c > 0$ maka $ac < bc$ atau

$a > b$ dan $c > 0$ maka $ac > bc$

c. $a < b$ maka $a+c < b + c$ atau

$a > b$ maka $a+c > b + c$

**Contoh 1.9**

**Buktikanlah bahwa $n + 5 \leq n^2$ untuk setiap bilangan asli $n \geq 6$**

**Penyelesaian:**

$5n + 5 \leq n^2$ untuk setiap bilangan asli $n \geq 6$

Langkah 1: tunjukkan n = 6 benar

$5 (6) + 5 \leq 6^2$

$30 + 5 \leq 36$

$35 \leq 36$ (terbukti)

Langkah 2: asumsikan, n = k

$5n + 5 \leq n^2$

$5k + 5 \leq k^2$

Langkah 3: asumsikan, n = k + 1

$5n + 5 \leq n^2$

$5(k+1) + 5 \leq (k+1)^2$

$5k + 5 + 5 \leq (k+1)(k+1)$

$5k + 10 \leq k^2 + 2k + 1$

Pembuktian:

$5k + 5 \leq k^2$

$5k + 5 + 5 \leq k^2 + 5$

$5k + 10 \leq k^2 + 5$ (kanan)

$5k + 10 \leq k^2 + 2k + 1 - 2k + 4 \leq k^2 + 2k + 1$

$5k + 10 \leq k^2 + 2k + 1$ **bernilai benar (terbukti)**

**Contoh 1.10**

**Buktikanlah bahwa $2^n - 3 \geq 2^{n-2}$ untuk setiap bilangan asli n $\geq 5$**

**Penyelesaian:**

Langkah 1: tunjukkan n = 5 benar

$2^n - 3 \geq 2^{n-2}$

$2^5 - 3 \geq 2^{5-2}$

$32 - 3 \geq 2^3$

$29 \geq 8$

Langkah 2: asumsikan, n = k

$2^n - 3 \geq 2^{n-2}$

$2^k - 3 \geq 2^{k-2}$

Langkah 3: asumsikan, n = k + 1

$2^n - 3 \geq 2^{n-2}$

$2^{k+1} - 3 \geq 2^{k+1-2}$

$2^{k+1} - 3 \geq 2^{k-1}$

**Pembuktian**

$(2^k - 3) \geq 2^{k-2}$ $\qquad\qquad$ $2^{k+1} = 2^k . 2^1$

$2^1(2^k - 3) \geq 2^1 2^{k-2}$

$2^1 2^k - 6 \geq 2^{1+k-2}$

$2^{k+1} - 6 \geq 2^{k-1}$

$2^{k+1} - 3 - 3 \geq 2^{k-1}$

$2^{k+1} - 3 \geq 2^{k+1} - 3 - 3 \geq 2^{k-1}$

$2^{k+1} - 3 \geq 2^{k-1}$ **bernilai benar (terbukti**

**Contoh 1.11**

**Buktikanlah bahwa $n^3 + 20 \geq n^2 + 15n$ untuk n > 3**

**Penyelesaian:**

Langkah 1: tunjukkan n = 4 benar

$n^3 + 20 \geq n^2 + 15n$

$4^3 + 20 \geq 4^2 + (15.4)$

$64 + 20 \geq 16 + 60$

$84 \geq 76$ (terbukti)

Langkah 2: asumsikan, n = k

$n^3 + 20 \geq n^2 + 15n$

$k^3 + 20 \geq k^2 + 15k$

Langkah 3: asumsikan, n = k + 1

$n^3 + 20 \geq n^2 + 15n$

$(k+1)^3 + 20 \geq (k+1)^2 + 15(k+1)$

$(k+1)\ (k+1)\ (k+1) + 20 \geq (k+1)\ (k+1) + 15(k+1)$

$(k^2 + 2k + 1)\ (k+1) + 20 \geq k^2 + 2k + 1 + 15k + 15$

$k^3 + k^2 + 2k^2 + 2k + k + 1 + 20 \geq k^2 + 17k + 16$

$k^3 + 3k^2 + 3k + 21 \geq k^2 + 17k + 16$

**Pembuktian**

$k^3 + 20 \geq k^2 + 15k$

$k^3 + 20 + 3k^2 + 3k + 1 \geq k^2 + 15k + 3k^2 + 3k + 1$

$k^3 + 3k^2 + 3k + 21 \geq 4k^2 + 18k + 1$

$k^3 + 3k^2 + 3k + 21 \geq k^2 + 17k + 16 + 3k^2 + k - 15 \geq k^2 + 17k + 16$

$k^3 + 3k^2 + 3k + 21 \geq k^2 + 17k + 16$ **bernilai benar (terbukti)**

**Latihan 1.3**

a) $n^2 > n + 1$ untuk setiap bilangan asli $n \geq 2$

b) $(n+1)^2 < n^3$ untuk setiap bilangan asli $n \geq 3$

c) $2n + 1 < 2^n$ untuk setiap bilangan asli $n \geq 3$

## C. Teorema Binomial

**Teorema 1.1**

Jika ($r \leq n$) maka $\binom{n}{r} = \binom{n}{n-r}$

**Pembuktian:**

Mengingat kembali konsep kombinasi dari sejumlah r objek yang diambil dari n objek. Banyaknya kombinasi dari r objek yang diambil dari n objek (r ≤ n) adalah

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

**Contoh 1.12**

1. Misalkan, ada 5 objek, yaitu a, b, c, d dan e. Apabila dari 5 objek ini diambil 3 objek maka banyaknya cara pengambilan 3 objek tersebut adalah

   $$\binom{5}{3} = \frac{5!}{2!\ 3!} = \frac{1.2.3.4.5}{(1.2)(1.2.3)} = 10 \text{ cara}$$

   Sepuluh cara pengambilan itu adalah abc, abd, abe, acd, ace, ade, bcd

2. Misalkan, dalam suatu kotak terdapat 3 kelereng merah dan 4 kelereng putih. Apabila kita mengambil 3 kelereng merah dari dalam kotak tersebut maka banyaknya cara pengambilan ada

   $$\binom{3}{3} = \frac{3!}{0!\ 3!} = \frac{1.2.3}{1.(1.2.3)} = 1 \text{ cara}$$

   Akan tetapi, apabila kita mengambil 3 kelereng dari dalam kotak itu maka banyaknya cara pengambilan ada

   $$\binom{7}{3} = \frac{7!}{4!\ 3!} = \frac{7.6.5.4!}{4!\,(1.2.3)} = 35 \text{ cara}$$

   Jika kita mengambil 4 kelereng dari dalam kotak tersebut maka banyaknya cara pengambilan ada

   $$\binom{7}{4} = \frac{7!}{3!\ 4!} = \frac{7.6.5.4!}{(1.2.3).\,4!} = 35 \text{ cara}$$

3. Misalkan, ada tiga kotak yang masing-masing berisi satu bola merah dan satu bola putih. Dari tiap-tiap kotak diambil satu bola sehingga terambil tiga bola. Banyaknya cara pengambilan 3 bola tersebut, agar terambil bola merah semua ada $\binom{3}{3} = 1$ cara. Banyaknya cara pengambilan 3 bola tersebut, agar terambil dua bola merah ada $\binom{3}{2} = 3$ cara. Banyaknya cara pengambilan 3 bola itu, agar terambil satu bola merah ada $\binom{3}{1} =$ 3 cara. Banyaknya cara pengambilan 3 bola itu, agar tak terambil bola merah ada $\binom{3}{0} =$ 1 cara.

Contoh terakhir ini akan digunakan untuk menyatakan suku banyak yang merupakan penjabaran dari $(m+p)^3$. Perpangkatan ini dapat dinyatakan sebagai perkalian berulang dengan 3 faktor sama, yaitu

(m + p) (m + p) (m + p) = mmm + mmp + mpm + pmm + ppm + pmp + mpp + ppp

Setiap suku dari ruas kanan kesamaan ini terdiri dari 3 faktor dan masing-masing faktor berturut-turut diambil dari faktor pertama, faktor kedua dan faktor ketiga dari ruas pertama. Memperhatikan Contoh 3 di atas maka:

banyaknya suku dengan tiga m adalah $\binom{3}{3} = 1$

banyaknya suku dengan dua m ada $\binom{3}{2} = 3$

banyaknya suku dengan satu m ada $\binom{3}{1} = 3$

banyaknya suku tanpa m ada $\binom{3}{0} = 1$

Pada kesamaan terakhir itu jika suku-suku sejenisnya dijumlahkan maka diperoleh:

$$(m+p)^3 = m^3 + 3m^2p + 3mp^2 + p^3$$

Koefisien-koefisien suku-suku dari ruas kanan dari kesamaan terakhir ini dapat dinyatakan dengan kombinasi-kombinasi banyaknya m dalam tiap sukunya sehingga kesamaan itu dapat ditulis sebagai berikut:

$$(p+m)^3 = \binom{3}{0}p^3 + \binom{3}{1}mp^2 + \binom{3}{2}m^2p + \binom{3}{3}m^3$$

Dengan argumentasi yang mirip dengan ilustrasi di atas, kita dapat menuliskan kesamaan-kesamaan berikut ini. Coba periksalah kebenarannya!

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

$$(a+x)^2 = \binom{2}{0}a^2 + \binom{2}{1}ax + \binom{2}{2}x^2$$

$$(a+x)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2x + \binom{3}{2}ax^2 + \binom{3}{3}x^3$$

$$(a+x)^4 = \binom{4}{0}a^4 + \binom{4}{1}a^3x + \binom{4}{2}a^2x^2 + \binom{4}{3}ax^3 + \binom{4}{4}x^4$$

$$(a+x)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}x + \binom{n}{2}a^{n-2}x^2 + \cdots + \binom{n}{k}a^{n-k}x^k + \cdots + \binom{n}{n}x^n$$

Kesamaan-kesamaan tersebut baru merupakan dugaan karena kesamaan- kesamaan itu, khususnya kesamaan terakhir diperoleh dengan penalaran induktif. Maka, kesamaan itu perlu dibuktikan kebenarannya. Kita akan membuktikan kebenaran kesamaan tersebut, tetapi kita perlu beberapa persiapan berikut ini.

Dari rumus kombinasi di atas, yaitu:

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

Kita dapat memahami bahwa:

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

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

Teorema 1.1 ini sering disebut sifat simetrik dari koefisien binomial. Sifat ini membantu kita untuk menghitung lebih mudah nilai suatu kombinasi.

**Contoh 1.13**

1. $\binom{20}{18} = \binom{20}{2} = \frac{20.19}{1.2} = 190$
2. $\binom{20}{18} = \binom{20}{2} = \frac{20.19}{1.2} = 190$

**Teorema 1.2**

Jika k dan r bilangan-bilangan asli dengan k > r maka

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

**Pembuktian:**

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

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

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

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

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

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

Sekarang kita siap untuk membuktikan kebenaran penjabaran suku dua berpangkat n di atas dengan mengambil a = 1 dan x = a, yang selanjutnya disebut Teorema Binomial.

**Teorema 1.3 (Teorema binomial)**

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}a + \binom{n}{2}a^2 + \binom{n}{3}a^3 + \cdots + \binom{n}{k}x^k + \cdots + \binom{n}{n}a^n$$

untuk setiap bilangan asli n.

Pembuktian: Induksi Matematika

(1) Untuk n = 1 maka $(1+x)^1 = \binom{0}{1} + \binom{0}{1} a = 1 + a$, benar

(2) Diasumsikan bahwa pernyataan benar untuk $n = k, yaitu$:

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

Selanjutnya, akan ditunjukkan benar untuk $n = k + 1$

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

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

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

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

Dari langkah – langkah (1) dan (2) dapat disimpulkan bahwa teorema terbukti benar untuk setiap bilangan asli n.

Koefisien – koefisien a pada ruas kanan pada teorema 1.3 disebut koesifien binomial.

**Contoh 1.14**

1. Koefisien $x^9$ dari penjabaran $(1+x)^{12}$ adalah $\binom{12}{9} = \frac{12.11.10}{1.2.3} = 660$
2. Koefisien $x^8$ dari penjabaran $(1+x)^{11}$ adalah $\binom{11}{3} = \frac{11.10.9}{1.2.3} = 165$

**Teorema 1.4**

Jika n.suatu bilangan asli maka

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

Pembuktian:

Apabila pada teorema binomial tersebut a = 1 maka diperoleh kesamaan

$$(1+x)^n = \binom{n}{0} + \binom{n}{1} a + \binom{n}{2} a^2 + \binom{n}{3} a^3 + \cdots + \binom{n}{k} x^k + \cdots + \binom{n}{n} a^n$$

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

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

**Teorema 1.5:**

Jika n, m dan k bilangan-bilangan asli dengan n > k > m maka

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

**Pembuktian:**

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

$$\binom{n}{k}\binom{k}{m} = \frac{n!}{(n-m)!\,m!}.\frac{(n-m)!}{(n-m-k+m)!\,(k-m)!}$$

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

**Contoh 1.15**

Suatu perkumpulan terdiri dan 15 orang. Akan dibentuk suatu pengurus dari perkumpulan tersebut yang terdiri 5 orang dan 2 orang di antaranya sebagai pengurus inti.

Maka, banyaknya pilihan pengurus itu adalah:

**Penyelesaian:**

$$\binom{15}{5}\binom{5}{2} = \frac{15.14.13.12.11}{1.2.3.4.5}.\frac{5.4}{1.2} = 30030$$

Pemilihan tersebut dapat pula dilakukan dengan memilih 2 orang pengurus inti dan 15 orang dan selanjutnya untuk melengkapi pengurus itu dipilih 3 orang dan 13 orang (yang 2 orang telah terpilih sebagai pengurus inti).

Maka, banyaknya pilihan pengurus ini adalah:

$$\binom{15}{5}\binom{13}{3} = \frac{15.14}{1.2}.\frac{13.12.11}{1.2.3} = 30030$$

Tampak di sini bahwa

$$\binom{15}{2}\binom{5}{2} = \binom{15}{2}\binom{13}{3}$$

**Teorema 1.6**

Jika n dan k bilangan-bilangan asli dengan n > k maka

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

**Pembuktian:**

Pada Teorema 1.5 tersebut, apabila m = 1 maka diperoleh:

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

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

# BAB II

## RELASI KETERBAGIAN

### A. Konsep Dasar Relasi Keterbagian

Bilangan semesta dalam teori bilangan adalah himpunan semua bilangan bulat. Bilangan – bilangan bulat dinyatakan dengan huruf – huruf latin kecil $a, b, c, \dots, m, n,$ dan sebagainya yang dapat bernilai positif, negative, atau nol. Namun, banyak pembahasan dalam teori bilangan yang semesta terbatas pada himpunan semua bilangan asli.

**Definisi 2.1**

Bilangan bulat $a$ membagi (habis) $b$ (ditulis $a| b$). Apabila ada suatu bilangan bulat $k$, sedemikian hingga $b = ka$ . Jika a tidak membagi (habis) a, maka ditulis $a \nmid b$

**Contoh 2.1**

a) $6 | 48$ sebab ada bilangan bulat, yaitu 6, sedemikian hingga 6.8 = 48

b) $2 | 18$ sebab ada bilangan bulat, yaitu 9, sedemikian hingga 2.9 = 18

c) $-4 | 20$ sebab ada bilangan bulat, yaitu – 5, sedemikian hingga $(-4).(-5) = 20$

d) $6 \nmid 20$ sebab ada bilangan bulat $k$, sedemikian hingga $8k = 27$

Bilangan bulat $k$ pada definisi 2.1 tersebut adalah tunggal sebab apabila ada bilangan bulat $m$. Selain $k$ sedemikian hingga $b = ma$ dan $b = ka$ maka $ma = ka$ sehingga $m = k$.

Jika $a = 0$ dan $b \neq 0$ maka tidak ada bilangan bulat $k$ sehigga $b = ka$. Namun, jika $a = 0$ dan $b = 0$, $k$ tidak tunggal agar berlaku $b = ka$.

Istilah “membagi habis” dan “terbagi habis” berturut – turut disingkat menjadi “membagi” dan “terbagi”. Pernyataan "$a$" membagi "$b$" dan "$b$" terbagi "$a$". Keduanya ditulis "$a$"|"$b$". Istilah – istilah lain yang mempunyai arti sama dengan $a|b$ adalah "$a$" adalah faktor dari "$b$". "$a$" adalah pembagi dari "$b$" atau "$b$" ialah kelipatan dari "$a$".

Apabila $a|b$ adalah $k$ bilangan - bilangan bulat dengan $a \neq 0$ dan $b$ dan $b = ka$ disebut hasil bagi dari $b$ oleh $a$, disebut pula bahwa $k$ adalah faktor dari $b$ yang menjadi komplemen (sekawan) dari $a$ atau dengan singkat dikatakan bahwa $a$ dan $k$ adalah pembagi – pembagi sekawan (komplementer) dari $b$.

**Latihan 2.1**

a. $51| 17 = \dots$

b. $3 | 11 = \dots$

c. $-7 | 84 = \dots$

**Teorema 2.1**

Jika $a|b$ dan $b|c$ maka $a|c$

**Pembuktian:**

Apabila $a|b$ menurut definisi 2.1 ada bilangan bulat $k$ sehingga $b = ka$. Jika diketahui pula $b|c$, ada bilangan bulat $c = mb$. Oleh karena $b = ka$ dan $c = mka$ sehingga menurut definisi 2.1 diperoleh $a|c$. Hal ini relasi keterbagian pada himpunan bilangan bulat mempunyai sifat transitif

**Teorema 2.2**

Jika $a|b$ maka $a|mb$ untuk setiap bilangan bulat $m$

**Pembuktian:**

Apabila $a|b$ yaitu a membagi habis b, maka a membagi habis setiap kelipatan b, yaitu a | mb, untuk setiap bilangan bulat m.

**Teorema 2.3**

Apabila $a|b$ dan $a|c$ maka a | (b + c), a | (b – c) dan a | bc.

**Pembuktian:**

Apabila a | b dan a | c, menurut definisi 2.1, maka diperoleh b = ka dan c = ma untuk bilangan-bilangan bulat k dan m. Dari dua kesamaan ini dapat diperoleh bahwa:

(i) b + c = (k + m) a berarti a | (b + c)

(ii) b – c = (k – m) a berarti a | (b – c) dan

(iii) b c = (kma) a berarti a | bc

**Teorema 2.4**

Apabila a | b dan a | c maka a | (mb + nc) untuk setiap bilangan bulat m dan n.

**Pembuktian:**

Karena a | b dan a | c, menurut teorema 2.2 maka a | mb dan a | nc untuk setiap bilangan-bilangan bulat m dan n. selanjutnya, menurut teorema 2.3, maka a | (mb + nc).

**Teorema 2.5**

(i) a | a untuk setiap bilangan bulat a (sifat reflektif).

(ii) Jika a | b maka ma | mb untuk setiap bilangan bulat m.

(iii) Jika ma | mb dengan m ≠ 0, maka a | b.

(iv) 1| a dan a | 0

(v) Jika 0 | a maka a = 0 (nol hanya membagi nol)

(vi) Jika a | b dengan b ≠ 0, maka | a | ≤ | b |

(vii) Jika a | b dengan b | a, maka | a | = | b |

## B. Faktor Persekutuan Terbesar (FPB)

Semua faktor bilangan bulat positif dari 30 adalah 1, 2, 3, 5, 6, 10, 15, dan 30. Sedangkan semua faktor bulat positif dari 45 adalah 1, 3, 5, 9, 15, dan 45. Maka faktor-faktor persekutuan (pembagi-pembagi bersama) dari 30 dan 45 adalah 1, 3, 5. Dan faktor persekutuan terbesar 30 dan 45 adalah 5.

Secara umum, pengertian tentang faktor persekutuan dari dua bilangan bulat dituliskan sebagai definisi berikut ini:

**Definisi 2.2**

Jika a dan b adalah bilangan-bilangan bulat, maka bilangan bulat disebut faktor persekutuan dari a dan b jika dan hanya jika d | a dan d | b.

Karena 1 adalah pembagi (faktor) dari setiap bilangan bulat, maka 1 adalah faktor persekutuan dari a dan b. Jadi himpunan faktor persekutuan dari a dan b tidak pernah kosong.

Setiap bilangan bulat, kecuali nol selalu membagi nol, sehingga jika a = b = 0, maka setiap bilangan bulat merupakan faktor persekutuan dari a dan b. Dalam hal ini, himpunan semua faktor persekutuan bulat positif dari a dan b merupakan himpunan tak hingga.

Apabila sekurang-kurangnya satu dari a dan b tidak sama dengan nol, maka himpunan semua faktor persekutuan bulat positif a dan b merupakan himpunan berhingga. Sehingga mesti ada anggota dari himpunan tersebut yang terbesar dan disebut faktor persekutuan terbesar (FPB) dari a dan b. secara formal, hal tersebut dinyatakan sebagai definisi berikut ini.

**Definisi 2.3**

Jika a dan b bilangan-bilangan bulat yang sekurang-kurangnya satu di antaranya tidak sama dengan nol, maka faktor persekutuan terbesar (FPB) dari a dan b ditulis "(a, b)" adalah suatu bilangan bulat positif d yang memenuhi

(i) d | a dan d | a, serta

(ii) Jika e | a dan e | b, maka e ≤ d.

Dari definisi tersebut dapat dimengerti bahwa jika (a, b) = d, maka d ≥ 1. Dan apabila ada faktor persekutuan lain, misalnya e, maka e ≤ d.

**Contoh 2.2**

Faktor bulat positif dari −12 adalah 1, 2, 3, 4, 6, 12.

Faktor bulat positif dari 30 adalah 1, 2, 3, 5, 6, 10, 15, 30.

Maka faktor persekutuan yang positif dari −12 dan 30 adalah 1, 2, 3, 6.

Jadi faktor persekutuan terbesar dari −12 dan 30 adalah 6, atau dapat ditulis secara singkat (12, 30) = 6.

**Latihan 2.2**

Tunjukkan bahwa $(-5, 5) = 5$; $(8, 15) = 1$; $(8, -36) = 4$; $(-6, -42) = 6$.

**Teorema 2.6**

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

**Pembuktian:**

Misalkan (a:d, b:d) = c, maka $c \geq 1$ dan c | (a : d) dan c | (b : d).

c | (a:d) maka ada bilangan bulat m, sehingga a : d = m c atau a = m c d.

c | (b:d) maka ada bilangan bulat n, sehingga b : d = n c atau b = n c d.

Karena a = m c d dan b = n c d, maka cd adalah faktor persekutuan dari a dan b. Karena (a, b) = d, maka $cd \leq d$, yaitu $c \leq 1$, sebab d suatu bilangan bulat positif. Karena $c \geq 1$ dan $c \leq 1$, maka c = 1.

**Definisi 2.4**

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.**

**Teorema 2.7**

Jika a dan b bilangan-bilangan bulat dengan a > 0, maka ada dengan tunggal pasangan bilangan-bilangan bulat q dan r yang memenuhi: b = q a + r, dengan $0 \leq r < a$.

**Keterangan:**

Bilangan-bilangan bulat q dan r dalam teorema itu berturut-turut disebut hasil bagi dan sisa dalam pembagian b oleh a.

**Pembuktian:**

Dibentuk himpunan S = {b – xa: x bilangan bulat dan $b - xa \geq 0$}. S bukan himpunan kosong sebab jika $x = -|b|$ dan karena a > 0, maka $(b-xa) \notin S$. Karena S beranggotakan bilangan bilangan bulat tak negatif berbentuk (b – xa), maka S pasti memiliki anggota terkecil, misalkan r. Sesuai dengan bentuk anggota dari S, maka r = b – qa, untuk suatu bilangan bulat q dan $r \geq 0$. Selanjutnya akan ditunjukkan bahwa r < a.

Andaikan $r \geq a$, maka r = a + k dengan $k \geq 0$. Jadi k = r – a, karena r = b – qa, maka k = b – qa – a = b – (1 + q) a. Ini berarti bahwa k adalah suatu anggota dari S. Tetapi $0 \leq k = r - a < r$. hal ini tidak mungkin, karena r adalah bilangan bulat tak negatif yang terkecil dalam S. Oleh kerena itu, pengadaian tersebut harus diingkar. Jadi r < a. Sehingga ada q dan r sedemikian sehingga b = qa + r dengan $0 \leq r < a$.

Selanjutnya kita akan menunjukkan ketunggalan dari q dan r. Misalkan bahwa b mempunyai dua representasi, yaitu:

$$b = aq + r = aq^* + r^* \text{ dengan } 0 \leq r < a \text{ dan } 0 \leq r^* < a.$$

maka r – r* = a (q – q). sehingga a | r – r*.

Jika r –r* ≠ 0 maka a ≤ | r – r* |, merupakan suatu kontradiksi.

Jadi r – r* = 0 dan q* - q = 0, sehingga r = r* dan q = q*.

Berdasarkan pembuktian tersebut, maka teorema tersebut dapat diperluas untuk a < 0, sehingga diperoleh akibat sebagai berikut:

Jika a dan b bilangan-bilangan bulat dengan b ≠ 0, maka ada dengan tunggal pasangan bilangan-bilangan bulat q dan r sedemikian hingga

$$b = aq + r \text{ dengan } 0 \leq r < |a|$$

Untuk membuktikan akibat ini, cukup memperhatikan untuk a yang negatif maka |a| > 0, sehingga teorema menghasilkan pasangan bilangan-bilangan bulat yang tungggal q dan r memenuhi:

$$b = aq + r \text{ dengan } 0 \leq r < |a|$$

Perhatikan bahwa |a| = -a dan mengambil q* = q, untuk mendapatkan

$$b = aq + r \text{ dengan } 0 \leq r < |a|$$

Sebagai ilustrasi, jika a = 21 dan b = 75, maka q = 3 dan r = 12, yaitu: 75 = 3.21 + 12.

Terlihat bahwa (75, 210 = (21, 12) = 3.

**Teorema 2.8**

Jika b = aq + r, maka (b,a) = (a, r).

**Keterangan:**

aq = hasil bagi r = sisa

**Pembuktian:**

Misalkan (b,a) = d dan (a, r) = c, maka kita akan menunjukkan bahwa c = d. Karena (b,a) = d, maka d | b dan d | a, dan karena b = aw + r, maka d|r. Dari d|a dan d|r, maka d adalah faktor persekutuan dari a dan r. Selanjutnya, karena (a, r) = c maka c|a dan c|r dank arena b = aq + r, maka c|b. Dari c|a dan c|b, maka c adalah faktor persekutuan dari a dan b. Tetapi karena (a, b) = d, maka d ≥ c. Dari d ≤ c dan d ≥ c, maka c = d, yaitu (b,a) = (a,r)

**Contoh 2.3**

Carilah FPB dari

1. (5767, 4453)

Penyelesaian:

Gunakan algoritma pembagian (teorema 2.8)

5767 = 1. 4453 + 1314, maka (5767, 4453) = (4453, 1314)

4453 = 3. 1314 + 511, maka (4453, 1314) = (1314, 511)

1314 = 2. 511 + 292, maka (1314, 511) = (511, 292)

511 = 1. 292 + 73, maka (511, 292) = (292, 73)

292 = 4. 73 + 0, maka (292, 73) = (73, 0) = 73

Jadi (5767, 4453) = 73

2. (247, 299)

Penyelesaian:

299 = 247.1 + 52

247 = 52.4 + 39

52 = 39.1 + 13

39 = 13.3 + 0

Jadi (247, 299) = 13

3. (9800,180)

Penyelesaian:

9800 = 180.54 + 80

180 = 80.2 + 20

80 = 20.4 + 0

Jadi (9800,180) = 20

**Latihan 2.3**

Tentukan FPB dari:

a. 10587 dan 534

b. 6409 dan 3556

c. 12345 dan 9999

d. 1525 dan 425

e. 457962 dan 1200

**Teorema 2.9**

Apabila a dan b bilangan-bilangan bulat tidak nol, maka ada bilangan-bilangan bulat x dan y sedemikian hingga

$$ax + by = (a, b).$$

**Pembuktian:**

Dibentuk himpunan S, yaitu himpunan semua kombinasi linier dari a dan b yang bernilai positif.

$$S = \{au + bv: u,v \text{ bulat dan } au + bv > 0 \}$$

S bukan himpunan kosong sebab jika $a > 0$ dan $u = 1$ dengan $v = 0$ maka $a \in S$ dan jika $a < 0$, dengan $u = -1$ dan $v = 0$, maka $|a| \in S$. Karena S memuat bilangan-bilangan bulat positif,

maka S memuat anggota yang terkecil, misalnya d. Karena d € S, maka ada bilangan - bilangan bulat x dan y sehingga ax + by = d.

Faktor persekutuan terbesar dari a dan b dapat dinyatakan sebagai kombinasi linier dari a dan b, yaitu bentuk ax + by dengan x dan y bilangan-bilangan bulat tertentu.

Misalnya:

$(-12, 30) = 6 = (-12).\ 2 + 30.1$

$(8, 15) = 1 = 8.\ 2 + 15.\ (-1)$

$(8, -36) = 4 = 8.\ 5 + (-36).\ 1$

$(-6, -42) = 6 = (-6).\ (-8) + (-42).\ 1$

Selanjutnya, akan ditunjukkan bahwa (a, b) = d. Perhatikan a dan d, menurut algoritma pembagian, maka ada bilangan-bilangan bulat q dan r sedemikian hingga

$$a = qd + r \text{ dengan } 0 \leq r < d$$

$$r = a - qd = a - q\ (ax + by)$$

$$r = a\ (1 - qx) + b\ (-qy)$$

Karena r > 0 dan r merupakan kombinasi linier dari a dan b, maka r € S. Hal ini bertentangan dengan fakta nahwa d adalah anggota terkecil dari S (ingat bahwa $0 \leq r < d$). Jadi r = 0, sehingga a = qd atau d | a. Dengan penalaran yang sama diperoleh d | b. Sehingga d adalah faktor prsekutuan dari a dan b.

Selanjutnya, jika c adalah sebarang faktor persekutuan dari a dan b, yaitu c | a dan c | b, maka c | ax + by, atau c | d, sehingga $c \leq d$. Ini berarti bahwa d = (a, b). Bukti teorema 2.9 tersebut hanya merupakan bukti eksistensi dan tidak memberikan cara mencari nilai-nilai x dan y. Hal ini akan dibahas kemudian. Sesuai dengan teorema 2.9 tersebut, apabila (a, b) = 1, maka ada bilangan-bilangan bulat x dan y sedemikian hingga ax + by = 1.

**Teorema 2.10**

Apabila a dan b dua bilangan bulat tidak nol, maka a dan b saling prima jika dan hanya jika ada bilangan-bilangan bulat x dan y yang memenuhi ax + by = 1.

**Pembuktian:**

Misalkan bahwa (a, b) = d, maka d | a dan d | b, sehingga menurut teorema 2.10 didapat d | (ax + by) atau d | 1. Karena $d \geq 1$, maka d = 1.

**Contoh 2.4**

1. Hitunglah (247, 299) dan tentukan bilangan-bilangan bulat m dan n yang memenuhi 247m + 299 n = (247, 299).

   Penyelesaian:

   299 = 247. 1 + 52

   247 = 5. 4 + 39

   52 = 39. 1 + 13

   39 = 13. 3

   Jadi (247, 299) = 13

   13 = 52 – 39 .1

   = 52 – (247 − 52. 4)

   = 52. 5 – 247

   = (299 – 247). 5 – 247

   13 = 299. 5 + 247 (− 6)

   Jadi m = - 6 dan n = 5

2. Hitunglah (963, 657) dan tentukan bilangan-bilangan bulat p dan q yang memenuhi

   Penyelesaian

   963 p + 657 q = (963, 657)

   963 = (1.657) + 306

   657 = 2. 306 + 45

   306 = 6. 45 + 36

   45 = 1. 36 + 9

   36 = 4.9

   Jadi (963, 657) =9

   9= 45 – 36

   = 45 – (306 – 6 x 45)

   = 7.45 – 306

   = 7 (657 – 2.306) −306

   = 7.657 – 15.306

   = 7.657 – 15 (963 – 657)

   = 22.657 – 15.963

   P= −15, q = 22

## C. Persamaan Linear Diophantine

Persamaan Diophantine adalah persamaan aljabar dalam satu atau lebih variabel dengan koefisien bilangan bulat, yang bertujuan mencari solusi bulatnya.

**Teorema 2.11**

Misalkan a dan b bilangan – bilangan bulat dengan (a, b) = d. Jika d ∤ c. Maka persamaan linear Diophatus $ax + by$ tidak mempunyai. Jika d|c, maka persamaan tersebut mempunyai takhingga solusi. Selanjutnya, jika $x = x_0$ dan $y = y_0$ adalah penyelesaian khusus dari persamaan itu, maka semua penyelesaian dari persamaan itu adalah

$$x = x_0 + \frac{b}{d}.t \; dan \; y = y_0 - \frac{a}{d}\,t$$

**Keterangan:**

d = FPB (a,b)

$(x_0, y_0) = solusi\ khusus$

k = variable baru yang harus di isi untuk mendapat persamaan khusus yang di inginkan;

k anggota bilangan bulat

**Pembuktian:**

Misalkan d = (a, b) dan $(x_0, y_0)$ adalah solusi dari ax + by = c. Maka a$x_0$ + b$y_0$ = c. Karena d = (a, b) maka d membagi habis a dan b. Karena d membagi habis a dan b maka d juga membagi habis a $x_0$ + b$y_0$ = c. Akitnya d membagi habis c.

Misalkan d membagi habis c. Maka c = dk untuk suatu k bilangan bulat. Karena d = (a, b) maka terdapat bilangan bulat r dan t sehingga ar + bt = d. Perhatikan bahwa

ar + bt = d

ar k + bt k = dk

ark + btk = c

a(rk) + b(tk) = c

Karena rk dan tk adalah bilangan bulat, maka x = rk dan y = tk adalah solusi persamaan linear Diophantine ax + by = c

Misalkan ($x_0$, $y_0$) adalah solusi khusus dari persamaan ax+by = c dan (x′, y′) adalah solusi lain dari ax + by = c. Maka

$$ax' + by' = ax_0 + by_0$$

Dengan membagi kedua ruas dengan d, dipeoleh

$$\frac{a}{d}x' + \frac{b}{d}y' = \frac{a}{d}x_0 + \frac{b}{d}y_0$$

yang ekuivalen dengan

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

Karena d = (a, b) maka

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Berdasarkna $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$ maka $\frac{a}{d}$ membagi habis $\frac{b}{d}(y_0 - y')$. Karena $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ maka $\frac{a}{d}$ membagi habis $(y_0 - y')$. Oleh karena itu, terdapat bilangan bulat n sedemikian hingga

$$y_0 - y' = \frac{a}{d}n$$

atau

$$y' = y_0 - \frac{a}{d}n$$

dengan mensubtitusikan $y_0 - y' = \frac{a}{d}n$ ke persamaan $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$ diperoleh

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}\frac{a}{d}(y_0 - y')$$

Karena $\frac{a}{d} \neq 0$ maka

$$(x' - x_0) = \frac{b}{d}n$$

Atau

$$x' = x_0 + \frac{b}{d}n$$

Sehingga untuk solusi (x', y') persamaan linear Diophantine terdapat n $\in \mathbb{Z}$

Sedemikian sehingga

$$x = x_0 + \frac{b}{d}.t \; dan \; y = y_0 - \frac{a}{d}\,t$$

**Contoh 2.5**

Tentukan penyelesaian persamaan linear Diophantine berikut:

1. 33x + 63 y = 23 dengan x dan y elemen bilangan bulat!

**Penyelesaian:**

algoritma pembagian

63 = 1. 33+ 30

33 = 1.30 + 3

30 = 3.10 + 0

(33, 63) = 3

Karena 3 tidak habis dibagi membagi 23 maka tidak ada solusi bilangan bulat (x, y) yang memenuhi

2. 36x + 21y = 18 dengan x dan y elemen bilangan bulat!

**Penyelesaian:**

Algoritma pembagian

36 = 21. 1 + 15

21 = 15. 1 + 6

15 = 6. 2 + 3

6 = 2. 3 + 0

(36, 21) = 3

Karena 3 habis dibagi membagi 18 maka ada solusi bilangan bulat (x, y) yang memenuhi

Selanjutnya dari kesamaan – kesamaan tersebut disusun sebagai berikut:

3 = 15 – 6. 2

= 15 – (21 – 15) .2

= 15 – 21.2 + 15.2

= 15.3 – 21.2

= (36 – 21). 3 – 21.2

= 36.3 – 21.3 – 21.2

= 36.3 – 21.5

3 = 36 (3) + 21 (−5)

Nilai konstanta pada soal adalah 18 maka kedua ruas dikalikan 6, sehingga diperoleh

3. (6) = 36 (3) (6) + 21 (−5) (6)

18 = 36 (18) + 21 (− 30)

Ini berarti $x_0$ = 18 dan $y_0$ = − 30 merupakan solusi dari soal tersebut disebut penyelesaian khusus.

Kesamaan terakhirnya dapat diubah sebagai berikut:

$x = x_0 + \frac{b}{d}.t = 18 + \frac{21}{3}.t = 18 + 7t$

$y = y_0 - \frac{a}{d}\,t = -30 - \left(\frac{21}{3}\right)t = -30 - 7t$

Jadi penyelesaian persamaan linear Diophantine $x = 18 + 7t$ dan $y = -30 - 7t$

3. 56x + 22y = 124 dengan x dan y elemen bilangan bulat!

**Penyelesaian:**

Pertama cari nilai dari FPB (56,22) menggunakan algoritma Euclid (pembagian)

FPB (56, 22)

56 = 2. (22) + 12 $\qquad$ 12 = 56 – 2(22)

22 = 1. (12) + 10 $\qquad$ 10 = 22 −12

12 = 1. (10) + 2 $\qquad$ 2 = 12 −10

10 = 5. (2) + 0

FPB (6, 4) = 2

Karena 2 | 124, maka persamaan 56x + 22y =124 memiliki solusi bilangan bulat.

Gunakan pembalikan algoritma Euclid:

2 = 12 – 10

2 = 12 – (22 – 12)

2 = 12 − 22 + 12

2 = 2 (12) – 22

2 = 2(56 – 2.22) – 22

2 = 56(2) – 4 .22 – 22

2 = 56(2) – 22 (5)

2 = 56(2) + (22) (−5)

Kalikan dengan 62 agar bentuknya sama dengan persamaan pada soal:

124 = 56 (124) + 22(−310)

Maka, $x_0$ = 124 dan $y_0$ = −310

Tulis yang sudah diketahui dan dihasilkan dari perhitungan

Solusi umumnya kita tentukan dengan cara:

a = 56 b = 22 d = 2 $x_0$ = 124 $y_0$ = − 310

$$x = x_0 + \frac{b}{d}.k$$

$$x = 124 + \frac{22}{2}.k$$

$$x = 124 + 11.k$$

$$y = y_0 - \frac{a}{d}\,k$$

$$y = -310 - \frac{56}{2}\,k$$

$$y = -310 - 28\,k$$

Pembuktian:

$x = 124 + 11.k$ dan $y = -310 - 28\,k$

Misal: k = 0 (k sebarang)

Diperoleh:

$x = 124 + 11.0$ dan $y = -310 - 28.0$

$x = 124$ dan $y = -310$

Subtitusikan nilai x dan y kepersamaan linear Diophantine

56x + 22y =124

56 (124) + 22 ( $-310$) = 124

6944 – 6820 = 124

124 = 124 **(terbukti benar)**

**Teorema 2.12**

Jika a | bc dan (a, b) = 1, maka a | c.

**Pembuktian:**

Misalkan: 8 | 24 dan 6 | 24 maka tidak benar bahwa 8.6 | 24. Tetapi apabila diberi tambahan ketentuan bahwa (a, b) = 1, maka dapat disimpulkan bahwa ab | c. Pembuktiannya adalah karena (a, b) = 1, menurut teorema 2.10 tersebut, maka ada bilangan-bilangan bulat x dan y sedemikian hingga:

ax + by = 1

Jika kedua ruas dikalikan c, maka diperoleh persamaan:

acx + bcy = c Pers (1)

Karena a | c dan b | c maka ada bilangan-bilangan bulat r dan t sedemikian hingga c = ar dan c = bt. Sehingga pers (1) menjadi:

abtx + abry = c

ab (tx + ry) = c

Ini berarti bahwa ab | c. Uraian tentang akibat dari teorema 2.10 tersebut dinyatakan sebagi berikut: Akibat: Jika a | c dan b | c dengan (a, b) = 1, maka ab | c.Apabila diketahui bahwa a | bc, apakah kita dapat menyimpulkan bahwa a | c atau a | c ? Diambil sebagai contoh: 6| (3.4) maka tidak benar apabila mengambil kesimpulan bahwa 6 | 3 ataupun 6 | 4. Tetapi apabila a | bc ditambah ketentuan (a, b) = 1, maka kita dapat menyimpulkan bahwa a | c. Hal ini ditujukkan sebagai berikut:

Karena (a, b) = 1, maka ada bilangan-bilangan bulat x dan y sedemikian hingga:

ax + by =1

Jika kedua ruas dari persamaan ini dikalikan dengan c maka diperoleh:

$$acx + bcy = c$$

Karena a | bc dan a | ac maka a | (acx + bcy) atau a | c.

## D. Kelipatan Persekutuan Kecil (KPK)

Di sekolah dasar dan lanjutan telah mempelajari kelipatan persekutuan terkecil (KPK). Misalnya, kelipatan bulat positif dari 3 adalah 3, 6, 9, 12, 15, 18, …

Kelipatan bulat positif dari 4 adalah 4, 8, 12, 16, 20, 24, 28, …

Maka kelipatan persekutuan terkecil dari 3 dan 4 adalah 12, 24, 36, 48,

Selanjutnya istilah "kelipatan bulat positif" hanya dikatakan lebih singkat menjadi "kelipatan" saja. Selanjutnya secara umum pengertian kelipatan persekutuan dari dua bilangan bulat dinyatakan dalam definisi berikut ini.

**Definisi 2.5**

Misalkan a dan b adalah bilangan-bilangan bulat. m adalah kelipatan persekutuan dari a dan b jika dan hanya jika a | m dan b | m.

Nol (0) adalah suatu kelipatan persekutuan dari a dan b. ab dan – ab masing-masing juga merupakan suatu kelipatan persekutuan dari a dan b. Jadi himpunan semua kelipatan persekutuan bulat positif dari a dan b tidak pernah sama dengan himpunan kosong.

Himpunan semua kelipatan bulat positif dari 6 adalah {6, 12, 18, 24, …}.

Himpunan semua kelipatan bulat positif dari $-9$ adalah {9, 18, 27, 36, …}.

Jadi himpunan semua kelipatan persekutuan dari 6 dan $-9$ adalah {18, 36, 54, 72, …}. Sehingga kelipatan persekutuan terkecil dari 6 dan $-9$ adalah 18.

Ingat bahwa dalam himpunan bagian dari himpunan bilangan-bilangan bulat positif selalu mempunyai anggota terkecil. Sehingga KPK dari setiap dua bilangan bulat selalu ada.

Secara formal, KPK dari dua bilangan bulat didefinisikan sebagai berikut:

**Definisi 2.6**

Kelipatan persekutuan terkecil (KPK) dari dua bilangan bulat tidak nol a dan 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 $m \leq c$.

Dalam definisi ini dapat dimengerti bahwa kelipatan dari setiap dua bilangan bulat yang tidak no; selalu merupakan suatu bilangan bulat positif. Dalam (i) pada definisi itu mengatakan bahwa masing-masing dari dua bilangan itu membagi kelipatan persekutuan terkecilnya.

Sedangkan (ii) mengatakan bahwa kelipatan persekutuan lainnya tidak lebih kecil dari KPK dari dua bilangan itu.

**Contoh 2.6**

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

Kelipatan persekutuan yang lain, misalnya 48, 72, 96, … masing-masing lebih besar dari 24.

Perhatikan pada contoh tersebut, yaitu himpunan semua kelipatan persekutuan bulat positif fari 6 dan -9 adalah {18, 36, 54, 72, …} dan KPK dari 6 dan -9 adalah 18 atau ditulis [6, -9] = 18. Tampak di sini bahwa semua kelipatan persekutuan dari 6 dan -9 selalu terbagi oleh 18. Hal ini dapat dikatakan bahwa setiap kelipatan persekutuan dari dua bilangan bulat selalu terbagi oleh KPK dari dua bilangan tersebut. Hal ini dinyatakan sebagai teorema berikut ini.

**Teorema 2.13**

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] | c.

**Pembuktian:**

Misalkan [a, b] = m, maka harus ditunjukkan bahwa m | c. Andaikan m | c, maka menurut logaritma pembagian, ada bilangan-bilangan bulat q dan r sedemikan hingga:

$$c = qm + r \text{ dengan } 0 < r < m$$

Karena c adalah kelipatan persekutuan dari a dan b, maka a | c dan b | c. Karena [a, b] = m maka a | m dan b | m. a | m maka a | qm dan a | c, maka a | (c – qm). Ini berarti a | r. Demikian pula b | m maka b | qm dank arena b | c, maka b | (c – qm). Berarti b | r. Karena a | r dan b | r maka r adalah kelipatan persekutuan dari a dan b. Tetapi karena [a, b] = m dan 0 < r < m, maka hal tersebut tidak mungkin (kontradiksi). Jadi pengandaian di atas tidak benar, berarti m | c atau [a, b] | c.

**Teorema 2.14**

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

**Pembuktian:**

Misalkan [a, b] = d, maka a | d dan b | d, sehingga ac | dc dan bc | dc. Hal ini berarti dc adalah kelipatan persekutuan dari ac dan bc. Dan merupakan teorema 2.12, maka [ac, bc] | dc. Karena [ac, bc] adalah suatu kelipatan dari ac, maka [ac, bc] adalah suatu kelipatan dari c. Misalkan [ac, bc] = mc maka mc | dc, sehingga m | d. Karena [ac, bc] = mc, maka ac | mc dan bc | mc, sehingga a | m dan b | m, dan menurut teorema 2.12, maka [a, b] | m, yaitu d | m dank arena m | d, maka d = m. Sehingg dc = mc, yaitu c[a, b] = [ac, bc].

**Contoh 2.7**

1. [105, 45] = [ 15.7, 15.3]
   [105, 45] = 15 [7, 3]
   [105, 45] = 15. 21
   [105, 45] = 315
2. [18, 30] = [6.3, 6.5]
   [18, 30] = 6 [3, 5]
   [18, 30] = 6. 15
   [18, 30] = 90

**Teorema 2.15**

Jika $a$ dan $b$ bilangan – bilangan bulat yang keduanya positif, maka

(a, b) [a, b] = ab

**Pembuktian:**

Jelas bahwa ab adalah suatu kelipatan persekutuan dari a dan b, menurut teorema 2.12, maka [a, b] | ab. Di lain pihak, menurut akibat dari teorema 2.10, karena a | [a, b] dan b | [a, b] dengan (a, b) = 1, maka ab | [a, b] dank arena [a, b] | ab, maka disimpulkan [a, b] = a

**Contoh 2.8**

(1) Karena (16,20) = 4 dan [16, 20] = 80, terdapat hubungan (16,20) [16, 20] = 4. 80 = 16. 20
(2) Karena (25 ,18) = 1 dan [25, 18] = 450, terdapat hubungan (25 ,18) [25, 18] = 1.450 = 25.18

# BAB III
## BASIS BILANGAN BULAT

Lambang bilangan bulat adalah dengan notasi decimal (basis sepuluh). Lambang bilangan bulat yang digunakan dalam basis sepuluh adalah 1, 2, 3, 4, 5, 6, 7, 8, 9.

Contoh:

$4275 = 4.\ 10^3 + 2.\ 10^2 + 7.\ 10^1 + 5.\ 10^0$

**Teorema 3.1**

Misalkan b suatu bilangan 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 tidak negative, $a_j$ suatu bilangan bulat dengan

$$0 \leq a_j \leq b - 1 \text{ untuk } j = 1, 2, \ldots, \text{dengan } a_k \neq 0$$

Keterangan: n dituliskan dalam basis b

Pembuktian:

Untuk memperoleh representasi dari $n$ seperti yang diinginkan, menerapkan algoritma pembagian sebagai berikut:

*Pertama:* membagi $n$ dengan $b$ untuk mendapatkan

$$n = bq_o + a_o,\ \ 0 \leq a_o \leq b - 1$$

Jika $q_o \neq 0$ membagi $q_o$ dengan $b$ dan mendapatkan bahwa

$$q_o = bq_1 + a_1,\ \ 0 \leq a_1 \leq b - 1$$

Lanjutkan proses ini untuk memperoleh seperti berikut:

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

$$q_2 = bq_3 + a_3,\ \ 0 \leq a_3 \leq b - 1$$

$$\vdots$$

$$q_{k-2} = bq_k - 1 + a_k - 1,\ \ 0 \leq a_{k-1} \leq b - 1$$

$$q_{k-1} = b.0 + a_k, \ldots \ \ 0 \leq a_k \leq b - 1$$

Langkah terakhir dari proses ini terjadi apabila memperoleh hasil bagi 0 dengan hasil bagi yang memenuhi bentuk berikut:

$$n > q_o > q_1 > q_2 \ldots \geq 0$$

Karena barisan $q_o, q_1, q_2, ...$ adalah suatu barisan turun dari bilangan bulat tak negatif. Barisan ini akan berakhir pada suku 0. Selanjutnya, dari persamaan pertama $q_o$ disubtitusikan dalam persamaan kedua dan diperoleh berikut ini,

$$= bq_o + a_o$$
$$= b(bq_1 + a_1) + a_o$$
$$= b^2q_1 + ba_1 + a_o$$

Proses subtitusi dilanjutkan untuk $q_1, q_1, q_{3,}$ ... dan diperoleh seperti berikut:

$$n = b^3q_2 + b^2a_2 + ba_1 + a_o$$
$$n = b^4q_3 + b^3a_3 + b^2a_2 + ba_1 + a_o$$
$$\vdots$$
$$n = a_kb^k + a_{k-1}b^{k-1} + \cdots + a_2b^2 + a_1b + a_o$$

$0 \leq a_j \leq b - 1$ untuk $j = 0, 1, 2, \ldots, k$ dan $a_i \neq 0$ karena $a_k = q_{k-1}$ adalah hasil bagi terakhir yang tidak sama dengan 0 persamaan tersebut terbukti.

**Contoh 3.1**

Misalkan $b$ = 5 sebagai basis penulisan maka lambang dasarnya adalah 0, 1, 2, 3, 4. Misalkan suatu bilangan bulat $n$ dinyatakan sebagai:

$$n = 3.\ 5^4 + 2.\ 5^3 + 0.\ 5^2 + 1.\ 5^1 + 4$$

Maka itu, dalam basis 5, $n$ tersebut ditulis sebagai $n = 32014_5$.

Jika $n$ ingin ditulis sebagai basis decimal (sepuluh) lakukan dengan mehitung jumlahan dari perpangkatan lima tersebut, yaitu:

$$n = 3.\ 5^4 + 2.\ 5^3 + 0.\ 5^2 + 1.\ 5^1 + 4$$
$$n = 3.\ 625 + 2\ .125 + 0.\ 25 + 1.\ 5 + 4$$
$$n = 1875 + 250 + 9$$
$$n = 2134_{10}$$

Jika ingin menulis lambing bilangan $n$ tersebut dalam basis lainnya, misalnya basis 8. Gunakan seperti proses pembuktian teorema sebelumnya (algoritma pembagian), yaitu:

a = bq + r

$2134_{10}$ = 8. 266 + 6

$2134_{10}$ = 8. (8.33 + 2) + 6

$2134_{10}$ = 8 .8 .33 + 8. 2 + 6

$2134_{10}$ = $8^2$.33 + 8.2 + 6

$2134_{10}$ = $8^2$ (8.4 + 1) + 8.2 + 6

$2134_{10}$ = $8^2$. 8.4. + $8^2$ .1 + 8.2 + 6

$2134_{10} = 8^3. 4 + 8^2 .1 + 8.2 + 6$

$2134_{10} = 4126_8$

Ini berarti $2134_{10} = 4126_8$

Jadi jika diurutkan dari basis 5, basis 10 dan basis 8 secara berturut – turut dapat dituliskan $32014_5 = 2134_{10} = 4126_8$

**Catatan:**

Penulisan lambang bilangan dengan basis 10 tidak perlu ditulis indeks 10 seperti $2134_{10}$, cukup ditulis 2134.

Berdasarkan teorema 3.1, setiap bilangan bulat positif dapat ditulis dalam basis 2 yaitu n = $a_k\ 2^k + a_{k-1}\ 2^{k-1} + a_{k-2}\ 2^{k-2} + ... + \ a_1\ 2 + a_0$ dengan $a_i$ adalah 0 atau 1

**Contoh 3.2**

$100110_2$ $= 1. 2^5 + 0. 2^4 + 0. 2^3 + 1. 2^2 + 1. 2^1 + 0. 2^0$

$= 1. 32 + 0. 16 + 0. 8 + 1. 4 + 1. 2 + 0. 1$

$= 32 + 0 + 0 + 4 + 2 + 0$

$= 38$

Jadi $1001102_2 = 38$ (dalam basis 10)

Basis 10 disebut pula basis decimal, Basis 2 di sebut biner, basis 4 disebut *quarter*, basis 8 disebut *oktal*, dan basis 16 disebut *heksadesimal* atau secara singkat *heks*. Koefisien *a*, dalam ekspansi jumlahan itu, disebut angka (digits). Angka *biner* biasa disebut dengan *bits* yang merupakan istilah dalam komputer.

Untuk mengubah penulisan lambang bilangan dari basis decimal ke basis non desimal, dapat menggunakan proses algoritma pembagian berulang – ulang dengan cara menuliskan sisa – sisa pembagian itu dengan urutan dari bawah ke atas.

**Contoh 3.3**

Tulislah 116 dalam lambang bilangan dengan basis 2

116 = 2. 58 + 0

58 = 2 .29 + 0

29 = 2 .14 + 1

14 = 2.7 + 0

3 = 2.3 + 1

3 = 2.1 + 1

1 = 2. 0 + 1

$116 = 1110100_2$

Jadi, 116 dalam lambang bilangan dengan basis 2 dapat ditulis $1110100_2$

Untuk mengubah penulisan lambang bilangan dari basis non desimal ke desimal, kita tuliskan lambang bilangan dengan basis non desimal dalam bentuk Panjang (bentuk jumlahan dari perpangkatan basis tersebut)

**Contoh 3.4**

Tulislah $3201_4$ dalam basis desimal (basis sepuluh)

$3201_4 = 3.\ 4^3 + 2.\ 4^2 + 0.\ 4^1 + 1.\ 4^0$

$3201_4 = 3.64 + 2.16 + 0.4 + 1.1$

$3201_4 = 192 + 32 + 0 + 1$

$3201_4 = 225$

Jadi $3201_4 = 225_{10}$ (cukup ditulis 225)

Komputer, selain menggunakan basis 2 juga menggunakan basis 8 atau basis 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

**Keterangan:** Huruf A, B, C, D, E, F berfungsi untuk menyatakan angka – angka yang bersesuaian dengan 10, 11, 12, 13, 14, dan 15 (dalam basis decimal)

**Contoh 3.5**

Berikut contoh cara mengubah lambang bilangan heksadesimal (basis 16) ke decimal.

a. $2AC3_{16} = \cdots$

**Penyelesaian:**

$2AC3_{16} = 2.\ 16^3 + 10.\ 16^2 + 12.\ 16^1 + 3.\ 16^0$

$2AC3_{16} = (2.\ 4096) + (10.256) + (12.16) + (3.1)$

$2AC3_{16} = 8192 + 2560 + 192 + 3$

$2AC3_{16} = 10947$

b. $\mathrm{FA0}_{16} = 15.\ 16^2 + 10.\ 16^1 + 0$

$\mathrm{FA0}_{16} = (15.\ 256) + 160 + 0$

$\mathrm{FA0}_{16} = 3840 + 160$

$\mathrm{FA0}_{16} = 4000$

**Latihan 3**

1. $A2FD_{16}$ = …

**2.** $CAB7_{16}$ **= …**

**Berikut Tabel 3.1 Konversi Penulisan Lambang Bilangan Desimal**

| (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 | 1000 | 100 | 20 | 10 |

**Basis 2 ke Basis 8**

Untuk mengubah lambang bilangan dari basis 2 ke basis 8. Maka bilangan dalam basis 2 tersebut dikelompokkan **tiga angka dari kanan**. Selanjutnya gantilah tiap kelompok tersebut dengan angka yang sesuai dengan angka – angka pada basis 8

**Contoh 3.6**

1. $1010110_2$ = 1. 010. $110_2$ dikelompokkan tiga angka - tiga angka dari kanan) = $126_8$
2. $1000010001_2$ = …
3. $11001000100_2$ = …

**Basis 8 ke Basis 2**

Untuk mengubah lambang bilangan dari basis 8 ke basis 2, maka kita hanya mengganti 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

1. $2_8 = 010_2$
2. $1_8 = 001_2$
3. $7015_8$ = 111. 000. 001. $101_2$ = $111000001101_2$
4. $20312_8$ = …
5. $40467_8$ = …

**Basis 2 ke Basis 4**

Untuk mengubah lambang bilangan dari basis 2 ke basis 4. Kita mengelompokkan dua angka – dua angka dari kanan pada lambang bilangan basis 2. Selanjutnya, hanya mengganti tiap kelompok dua itu dengan angka yang sesuai dengan angka pada basis 4.

**Contoh 3.7**

1. $1_4 = 01_2$
2. $2013_4 = \ldots$
3. $1032_4 = \ldots$

**Basis 4 ke Basis 2**

Untuk mengubah lambang bilangan dari basis 4 ke basis 2, maka kita hanya mengganti angka - angka pada lambang bilangan basis 4 dengan angka – angka yang sesuai dengan basis 2. Dengan catatan tiap satu angka pada basis 4 disediakan dua tempat pada basis 2

**Contoh 3.8**

1. $101101001_2 = 1.01.10.10.01_2 = 11221_4$
2. $111101011_2 = \ldots$

**Basis 2 ke Basis 16**

Untuk mengubah lambang bilangan dalam basis 2 ke basis ke 16 atau sebaliknya, satu angka pada lambang bilangan basis 16 di sediakan empat tempat pada lambang bilangan basis 2.

**Contoh 3.9**

1. $10010011101_2 = 100.1001.1101_2 = 49D_{16}$
2. $CAB7_{16} = 1100.1010.1011.0111_2 = 1100101010110111_2$
3. $101100111002_2 = \ldots$
4. $FE2D_{16} = \ldots$

Cara tersebut dapat dilakukan untuk mengubah lambang bilangan dalam basis 3 ke basis 9, basis 4 ke basis 16 aatau sebaliknya. Secara umum cara tersebut dapat digunakan untuk mengubah lambang bilangan dalam basis k ke basis $k^t$ Atau sebaliknya, dengan k dan t adalah bilangan – bilangan asli dan $k > 1$

**Contoh 3.10**

1. $3230120_4 = 3.\ 23.10.20_4 = 3B18_{16}$
2. $2220313_4 = \ldots$

# BAB IV

## FAKTORISASI BILANGAN BULAT

### A. Bilangan Prima

Jika dua bilangan bulat positif saling prima (prima relatif atau koprima ) yaitu faktor persekutuan terbesar dari dua bilangan itu sama dengan 1. Apabila $a_1, a_2, a_3, \ldots a_n$ adalah bilangan bulat positif sedemikian hingga $(a_1, a_2, a_3, \ldots a_n) = 1$ maka di bahwa $a_1, a_2, a_3, \ldots a_n$ saling prima**.**

Jika $(a_i, a_j) = 1$ untuk setiap i, j = 1, 2, 3, …, n maka dikatakan bahwa bilangan - bilangan bulat dengan $a_1, a_2, a_3, \ldots a_n$ $i \neq j$ di sebut saling prima dua – dua atau saling prima sepasang demi sepasang.

**Contoh 4.1**

1. (5,8,9) = 1 maka 5, 8 dan 9 dikatakan tiga bilangan yang saling prima dan tiga bilangan saling prima sepasang demi sepasang karena (5,8) = (5,9) = (8,9) = 1
2. (3,4,8,9) = 1 maka 3, 4, 8, dan 9 adalah empat bilangan yang saling prima, tetapi bukan merupakan empat bilangan yang saling prima sepasang demi sepasang karena (3,9) = 3 dan (4,8) = 4 meskipun (3,4) = (3, 8) = (9,4) = (9,8) = 1

**Latihan 4.1**

Buktikan bilangan bulat berikut saling prima atau saling prima sepasang demi sepasang !

a. 7,8,11

b. 2, 7,8, 11

Misalkan a dan b bilangan bulat positif maka menurut algoritma pembagaian ada bilangan – bilangan q dan r sedemikian hingga

$$b = qa + r\ d,\ 0 \leq r < a$$

Apabila a dan b bilangan – bilangan b oleh b saling prima dengan a maka b bilang saling prima dengan a pula.

**Definisi 4.1**

Bilangan bulat positif yang lebih dari 1 dan tidak mempunyai faktor bulat positif, kecuali 1 dan bilangan bulat itu sendiri dan bukan bilangan prima disebut bilangan komposit (tersusun).

**Teorema 4.1**

Bilangan bulat positif yang lebih dari 1 dapat dibagi oleh suatu bilangan prima.

**Pembuktian:**

Ambil sebarang bilangan bulat positif n > 1. Apabila n suatu bilangan prima maka n|n. Apabila n suatu bilangan komposit, n mempunyai faktor bulat positif, selain 1 n sendiri, misalnya $d_1$, yaitu $d_1|n$. Maka itu ada bilangan bulat positif $n_1$ sedemikian hingga

$$n = d_1 n_1 \; dengan \; 0 \leq n_1 < n$$

Jika $n_1$ suatu bilangan prima $n_1|n$ sehingga teorema tersebut terbukti. Akan tetapi,

jika $n_1$ suatu bilangan komposit, $n_1$ mempunyai faktor bulat positif. Selain 1 dan $n_1$, misalnya $d_2$ yaitu $d_1|n_1$, sehingga ada bilangan bulat positif $n_2$ sedemikian hingga

$$n_1 = d_2 n_2 \; dengan \; 0 \leq n_2 < n_1$$

Jika $n_2$ suatu bilangan prima $n_2|n$. Oleh karena $n_1|n$ maka $n_2|n_1$. Jadi, n terbagi oleh bilangan prima $n_2$ itu bearti teorema terbukti. Akan tetapi, jika $n_2$ suatu bilangan komposit, $n_2$ mempunyai faktor bulat positif. Selain 1 dan $n_2$ misalnya

$d_3$ yaitu $d_3|n_2$. Ini berarti ada bilangan bualat positif $n_3$ sedemikian hingga

$$n_2 = d_3 n_3 \; dengan \; 0 \leq n_3 < n_2$$

Jika $n_3$ suatu bilangan prima $n_3|\, n_2$. Karena $n_2|\, n_1$ maka $n_2|n$. Jadi, n terbagi oleh bilangan prima $n_3$, itu berarti teorema terbukti. Akan tetapi, jika $n_3$ suatu bilangan komposit, proses seperti di atas dapat dilanjutkan sedemikian hingga diperoleh suatu barisan berikut:

$$n, n_1, n_2, n_3, \ldots dengan \; n > n_1 > n_2 > \; n_3 \ldots > 1$$

Penguraian atas faktor – faktor komposit ini tentu berakhir pada suatu faktor prima karena faktor – faktor dan selalu lebih dari 1. Misalnya pemfaktoran tersebut berakhir pada faktor prima maka

$$n_k \big| n_{k-1}, \; n_k \big| n_{k-1}, \ldots n_2 \,|n_1 \; dan \; n_1 \,|n \; sehingga \; n_k \,|n$$

**Teorema 4.2**

Setiap bilangan bulat positif yang lebih besar dari 1 adalah suatu bilangan prima atau bilangan itu dapat dinyatakan sebagai perkalian bilangan – bilangan prima.

**Pembuktian**

Ambil sebarang bilangan bulat positif n > 1. Ada suatu bilangan prima $p_1$ sedemikian hingga $p_1 \,|n$ maka itu, ada suatu bilangan positif $n_1$ sehingga

$$n_1 = p_1 n_1 \; dengan \; 1 \leq n_1 < n$$

Jika $n_1 = 1$ maka $n = p_1$ sehingga n suatu bilangan prima. Jika $n_1 > 1$ sedemikian hingga $p_2|n_1$ maka itu, ada suatu bilangan positif $n_2$ sehingga

$$n_1 = p_2 n_2 \; dengan \; 1 \leq n_2 < n_1$$

Jika $n_2 = 1$ maka $n_1 = p_2$ sehingga n = $p_1 p_2$ . Itu berarti teorema terbukti. Akan tetapi, Jika $n_2 > 1$, ada suatu bilangan prima $p_3$ sedemikian hingga

$$n_3 = p_3 n_3 \; dengan \; 1 \leq n_3 < n_2$$

Jika $n_3 = 1$ maka $n_2 = p_3$ sehingga $n = p_1 \; p_2 \; p_3$. Itu berarti teorema terbukti. Akan tetapi, Jika $n_3 > 1$ maka proses di atas dapat dilanjutkan sehingga berakhir pada $n_k = 1$ sehingga diperoleh $n = p_1 \; p_2 \; p_3 \; ... \; p_k$ yaitu bilangan bulat positif n > 1 dapat dinyatakan sebagai perkalian bilangan prima.

Suatu bilangan positif yang lebih besar dari 1 dapat dinyatakan sebagai perkalian bilangan – bilangan prima. Mungkin saja diantara faktor – faktor yang sama ditulis sebagai bilangan berpangkat. Teorema 4.2 ini juga dapat digunakan untuk menentukan FPB dan KPK dari dua atau lebih, yaitu dengan menyatakan masing – masing bilagan bulat itu dalam bentuk kanoniknya. Bentuk kanonik merupakan representasi dari n sebagai perkalian bilangan – bilangan prima. Jika n adalah bilangan bulat yang lebih dari 1 maka :

n = $P_1^{a_1} \; P_2^{a_2} P_3^{a_3} \; ... \; P_k^{a_k}$ pers ini merupakan bentuk kanonik dari n atau representasi dari n sebagai hasil perkalian bilangan – bilangan prima dengan :

$p_1, p_2, p_3, \ldots p_k$ adalah faktor – faktor prima dari n

$a_1, a_2, a_3, \ldots a_k$ adalah eksponen – eksponen bilangan bulat tak negatif

Misalkan m, n, t, adalah bilangan – bilangan bulat positif yang lebih dari 1 dengan bentuk kanoniknya adalah sebagai berikut:

$$\text{m} = P_1^{a_1} \; P_2^{a_2} P_3^{a_3} \; ... \; P_k^{a_k}$$

$$\text{n} = P_1^{b_1} \; P_2^{b_2} P_3^{b_3} \; ... \; P_k^{b_k}$$

$$\text{t} = P_1^{c_1} \; P_2^{c_2} P_3^{c_3} \; ... \; P_k^{c_k}$$

**Keterangan:**

FPB (m, n, t ) = $P_1^{d_1} \; P_2^{d_2} P_3^{d_3} \; ... \; P_k^{d_k}$ dengan $d_i = \min (a_I, b_i, c_i)$ untuk i = 1, 2, 3, … k

KPK (m, n, t ) = $P_1^{e_1} \; P_2^{e_2} P_3^{e_3} \; ... \; P_k^{e_k}$ dengan $e_i = \text{mak} (a_I, b_i, c_i)$ untuk i = 1, 2, 3, … k

**Contoh 4.2**

1. Tentukan FPB dan KPK dari 56, 84, dan 140!

**Penyelesaian:**

Faktorisasi prima dari 56, 84, dan 140 diperoleh:

$56 = 2^3.7^1$

$84 = 2^2. 3^1.7^1$

$140 = 2^2. 5^1. 7^1$

Bentuk ikonik faktorisasi prima dari 56, 84, dan 140 diperoleh:

$56 = 2^3.3^0.5^0.7^1$

$84 = 2^2.\ 3^1.\ 5^0\ .7^1$

$140 = 2^2.\ 3^0\ 5^1.\ 7^1$

FPB (56, 84, dan 140) adalah

$= 2^{\text{min }(3,2,2)}.\ 3^{\text{min }(0,1,0)}.\ 5^{\text{min }(0,0,1)}\ .7^{\text{min }(1,1,1)}$

$= 2^2.\ 3^0.\ 5^0.\ 7^1$

$= 4.\ 1.\ 1.\ 7 = 28$

KPK (56, 84, dan 140) adalah

$= 2^{\text{mak }(3,2,2)}.\ 3^{\text{mak }(0,1,0)}.\ 5^{\text{mak }(0,0,1)}\ .7^{\text{mak }(1,1,1)}$

$= 2^3.\ 3^1.\ 5^1.\ 7^1$

$= 8.\ 3.\ 5.\ 7$

$= 840$

Jadi nilai FPB dan KPK dari 56, 84, dan 140 adalah 28 dan 840

2. Tentukan FPB dan KPK dari 252, 216, dan 198!

**Penyelesaian:**

Faktorisasi prima dari 252, 216, dan 198 diperoleh:

$252 = 2^2\ .3^2.\ 7^1$

$216 = 2^3.\ 3^3$

$198 = 2^1.\ 3^2.\ 11^1$

Bentuk ikonik faktorisasi prima dari 252, 216, dan 198 diperoleh:

$252 = 2^2.3^2.7^1.11^0$

$216 = 2^3.\ 3^3.\ 7^0.11^0$

$198 = 2^1.\ 3^2.\ 7^0.11^1$

FPB (198, 216, 252) adalah

$= 2^{\text{min }(1,3,2)}.\ 3^{\text{min }(2,3,2)}.\ 7^{\text{min }(0,0,1)}\ .11^{\text{min }(1,0,0)}$

$= 2^1.\ 3^2.\ 7^0.\ 11^0$

$= 2.\ 9.\ 1.\ 1$

$= 18$

KPK (198, 216, 252) adalah

$= 2^{\text{maks }(1,3,2)}.\ 3^{\text{ maks }(2,3,2)}.\ 7^{\text{ maks }(0,0,1)}.11^{\text{ maks }(1,0,0)}$

$= 2^3.\ 3^3.\ 7^1.\ 11^1$

$= 8.\ 27.\ 7.\ 11 = 16.632$

Jadi nilai FPB dan KPK dari 252, 216, dan 198 adalah 18 dan 16632

3. Tentukan FPB dan KPK dari 135, 180, dan 225!

**Penyelesaian:**

Faktorisasi prima dari 135, 180, dan 225 diperoleh:

$135 = 3^3. 5^1$

$180 = 2^2\ 3^2. 5^1$

$225 = 3^2.5^2$

Bentuk ikonik faktorisasi prima dari 135, 180, dan 225 diperoleh:

$135 = 2^0. 3^3. 5^1$

$180 = 2^2. 3^2. 5^1$

$225 = 2^0. 3^2.5^2$

FPB (135, 180, dan 225) adalah

$= 2^{\min(0,2,0)}. 3^{\min(3,2,2)}. 5^{\min(1,1,2)}$

$= 2^0. 3^2. 5^1$

$= 1. 9. 5$

$= 45$

KPK (135, 180, dan 225) adalah

$= 2^{\text{maks}(0,2,0)}. 3^{\text{maks}(3,2,2)}. 5^{\text{maks}(1,1,2)}$

$= 2^2. 3^3. 5^2$

$= 4. 27. 25$

$= 2700$

Jadi nilai FPB dan KPK dari 135, 180, dan 225 adalah 45 dan 2700

**Teorema 4.3**

Jika n suatu bilangan komposit, n memiliki faktor k dengan $1 < k < \sqrt{n}$

Pembuktian:

Karena n suatu bilangan komposit, ada bilangan positif k dan m sedemikian hingga

$$km = n\ dengan\ 1 < k < n\ \ dan\ 1 < m < n$$

Apabila k dan m kedua – keduanya lebih besar dari $\sqrt{n}$ yaitu, $k > \sqrt{n}$ dan $m > \sqrt{n}$ maka $n = km > \sqrt{n}.\sqrt{n} = n$. Terdapat $n > n$, hal ini tidak mungkin. Oleh karena itu, salah satu dari $k$ atau $m$ harus tidak lebih kecil dari $\sqrt{n}$. Misalnya $k$ yaitu: $1 < k \leq \sqrt{n}$. Jadi n memiliki faktor $k$ dengan $1 < k \leq \sqrt{n}$.

**Teorema 4.4**

Jika bilangan bulat positif $n$ tidak memiliki faktor prima $p$ dengan $1 < p \leq \sqrt{n}$. Maka $n$ suatu bilangan prima.

**Pembuktian:**

Menyatakan terlebih dahulu kontraposisinya, yaitu Jika $n$ suatu bilangan komposit, $n$ memiliki faktor prima $p$ dengan $1 < p < \sqrt{n}$

**Contoh 4.3**

Carilah bilangan prima yang kurang dari 100 (Gunakan Saringan Erastosthenes)

Penyelesaian:

1. Menentukan bilangan prima yang kurang dari 10: 2, 3, 5, 7.
2. Mencoret semua kelipatan bilangan prima yang diperoleh pada point 1 kecuali bilangan primanya. Misalnya: kelipatan 2: 4, 6, …, 100 dicoret kecuali 2. Kelipatan 3: 6, 9, …, 99. dicoret kecuali 3, Kelipatan 5: 10, 15, …, 100 dicoret kecuali 5 dan Kelipatan 7: 14, 21, …, 98 dicoret kecuali 7.

Untuk lebih jelasnya lihat saringan erastosthenes berikut:

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

Jadi bilangan prima yang kurang dari 100 adalah 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

**Latihan 4.2**

1. Tentukan nilai FPB dan KPK pada soal berikut menggunakan bentuk kanonik dari hasil perkalian
   a. 158, 188
   b. 2008, 1234
   c. 12378, 3054
   d. 23141, 291371
   e. 6552, 4563

2. Carilah himpunan bilangan prima yang kurang dari 196 dan 255 menggunakan Saringan Erastosthenes

## B. Faktorisasi Tunggal

Faktorisasi tunggal merupakan pemfaktoran suatu bilangan bulat positif atas faktor – faktor prima tunggal . Akan dipelajari beberapa teorema sebagai dasar dalam memahami materi tersebut.

**Teorema 4.5**

Jika $p$ suatu bilangan prima dan $p \mid ab$ maka $p \mid b$.

**Pembuktian:**

Karena $p$ suatu bilangan prima, untuk sebarang bilangan bulat $a$ berlaku $(a,p) = 1$ atau $(a,p) = p$. Jika $(a,p) = 1$ dan $p \mid ab$ maka $p \mid b$. Jika $(a,b) = p$ maka $p \mid a$. Jadi, terbukti $p \mid a$ atau $p \mid b$.

Teorema 4.5 ini dapat diperluas untuk bilangan – bilangan $a_1\ a_2\ a_3 \dots\ a_n$ maka $p \mid ab$

**Teorema 4.6**

Pemfaktoran suatu bilangan bulat positif yang lebih besar dari atas faktor - faktor prima adalah tunggal, kecuali urutan dari faktor – faktornya.

**Pembuktian:**

Ambil sebarang bilangan bulat positif $n > 1$. Jika $n$ suatu bilangan prima, n adalah faktornya sendiri.

Jika $n$ suatu bilangan komposit dan diasumsikan bahwa pemfaktoran $n$ atas faktor – faktor prima tungga, Misalnya

$$n = p_1\ p_2\ p_3 \dots\ p_t\ dan\ n = q_1\ q_2\ q_3 \dots\ q_r$$

Dengan $p_i\ dan\ q_i$ adalah bilangan prima untuk $i = 1,2,3, \dots, t$ dan $j = 1,2,3, \dots, r$ . serta $p_1 \geq p_2 \geq p_3 \dots\ p_t$ dan $q_1 \geq q_2 \geq q_3 \dots\ q_r$, dengan $t \leq r$. Karena $n = p_1\ p_2\ p_3 \dots\ p_t$ maka $p_1 | n$ sehingga $p_1 | q_1 q_2\ q_3 \dots\ q_r$. Selanjutnya, Jika $p_1 = q_k$ untuk suatu $k$ dengan $1 \leq k \leq r$. Mengingat $q_1 \geq q_2 \geq q_3 \dots\ q_r$ maka $p_1 \leq q_1$. Karena $n = q_1 q_2 \dots q_r$ maka $q_1 | p_1 p_2\ p_3 \dots\ p_t$. Menurut $q_1 = p_m$ untuk suatu m dengan $1 \leq m \leq t$ mengingat $p_1 \geq p_2 \geq p_3 \dots\ p_t$ maka $q_1 \leq p_1$. Karena $p_1 \leq q_1$ dan $q_1 \leq p_1$ maka $p_1 = q_1$ sehingga dari permisalan $n$ di atas kita memperoleh bahwa $p_2\ p_3 \dots\ p_t = q_2\ q_3 \dots\ q_r$

Jika uraian tersebut di teruskan, akan di peroleh:

$$p_2 = q_2\ sehingga\ p_3\ p_4 \dots\ p_t = q_3\ q_4 \dots\ q_r$$

$$p_3 = q_3\ sehingga\ p_4\ p_5 \dots\ p_t = q_4\ q_5 \dots\ q_r$$

dan seterusnya.

Apabila $t = r$ proses tersebut akan berakhir pada $p_t \leq q_r$ dan teorema terbukti. Akan tetapi, apabila t < r akan diperoleh bahwa

$$1 = q_{r+1}\, q_{r+2} \ldots\, q_r$$

Hal ini mustahil karena $q_{r+1}\, q_{r+2} \ldots\, q_r$ adalah bilangan – bilangan prima maka harus $t = r$

Sehingga $p_1 = q_1,\ p_2 = q_2, \ldots p_t = q_r$ artinya bilangan bulat positif n tersebut hanya dapat dinyatakan sebagai hasil kali faktor – faktor primanya secara tunggal.

**Teorema 4.7**

Banyaknya bilangan prima adalah tak berhingga

**Pembuktian**

Misalkan, $p_1 = 2$ , $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ ... adalah urutan bilangan – bilangan prima dan andaikan ada bilangan prima terbesar, misalkan $p_n$ Sekarang dibentuk suatu bilangan bulat positif.

$$N = p_1 p_2 \ldots p_n + 1$$

Karena N > 1, dimana N dapat dibagi oleh suatu bilangan prima sehingga N dapat dibagi oleh sekurang – kurangnya satu bilangan prima dari $p_1,\ p_2, \ldots p_n$. Misalnya bilangan prima $p_k$ dengan $1 \leq k \leq n$ membagi N yaitu $p_k | N$

$N = p_1 p_2 \ldots p_n + 1$ dengan $p_k | N$ dan $p_k |\, p_1 p_2 \ldots p_n$ maka $p_k | 1$

Hal ini tidak mungkin karena $p_k$ suatu bilangan prima. Oleh karena itu, pengandaian bahwa ada bilangan prima terbesar adalah tidak benar sehingga pengandaian tersebut salah. Hal ini diperoleh bahwa tidak ada bilangan prima terbesar. Dengan kata lain, banyaknya bilangan prima adalah tak hingga

Pada pembuktian ini yang menarik adalah pembentukan bilangan bulat positif N sebagai hasil kali semua bilangan prima ditambah 1. Apakah N tersebut suatu bilangan prima?

Misalnya dimulai untuk bilangan prima pertama yaitu 2 maka diperoleh:

$$N_1 = 2 + 1 = 3$$

$$N_2 = 2.3 + 1 = 7$$

$$N_3 = 2.3.5 + 1 = 32$$

$$N_4 = 2.3.5.7 + 1 = 211$$

$$N_5 = 2.3.5.7.11 + 1 = 2311$$

**Teorema 4.8**

Dalam suatu barisan bilangan prima, jika $p_n$ menyatakan bilangan prima ke $n$ maka $p_n \leq 2^{2^{x-1}}$

**Pembuktian:**

menggunakan induksi matematika pada $n$. Untuk $n = 1$ diperoleh $p_n \leq 2^{2^0}$ yaitu $p_n \leq 2$. Hal ini memang benar sebab bilangan prima pertama adalah 2. Selanjutnya, sebagai Hipotesis, teorema diasumsikan benar untuk $n = k$, yaitu: $p_k \leq 2^{2^{k-1}}$. Harus dibuktikan bahwa teorema benar untuk $n = k + 1$ yaitu: $p_{k+1} \leq 2^{2^k}$

Perhatikan bentuk berikut ini!

$$p_{k+1} \leq p_1\, p_2 p_3 \ldots p_k + 1$$

$$p_{k+1} \leq (2\,(\,2^2)\left(2^{2^2}\right)\left(2^{2^3}\right) \ldots \left(2^{2^{k-1}}\right)) + 1$$

$$p_{k+1} \leq (2^{1+2+2^2+\,2^3+\,\ldots+\,2^{k-1}}\,) + 1$$

Jika $1 + 2 + 2^2 + \ 2^3 + \ \ldots + \ 2^{k-1} = \ 2^k - 1$, yaitu suatu deret geometri dengan rasio 2. Sehingga diperoleh:

$$p_{k+1} \leq (2^{2^{k-1}}\,) + 1$$

Karena $2^{2^k-1} > 1$ untuk setiap bilangan asli k, maka ketidaksamaan itu menjadi

$$p_{k+1} \leq 2^{2^k-1} + 2^{2^k-1}$$

$$p_{k+1} \leq 2^{2^k}$$

Karena teorema tersebut benar untuk n = 1 dan benar untuk n = k dan telah ditunjukkan benar untuk n = k + 1, maka teorema benar untuk setiap bilangan asli n.

# BAB V

## KEKONGRUENAN

### A. Definisi dan Sifat Kekongruenan

**Definisi 5.1**

Misalkan a dan b adalah suatu bilangan bulat. Jika m suatu bilangan bulat positif yang lebih besar dari 1. Maka a dikatakan kongruen dengan b modulo m (di tulis a $\equiv b\ (mod\ m)$ jika m membagi habis (a – b) atau a $\equiv$ b (mod m) jika a dan b memberikan sisa yang sama bila di bagi oleh m. Jika m tidak membagi (a – b) maka dikatakan bahwa a tidak kongruen dengan b modulo m (di tulis a $\not\equiv$ b (mod m))

**Contoh 5.1**

1. $25 \equiv 1 \pmod 4$ sebab (25 – 1) = 24 terbagi oleh 4
2. $31 \not\equiv 5 \pmod 6$ sebab (31 – 5) = 26 tidak terbagi oleh 6
3. $8 \equiv 4 \pmod 2$ sebab (8 – 4) habis dibagi oleh 2
4. $5 \equiv -4 \pmod 9$ sebab (5 – (– 4)) habis dibagi oleh 9
5. $31 \neq 5 \pmod 6$ sebab (31 – 5) tidak habis dibagi oleh

**Teorema 5.1**

$a \equiv b \pmod m$ jika dan hanya jika ada bilangan k sehingga $a = mk + b$

**Pembuktian:**

Jika m > 0 maka $m|\ (a - b)$ jika dan hanya jika $a \equiv b \pmod m$. $m|\ (a - b)$ ada bilangan k sehingga (a – b) = mk, sama artinya dengan $a = mk + b$. Sehingga $a \equiv b \pmod m$ jika dan hanya jika ada bilangan k sehingga $a = mk + b$.

**Contoh 5.2**

1. $26 \equiv 4 \pmod{11}$ sama artinya dengan 26 = 11. 2 + 4
2. $53 \equiv 5 \pmod 8$ sama artinya dengan 53 = 8.6 + 5

**Teorema 5.2**

Setiap bilangan bulat kongruen modulo m dengan tepat satu diantara 0, 1, 2, 3, …, (m – 1)

**Pembuktian:**

Jika a dan m bilangan – bilangan bulat dan m > 0. Maka a dan m bilangan – bilangan bulat dan m > 0. Menurut alqoritma pembagian, maka a dapat dinyatakan sebagai

$$a = mq + r \text{ dengan } 0 \leq r < m.$$

Ini berarti bahwa $a - r = mq$ yaitu $a \equiv r \pmod{m}$ Karena $0 \leq r < m$ maka ada m buah pilihan r yaitu 1, 2, 3, ..., (m – 1). Jadi setiap bilangn bulat kongruen modulo m dengan tepat satu di antara 0, 1, 2, 3, … (m – 1).

**Contoh 5.3**

1. Residu terkecil dari 71 modulo 2 adalah 1, karena sisa 71: 2 adalah 1
2. Residu terkecil dari 71 modulo 3 adalah 2, karena sisa 71: 3 adalah 2
3. Residu terkecil dari 34 modulo 5 adalah 4, karena sisa 34: 5 adalah 4.

**Definisi 5.2**

Pada $a \equiv b \pmod{m}$ dengan $0 \leq r < m$ maka r disebut residu terkecil dari a modulo m. untuk kekongruenan modulo m ini, {0,1,2,3, …, (m – 1)} disebut himpunan residu terkecil modulo m.

**Contoh 5.4**

1. Himpunan residu terkecil modulo 5 adalah (0, 1, 2, 3, 4)
2. Himpunan residu terkecil modulo 9 adalah (0, 1, 2, 3, 4, 5, 6, 7, 8)
3. Himpunan residu terkecil modulo 25 adalah (0, 1, 2, 3, 4, …,24)

**Teorema 5.3**

$a \equiv b \pmod{m}$ jika dan hanya jika a dan b memiliki sisa yang sama jika dibagi m.

**Pembuktian:**

Jika $a \equiv b \pmod{m}$ jika dan hanya jika a dan b memiliki sisa yang sama jika dibagi m. Maka $a \equiv r \pmod{m}$ dan $b \equiv r \pmod{m}$ dengan r adalah residu terkecil modulo m atau $0 \leq r < m$.

$a \equiv r \pmod{m}$ berarti jika a memiliki sisa r jika dibagi m maka $a = mq + r$ untuk suatu q

$b \equiv r \pmod{m}$ berarti jika a memiliki sisa r jika dibagi m maka $b = mt + r$ untuk suatu t

Dari kedua persamaan diperoleh bahwa:

$$a - b = m(q - t) \text{ berarti } m \mid (a - b) \text{ atau } a \equiv b \pmod{m}$$

**Contoh 5.5**

1. Jika $n \equiv 7 \pmod{8}$ maka $n = 8k + 7$ untuk suatu bilangan k dan n dibagi 8 bersisa 7. Misalnya $47 \equiv 7 \pmod{8}$ maka $8 \mid (47 - 7)$ atau (47 – 7) = 8.5 sehingga 47 = 8.5 + 7
2. $14 \equiv 9 \pmod{5}$

   $14 \equiv 4 \pmod{5}$ berarti 14 = 5.2 + 4

   $9 \equiv 4 \pmod{5}$ berarti 9 = 5.1 + 4

**Definisi 5.3**

Himpunan bilangan bulat $r_1, r_2, r_3, \ldots, r_m$ disebut sistem residu lengkap modulo m bila dan hanya bila setiap bilangan bulat kongruen modulo m dengan satu dan hanya satu diantara $r_1, r_2, r_3, \ldots, r_m$

**Contoh 5.6**

{45, -9, 12, -22, 24} adalah sistem residu lengkap modulo 5.

**Penyelesaian:**

himpunan residu terkecil modulo 5 adalah {0,1,2,3,4}

$45 \equiv 0 \pmod 5$

$-9 \equiv 1 \pmod 5$

$12 \equiv 2 \pmod 5$

$-22 \equiv 3 \pmod 5$

$24 \equiv 4 \pmod 5$

**Teorema 5.4**

Jika $a \equiv b \pmod m$ *dan* $c \equiv d \pmod m$ maka $a + c \equiv b + d \pmod m$

**Pembuktian:**

$a \equiv b \pmod m$ berarti a = m.s + b untuk suatu bilangan bulat s.

$c \equiv d \pmod m$ berarti c = m.t + d untuk suatu bilangan bulat t.

Jika dua ruas dua persamaan ini dijumlahkan akan diperoleh:

$a + c = (m.s + b) + (m.t + d)$

$a + c = m(s + t) + (b + d)$

$(a + c) - (b + d) = m(s + t)$

Ini berarti $a + c \equiv b + d \pmod m$

**Teorema 5.5**

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

**Pembuktian:**

$a \equiv b \pmod m$ berarti a = m.s + b untuk suatu bilangan bulat s.

$c \equiv d \pmod m$ berarti c = m.t + d untuk suatu bilangan bulat t.

Jika kedua ruas persamaan pertama dikalikan x dan kedua ruas persamaan kedua dikalikan y diperoleh

$$ax = msx + bx$$

$$ay = mty + by$$

Jika ruas – ruas dua persamaan ini dijumlahkan maka diperoleh

$$ax + cy = (msx + bx) + (mty + dy)$$
$$ax + cy = m(sx + ty) + (bx + dy)$$
$$(ax + cy) - (bx + dy) = m(sx + ty)$$

Persamaan terakhir ini berarti bahwa

$$m| ax + cy) - (bx + dy) \text{ atau}$$
$$ax + cy \equiv bx + dy \pmod{m}$$

**Teorema 5.6**

Jika $ac \equiv bc \pmod{m}$ dengan (c, m) = 1 maka $a \equiv b \pmod{m}$

**Pembuktian:**

$ac \equiv bc \pmod{m}$ ini berarti m| ac – bc atau m| c (a – b)

m| c (a – b) dengan (c, m) = 1 maka m| (a – b) berarti $a \equiv b \pmod{m}$

**Contoh 5.7**

Tentukanlah bilangan – bilangan bulat y yang memenuhi perkongruenan $3y \equiv 1 \pmod{7}$

**Penyelesaian:**

Karena $1 \equiv 15 \pmod{7}$ maka dapat mengganti 1 pada pengkongruenan tersebut dengan 15. Sehingga diperoleh

$$3y \equiv 15 \pmod{7}.$$

Selanjutnya, karena (3,7) = 1 maka dapat membagi 3 pada ruas – ruas pengkongruenan diperoleh:

$$3y \equiv 15 \pmod{7}.$$
$$y \equiv 5 \pmod{7}$$

Pengkongruenan ini dapat dituliskan menjadi

$$y = 5 + 7k$$

jadi, bilangan – bilangan bulat y yang memenuhi perkongruenan $3y \equiv 1 \pmod{7}$ adalah $y = 5 + 7k$ , untuk setiap bilangan bulat k

**Teorema 5.7**

Jika $ac \equiv bc \pmod{m}$ dengan (c, m) = d maka $a \equiv b \left(\text{mod } \frac{m}{d}\right)$

Pembuktian

ac ≡ bc (mod m) bearti m| (ac – bc) atau m| c (a – b) maka $\frac{m}{d} | \frac{c}{d}(a-b)$. Karena d adalah FPB dari c dan m, maka $\frac{m}{d}$ dan $\frac{c}{d}$ adalah bilangan - bilangan bulat. Karena (c, m) = d, maka $(\frac{m}{d}, \frac{c}{d}) = 1$ . Karena $(\frac{m}{d}, \frac{c}{d}) = 1$ dan $\frac{m}{d} | \frac{c}{d}(a-b)$, maka $\frac{m}{d} | (a-b)$, berarti

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

**Contoh 5.8**

Tentukan nilai x yang memenuhi $2x \equiv 4 \pmod 6$.

**Penyelesaian:**

Dengan menggunakan ac ≡ bc (mod m) dengan (c, m) = d maka $a \equiv b \left(\text{mod } \frac{m}{d}\right)$

$2x \equiv 2.2 \pmod 6$ karena (2, 6) = 2 maka $x \equiv 2 \pmod 3$. Jadi nilai – nilai x adalah (3k + 2) untuk setiap bilangan bulat k.

**Teorema 5.8**

Misalnya m suatu bilangan bulat positif, bilangan – bilangan bulat a dan b masing – masing saling prima dengan m. jika bilangan – bilangan bulat x dan y sedemikian hingga

$a^x \equiv b^x (\text{mod m})$ dan $a^y \equiv b^y (\text{mod m})$ maka

$$a^{(x,y)} \equiv b^{(x,y)} (\text{mod m})$$

**Pembuktian:**

Untuk x dan y bilangan – bilangan bulat, maka ada bilangan – bilangan bulat u dan v sedemikian hingga:

$$ux - uy = (x,y)$$

Dari ketentuan diperoleh

$$a^{ux} \equiv b^{ux} (\text{mod m}) \text{ dan } a^{vy} \equiv b^{vy} (\text{mod m})$$

Selanjutnya, $a^{ux}\, b^{vy} \equiv a^{vy} b^{ux} (\text{mod m})$ maka $a^{ux.vy} \equiv b^{ux.vy} (\text{mod m})$ karena (a, m) = (b, m) = 1 maka:

$$a^{(x,y)} \equiv b^{(x,y)} (\text{mod m})$$

## B. Aplikasi Kekongruenan

Kekongruenan modulo 9 dapat digunakan untuk memeriksa kebenaran perkalian dan penjumlahan bilangan – bilangan bulat

$10000 - 1 = 9999 = 9k_1$ sehingga $10000 \equiv 1 \pmod 9$

$1000 - 1 = 999 = 9k_2$ sehingga $1000 \equiv 1 \pmod 9$

$100 - 1 = 99 = 9k_3$ sehingga $100 \equiv 1 \pmod 9$

$10 - 1 = 9 = 9k_4$ sehingga $10 \equiv 1 \pmod 9$

Selanjutnya akan ditunjukkan bahwa setiap bilangan bulat modulo 9 kongruen dengan jumlah angka - angkanya.

**Contoh 5.9**

1. 8234 ≡ 8000 + 200 + 30 + 4 (mod 9)

   ≡ 8 (1000) + 2 (100) + 3 (10) + 4 (mod 9)

   ≡ 8 (1) + 2 (1) + 3 (1) + 4 (mod 9)

8234 ≡ 17 (mod 9)

Selanjutnya dengan cara yang sama

17 ≡ 10 + 7 (mod 9)

≡ 1 + 7 (mod 9)

17 ≡ 8 (mod 9)

Jadi, 8234 ≡ 8 (mod 9)

2. 1234 ≡ 1000 + 200 + 30 + 4 (mod 9)

   ≡ 1 (1000) + 2 (100) + 3 (10) + 4 (mod 9)

   ≡ 1 (1) + 2 (1) + 3 (1) + 4 (mod 9)

1234 ≡ 10 (mod 9)

Karena 10 > 9 maka

1234 ≡ 1 (mod 9)

**Teorema 5.9**

$10^n \equiv 1 \pmod 9$ untuk n = 1, 2, 3, …

Bukti:

$10^n - 1$ = 999… 9 (n angka semuannya 9) terbagi oleh 9

Jadi, $i10^n \equiv 1 \pmod 9$

**Teorema 5.10**

Setiap bilangan bulat modulo 9 kongruen dengan jumlah – jumlahnya

**Pembuktian:**

Ambil sembarang bilangan bulat n yang angka – angkanya secara berturut – turut adalah:

$$n = d_k, d_{k-1}, d_{k-2} \ldots d_2, d_1, d_0$$

$$n = d_k\, 10 + d_{k-1}\, 10^{k-1} + d_{k-2}\, 10^{k-2} + \ldots + d_2\, 10^2 + d_1 10 + d_0$$

$dengan\ 0 \le d_i \le 9$ untuk i = 0, 1, 2, … k dan $d_k \neq 0$

Menggunakan teorema 5.9 yaitu: $10^n \equiv 1 \pmod 9$ untuk n = 1, 2, 3, … sehingga

$$n \equiv d_k\,(1) + d_{k-1}\,(1) + d_{k-2}\,(1) + \ldots + d_2(1) + d_1(1) + d_0\ (mod\ 9)$$

$$n \equiv d_k + d_{k-1} + d_{k-2} + \ldots + d_2 + d_1 + d_0 \ (mod\ 9)$$

Jadi, bilangan bulat n kongruen modulo 9 dengan jumlah angka – angkanya. Perhatikn mosalkan a + b = c maka tentukan a + b ≡ c (mod 9). Jika a ≡ m (mod 9), b ≡ $n$ (mod 9) dan c ≡ $p$ (mod 9) maka dapat di simpulkan bahwa

m + n ≡ p (mod 9)

Prinsip ini dapat digunakan untuk memeriksa kebenaran suatu penjumlahan maupun pengurangan bilangan – bilangan bulat yang biasa disebut dengan *Koreksi Sembilan*,

**Contoh 5.10**

Periksalah kebenaran penjumlahan berikut ini dengan prinsip di atas (kekongruenan mod 9)!

248 + 324 + 672 = 1244

Penyelesaian:

248 ≡ 200 + 40 + 8 (mod 9)

248 ≡ 2 (100) + 4 (10) + 8 (mod 9)

248 ≡ 2 + 4 + 8 (mod 9)

248 ≡ 14 (mod 9)

248 ≡ 10 + 4 (mod 9)

248 ≡ 1 + 4 (mod 9)

**248 ≡ 5 (mod 9)**

Dengan cara yang sama seperti di atas

324 ≡ 3 + 2 + 4 (mod 9)

324 ≡ 9 (mod 9)

324 ≡ 0 (mod 9)

672 ≡ 6 + 7 + 2 (mod 9)

672 ≡ 15 (mod 9)

$672 \equiv 6 \pmod 9$

Jadi $248 + 324 + 672 = 5 + 0 + 6 \pmod 9$

$= 11 \pmod 9$

$= 2 \pmod 9$ … (i)

Sedangkan $1244 \equiv 1 + 2 + 4 + 4 \pmod 9$

$\equiv 11 \pmod 9$

$\equiv 2 \pmod 9$ … (ii)

Dari kekongruenan (i) dan (ii) berarti :

$248 + 324 + 672 = 1244$ (benar)

Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka $ac \equiv bd \pmod m$

Prinsip ini dapat digunakan untuk memeriksa **kebenaran suatu perkalian**

**Contoh 5.11**

Benarkah $84 \times 428 = 35952$?

**Penyelesaian:**

$84 \equiv 8 + 4 \pmod 9$

$\equiv 12 \pmod 9$

$\equiv 3 \pmod 9$

$428 \equiv 4 + 2 + 8 \pmod 9$

$\equiv 14 \pmod 9$

$\equiv 5 \pmod 9$

Maka $84 \times 428 \equiv 3 \times 5 \equiv 15 \pmod 9$

$\equiv 6 \pmod 9$ … (i)

Sedangkan $35.952 \equiv 3 + 5 + 9 + 5 + 2 \pmod 9$

$\equiv 24 \pmod 9$

$\equiv 2 + 4 \pmod 9$

$\equiv 6 \pmod 9$ … (ii)

Dari (i) dan (ii) dapat disimpulkan **benar**

Perlu diperhatikan bahwa pemeriksaan kebenaran penjumlahan, pengurangan, perkalian dan pembagian dengan kekongruenan modulo. Ini belum menjamin bahwa operasi yang dilakukan itu benar atau salah. Tetapi cara ini dilakukan setelah mengerjakan operasi hitung tersebut mungkin dalam mengoperasikan keliru menjumlah puluhannya, raturasan dan lainnya. Dengan kata lain, koreksi 9 tersebut bukan merupakan syarat cukup. Tetapi hanya merupakan syarat perlu untuk memerikasi kebenaran hasil operasi.

**Contoh 5.12**

10 + 11 = 30

Penyelesaian:

$10 + 11 \equiv 3 \ (mod\ 9)$ dan $30 \equiv 3 \ (mod\ 9)$

Jika dilakukan menggunakan aplikasi kekongruenan 10 + 11 = 30 bernilai benar. Tetapi pada konsep operasi hitung penjumlahan 10 + 11 = 30 bernilai salah.

Selain itu, kekongruenan modulo 9 dapat digunakan untuk menguji keterbagian suatu bilangan bulat oleh 9. Suatu bilangan terbagi 9 bila dan hanya bila sisa pembagian itu 0 (nol).

n ≡ a (mod 9) bila dan hanya bila n dan a masing – masing mempunyai sisa yang sama jika dibagi 9. Jadi, jika n ≡ a (mod 9) maka n terbagi oleh 9 bila dan hanya bila a terbagi habis oleh 9. Padahal n kongruen modulo 9 dengan jumlah angka – angkanya. Dengan kata lain, suatu bilangan bulat terbagi habis oleh 9, apabila jumlah angka – angkanya terbagi oleh 9.

**Contoh 5.13**

1. $7587 \equiv 7 + 5 + 8 + 7 \equiv 27 \equiv 9 \ (mod\ 9)$
   Karena 9 | 9 maka 9 | 7587
2. $47623 \equiv 4 + 7 + 6 + 2 + 3 \equiv 22 \equiv 4 \ (mod\ 9)$
   Karena 9 | 9 maka 9 ∤ 47623

Apabila suatu bilangan bulat yang terbagi oleh 9 akan terbagia oleh 3? Misalkan 9| n dan 3|9 dengan sifat transitif diperoleh 3|n. Karena suatu bilangan bulat terbagi oleh 9 bila dan hanya bila jumlah angka – angkanya terbagi oleh 9, maka n terbagi oleh 3 bila dan hanya bila jumlah angka – angkanya terbagi oleh 3.

**Contoh 5.14**

1. $12456 \equiv 1 + 2 + 4 + 5 + 6 \equiv 18 \equiv 9 \ (mod\ 9)$
   Karena 3 | 9 maka 3 | 12456
2. $42641 \equiv 4 + 2 + 6 + 4 + 1 \equiv 17 \equiv 8 \ (mod\ 9)$
   Karena 3 | 8 maka $3 \nmid 42641$

## C. Perkongruenan Linear

Kalimat terbuka yang menggunakan relasi kekongruenan disebut perkongruenan, Misalnya
$3x \equiv 4 \pmod 5$

**Teorema 5.11**

$Jika\ (a, m) \nmid b$ maka perkongruenan linier $ax \equiv b \pmod m$ tidak memiliki solusi

Pembuktian

Kontraposisi : Jika $ax \equiv b \pmod m$ memiliki solusi maka $(a, m) | b$. Misal r adalah solusi dari $ax \equiv b \pmod m$ maka $ar \equiv b \pmod m$ sehingga ar – b = km untuk suatu bilangan bulat k. perhatikan ar – b = km. karena (a, m) | a dan (a, m) | km maka (a, m) | b. Terbuktilah kontraposisi dari teorema itu, sehingga terbukti pula teorema tersebut.

Contoh:

$6x \equiv 7 \pmod 8$ karena (6, 8) = 2 dan $2 \nmid 7$ maka pengkoruenan linier $6x \equiv 7 \pmod 8$ tidak memiliki solusi.

**Teorema 5.12**

$Jika\ (a, m) = 1$ maka perkongruenan linier $ax \equiv b \pmod m$ memiliki tepat satu solusi

**Pembuktian:**

Karena $(a, m) = 1$ maka ada bilangan bulat r dan s sehingga ar + ms = 1. Jika kedua ruas dari persamaan ini dilakukan b diperoleh:

(ar) b + (ms) b = b

a (rb) + m (sb) = b

a (rb) – b = - (sb) m

Persamaan terakhir ini berarti a (rb) – b adalah kelipatan m. $a\ (rb) \equiv b \pmod m$. Maka residu terkecil dari rb modulo m adalah solusi dari perkongruenan linear itu. Selanjutnya tinggal

menunjukkan bahwa solusi itu tunggal, andaikan solusi perkongruenan linear itu tidak tunggal, misalnya r dan s masing – masing solusi dari ax ≡ b (mod m), maka

ar ≡ b (mod m) dan as ≡ b (mod m)

dengan sifat transitif diperoleh ar ≡ as (mod m) karena (a, m) = 1 maka r ≡ s (mod m). Ini berarti m| (r – s). Tetapi karena r dan s adalah solusi dari perkongruenan itu, maka r dan s masing – masing residu terkecil modulo m, $0 \leq r < m$ dan $0 \leq s < m$. Dari kedua ketidaksamaan ini diperoleh bahwa $m \leq r - s < m$, karena m| (r – s) maka r – s = 0 atau r = s. Ini berarti bahwa solusi dari perkongruenan linear tersebut tunggal (terbukti).

Salah satu cara menyelesaikan perkongruenan linier adalah memanipulasi koefisien atau konstanta pada perkongruenan itu, sehingga memungkinkan untuk melakukan kanselasi (penghapusan).

**Contoh 5.15**

1. Selesaikan 4 x ≡ 1 (mod 15)

**Penyelesaian:**

Jika $(4, 15)|1\ dan\ 1|1$ maka perkongruenan linier tersebut memiliki solusi

Jika $(4, 15) = 1$ maka perkongruenan linier tersebut memiliki tepat satu solusi

4 x ≡ 1 (mod 15)

4x ≡ 1 (mod 15)

4x ≡ 16 (mod 15)

x ≡ 4 (mod 15)

Karena (4, 15) = 1 maka memungkinkan melakukan kanselasi (penghapusan) 4 pada pengkongruenan x ≡ 4 (mod 15)

Jadi, Solusi dari pengkongruenan 4x ≡ 1 (mod 15) adalah 4.

2. Selesaikan 14 x ≡ 27 (mod 31)

**Penyelesaian:**

Jika $(14, 31) = 1\ dan\ 1|27$ maka perkongruenan linier tersebut memliki solusi

Jika $(14, 31) = 1$ maka perkongruenan linier tersebut memiliki tepat satu solusi

14 x ≡ 27 (mod 31) karena 27 ≡ 58 (mod 31)

14 x ≡ 58 (mod 31) karena (2,31) = 1 maka menghapus 2

7x ≡ 29 (mod 31) karena 29 ≡ 91 (mod 31)

7x ≡ 91 (mod 31) karena (7,31) = 1 maka menghapus 7

x ≡ 13 (mod 31)

Jadi, 13 adalah solusi 14 x ≡ 27 (mod 31)

Jilka (a, m) = 1 maka pengkongruenan ax ≡ 1 (mod m) mempunyai tepat satu solusi pula. Solusi pengkongruenan itu disebut invers dari a modulo m yang diberi symbol $a^{-1}$ (mod m)

**Contoh 5.16**

Carilah $2^{-1}$ (mod 13)

Penyelesaian:

2x ≡ 1 $(mod\ 13)$

2x ≡ 14 $(mod\ 13)$

x ≡ 7 $(mod\ 13)$

jadi $2^{-1}$ (mod 13) adalah 7

**Latihan 5.1**

Periksa bahwa

a. $3^{-1}$ (mod 13) adalah 9

b. $4^{-1}$ (mod 13) adalah 10

c. $5^{-1}$ (mod 13) adalah 8

**Teorema 5.13**

Jilka (a, m) = 1 dan d|b maka perkogruenan linear ax ≡ $b$ $(mod\ m)$ memiliki tepat d solusi.

**Contoh 5.17**

Selesaikan 6x ≡ 15 $(mod\ 33)$

**Penyelesaian:**

Jika $(6, 33)|3$ dan 3|15 maka perkongruenan linier tersebut memiliki solusi

Jika $(6, 33) = 3$ dan 3|15 maka perkongruenan linier tersebut memiliki tepat 3 solusi

6x ≡ 15 $(mod\ 33)$

2x ≡ 5 $(mod\ 11)$

2x ≡ 16 $(mod\ 11)$

x ≡ 8 $(mod\ 11)$

Maka bilangan – bilangan bulat positif yang memenuhi x ≡ 8 $(mod\ 11)$ dan merupakan residu terkecil modulo 33 adalah, 8, 19, 30. Jadi solusi dari 6x ≡ 15 $(mod\ 33)$ adalah 8, 19, 30.

Cara lainnya untuk mencari inver dari modulo a

**Contoh 5.18**

13. x ≡ 8 (mod 30)

**Penyelesaian:**

Jika $(13, 30) = 1$ dan 1| 8 maka perkongruenan linier tersebut memliki solusi

Jika $(13, 30) = 1$ maka perkongruenan linier tersebut memliki tepat satu solusi

13. x ≡ 1 (mod 30)

13. x = 1 + 30.k  k sembarang bilangan bulat

Jika k = 3

13. x = 1 + 90  (i)

13. x = 91

13. 7 = 91

91 = 91

$\bar{a}$ = 7

Subtitusikan nilai $\bar{a}$ = 7 ke (i):

13 x ≡ 8 (mod 30)

13 .7 ≡ 8.7 (mod 30)

91 x ≡ 56 (mod 30)

1.x ≡ 56 (mod 30)  56 = 30. 1 + 26

x ≡ 26 (mod 30)

Jadi, 26 adalah solusi 13 x ≡ 8 (mod 30)

Jika perkongruenan menggunakan persamaan linier Diophantus ax + by = c, berarti $ax \equiv c\ (mod)$. Dapat pula ax + by = c berarti $by \equiv c\ (mod\ a)$. Oleh karena itu, untuk menyelesaikan persamaan ax + by = c dengan a, b, c, x dan y bilangan – bilangan bulat dapat menyelesaikan salah satu perkongruenan

$$ax \equiv c\ (mod) \text{ dan } by \equiv c\ (mod\ a).$$

**Contoh 5.19**

Carilah nilai x dan y pada persamaan berikut: 9 x + 16y = 35

Penyelesaian:

$by \equiv c\ (mod\ a)$

9x + 16y = 35 berarti

$16y \equiv 35\ (mod\ 9)$.  9. 3 + 8 = 35

$16y \equiv 8\ (mod\ 9)$.  (8,9) = 1 maka menghapus 8

$2y \equiv 1\ (mod\ 9)$.

$2y \equiv 10\ (mod\ 9)$  (2,9) = 1 maka menghapus 2

$y \equiv 5\ (mod\ 9)$.

Berarti $y = 5 + 9t$ untuk t bilangan bulat

Nilai y ini di subtitusikan pada 9x + 16y = 35 maka memberikan:

$$9x + 16y = 35$$

$$9x + 16\,(5 + 9t) = 35$$

$$9x + 80 + 144\,t = 35$$

$$9x + 144\,t = -45$$

$$x + 16\,t = -5$$

$$x = -5 - 16\,t$$

sehingga himpunan penyelesaian dari 9x + 16y = 35 adalah:

x = - 5 – 16 t dan $y = 5 + 9t$ untuk t bilangan bulat

Jika t = 0 maka x = - 5 dan y = 5 sehingga (- 5, 5) adalah salah satu penyelesaian dari persamaan 9x + 16y = 35

Syarat perkongreuenan untuk menyelesaikan persamaan linier Diophantus:

1. ax + by = c dengan $ab \neq 0$ tidak mempunyai penyelesaian solusi, apabila (a,b) $\nmid c$
2. ax + by = c dengan $ab \neq 0$ mempunyai penyelesaian solusi, apabila (a,b) $\mid c$

Contoh: 2x + 4y = 5, $2.4 \neq 0$, (2,4) = 2 dan $2 \nmid 5$ sehingga persamaan tersebut tidak mempunyai solusi

**Contoh 5.20**

Carilah bilangan – bilangan bulat positif x dan y yang memenuhi

7x + 15y = 51

**Penyelesaian:**

7x + 15y = 51 terlihat $7.5 \neq 0$, (7,15) = 1 dan $1 \nmid 51$ sehingga persamaan tersebut mempunyai solusi

$by \equiv c\ (mod\ a)$

7x + 15y = 51 berarti

$15y \equiv 51\ (mod\ 7)$. (3,7) = 1 maka menghapus 3

$5y \equiv 17\ (mod\ 7)$. 17 = 10. 1 + 7

$5y \equiv 10\ (mod\ 7)$ (5,7) = 1 maka menghapus 5

$y \equiv 2\ (mod\ 7)$ (2,9) = 1 maka menghapus 1

Jadi y = 2 + 7t untuk t bilangan cacah maka subtitusikan ke pers

$$7x + 15y = 51$$

$$7x + 15\,(2 + 7t) = 51$$

$$7x + 105t + 35 = 51$$

$$7x + 105t = 21$$

$$7x = 21 - 105t$$

$$x = 3 - 15t$$

karena x bilangan bulat positif dan t bilangan cacah maka x = 3, yaitu untuk t = 0 sehingga y = 2. Jadi bilangan – bilangan bulat positif x dan y yang memenuhi persamaan tersebut berturut – turut 3 dan 2.

Keterangan:

Bilangan cacah adalah himpunan bilangan bulat yang tidak negatif atau himpunan bilangan asli ditambah 0.

Bilangan bulat positif adalah himpunan suatu bilangan yang memiliki nilai positif atau disebut juga dengan bilangan asli.

**Teorema 5.14**

persamaan linier Diophantus a'x + b'y = c' yang diperoleh dari ax + by = c dengan a' = $\frac{a}{(a,b)}$ dan b' = $\frac{b}{(a,b)}$ dan c' = $\frac{c}{(a,b)}$ mempunyai suatu penyelesaian (solusi) x = r dan y = s maka himpunan semua penyelesaian dari ax + by = c adalah

$$\{(x,y) \mid x = r + b't,\ y = s - a't \text{ untuk } t \text{ bilangan bulat}\}$$

**Contoh 5.21**

Selesaikan persamaan linier Diophantus: 12 x + 18y = 48

**Penyelesaian:**

ax + by = c

12 x + 18y = 48

a' = $\frac{a}{(a,b)} = \frac{12}{(12,18)} = \frac{12}{6} = 2$

b' = $\frac{b}{(a,b)} = \frac{18}{(12,18)} = \frac{18}{6} = 3$

c' = $\frac{c}{(a,b)} = \frac{48}{(12,18)} = \frac{48}{6} = 8$

2x + 3y = 8 ubah dalam bentuk perkongruenan menjadi $2x \equiv 8 \pmod 3$ dan $3y \equiv 8 \pmod 2$.

Dalam teorema 5.13, x = s dan y = r maka

$2x \equiv 8 \pmod 3$ gunakan residu terkecil

$2x \equiv 2 \pmod 3$

$35\ y_1 \equiv 1 \pmod 3$ $\quad 3.11 + 2 = 35$

ka + s = m maka 2. 3 + 2 = 8 maka y = 2

silahkan buktikan sendiri x = r = 1

Jadi himpunan penyelesaian pada persamaan tersebut adalah

$$x= 1 + 3t \text{ dan } y = 2 – 2t, t \text{ bilangan bulat}$$

## D. Teorema Sisa Cina (Tsc)

**Teorema 5.15**

Sistem pengkongruenan linear $x \equiv a_i \pmod{m_i}$, i = 1, 2, 3, …, k dengan $(m_i, m_j) = 1$ untuk setiap $i \neq j$ memiliki solusi bersama modulo M dan solusi bersama itu tunggal dengan $M = m_1, m_2, \dots m_k$

**Pembuktian:**

Misalnya: $M = m_1, m_2, \dots m_k$ dan $M_r = \frac{M}{M_r}$ maka $(M_r, M_r) = 1$, sehingga perkongruenan $M_r y \equiv 1 \ (mod\ m)$ mempunyai solusi $s_r$. Jika kedua ruas dari pengkongruenan ini dikalikan a, maka diperoleh $x \equiv a_r\ M_r\ s_r \equiv a_r\ (mod\ m_r)$ sehingga:

$$x = a_1\ M_1\ s_1 + a_2\ M_2\ s_2 + \cdots + a_r\ M_r\ s_r$$

Adalah solusi bersama dari sistem pengkongruenan semula, sebab $m_r | M_j$ untuk $r \neq j$ maka $M_j \equiv 0\ (mod\ m_r)$.

**Catatan:**

$(m_i, m_j) = 1$ untuk setiap $i \neq j$ dengan i = 1, 2, 3, …, k dikatakan $M = m_1, m_2, \dots m_k$ saling prima dua – dua (saling prima sepasang demi sepasang)

Misalkan $n_1, n_2, \dots, n_r$ bilangan bulat positif sehingga FPB $(n_i, n_j) = 1$ untuk $i \neq j$. Maka sistem kongruensi linear satu variabel berikut:

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

⋮

$x \equiv a_r \pmod{n_r}$

Mempunyai penyelesaian, dengan penyelesaian tersebut tunggal terhadap modulo, $N = n_1, n_2, \dots n_r$

**Langkah Pengerjaan TSC**

1. Cari $N = n_1, n_2, \dots, n_r$

   Dengan:

   $N_1 = \frac{N}{n_1}$ , $N_2 = \frac{N}{n_2}$ , $N_r = \frac{N}{n_r}$

2. Cari solusi dari pers. Kongruensi

   $N_1\ y_1 \equiv 1 \pmod{n_1}$

   $N_2\ y_2 \equiv 1 \pmod{n_2}$

   ⋮

   $N_r\ y_r \equiv 1 \pmod{n_r}$

3. Solusi dari sistem kongruensi

   $x_1 \equiv a_1 \pmod{n_1}$

   $x_2 \equiv a_2 \pmod{n_2}$

   ⋮

   $x_r \equiv a_r \pmod{n_r}$

$x \equiv (a_1 N_1 y_1 + a_2 N_2 y_2 + \ldots + a_r N_r y_r \pmod{N}$

**Contoh 5.22**

1. Tentukan solusi sistem perkongruenan:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

Diketahui:

$a_1 = 1 \quad a_2 = 2 \quad a_3 = 3$

$n_1 = 3 \quad n_2 = 5 \quad n_3 = 7$

**Langkah 1: Mencari N**

$N = n_1\ n_2\ n_3 = 3.\ 5.\ 7 = 105$

$N_1 = \frac{N}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{N}{n_2} = \frac{105}{5} = 21$

$N_3 = \frac{N}{n_3} = \frac{105}{7} = 15$

**Langkah 2 Mencari inversnya**

$N_1\ y_1 \equiv 1 \pmod 3$

$35\ y_1 \equiv 1 \pmod 3$ $\quad 3.11 + 2 = 35$

$y_1 = 2$

$N_2\ y_2 \equiv 1 \pmod 5$

$21\ y_2 \equiv 1 \pmod 5$ $\quad 5.4 + 1 = 21$

$y_2 = 1$

$N_3\ y_3 \equiv 1 \pmod 7$

$15\ y_3 \equiv 1 \pmod 7$ $\quad 7.2 + 1 = 15$

$y_3 = 1$

**Langkah 3: Mencari Solusi**

$x \equiv (a_1 N_1 y_1 + a_2 N_2 y_2 + \ldots + a_r N_r y_r \pmod N)$

$x \equiv (1.35.2 + 2.21.1 + 3.15.1 \pmod{105})$

$x \equiv (70 + 42 + 45) \pmod{105}$

$x \equiv 157 \pmod{105}$ sederhanakan $105.1 + 52$

$x \equiv 52 \pmod{105}$

Jadi solusi dari sistem perkongruenan tersebut adalah $x \equiv 52 \pmod{105}$

2. Tentukan Solusi Sistem Perkongruenan:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 4 \end{cases}$$

Diketahui:

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 1$

$n_1 = 3 \quad n_2 = 5 \quad n_3 = 4$

**Langkah 1: Mencari N**

$N = n_1\ n_2\ n_3 = 3.\ 5.\ 4 = 60$

$N_1 = \frac{N}{n_1} = \frac{60}{3} = 20$

$N_2 = \frac{N}{n_2} = \frac{60}{5} = 12$

$N_3 = \frac{N}{n_3} = \frac{60}{4} = 15$

**Langkah 2: Mencari inversnya**

$N_1\ y_1 \equiv 1 \pmod 3$

$20\ y_1 \equiv 1 \pmod 3$ $\quad 3.6 + 2 = 20$

$y_1 = 2$

$N_2\ y_2 \equiv 1 \pmod 5$

$12\ y_2 \equiv 1 \pmod 5$ $\quad 5.2 + 2 = 12$

$y_2 = 2$

$N_3\ y_3 \equiv 1 \pmod 4$

$15\ y_3 \equiv 1 \pmod 4$ $\quad 4.3 + 2 = 15$

$y_3 = 3$

**Langkah 3: Mencari Solusi**

$x \equiv (a_1 N_1 y_1 + a_2 N_2 y_2 + \ldots + a_r N_r y_r \pmod N)$

$x \equiv (2.20.2 + 3.12.2 + 1.15.3 \pmod{60})$

$x \equiv (80 + 72 + 45) \pmod{60}$

$x \equiv 197 \pmod{60}$ Sederhanakan

$x \equiv 17 \pmod{60}$

Jadi solusi dari sistem perkongruenan tersebut adalah

$x \equiv 17 \pmod{60}$

3. Alkisah seorang Nenek pergi ke pasar dengan membawa keranjang berisi telur.Di pasar keranjang tersebut ditaruh di bawah, tanpa sengaja seorang pemuda menginjak keranjang tersebut sehingga pecah semua telur yang berada didalam keranjang. Pemuda tersebut berniat menganti kerugian dan bertanya kepada si nenek berapa jumlah telur di keranjang. Akan tetapi si Nenek tidak ingat berapa jumlah telur di keranjang. Si Nenek hanya ingat jika jumlah telur tersebut dibagi 3 maka sisanya 2 telur. Jika dibagi 5 maka sisanya 3 telur dan jika dibagi 7 maka sisanya 2 telur. Berapa jumlah telur terkecil yang mungkin dimiliki si Nenek? Bagaimana mencari solusi dari sistem linear kongkruen? Tentukan Solusi Sistem Perkongruenan:

**Penyelesaian:**

Jika di ubah ke dalam bentuk kongruenan

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Diketahui:

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

$n_1 = 3 \quad n_2 = 5 \quad n_3 = 7$

**Langkah 1: Mencari N**

$N = n_1 n_2 n_3 = 3.5.7 = 105$

$N_1 = \frac{N}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{N}{n_2} = \frac{105}{5} = 21$

$N_3 = \frac{N}{n_3} = \frac{105}{7} = 15$

**Langkah 2: Mencari inversnya**

$N_1 y_1 \equiv 1 \pmod 3$

$35\, y_1 \equiv 1 \pmod 3$ $33.1 + 2$

$2\ y_1 \equiv 1 \pmod 3$  $3.1 + 1 = 2.2$

$y_1 \equiv 2 \pmod 3$

$y_1 = 2$

$N_2\ y_2 \equiv 1 \pmod 5$

$21\ y_2 \equiv 1 \pmod 5$  $5.4 + 1$

$y_2 \equiv 1 \pmod 5$

$y_2 = 1$

$N_3\ y_3 \equiv 1 \pmod 7$

$15\ y_3 \equiv 1 \pmod 7$  $7.2 + 1$

$y_3 \equiv 1 \pmod 7$

$y_3 = 1$

**Langkah 3: Mencari Solusi**

$x \equiv (a_1\ N_1\ y_1 + a_2\ N_2\ y_2 + \ldots + a_r\ N_r\ y_r \pmod N)$

$x \equiv (2.35.2 + 3.21.1 + 2.15.1 \pmod{105})$

$x \equiv (140 + 63 + 30) \pmod{105}$

$x \equiv 233 \pmod{105}$  Sederhanakan

$x \equiv 23 \pmod{105}$

Jadi solusi dari sistem perkongruenan tersebut adalah $x \equiv 23 \pmod{105}$ atau jumlah telur yang ada di keranjang adalah 23 butir.

**Latihan 5.2**

Tentukan solusi sistem perkongruenan menggunakan TSC

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 7 \end{cases}$$

## A. Sistem Perkongruenan Linier

**Teorema 5.16**

Misalnya m suatu bilangan asli dan $(\Delta, m) = 1$ dengan $\Delta = ad - bc$ maka sistem pengkongruenan linier

$$ax + by \equiv e \pmod m$$
$$cx + dy \equiv f \pmod m$$

mempunyai penyelesaia (x, y) dengan

$$x \equiv \Delta^{-1}\ (de - bf)(mod\ m)$$
$$y \equiv \Delta^{-1}\ (af - ce)(mod\ m)$$

dengan $\Delta^{-1}$ adalah invers dari $\Delta$ dari modulo m

Pembuktian:

Mengalikan perkongruenan pertama dengan d dan perkongruenan kedua dengan b sehingga diperoleh:

$$\text{adx} + \text{bdy} \equiv \text{de} \pmod{\text{m}}$$

$$\text{bcx} + \text{bdy} \equiv \text{bf} \pmod{\text{m}}$$

hasil pengurangan dari pengkongruenan pertama dan kedua adalah

$$(\text{ad} - \text{bc})\,\text{x} \equiv \text{de} - \text{bf} \pmod{\text{m}}$$

dan karena $\Delta = ad - bc$ maka

$$\Delta\text{x} \equiv \text{de} - \text{bf} \pmod{\text{m}}$$

Selanjutnya karena $(\Delta, m) = 1$ maka $\Delta$ maka mempunyai invers modulo m, yaitu: $\Delta^{-1}$. Jika kedua ruas perkongruenan terakhir dikalikan dengan $\Delta^{-1}$ maka diperoleh:

$$\text{x} \equiv \Delta^{-1}(\text{de} - \text{bf}) \pmod{\text{m}}$$

Dengan cara yang seperti tersebut, pada sistem pengkongruenan semula., lakukan perkalian perkongruenan pertama dengan c dan perkongruenan kedua dengan a sehingga diperoleh:

$$\text{acx} + \text{bcy} \equiv \text{ce} \pmod{\text{m}}$$

$$\text{acx} + \text{ady} \equiv \text{af} \pmod{\text{m}}$$

hasil pengurangan dari pengkongruenan pertama dan kedua adalah

$$(\text{ad} - \text{bc})\,\text{y} \equiv \text{af} - \text{ce} \pmod{\text{m}}$$

dan karena $\Delta = ad - bc$ maka

$$\Delta\text{y} \equiv \text{af} - \text{ce} \pmod{\text{m}}$$

Selanjutnya karena $(\Delta, m) = 1$ maka $\Delta$ maka mempunyai invers modulo m, yaitu: $\Delta^{-1}$. Jika kedua ruas perkongruenan terakhir dikalikan dengan $\Delta^{-1}$ maka diperoleh:

$$\text{x} \equiv \Delta^{-1}(\text{af} - \text{ce}) \pmod{\text{m}}$$

Jadit terbukti

$$x \equiv \Delta^{-1}\,(de - bf)(mod\ m)$$

$$y \equiv \Delta^{-1}\,(af - ce)(mod\ m)$$

**Definisi 5.4**

Misalkan A = $a_{ij}$ dan B = $b_{ij}$ masing – masing matriks berukuran $n\,x\,k$ yang elemen – elemennya bilangan – bilangan bulat. Matriks A kongruen modulo matriks B, dinotasikan $A \equiv B\ (mod\ m)$, $a_{ij} \equiv b_{ij}\ (mod\ m)$ untuk setiap pasangan (i,j) dengan $1 \leq i \leq n$ dan $1 \leq j \leq k$

Contoh:

$\begin{pmatrix}15 & 3\\ 8 & 12\end{pmatrix} \equiv \begin{pmatrix}4 & 3\\ -3 & 1\end{pmatrix} (mod\ 11)$

Karena $15 \equiv 4\ (mod\ 11)$, $8 \equiv -3\ (mod\ 11)$, $12 \equiv 1\ (mod\ 11)$,

**Teorema 5.17**

Jika A = $a_{ij}$ dan B = $b_{ij}$ adalah matriks – matriks berukuran $n\ x\ k$ dengan dinotasikan $A \equiv B\ (mod\ m)$, C = $c_{ij}$ ialah matriks berukuran $k\ x\ p$ dan D = $d_{ij}$ ialah matriks berukuran $t\ x\ n$ maka $AC \equiv BC\ (mod\ m)$ dan $DA \equiv DB\ (mod\ m)$

Bukti:

Misalkan $AC = E = e_{ij}$ ialah matriks berukuran $n\ x\ p$ dengan $e_{ij} = \sum_{r=1}^{k} a_{ir}\, c_{rj}$ dan BC = G = $g_{ij}$ ialah matriks berukuran $n\ x\ p$ dengan $g_{ij} = \sum_{r=1}^{k} b_{ir}\, c_{rj}$. Karena $A \equiv B\ (mod\ m)$ maka $a_{ij} \equiv b_{ij}\ (mod\ m)$ untuk setiap i dan j sehingga $a_{ir}\, c_{rj} \equiv b_{ij}\ (mod\ m)$ untuk setiap $1 \leq r \leq k$. Akibatnya $\sum_{r=1}^{k} a_{ir}\, c_{rj} \equiv \sum_{r=1}^{k} b_{ir}\, c_{rj}\ (mod\ m)$ untuk $e_{ij} \equiv g_{ij} (mod\ m)$. Hal ini berarti $AC \equiv BC\ (mod\ m)$ dan $DA \equiv DB\ (mod\ m)$

**Definisi 5.5**

Jika A dan $A^{-1}$ adalah matriks – matriks berukuran n x n yang elemen- elemennya bilangan bulat sedemikian hingga bulat sederhana $AA^{-1} \equiv AA^{-1} \equiv I\ (mod\ m)$, dengan I ialah matriks identitas berukuran n, maka $A^{-1}$ disebut invers dari A modulo m.

Contoh:

$\begin{pmatrix}1 & 3\\ 2 & 4\end{pmatrix}\begin{pmatrix}3 & 4\\ 1 & 2\end{pmatrix} = \begin{pmatrix}6 & 10\\ 10 & 16\end{pmatrix} \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\ (mod\ 5)$

$\begin{pmatrix}3 & 4\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & 3\\ 2 & 4\end{pmatrix} = \begin{pmatrix}11 & 25\\ 5 & 1\end{pmatrix} \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\ (mod\ 5)$

Tampak bahwa $\begin{pmatrix}3 & 4\\ 1 & 2\end{pmatrix}$ adalah invers dari $\begin{pmatrix}3 & 4\\ 1 & 2\end{pmatrix}\ (mod\ 5)$

Teorema 18

Misalkan $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ adalah matriks yang elemen bilangan – bilangan bulat, sedemikian hingga $\det A = \Delta = ad - bc$ prima relatif terhadap bilangan bulat positif m. maka

$$A^{-1} = \Delta^{-1}\begin{pmatrix}a & -b\\ -c & d\end{pmatrix}$$

**Definisi 5.6**

Misalkan A suatu matriks persegi berukuran n. Adjoint dari A diberi symbol adj (A) adalah suatu matriks persegi berukuran n yang elemen pada baris ke – i kolom ke- j ialah $d_{ij}$ dengan

$d_{ij}$ sama dengan $(-1)^{i+j}$ determinan matriks yang diperoleh dari A dengan menghapus semua elemen pada baris ke – i dan kolom ke-j.

**Teorema 5.18**

Jika A suatu matriks persegi dengan $\Delta = \det A \neq 0$ maka A $adj\ (A) = (\det A)\ I$.

**Teorema 5.19**

Jika A suatu matriks persegi yang elemen – elemennya bilangan bulat dan m suatu bilangan bulat positif sedemikian hingga $(\Delta, m) = 1$ maka invers dari modulo m adalah

$$A^{-1} = \Delta^{-1} adj\ (A)$$

Bukti:

$(\Delta, m) = 1$ maka $\Delta^{-1}$ ada. Karena $\Delta \neq 0$ maka A adj (A) = $\Delta I$ sehingga:

$$A\ \Delta^{-1} adj\ (A) \equiv \Delta\ \Delta^{-1} I \equiv I\ (mod\ m)$$

$$\Delta^{-1} adj\ (A)\ A \equiv \Delta\ \Delta^{-1} I \equiv I\ (mod\ m)$$

Ini menunjukkan bahwa $A^{-1} = \Delta^{-1} adj\ (A)$ adalah invers dari A mod m.

**Contoh 5.23**

1. Selesaikan sistem persamaan pengkongruenan berikut ini menggunakan Metode Eliminasi & Subtitusi dan Metode Invers

   $2x + 5y + 6z \equiv 3 \pmod 7$

   $2x + z \equiv 4 \pmod 7$

   $x + 2y + 3z \equiv 1 \pmod 7$

**Penyelesaian:**

**Metode Eliminasi**

$2x + 5y + 6z \equiv 3 \pmod 7$ … persamaan 1

$2x + z \equiv 4 \pmod 7$ …persamaan 2

$x + 2y + 3z \equiv 1 \pmod 7$ …persamaan 3

Eliminasi variabel y menggunakan pers (1) dan pers (2)

$2x + 5y + 6z \equiv 3 \pmod 7$ x 2 $\quad 4x + 10y + 12z \equiv 6 \pmod 7$

$x + 2y + 3z \equiv 1 \pmod 7$ x 5 $\quad 5x + 10y + 15z \equiv 5 \pmod 7$

$-x - 3z \equiv 1 \pmod 7$

$x + 3z \equiv -1 \pmod 7$ persamaan 4

Eliminasi variabel z menggunakan pers (2) dan pers (4)

$2x + z \equiv 4 \pmod 7$ x 3 $6x + 3z \equiv 12 \pmod 7$

$x + 3z \equiv -1 \pmod 7$ x 1 $x + 3z \equiv -1 \pmod 7$

$5x \equiv 13 \pmod 7$

$5x \equiv 13 \pmod 7$

$5x \equiv 20 \pmod 7$

$x \equiv 4 \pmod 7$

Eliminasi variabel x menggunakan pers (2) dan pers (4)

$2x + z \equiv 4 \pmod 7$ x 1 $2x + z \equiv 4 \pmod 7$

$x + 3z \equiv -1 \pmod 7$ x 2 $2x + 6z \equiv -2 \pmod 7$

$-5z \equiv 6 \pmod 7$

$5z \equiv -6 \pmod 7$

$5z \equiv -6 \pmod 7$

$5z \equiv 1 \pmod 7$

$5z \equiv 8 \pmod 7$

$5z \equiv 15 \pmod 7$

$z \equiv 3 \pmod 7$

Subtitusi nilai x dan z ke pers (1)

$x + 2y + 3z \equiv 1 \pmod 7$

$4 \pmod 7 + 2y + 3(3 \pmod 7) \equiv 1 \pmod 7$

$4 \pmod 7 + 2y + 9 \pmod 7 \equiv 1 \pmod 7$

$13 \pmod 7 + 2y \equiv 1 \pmod 7$

$2y \equiv 1 \pmod 7 - 13 \pmod 7$

$2y \equiv -12 \pmod 7$

$2y \equiv -5 \pmod 7$

$2y \equiv 2 \pmod 7$

$y \equiv 1 \pmod 7$

Jadi nilai masing – masing x, y dan z adalah

$x \equiv 4 \pmod 7$ $y \equiv 1 \pmod 7$ $z \equiv 3 \pmod 7$

**Metode Invers**

$2x + 5y + 6z \equiv 3 \pmod 7$

$2x + z \equiv 4 \pmod 7$

$x + 2y + 3z \equiv 1 \pmod 7$

Langkah 1: ubah dalam bentuk matriks

$$A = \begin{bmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{bmatrix} \pmod 7$$

Langkah 2: Cari nilai $\Delta^{-1}$

Rumus: $\Delta \,.\, \Delta^{-1} \equiv 1 \pmod m$

$$\Delta = \det A$$

Mencari determinan A menggunakan metode sarrus

$$\begin{vmatrix} 2 & 5 & 6 & 1 & 5 \\ 2 & 0 & 1 & 2 & 0 \\ 1 & 2 & 3 & 1 & 2 \end{vmatrix} = (0 + 5 + 24) - (30 + 4 + 0) = -5$$

$\Delta \,.\, \Delta^{-1} \equiv 1 \pmod m$

$-5\,\Delta^{-1} \equiv 1 \pmod 7$

$5\,\Delta^{-1} \equiv -1 \pmod 7$

$5\,\Delta^{-1} \equiv 6 \pmod 7$

$5\,\Delta^{-1} \equiv 13 \pmod 7$

$5\,\Delta^{-1} \equiv 20\ mod\ (7)$

$\Delta^{-1} \equiv 4 \pmod 7$

langkah 3: mencari Adj (A)

Menentukan adj A yaitu dengan menggunakan metode kofaktor

$$\begin{bmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

$$K_{ij} = (-1)^{i+j} \left| M_{ij} \right| = (-1)^{i+j} \det(M_{ij})$$

$$\mapsto k_{11} = (-1)^{1+1} \begin{vmatrix} 0 & 1 \\ 2 & 3 \end{vmatrix} = (0 - 2) = -2$$

$$\mapsto k_{12} = (-1)^{1+2} \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = -(6 - 1) = -5$$

$$\mapsto k_{13} = (-1)^{1+3} \begin{vmatrix} 2 & 0 \\ 1 & 2 \end{vmatrix} = 4 - 0 = 4$$

$$\mapsto k_{21} = (-1)^{2+1} \begin{vmatrix} 5 & 6 \\ 2 & 3 \end{vmatrix} = -(15 - 12) = -3$$

$$\mapsto k_{22} = (-1)^{2+2} \begin{vmatrix} 2 & 6 \\ 1 & 3 \end{vmatrix} = 6 - 6 = 0$$

$$\mapsto k_{23} = (-1)^{2+3} \begin{vmatrix} 2 & 5 \\ 1 & 2 \end{vmatrix} = -(4 - 5) = 1$$

$$\mapsto k_{31} = (-1)^{3+1}\begin{vmatrix}5 & 6\\ 0 & 1\end{vmatrix} = 5 - 0 = 5$$

$$\mapsto k_{32} = (-1)^{3+2}\begin{vmatrix}2 & 6\\ 2 & 1\end{vmatrix} = -(2 - 12) = 10$$

$$\mapsto k_{33} = (-1)^{3+3}\begin{vmatrix}2 & 5\\ 2 & 0\end{vmatrix} = 0 - 10 = -10$$

$$AdjA = (Kof(A))^T$$

$$AdjA = \begin{bmatrix}-2 & -5 & 4\\ -3 & 0 & 1\\ 5 & 10 & -10\end{bmatrix}^T$$

$$AdjA = \begin{bmatrix}-2 & -3 & 5\\ -5 & 0 & 10\\ 4 & 1 & -10\end{bmatrix}$$

Langkah 4: mencari $A^{-1}$

$$A^{-1} = \Delta^{-1}\,.\,Adj\ (A)$$

$$= 4\begin{bmatrix}-2 & -3 & 5\\ -5 & 0 & 10\\ 4 & 1 & -10\end{bmatrix} = \begin{bmatrix}-8 & -12 & 20\\ -20 & 0 & 40\\ 16 & 4 & -40\end{bmatrix}$$

Langkah 5: mencari residu terkecil (tidak boleh angka negatif)

$$A^{-1} \equiv \begin{bmatrix}-8 & -12 & 20\\ -20 & 0 & 40\\ 16 & 4 & -40\end{bmatrix} (\,mod\ 7)$$

$$A^{-1} \equiv \begin{bmatrix}6 & 2 & 6\\ 1 & 0 & 5\\ 2 & 4 & 2\end{bmatrix} (\,mod\ 7)$$

Langkah 6: mencari nilai x y dan z

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv A^{-1}\begin{bmatrix}p\\ q\\ r\end{bmatrix} (mod\ m)$$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}6 & 2 & 6\\ 1 & 0 & 5\\ 2 & 4 & 2\end{bmatrix}\begin{bmatrix}3\\ 4\\ 1\end{bmatrix} (mod\ 7)$$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}18 + 8 + 6\\ 3 + 0 + 5\\ 6 + 16 + 2\end{bmatrix} (mod\ 7)$$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}32\\ 8\\ 24\end{bmatrix} (mod\ 7)$$

x ≡ 32 (mod 7) x ≡ 4 $(mod\ 7)$

y ≡ 8 (mod 7) y ≡ 1 $(\,mod\ 7)$

z ≡ 24 (mod 7) z ≡ 3 $(\,mod\ 7)$

Jadi, penyelesaian sistem pengkongruenan pada persamaan tersebut adalah

x ≡ 4 ( $mod$ 7)  y ≡ 1 ( $mod$ 7)  z ≡ 3 ( $mod$ 7)

2. Selesaikan sistem persamaan pengkongruenan berikut ini menggunakan Metode Invers

2x + 3y + z ≡ 1 (mod 3)

x + 4y + 6z ≡ 1 (mod 3)

3x + 5y + z ≡ 1 (mod 3)

**Metode Invers**

2x + 3y + z ≡ 1 (mod 3)

x + 4y + 6z ≡ 1 (mod 3)

3x + 5y + z ≡ 1 (mod 3)

Langkah 1: ubah dalam bentuk matriks

$$A \equiv \begin{bmatrix} 2 & 3 & 1 \\ 1 & 4 & 6 \\ 3 & 5 & 1 \end{bmatrix} (mod\ 3)$$

Langkah 2: Cari nilai $\Delta^{-1}$

Rumus: $\Delta \,.\, \Delta^{-1} \equiv 1$ (mod m)

$$\Delta = \det A$$

Mencari determinan A menggunakan metode sarrus

$$\begin{vmatrix} 2 & 3 & 1 \\ 1 & 4 & 6 \\ 3 & 5 & 1 \end{vmatrix} \begin{matrix} 2 & 3 \\ 1 & 4 \\ 3 & 5 \end{matrix} = (8 + 54 + 5) - (12 + 60 + 3) = -8$$

$\Delta = -8$

$\Delta \,.\, \Delta^{-1} \equiv 1$ (mod m)

$-8\ \Delta^{-1} \equiv 1$ (mod 3)

$8\ \Delta^{-1} \equiv -1$ (mod 3)

$8\ \Delta^{-1} \equiv 8\ mod\ (3)$

$\Delta^{-1} \equiv 1$ (mod 3)

Langkah 3: mencari Adj (A)

Menentukan adj A yaitu dengan menggunakan metode kofaktor

$$\begin{bmatrix} 2 & 3 & 1 \\ 1 & 4 & 6 \\ 3 & 5 & 1 \end{bmatrix}$$

$$K_{ij} = (-1)^{i+j} \left| M_{ij} \right| = (-1)^{i+j}\ det(\ M_{ij})$$

$$\Longmapsto k_{11} = (-1)^{1+1} \begin{vmatrix} 4 & 6 \\ 5 & 1 \end{vmatrix} = (4 - 30) = -26$$

$$\Longmapsto k_{12} = (-1)^{1+2} \begin{vmatrix} 1 & 6 \\ 3 & 1 \end{vmatrix} = -(1 - 18) = -(-17) = 17$$

$$\mapsto k_{13} = (-1)^{1+3}\begin{vmatrix}1 & 4\\ 3 & 5\end{vmatrix} = 5 - 12 = -7$$

$$\mapsto k_{21} = (-1)^{2+1}\begin{vmatrix}3 & 1\\ 5 & 1\end{vmatrix} = -(3 - 5) = -(-2) = 2$$

$$\mapsto k_{22} = (-1)^{2+2}\begin{vmatrix}2 & 1\\ 3 & 1\end{vmatrix} = 2 - 3 = -1$$

$$\mapsto k_{23} = (-1)^{2+3}\begin{vmatrix}2 & 3\\ 3 & 5\end{vmatrix} = -(10 - 9) = -1$$

$$\mapsto k_{31} = (-1)^{3+1}\begin{vmatrix}3 & 1\\ 4 & 6\end{vmatrix} = 18 - 4 = 14$$

$$\mapsto k_{32} = (-1)^{3+2}\begin{vmatrix}2 & 1\\ 1 & 6\end{vmatrix} = -(12 - 1) = -11$$

$$\mapsto k_{33} = (-1)^{3+3}\begin{vmatrix}2 & 3\\ 1 & 4\end{vmatrix} = 8 - 3 = 5$$

$$AdjA = (Kof(A))^T$$

$$AdjA = \begin{bmatrix}-26 & 17 & -7\\ 2 & -1 & -1\\ 14 & -11 & 5\end{bmatrix}^T$$

$$AdjA = \begin{bmatrix}-26 & 2 & 14\\ 17 & -1 & -11\\ -7 & -1 & 5\end{bmatrix}$$

Langkah 4: mencari $A^{-1}$

$$A^{-1} = \Delta^{-1}\,.\,Adj\,(A)$$

$$= 1\begin{bmatrix}-26 & 2 & 14\\ 17 & -1 & -11\\ -7 & -1 & 5\end{bmatrix} = \begin{bmatrix}-26 & 2 & 14\\ 17 & -1 & -11\\ -7 & -1 & 5\end{bmatrix}$$

Langkah 5: mencari residu terkecil (tidak boleh angka negatif)

$$A^{-1} \equiv \begin{bmatrix}-26 & 2 & 14\\ 17 & -1 & -11\\ -7 & -1 & 5\end{bmatrix}(mod\ 3)$$

$$A^{-1} \equiv \begin{bmatrix}1 & 2 & 2\\ 2 & 2 & 1\\ 2 & 2 & 2\end{bmatrix}(mod\ 3)$$

Langkah 6: mencari nilai x y dan z

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv A^{-1}\begin{bmatrix}p\\ q\\ r\end{bmatrix}(mod\ m)$$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}1 & 2 & 2\\ 2 & 2 & 1\\ 2 & 2 & 2\end{bmatrix}\begin{bmatrix}1\\ 1\\ 1\end{bmatrix}(mod\ 3)$$

$$\begin{bmatrix}x\\ y\\ z\end{bmatrix} \equiv \begin{bmatrix}1+2+2\\ 2+2+1\\ 2+2+2\end{bmatrix}(mod\ 3)$$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 5 \\ 6 \end{bmatrix} (mod\ 3)$$

x ≡ 5 (mod 3) x ≡ 2 $(mod\ 3)$

y ≡ 5 (mod 3) y ≡ 2$(\ mod\ 3)$

z ≡ 6 (mod 3) z ≡ 0 $(\ mod\ 3)$

**Pembuktian:**

Subtitusikan nilai x y dan z ke pers 1

$2x + 3y + z \equiv 1 \pmod 3$ Persamaan 1

$2.2 + 3.2 + 0 \equiv 1 \pmod 3$

$10 \equiv 1 \pmod 3$

$10 \equiv 4 \pmod 3$

$10 \equiv 7 \pmod 3$

$10 \equiv 10 \pmod 3$ (terbukti benar)

Subtitusikan nilai x y dan z ke pers 2

$x + 4y + 6z \equiv 1 \pmod 3$

$2 + 8 + 0 \equiv 1 \pmod 3$

$10 \equiv 10 \pmod 3$ (terbukti benar)

Subtitusikan nilai x y dan z ke pers 2

$3x + 5y + z \equiv 1 \pmod 3$

$6 + 10 + 0 \equiv 1 \pmod 3$

$16 \equiv 16 \pmod 3$ (terbukti benar)

Jadi, penyelesaian sistem pengkongruenan pada persamaan tersebut adalah

x ≡ 2 $(mod\ 3)$ y ≡ 2$(\ mod\ 3)$ z ≡ 0 $(\ mod\ 3)$

# BAB VI

## TEOREMA FERMAT DAN WILSON

### A. Teorema Fermat

Teorema fermat digunakan untuk menguji keprimaan suatu bilangan bulat

**Teorema 6.1**

Jika (a,m) = 1 Maka residu – residu (sisa) terkecil modulo m = {a, 2a, 3a, …, (m−1) a ialah suatu permutasi dari 1, 2, 3, …, (m−1).

Teorema 6.1 dapat juga dikatakan bahwa jika (a, m) = 1, maka setiap bilangan bulat kongruen modulo m dengan tepat satu dari. ingat bahwa setiap bilangan bulat akan kongruen modulo m dengan tepat 0, a, 2a, 3a, … (m – 1) a satu dari 0, 1, 2, 3, 4, … (m – 1).

**Pembuktian:**

Perhatikan barisan bilangan: 0, a, 2a, 3a, … (m – 1) a … (1)

Bilangan – bilangan pada barisan ini tidak ada satu pun yang kongruen modulo dengan 0 (nol). Mengapa? Selanjutnya, kita harus membuktikan bahwa bilangan – bilangan (suku – suku) dalam barisan (1) masing – masing kongruen modulo m dengan tepat satu dari

$$1, 2, 3, \ldots, (m-1)$$

Andaikan ada dua suku dari barisan (1) yang kongruen modulo m. Misalnya:

$$ra \equiv sa \pmod{m} \quad \text{dengan } 1 \leq r < s < m$$

Karena (a, m) = 1 maka dapat menghilangkan a dari kekongruenan itu, sehingga diperoleh

$$r \equiv s \pmod{m}$$

Tetapi, karena ra dan sa adalah suku – suku dari barisan (1) maka r dan s adalah residu – residu terkecil modulo m sehingga r = s. Hal ini kontradiksi dengan pengandaian bahwa$1 \leq r < s < m$, maka pengandaian tersebut tidak benar. Jadi, tidak ada dua suku – suku barisan (1) yang kongruen modulo m. Ini berarti bahwa suku – suku dalam barisan (1) masing – masing kongruen modulo m dengan tepat satu dari 1, 2, 3, … (m – 1)

**Contoh 6.1**

Perhatikan barisan bilangan 4, 8, 12, 16, 20, 24. Tentukan residu terkecil modulo 7!

**Penyelesaian:**

$4 \equiv 4 \pmod{7}$ Karena $7 \mid (4-4)$ $7 \mid 0$

$8 \equiv 1 \pmod{7}$ Karena $7 \mid (8-1)$ $7 \mid 7$

$12 \equiv 5 \pmod{7}$ Karena $7 \mid (12-5)$ $7 \mid 7$

$16 \equiv 2 \pmod 7$ Karena $7 \mid (16-2)$ $7 \mid 14$

$20 \equiv 6 \pmod 7$ Karena $7 \mid (20-6)$ $7 \mid 14$

$24 \equiv 3 \pmod 7$ Karena $7 \mid (24-3)$ $7 \mid 21$

Tampak bahwa pada enam kekongruenan tersebut bahwa residu – residu terkecil modulo 7 dari suku – suku pada barisan 4, 8, 12, 16, 20, 24 adalah suatu permutasi dari 1, 2, 3, 4, 5, 6. Jika semua bilangan pada ruas kiri dari 6 kekongruenan ini dikalikan maka hasilnya akan kongruen mod 7 dengan hasil kali semua bilangan pada ruas kanannya,yaitu:

$$4, 8, 12, 16, 20, 24 \equiv 4, 1, 5, 2, 6, 3 \pmod 7$$

$$4^6 (1 .2. 3. 4. 5) \equiv 1. 2. 3. 4. 5. 6 \pmod 7$$

$$4^6. 6! \equiv 6! \ (mod\ 7)$$

$$4^6 \equiv 1 \ (mod\ 7)$$

**Latihan 6.1**

Tunjukkan bahwa:

1. $5^6 \equiv 1 \ (mod\ 7)$
2. $3^{10} \equiv 1 \ (mod\ 11)$
3. $4^{12} \equiv 1 \ (mod\ 13)$
4. $8^4 \equiv 1 \ (mod\ 5)$
5. $13^{16} \equiv 1 \ (mod\ 17)$

**Teorema 6.2 (Teorema Fermat)**

Jika p suatu bilangan prima dan (a,p) = 1 maka $a^{p-1} \equiv 1 \pmod p$ bermakna sama $P \mid (a^{p-1} - 1)$

Pembuktian:

Ambil sebarang bilangan prima p dan bilangan bulat a sedemikian (a, p) = 1, menurut teorema 6.1, residu – residu terkecil mod p dari a, 2a, 3a, …, $(p-1)\ a$ ialah suatu permutasi dari 1, 2, 3, …, $(p-1)$. Sehingga hasilkali – hasilkalinya akan kongruen mod p juga, yaitu:

$$a, 2a, 3a, \ldots, (p-1)\ a \equiv 1, 2, 3, \ldots, (p-1) \ (mod\ p)$$

$$a^{p-1} \ (a, 2a, 3a, \ldots, (p-1)\ a) \equiv (p-1) \ (mod\ p)$$

$$a^{p-1} \ (p-1)\ ! \equiv (p-1)! \ (mod\ p)$$

Karena p dan (p – 1)! Saling prima. Maka $(p-1)!$ dicoret, sehingga diperoleh:

$$a^{p-1} \equiv 1 \ (mod\ p)$$

**Contoh 6.2**

jika P = 5 dan a = 2. Tunjukkan $16 \equiv 1 \pmod 5$ bernilai benar

Penyelesaian:

$$2^{5-1} \equiv 1 \ (mod\ p)$$

$$2^4 \equiv 1 \ (mod\ 5)$$

$$16 \equiv 1 \ (mod\ 5)$$

Jadi, $16 \equiv 1 \pmod 5$ bernilai benar karena p = 5 suatu bilangan prima dan (2,5) = 1

**Teorema 6.3**

Jika p suatu bilangan prima maka $a^p \equiv a \ (mod\ p)$ untuk setiap bilangan bulat a.

**Pembuktian:**

Ambil sebarang bilangan prima p dan sebarang bilangan bulat a maka (a, p) = 1 atau (a, p) = p. Jika (a, p) = 1 maka menurut teorema 6.2 diperoleh

$$a^{p-1} \equiv 1 \ (\text{mod } p)$$

kedua ruas dikalikan a maka diperoleh

$$a^p \equiv a \ (\text{mod } p)$$

Jika (a, p) = p maka p | a sehingga $a \equiv 0 \pmod p$ dan $a^p \equiv a \pmod p$. jadi

$$a^p \equiv a \ (\text{mod } p) \quad \text{terbukti}$$

**Bilangan komposit** adalah bilangan asli lebih dari 1 yang bukan merupakan bilangan prima. Bilangan komposit dapat dinyatakan sebagai faktorisasi bilangan bulat, atau hasil perkalian dua bilangan prima atau lebih. Sepuluh bilangan komposit yang pertama adalah 4, 6, 8, 9, 10, 12, 14, 15.

**Teorema 6.4**

Jika p dan q adalah bilangan – bilangan prima berlainan sedemikian hingga $a^p \equiv a \pmod q$ dan $a^q \equiv a \pmod p$ maka

$$a^{pq} \equiv a \ (\text{mod } pq)$$

**Pembuktian**

Menurut teorema 6.3, karena p suatu bilangan prima, maka $(a^q)^p \equiv a^q (mod\ p)$. Selanjutnya karena diketahui bahwa $a^q \equiv a (mod\ p)$. Maka kekongruenan tersebut $a^{pq} \equiv a (mod\ p)$. Hal ini berarti bahwa $p | (a^{pq} - a)$ … (i)

Menurut teorema 6.3, karena q suatu bilangan prima, maka $(a^p)^q \equiv a^p (mod\ q)$. Selanjutnya karena diketahui bahwa $a^p \equiv a (mod\ q)$. Maka kekongruenan tersebut $a^{pq} \equiv a (mod\ q)$.

Hal ini berarti bahwa $q | (a^{pq} - a)$ … (ii)

Dari (i) dan (ii) disimpulkan $pq|\ (a^{pq} - a)$ dan dapat dinyatakan sebagai

$$a^{pq} \equiv a \pmod{pq}$$

**Contoh 6.3**

1. Tentukan sisa pembagian $9^{60}$ dengan 13!

   $9^{60}$ oleh 13

   a = 9 dan p = 13 nilai p termasuk bilangan prima

   (a, p) = (9,13) = 1

   Karena kedua syarat sudah terpenuhi maka teorema 6.1 bisa digunakan

   $a^{p-1} \equiv 1 \pmod{p}$

   $9^{13-1} \equiv 1 \pmod{13}$

   $9^{12} \equiv 1 \pmod{13}$

   $9^{60} = 9^{12.5}$

   $9^{60} \equiv (9^{12})^5 \pmod{13}$

   $9^{60} \equiv 1^5 \pmod{13}$

   $9^{60} \equiv 1 \pmod{13}$

   Maka sisa pembagian $9^{60}$ dengan 13 adalah 1

2. Berapakah sisa pembagian $7^{112}$ oleh 13!

   Penyelesaian:

   sisa pembagian $7^{112}$ oleh 13

   a = 7 dan p = 13 nilai p termasuk bilangan prima

   (a, p) = (7,13) = 1

   Karena kedua syarat sudah terpenuhi maka teorema 6.1 bisa digunakan

   $a^{p-1} \equiv 1 \pmod{p}$

   $7^{13-1} \equiv 1 \pmod{13}$

   $7^{12} \equiv 1 \pmod{13}$

   $7^{112} = 7^{12.9+4}$ $\qquad 12.9 + 4 = 112$

   $7^{112} = (7^{12})^9\ 7^4$

   $7^{112} = (7^{12})^9\ (7^2)^2$

   $7^{112} = (7^{12})^9\ (49)^2$

   $7^{112} \equiv (7^{12})^9\ (39 + 10)^2 \pmod{13}$

   Ingat: $7^{12} \equiv 1 \pmod{13}$ dan $39 \bmod (13) = 0$

   $7^{112} \equiv (1)^9\ (0 + 10)^2 \pmod{13}$

   $7^{112} \equiv 1\ 100 \pmod{13}$

$7^{112} \equiv 100 \bmod (13)$

$7^{112} \equiv (91 + 9) \bmod (13)$ $91 \bmod (13) = 0$

$7^{112} \equiv (0 + 9) \bmod (13)$

$7^{112} \equiv 9 \bmod (13)$

sisa pembagian, maka $7^{112}$ oleh 13 adalah 9

3. Apakah 41 adalah bilangan prima, buktikan!

   Penyelesaian:

   Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

   Misalnya: 2. Selanjutnya diperiksa apakah $2^{41} \equiv 2 \pmod{41}$?

   $2^{41} \equiv 2^{10.4+1} \pmod{41}$ Cari $2^n$ mendekati mod 41

   $2^{41} \equiv (2^{10})^4\ 2^1 \pmod{41}$

   $2^{41} \equiv (2^{10})^4\ 2^1 \pmod{41}$

   $2^{41} \equiv (1024)^4\ 2^1 \pmod{41}$

   $2^{41} \equiv (1025 - 1)^4\ 2^1 \pmod{41}$ $1025 \bmod (41) = 0$

   $2^{41} \equiv (-1)^4\ 2^1 \pmod{41}$

   $2^{41} \equiv 1.\ 2^1 \pmod{41}$

   $2^{41} \equiv 2 \pmod{41}$

   Dari hasil perhitungan diperoleh $2^{41} \equiv 2 \pmod{41}$. Karena $2^{41} \equiv 2 \pmod{41}$. Maka dapat disimpulkan bahwa bilangan 41 termasuk bilangan prima. Buktinya 41 = 1.41

4. Apakah 53 adalah bilangan prima, buktikan!

   Penyelesaian:

   Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

   Misalnya: 2. Selanjutnya diperiksa apakah $2^{53} \equiv 2 \pmod{53}$?

   $2^{53} \equiv 2^{6.8+5} \pmod{53}$ Cari $2^n$ mendekati (mod 53)

   $2^{53} \equiv (2^6)^8\ 2^5 \pmod{53}$ $2^6 = 64 \equiv 11 \pmod{53}$

   $2^{53} \equiv (11)^8\ 2^5 \pmod{53}$

   $2^{53} \equiv (11^2)^4\ 2^5 \pmod{53}$

   $2^{53} \equiv (121)^4\ 2^5 \pmod{53}$

   $2^{53} \equiv (106 + 15)^4\ 2^5 \pmod{53}$ $106 \pmod{53} = 0$

   $2^{53} \equiv (0 + 15)^4\ 2^5 \pmod{53}$

   $2^{53} \equiv (15)^4\ 2^5 \pmod{53}$

   $2^{53} \equiv (15^2)^2\ 2^5 \pmod{53}$

   $2^{53} \equiv (225)^2\ 2^5 \pmod{53}$ $212 \pmod{53} = 0$

$2^{53} \equiv (0+13)^2\, 2^5 \pmod{53}$

$2^{53} \equiv (13)^2\, 2^5 \pmod{53}$

$2^{53} \equiv 169.\, 2^5 \pmod{53}$

$2^{53} \equiv (159 + 10)\, 2^5 \pmod{53}$ $159 \pmod{53} = 0$

$2^{53} \equiv (0 + 10).\, 32 \pmod{53}$

$2^{53} \equiv 10.\, 32 \pmod{53}$

$2^{53} \equiv 320 \pmod{53}$ $318 \pmod{53} = 0$

$2^{53} \equiv (318 + 2) \pmod{53}$

$2^{53} \equiv (0 + 2) \pmod{53}$

$2^{53} \equiv 2 \pmod{53}$

Dari hasil perhitungan diperoleh $2^{53} \equiv 2 \pmod{53}$. Karena $2^{53} \equiv 2 \pmod{53}$. Maka dapat disimpulkan bahwa bilangan 53 termasuk bilangan prima. Buktinya 53 = 1.53

5. Apakah 117 termasuk bilangan komposit atau bilangan prima, buktikan!

   Penyelesaian:

   Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

   Misalnya: 2. Selanjutnya diperiksa apakah $2^{117} \equiv 2 \pmod{117}$?

   $2^{117} \equiv 2^{7.16+5} \pmod{117}$ Cari $2^n$ mendekati mod 117

   $2^{117} \equiv (2^7)^{16}\, 2^5 \pmod{117}$ $2^7 = 128 \equiv 11 \pmod{117}$

   $2^{117} \equiv (11)^{16}\, 2^5 \pmod{117}$

   $2^{117} \equiv ((11)^2)^8\, 2^5 \pmod{117}$

   $2^{117} \equiv (121)^8\, 2^5 \pmod{117}$

   $2^{117} \equiv (117 + 4)^8\, 2^5 \pmod{117}$

   $2^{117} \equiv (0 + 4)^8\, 2^5 \pmod{117}$

   $2^{117} \equiv (4)^8\, 2^5 \pmod{117}$

   $2^{117} \equiv ((2^2)^8)\, 2^5 \pmod{117}$

   $2^{117} \equiv 2^{16}\, 2^5 \pmod{117}$

   $2^{117} \equiv 2^{21} \pmod{117}$

   $2^{117} \equiv ((2)^7)^3 \pmod{117}$ $2^7 \equiv 11 \pmod{117}$

   $2^{117} \equiv (11)^3 \pmod{117}$

   $2^{117} \equiv (11)^2\, 11^1 \pmod{117}$

   $2^{117} \equiv 121 .11^1 \pmod{117}$ $(117 + 4) \bmod 117$

   $2^{117} \equiv 4 .11^1 \pmod{117}$

   $2^{117} \equiv 44 \pmod{117}$

Dari hasil perhitungan diperoleh $2^{117} \equiv 44 \pmod{117}$. Karena $2^{117} \not\equiv 2 \bmod 117$. Maka dapat disimpulkan bahwa bilangan 117 termasuk bilangan komposit. Buktinya 117 = 9.13

6. Apakah 119 termasuk bilangan komposit atau bilangan prima, buktikan!

   Penyelesaian:

   Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

   Misalnya: 2. Selanjutnya diperiksa apakah $2^{119} \equiv 2 \pmod{119}$?

   $2^{119} \equiv 2^{7.16+7} \pmod{119}$ Cari $2^n$ mendekati mod 119

   $2^{119} \equiv (2^7)^{16}\, 2^7 \pmod{119}$ $2^7 = 128 \equiv 9 \pmod{119}$

   $2^{119} \equiv (9)^{16}\, .9 \pmod{119}$

   $2^{119} \equiv (9^2)^8\, 9 \pmod{119}$

   $2^{119} \equiv (81)^8\, 9 \pmod{119}$

   $2^{119} \equiv (119 - 81)^8\, 9 \pmod{119}$

   $2^{119} \equiv (-38)^8\, 2^7 \pmod{119}$

   $2^{119} \equiv (-38^2)^4\, 2^7 \pmod{119}$

   $2^{119} \equiv (1444)^4\, 9 \pmod{119}$

   $2^{119} \equiv (1428 + 16)^4\, 9 \pmod{119}$ 1428 mod 119 = 0

   $2^{119} \equiv (0 + 16)^4\, 9 \pmod{119}$

   $2^{119} \equiv (16^2)^2\, 9 \pmod{119}$

   $2^{119} \equiv (256)^2\, 9 \pmod{119}$

   $2^{119} \equiv (238 + 18)^2\, 9 \pmod{119}$ 238 mod 119 = 0

   $2^{119} \equiv (0 + 18)^2\, 9 \pmod{119}$

   $2^{119} \equiv (18)^2\, 9 \pmod{119}$

   $2^{119} \equiv (324)\, 9 \pmod{119}$

   $2^{119} \equiv (238 + 86).\, 9 \pmod{119}$ 238 mod 119 = 0

   $2^{119} \equiv 86.\, 9 \pmod{119}$

   $2^{119} \equiv 774 \pmod{119}$

   $2^{119} \equiv (714 + 60) \pmod{119}$ 714 mod 119 = 0

   $2^{119} \equiv 60 \pmod{119}$

   Dari hasil perhitungan diperoleh $2^{119} \equiv 60 \pmod{119}$. Karena $2^{119} \not\equiv 2 \bmod 119$. Maka dapat disimpulkan bahwa bilangan 119 termasuk bilangan komposit. Buktinya 119 = 7.17

7. Apakah 123 termasuk bilangan komposit atau bilangan prima, buktikan!

   Penyelesaian:

   Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

Misalnya: 2. Selanjutnya diperiksa apakah $2^{123} \equiv 2 \pmod{123}$?

$2^{123} \equiv 2^{7.17+4} \pmod{123}$

$2^{123} \equiv (2^7)^{17}\, 2^4 \pmod{123}$ $\quad 2^7 = 128 \equiv 5 \pmod{123}$

$2^{123} \equiv (5)^{17}\, 2^4 \pmod{123}$

$2^{123} \equiv (5)^{3.5+2}\, 2^4 \pmod{123}$

$2^{123} \equiv ((5)^3)^5 . 5^2\, 2^4 \pmod{123}$

$2^{123} \equiv (125)^5\, 5^2\, 2^4 \pmod{123}$

$2^{123} \equiv (125 - 123)^5\, 5^2\, 2^4 \pmod{123}$

$2^{123} \equiv 2^5 .5^2 .2^4 \pmod{123}$

$2^{123} \equiv 2^9\, 5^2 \pmod{123}$

$2^{123} \equiv 2^7.2^2\, 5^2 \pmod{123}$ $\quad 2^7 = 128 \equiv 5 \pmod{123}$

$2^{123} \equiv 5.2^2\, 5^2 \pmod{123}$

$2^{123} \equiv 5^3 .\, 2^2 \pmod{123}$

$2^{123} \equiv 125 .\, 2^2 \pmod{123}$

$2^{123} \equiv (125- 123) .\, 2^2 \pmod{123}$

$2^{123} \equiv 2^1 .\, 2^2 \pmod{123}$

$2^{123} \equiv 2^3 \pmod{123}$

$2^{123} \equiv 8 \pmod{123}$

Dari hasil perhitungan diperoleh $2^{123} \equiv 8 \pmod{123}$. Karena $2^{123} \not\equiv 2 \bmod 123$. Maka dapat disimpulkan bahwa bilangan 123 termasuk bilangan komposit. Buktinya 123 = 3.41

8. Apakah 131 termasuk bilangan komposit atau bilangan prima, buktikan!

Penyelesaian:

Untuk memeriksa ini di pilih bilangan positif yang cukup kecil.

Misalnya: 2. Selanjutnya diperiksa apakah $2^{131} \equiv 2 \pmod{131}$?

$2^{131} \equiv 2^{7.18+5} \pmod{131}$ $\quad$ Cari $2^n$ mendekati mod 131

$2^{131} \equiv (2^7)^{18}\, 2^5 \pmod{131}$ $\quad 2^7 = 128 \equiv -3 \pmod{131}$

$2^{131} \equiv (-3)^{18}\, 2^5 \pmod{131}$

$2^{131} \equiv (-3)^{18}\, 2^5 \pmod{131}$

$2^{131} \equiv ((-3)^6)^3\, 2^5 \pmod{131}$

$2^{131} \equiv (729)^3\, 2^5 \pmod{131}$ $\quad 786 \bmod (131) = 0$

$2^{131} \equiv (786 - 57)^3\, 2^5 \pmod{131}$ $\quad 786 \bmod (131) = 0$

$2^{131} \equiv (-57)^3\, 2^5 \pmod{131}$

$2^{131} \equiv (-57)^{2+1} 2^5 \pmod{131}$

$2^{131} \equiv (-57)^2 (-57) 2^5 \pmod{131}$

$2^{131} \equiv 3249 (-57) 2^5 \pmod{131}$ 3275 mod (131) = 0

$2^{131} \equiv (3275 - 26) (-57) 2^5 \pmod{131}$

$2^{131} \equiv (-26).(-57) 2^5 \pmod{131}$

$2^{131} \equiv 1482. 2^5 \pmod{131}$

$2^{131} \equiv (1441 + 41). 2^5 \pmod{131}$ 1441 mod (131) = 0

$2^{131} \equiv 41.32 \pmod{131}$

$2^{131} \equiv 1312 \pmod{131}$

$2^{131} \equiv (1310 + 2) \pmod{131}$ 1310 mod (131) = 0

$2^{131} \equiv 2 \pmod{131}$

Dari hasil perhitungan diperoleh $2^{131} \equiv 2 \pmod{131}$. Karena $2^{131} \equiv 2 \pmod{131}$. Maka dapat disimpulkan bahwa bilangan 131 termasuk bilangan prima. Buktinya 131 = 1.131

**B. Teori Wilson**

**Teorema 6.5**

Jika p suatu bilangan prima, maka kekongruenan $x^2 \equiv 1 \pmod{p}$ mempunyai tepat dua solusi, yaitu 1 dan p – 1

**Pembuktian:**

Misalkan a suatu penyelesaian dari $x^2 \equiv 1 \pmod{p}$. Maka $a^2 \equiv 1 \pmod{p}$

$a^2 - 1 \equiv 0 \pmod{p}$

$(a + 1)(a - 1) \equiv 0 \pmod{p}$ Hal ini berarti $p \mid (a + 1)(a - 1)$.

Tetapi p bilangan prima, maka $p \mid (a + 1)$ atau $p \mid (a - 1)$. Sehingga $(a - 1) \equiv 0 \pmod{p}$ atau $(a + 1) \equiv 0 \pmod{p}$ Dengan demikian $a \equiv 1 \pmod{p}$ atau $a \equiv -1 \pmod{p}$ Akibatnya $a \equiv 1 \pmod{p}$ atau $a \equiv (p - 1) \pmod{p}$ Karena a adalah suatu penyelesaian dari $x^2 \equiv 1 \pmod{p}$, maka a adalah residu terkedil modulo p. Tetapi 1 dan (p – 1) adalah residu terkecil modulo p. Akibatnya a = 1 atau a = (p – 1) Dengan demikian penyelesaian $x^2 \equiv 1 \pmod{p}$ adalah (p – 1) atau 1.

**Teorema 6.6**

Misalkan p bilangan prima selain 2 dan a' adalah penyelesaian dari $ax \equiv 1 \pmod{p}$ dengan $a \in \{1, 2, 3, \ldots, (p - 1)\}$, maka:

(i) Jika $\boldsymbol{a \not\equiv b}$ $(\mathbf{mod}\ \boldsymbol{p})$, maka $\boldsymbol{a' \not\equiv b'}$ (mod p), dan

(ii) $\boldsymbol{a' \equiv a}$ (mod p) hanya jika a = 1 atau a = p – 1

**Pembuktian:**

Misalkan a, b ∈{1, 2, 3, …, (p – 1)}, maka FPB(a, p) = 1 dan FPB(b, p) = 1. Sehingga dengan teorema sebelumnya diperoleh ax ≡ 1 (mod p) dan bx ≡ 1 (mod p) masing-masing mempunyai tepat satu solusi, misalnya $\boldsymbol{a'}$ dan $\boldsymbol{b'}$. Akibatnya $\boldsymbol{aa'} \equiv 1$ (mod p) dan $\boldsymbol{bb'} \equiv 1$ (mod p)

(i) Akan dibuktikan dengan kontra positif. Misalkan $\boldsymbol{a' \equiv b'}$ (mod p), maka $\boldsymbol{aa' \not\equiv ab'}$ (mod p). Tetapi $\boldsymbol{aa'} \equiv 1$ (mod p), sehingga $\boldsymbol{ab'} \equiv 1$ (mod p). Akibatnya $\boldsymbol{ab'b} \equiv$ b (mod p). Tetapi $\boldsymbol{bb'} \equiv 1$ (mod p), sehingga $\boldsymbol{a \equiv b}$ (mod p)

(ii) Misalkan $\boldsymbol{a' \equiv a}$ (mod p), maka $\boldsymbol{a \,.\, a \equiv a^2}$ (mod p). Tetapi $\boldsymbol{aa'} \equiv 1$ (mod p), sehingga $\boldsymbol{a^2} \equiv 1$ (mod p). Menurut teorema sebelumnya $\boldsymbol{a^2} \equiv 1$ (mod p) hanya dipenuhi jika a = 1 atau a = p – 1

**Teorema 6.7**

Misalkan p dan q adalah dua bilangan prima yang berbeda. Jika $\boldsymbol{a^p} \equiv 1$ (mod q) dan $\boldsymbol{a^q} \equiv 1$ (mod p), maka $\boldsymbol{a^{pq}} \equiv 1$ (mod pq).

**Pembuktian:**

Misalkan p dan q adalah dua bilangan prima yang berbeda, a bilangan bulat dan $\boldsymbol{a^p} \equiv 1$ (mod q) serta $\boldsymbol{a^q} \equiv 1$ (mod p). Maka $\boldsymbol{a^p}$ dan $\boldsymbol{a^q}$ adalah bilangan-bilangan bulat. Menurut teorema Fermat, $(\boldsymbol{a^q})^{\boldsymbol{p}} \equiv \boldsymbol{a^q}$ (mod p) dan $(\boldsymbol{a^p})^{\boldsymbol{q}} \equiv \boldsymbol{a^p}$ (mod q). Tetapi $\boldsymbol{a^q} \equiv 1$ (mod p) dan $\boldsymbol{a^p} \equiv 1$ (mod q). Akibatnya $\boldsymbol{a^{qp}} \equiv 1$ (mod p) dan $\boldsymbol{a^{pq}} \equiv 1$ (mod q). Sehingga p | $\boldsymbol{a^{pq}}$- 1 dan q | $\boldsymbol{a^{pq}}$- 1. Karena p dan q adalah dua bilangan prima yang berbeda, akibatnya pq | $\boldsymbol{a^{pq}}$- 1. Ini berarti

$$\boldsymbol{a^{pq}} \equiv 1 \text{ (mod pq)}$$

**Teorema 6.8**

p suatu bilangan prima jika dan hanya jika (p –1)! ≡ –1 (mod p)

**Pembuktian:**

Jika di pasangkan a dan a’ dari 2, 3, 4, …, (p – 2) sehingga sedemikian sehingga aa’ ≡ 1 (mod p) dan terdapat $\frac{1}{2}(p-3)$ pasangan bilangan – bilangan tersebut yang kongruen mod p dengan 1. Jika ruas – ruas kiri dari $\frac{1}{2}(p-3)$ kekongruenan mod p tersebut dikalikan, maka hasilkalinya akan kongruen mod p dengan 1 pula, yaitu:

$$2, 3, 4, 5, \ldots (p-2) \equiv 1 \text{ (mod p)}$$

$$1, 2, 3, 4, \ldots (p-2)(p-1) \equiv (\text{p} - 1) \text{ (mod p)}$$

$$(p-1)! \equiv (\text{p} - 1) \text{ (mod p)}$$

**Contoh 6.4**

1. Tentukan solusi pengkongruenan berikut : $x^2 \equiv 1 \pmod 7$

   penyelesaian:

   diketahui bahwa himpunan residu – residu terkecil modulo 7 yaitu: 1, 2, 3, 4, 5, 6.

   Solusinya adalah:

   a. solusi $x \equiv 1 \pmod 7$

   b. solusi $2x \equiv 1 \bmod 7$

      $2x \equiv 8 \bmod (7)$

      $x \equiv 4 \bmod (7)$

   c. solusi $3x \equiv 1 \bmod 7$

      $3x \equiv 8 \bmod (7)$

      $3x \equiv 15 \bmod (7)$

      $x \equiv 5 \bmod (7)$

   d. solusi $4x \equiv 1 \bmod 7$

      $4x \equiv 8 \bmod (7)$

      $x \equiv 2 \bmod (7)$

   e. solusi $5x \equiv 1 \bmod 7$

      $5x \equiv 1 \bmod 7$

      $5x \equiv 8 \bmod 7$

      $5x \equiv 15 \bmod 7$

      $x \equiv 3 \bmod (7)$

   f. solusi $6x \equiv 1 \bmod 7$

      $6x \equiv 1 \bmod 7$

      $6x \equiv 8 \bmod 7$

      $6x \equiv 15 \bmod 7$

      $6x \equiv 22 \bmod 7$

      $6x \equiv 29 \bmod 7$

      $6x \equiv 36 \bmod 7$

      $x \equiv 6 \bmod 7$

      Rangkuman solusi pengkongruenan dari $x^2 \equiv 1 \pmod 7$

      Solusi dari $x \equiv 1 \pmod 7$ adalah 1

      Solusi dari $2x \equiv 1 \pmod 7$ adalah 4

      Solusi dari $3x \equiv 1 \pmod 7$ adalah 5

Solusi dari $4x \equiv 1 \pmod 7$ adalah 2

Solusi dari $5x \equiv 1 \pmod 7$ adalah 3

Solusi dari $6x \equiv 1 \pmod 7$ adalah 6

Jadi solusi dari pengkongruenan dari $x^2 \equiv 1 \pmod 7$ adalah 1 dan 6. Jika menggunakan Teorema 6.1: kekongruenan $x^2 \equiv 1 \pmod 7$ mempunyai tepat dua solusi, yaitu 1 dan P – 1 atau 7 – 1 = 6 (terbukti sama)

2. Tunjukkan bahwa $10! \equiv -1 \pmod{11}$ bernilai benar

Penyelesaian:

$aa' \equiv 1 \pmod p$

Jika P = 11 maka a = 1, 2, 3, 4, … 10

Untuk a = 1 maka adalah:

a) $a' \equiv 1 \pmod{11}$

$a' = 1$

Untuk a = 2 maka adalah:

b) $a' \equiv 1 \pmod{11}$

$a' \equiv 12 \pmod{11}$

$a' = 6$

c) Untuk a = 3 maka adalah:

$3.\ a' \equiv 1 \pmod{11}$

$3.\ a' \equiv 12 \pmod{11}$

$a' = 4$

dan seterusnya untuk lebih jelasnya dapat dilihat pada tabel berikut

| a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| a' | 1 | 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |
| aa' | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Hasil kali semua bilangan pada ruas kiri akan kongruen mod 11 dengan 1 yaitu:

$2 \times 6 \times 3 \times 4 \times 5 \times 9 \times 7 \times 8 \equiv 1 \pmod{11}$. Jika kedua ruas dikalikan 10 maka diperoleh

$1.2.3.4.5.6.7.8.9.10 \equiv 10 \pmod{11}$.

$10! \equiv 10 \pmod{11}$.

$10! \equiv -1 \pmod{11}$ bernilai benar

3. Tentukan sisa pembagian dari 97! Dibagi dengan 101

Penyelesaian:

Dengan menggunakan teori Wilson:

$(n-1)! \equiv -1 \pmod n$

$(101-1)! \equiv -1 \pmod{101}$

$100! \equiv -1 \pmod{101}$

$100,99,98,97! \equiv -1 \pmod{101}$

Perhatikan bahwa:

$100 \equiv -1 \pmod{101}$

$99 \equiv -2 \pmod{101}$

$98 \equiv -3 \pmod{101}$

$100,99,98,97! \equiv -1 \pmod{101}$

$(-1).(-2).(-3)\,97! \equiv -1 \pmod{101}$

$(-6).\,97! \equiv -1 \pmod{101}$ Ruas kiri dan kanan masing – masing dikalikan - 1

$6.\,97! \equiv 1 \pmod{101}$

Jika $97! = x$ maka

$6.x. \equiv 1 \pmod{101}$

$6.x \equiv 102 \pmod{101}$

$6.17 = 102 \pmod{101}$

$102 = 102 \pmod{101}$

Jadi sisa pembagian dari 97! Dibagi dengan 101 adalah 17.

4. Buktikan $2^{340} \equiv 1 \pmod{341}$

Bukti:

34111 . 31 serta 11 dan 31 adalah dua bilangan prima yang berbeda. Maka

(i) $2^4 \equiv 16 \equiv 5 \pmod{11}$.

Maka $2^8 \equiv 5^2 \equiv 3 \pmod{11}$.

Sehingga $2^{16} \equiv 3^2 \equiv 9 \pmod{11}$.

Akibatnya $2^{32} \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$.

Dengan demikian $2^{31} \equiv 2 \pmod{11}$, sebab FPB(2, 11) = 1.

(ii) $2^5 \equiv 32 \equiv 1 \pmod{31}$.

Maka $2^{10} \equiv 1 \pmod{31}$

Sehingga $2^{11} \equiv 2 \pmod{31}$ sebab FPB(2, 31) = 1.

Dari (i) dan (ii) $2^{31} \equiv 2 \pmod{11}$ dan $2^{11} \equiv 2 \pmod{31}$, serta 11 dan 31 dua bilangan prima yang berbeda,maka menurut teorema 6.3 sebelumnya berlaku

$$2^{11}.\,2^{31} \equiv 2^{341} \equiv 2 \pmod{11.31}.$$

Dengan demikian $2^{341} \equiv 2 \pmod{341}$. Tetapi sebab FPB(2, 341) = 1, sehingga $2^{340} \equiv 1 \pmod{341}$

**Latihan 6.2**

1. Tentukan solusi dari persamaan kekongruenan berikut:
    a. $x^2 \equiv 1 \pmod{11}$
    b. $x^2 \equiv 1 \pmod{13}$
2. Tunjukkan bahwa point a dan b dibawah ini terbukti bernilai benar.
    a. $12! \equiv -1 \pmod{13}$
    b. $18! \equiv -1 \pmod{19}$
3. Tentukan sisa pembagian dari 67! dibagi 71

# BAB VII

## FUNGSI ARITMETIK

Fungsi aritmetik adalah sekumpulan operasi matematika dasar yang digunakan untuk memanipulasi angka-angka dan melakukan perhitungan matematis. Operasi-operasi tersebut meliputi penjumlahan, pengurangan, perkalian, pembagian, pemangkatan, perakaran, logaritma, dan lain sebagainya. Berdasarkan sifat-sifat yang dimiliki bilangan-bilangan bulat dapat didefinisikan fungsi-fungsi tertentu yang mempunyai peranan penting dalam Teori Bilangan. Fungsi-fungsi khusus tersebut sering disebut fungsi aritmetik (fungsi teori bilangan). Pada umumnya fungsi aritmetik didefinisikan/mempunyai daerah asal pada himpunan semua bilangan bulat positif, seperti berikut ini.

Fungsi aritmetik $f : \mathbb{Z}^+ \to \mathbb{Z}$ dengan $\mathbb{Z}$ adalah himpunan semua bilangan bulat dan $\mathbb{Z}^+$ adalah himpunan semua bilangan bulat positif.

### A. Fungsi Tau $(\tau)$

Fungsi tau, yang juga dikenal sebagai fungsi pembagi, adalah konsep dalam teori bilangan yang didefinisikan sebagai jumlah pembagi positif dari bilangan bulat. Dalam konteks ini, fungsi tau seringkali ditandai dengan simbol Yunani τ(n). Fungsi ini juga digunakan dalam berbagai aspek teori bilangan dan telah dipelajari oleh banyak matematikawan terkenal. Sebagai contoh, matematikawan Norwegia, Carl Friedrich Gauss, mengamati bahwa jika n adalah bilangan kuadrat sempurna, maka τ(n) adalah bilangan genap, dan jika n bukan kuadrat sempurna, maka τ(n) adalah bilangan ganjil

**Definisi 7. 1 fungsi τ(n)**

Misal n bilangan positif, $\tau(n)$ menyatakan banyaknya pembagi bulat positif dari n

**Contoh 7.1**

1. Semua pembagi bulat positif dari 18 adalah 1, 2, 3, 6, 9 dan 18 maka $\tau(18) = 6$

   **Pembuktian:**

   1 x 18 = 18  2 x 9 = 18  3 x 6 = 18
2. Semua pembagi bulat positif dari 12 adalah 1, 2, 3, 4, 6, 12 maka $\tau(12) = 6$
3. Semua pembagi bulat positif dari 13 adalah 1 dan 13 maka $\tau(13) = 2$
4. Semua pembagi bulat positif dari 5 adalah 1 dan 5 maka $\tau(5) = 2$
5. Perhatikan contoh soal 3 dan 4 ketika *p* suatu bilangan prima maka $\tau(p) = 2$

$\tau(n)$ yaitu banyaknya pembagi bulat positif dari *n* sering dinyatakan dengan rumus yang menggunakan notasi $\sum$ (sigma). Berikut ini beberapa contoh definisi notasi $\sum$, $\tau(n)$ dapat dirumuskan sebagai berikut:

**Contoh 7.2**

1. $\sum_{n=1}^{5} a_n = a_1 + a_1 + a_1 + a_1 + a_1$
2. $\sum_{n=2}^{6} n = 2 + 3 + 4 + 5 + 6$
3. $\sum_{n=1}^{5} 3 = 3 + 3 + 3 + 3 + 3$
4. $\sum_{d|12} d = 1 + 2 + 3 + 4 + 6 + 12$ yaitu jumlah semua pembagi bulat positif dari 12
5. $\sum_{d|12} \mathrm{I} = 1 + 1 + 1 + 1 + 1 + 1$ yaitu banyaknya pembagi bulat positif dari 12
6. $\sum_{d|18} f(d) = f(1) + f(2) + f(3) + f(6) + f(9) + f(18)$

Terlihat dari beberapa contoh soal 2 tersebut pemakaian notasi $\sum$, $\tau(n)$ dapat dirumuskan sebagai berikut:

$$\tau(n) = \sum_{d|n} \mathrm{I} \text{ untuk bilangan bulat } n \geq 1$$

**Keterangan:** $\tau(n)$ merupakan penjumlahan dari 1 sebanyak pembagi bulat positif dari n.

**Contoh 7.3**

1. Semua pembagi bulat positif dari 32 adalah 1, 2, 4, 8, 16 dan 32, maka
$$\sum_{d|32} \mathrm{I} = 1 + 1 + 1 + 1 + 1 + 1 = 6$$
2. Semua pembagi bulat positif dari 48 adalah 1, 2, 3, 4, 5, 6, 8, 12, 16, 24, dan 48, maka
$$\sum_{d|48} \mathrm{I} = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 10$$
3. Periksalah bahwa $\sum_{d|1} \mathrm{I} = 1$, $\sum_{d|2} 1 = 1 + 1 = 2$, $\sum_{d|4} 1 = 1 + 1 + 1 = 3$
4. Jika p suatu bilangan prima, maka $\sum_{d|p} \mathrm{I} = 1 + 1 = 2$

Dari uraian dan contoh 3 dapat dipahami bahwa apabila p suatu bilangan prima, maka pembagi - pembagi bulat positifnya hanyalah 1 dan p saja, sehingga. $\tau(p)$ = 2. Pembagi - pembagi bulat positif dari $\mathrm{p}^2$ adalah 1, p dan $\mathrm{p}^2$ sehingga

$$\tau(\mathrm{p}^2) = \sum_{d|p} \mathrm{I} = 1 + 1 + 1 = 3$$
$$\tau(\mathrm{p}^3) = \sum_{d|p} \mathrm{I} = 1 + 1 + 1 + 1 = 4$$
$$\tau(\mathrm{p}^4) = \sum_{d|p} \mathrm{I} = 1 + 1 + 1 + 1 + 1 = 5$$

Nampak bahwa jika *k* suatu bilangan bulat positif, maka

$$\tau(\mathrm{p}^k) = k + 1$$

**Keterangan:** $p$ adalah suatu bilangan prima.

**Contoh 7.4**

1. $64 = 2^6$, maka $\tau(64) = \tau(2^6) = 6 + 1 = 7$.

   Periksalah dengan mencacah semua pembagi bulat positif dari 64

2. $\tau(243) = \tau(3^5) = 5 + 1 = 6$

   Periksalah dengan mencacah semua pembagi bulat positif dari 243

Selanjutnya, apabila $p_1$ dan $p_2$ keduanya adalah bilangan prima dan n = $p_1 p_2$, maka pembagi-pembagi bulat positif dari n adalah 1, $p_1$, $p_2$ dan n = $p_1 p_2$ sehingga $\tau(n) = 4$. Jika m $p_1^2$, $p_2^3$, =, maka pembagi-pembagi bulat positif m dapat disusun sebagai berikut:

$$\begin{array}{llll} 1, & p_2, & p_2^2, & p_2^3 \\ p_1, & p_1 p_2, & p_1 p_2^2, & p_1 p_2^3 \\ p_1^2, & p_1^2 p_2, & p_1^2 p_2^2, & p_1^2 p_2^3 = m \end{array}$$

Terlihat pada bentuk tersebut jika $\tau(p_1^2 p_2^3) = 4 = 3 \text{ x } 4 = 12$

**Contoh 7.5**

1. $\tau(144) = \tau(2^4 . 3^2) = 5 \; x \; 3 = 15$
2. $\tau(1323) = \tau(3^3 . 7^2) = 4 \; x \; 3 = 12$
3. Periksalah bahwa $\tau(675) = 12$, $\tau(784) = 15$

Apabila n = $p^k q^t$ dengan p dan q bilangan-bilangan prima yang berlainan dan k, t adalah bilangan-bilangan bulat positif, maka:

$$\tau(n) = \tau(p^k q^t) = (k + 1)(t + 1)$$

**Pembuktian:**

Semua pembagi bulat positif dari n = $p^k q^t$ dapat disusun daftar sebagai berikut :

$$\begin{array}{lllll} 1, & p & p^2 & p^3, & \dots \quad p^k \\ q, & pq & p^2 q & p^3 q, & \dots \quad p^k q \\ q^2, & pq^2 & p^2 q^2 & p^3 q^2, & \dots \quad p^k q^2 \\ \vdots & \vdots & \vdots & \vdots & \dots \quad \vdots \\ q^t, & pq^t & p^2 q^t & p^3 q^t, & \dots \quad p^k q^t = n \end{array}$$

Dari daftar tersebut bahwa

$$\tau(n) = \tau(p^k q^t) = (k + 1)(t + 1)$$

Teorema dasar aritmatika menyatakan bahwa setiap bilangan bulat positif yang lebih besar dari 1 dapat difaktorkan secara tunggal atas factor-faktor prima.

Misal: $72 = 2^3 . 3^2$; $300 = 2^2 . 3 . 5^2$ Setiap bilangan bulat positif n ≥ 1 untuk setiap i =1, 2 ,3, …k maka n dapat ditulis dalam bentuk kanonik sebagai:

$$n = p_1^{a_1}, p_2^{a_2}, p_3^{a_3} \dots p_a^{a_k}$$

**Teorema 7.1**

Apabila bentuk kanonik dari bilangan bulat n adalah $n = p_1^{a_1}, p_2^{a_2}, p_3^{a_3} \dots p_a^{a_k}$,maka:

$\tau(n) = (a_1 + 1)\,(a_2 + 1)\,(a_3 + 1) \dots (a_k + 1)$

**Pembuktian:**

Apabila d suatu pembagi bulat positif dari n,maka d berbentuk

$$d = p_1^{t_1}, p_2^{t_2}, p_3^{t_k} \dots p_a^{a_k} \qquad 0 \le t_i \le a_i$$

maka banyaknya pembagi bulat positif dari n merupakan hasil kali banyaknya pilihan yang mungkin untuk $t_i$ dari $(a_i + 1)$ pilihan. Sehingga diperoleh

$$\tau(n) = (a_1 + 1)\,(a_2 + 1)\,(a_3 + 1) \dots (a_k + 1)$$

Rumus τ(n) tersebut sering dinyatakan dengan notasi Π (pi).

**Contoh 7.6**

1. $\prod_{i=I}^{5} d_i = d_1, d_2, d_3, d_4, d_5$
2. $\prod_{n=1}^{4} f(n) = f(1).f(2).f(3).f(4)$
3. $\prod_{i=I}^{n}(d_i + 1) = (d_1 + 1), (\,d_2 + 1), (d_3 + 1), \dots (d_n + 1)$

Teorema 7.1 dapat dituliskan dengan notasi Π sebagai berikut:

$$n = p_1^{a_1}, p_2^{a_2}, p_3^{a_3} \dots p_a^{a_k} = \prod_{i=I}^{k} p_i^{a_i} \; maka$$

$$\tau(n) = \prod_{i=I}^{k}(a_i + 1)$$

**Contoh 7.7**

1. $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$,maka

   $\tau\,(1260) = t\,(2^2 \cdot 3^2 \cdot 5 \cdot 7) = (2 + 1)\,(2 + 1)\,(1 + 1)\,(1 + 1) = 36$
2. $33.075 = 3^3 \cdot 5^2 \cdot 7^2$, maka $\tau\,(33.075) = \tau\,(3^3 \cdot 5^2 \cdot 7^2) = (3 + 1)\,(2 + 1)\,(2 + 1) = 36$
3. Periksalah bahwa $\tau\,(2310) = 10$, $\tau(210) = 8$, $\tau\,(1.156) = 9$

**Teorema 7.2**

Apabila *n* suatu bilangan bulat positif bukan prima, maka hasilkali semua pembagi bulat positif dari n adalah

$$K(n) = n^{1/2\,\tau(n)}$$

**Pembuktian:**

Misalkan d adalah suatu pembagi bulat positif dari n, maka ada $d^I$ (yaitu pembagi bulat positif dari n pula) sedemikian hingga $dd^I = n$. Hal ini mungkin saja terjadi bahwa $d = d^I$, yaitu jika n suatu kuadrat sempurna.

Karena banyaknya pembagi bulat positif dari n adalah τ(n),dengan mengalikan setiap pembagi dari n (misalnya d) dengan pembagi pasangannya (misalnya $d^I$) sedemikian hingga $dd^I = n$, maka akan diperoleh bahwa hasil kali semua pembagi bulat positif dari n adalah :

$$K(n) = n^{1/2\ \tau(n)}$$

**Contoh 7.8**

1. Pembagi-pembagi bulat positif dari 12 adalah 1,2,4,6 dan 12. τ(12) = 6. Hasilkan semua pembagi bulat positif dari 12 ditulis dengan notasi K (12) maka

   K(12) = 1 . 2 .3 . 4 . 6 . 12

   K(12) = (1 . 12) (2 .6) (3 . 4)

   K(12) = 12 . 12 .12

   K(12) = $(12)^3$
2. Semua pembagi bulat positif dari 28 adalah 1,2,4,7,14 dan 28. τ(28) = 6. Hasil kali semua pembagi bulat positif dari 28 adalah :

   K(28) = 1 . 2 . 4 . 7 . 14 . 28

   K(28) = (1 . 28) (2. 14) (4 . 7)

   K(28) = 28 . 28 . 28

   K(28) = $(28)^3$

**Catatan:**

Jika p suatu bilangan prima, maka K(p) = p, $K(p^2) = p^3$, $K(p^3) = p^6$, $K(p^4) = p^{10}$,

sederhana dapat ditulis $K(p^t) = P^{\frac{t(t+1)}{2}}$

**B. Fungsi Sigma ($\sigma$)**

Apabila τ (n) menyatakan banyaknya pembagi bulat positif dari n, maka $\sigma(n)$ menyatakan jumlah semua pembagi bulat positif dari n.

**Definisi 7.2 Fungsi Sigma ($\sigma$)**

Apabila n suatu bilangan bulat positif ,maka $\sigma(n)$ menyatakan jumlah semua pembagi bulat positif dari n. dengan menggunakan notasi ∑, ditulis

$$\sigma(n) = \sum_{d|n} d$$

**Contoh 7.9**

1. Semua pembagi bilangan bulat positif dari 12 adalah 1,2,3,4,6 dan 12 maka

   $\sigma(12)$ = 1+ 2 + 3 + 4 + 5 + 6 + 12 = 28
2. $\sigma(27)$ = 1 + 3 + 9 +27 = 40
3. Periksalah bahwa $\sigma(2)$ = 3, $\sigma(3)$= 4, $\sigma(5)$= 6, $\sigma(7)$= 8, $\sigma(11)$= 12

4. Jika p suatu bilangan prima,maka $\sigma(p)$= p + 1, $\sigma(p^2) = 1 + p + p^2$, $\sigma(p^3) = 1 + p + p^2 + p^3$ dan $\sigma(p^t) = 1 + p + p^2 + p^3 \ldots + p^t$

Mengingat rumus jumlah deret geometri yaitu:

$$1 + p + p^2 + p^3 \ldots + p^t = \frac{p^{t+1}-1}{p-1}$$

Jadi, jika p suatu bilangan prima dan t suatu bilangan bulat positif,

$$\sigma(p^t) = \frac{p^{t+1} - 1}{p - 1}$$

**Contoh 7.10**

1. $\sigma(32) = \cdots$

$$\sigma(p^t) = \frac{p^{t+1} - 1}{p - 1}$$

$$\sigma(32) = \sigma(2^5)$$

$$\sigma(2^5) = \frac{2^{5+1} - 1}{2 - 1}$$

$$\sigma(2^5) = \frac{2^6 - 1}{2 - 1}$$

$$\sigma(2^5) = \frac{64 - 1}{1}$$

$$\sigma(2^5) = 63$$

2. $\sigma(125) = \cdots$

Penyelesaian:

$$\sigma(p^t) = \frac{p^{t+1} - 1}{p - 1}$$

$$\sigma(125) = \sigma(5^3)$$

$$\sigma(5^3) = \frac{5^{3+1} - 1}{5 - 1}$$

$$\sigma(5^3) = \frac{5^4 - 1}{4}$$

$$\sigma(5^3) = \frac{625 - 1}{4}$$

$$\sigma(5^3) = \frac{624}{4}$$

$$\sigma(5^3) = 156$$

3. Periksalah bahwa $\sigma$ (27) = 40, $\sigma$ (49) = 57, $\sigma$ (125) = 156, $\sigma$ (64) = 127, $\sigma$ (42) = 96, $\sigma$ (6) = 12

Apabila p dan q adalah dua bilangan – bilangan prima yang berbeda dan n = pq,maka semua pembagi bulat positif dari n adalah 1,p,q dan pq = n, sehingga :

$$\sigma (n) = \sigma (pq) = 1 + p + q + pq = (1 + p) (1 + q)$$

Jika $m = p^2q^3$ dengan p dan q bilangan-bilangan prima yang berlainan,maka jumlah semua pembagi bilat positif dari m dapat disusun sebagai berikut :

$$\sigma (m) = (1 + p + p^2 + p^3) + (1 + pq + pq^2 + pq^3) + (p^2 + p^2q + p^2q^2 + p^2q^2)$$

$$\sigma (m) = (1 + p + p^2) (1 + q + q^2 + q^3)$$

$$\sigma(m) = \frac{p^3 - 1}{p - 1}\frac{q^4 - 1}{q - 1}$$

dapat disimpulkan bahwa apabila $n = p^k q^t$ denganp dan q keduanya bilangan prima yang berbeda dan k,t bilangan - bilangan bulat positif.maka :

$$\sigma(n) = \sigma(p^k q^t) = \frac{p^{k+1}-1}{p-1}\frac{q^{t+1}-1}{q-1} = \sigma(p^k q^t)$$

**Contoh 7.10**

1. $\sigma$ (15) = $\sigma$ (3.5) = $\sigma$ (3). $\sigma$ (5) = 4 . 6 = 24
2. $\sigma$ (45) = $\sigma$ (32.5) = $\sigma$ (32). $\sigma$ (5) =13 . 6 = 78
3. Periksalah bahwa $\sigma$ (504) = 1560, $\sigma$ (784) = 1764, $\sigma$ (847) = 1064

**Teorema 7.3**

Apabila bentuk kanonik dari bilangan bulat positif $n = \prod_{i=1}^{k} p_i^{a_i}$ maka $\sigma(n) = \prod_{i=1}^{k} \frac{p^{a_i+1}-1}{p_i-1}$

Bukti :

Perhatikan suku-suku dari perkalian

$(1 + p_1 + p_1^2 + p_1^3 + \ldots + p_1^{a_1}) (1 + p_2 + p_2^2 + p_3^3 + \ldots + p_2^{a_2}) \ldots.$

$$(1 + p_k + p_k^2 + p_k^3 + \ldots + p_k^{a_k})$$

Setiap suku dari hasil perkalian ini berbeda satu dengan lainnya dan masing-masing merupakan pembagian dari n, sehingga :

$$\sigma(n) = \prod_{i=1}^{k}(1 + p_i + p_i^2 + p_i^3 + \ldots + p_i^{a_i})$$

Sehingga

$$\sigma(n) = \prod_{i=1}^{k} \frac{p^{a_i+1} - 1}{p_i - 1}$$

**Contoh 7.11**

1. $\sigma$ (2130) $= \sigma$ (2 . 3 . 5 . 7 . 11)

   $\sigma$ (2130) $= \frac{2^2-1}{2-1} . \frac{3^2-1}{3-1} . \frac{5^2-1}{5-1} . \frac{7^2-1}{7-1}$

   $\sigma$ (2130) $= 3 . 4 . 6 . 8 . 12$

   $\sigma$ (2130) $= 6912$

2. $\sigma$ (5600) $= \sigma$ ($2^2 . 5^2 . 7$)

   $\sigma$ (5600) $= \frac{2^6-1}{2-1} . \frac{5^2-1}{5-1} . \frac{7^2-1}{7-1}$

   $\sigma$ (5600) $= 63 . 31 . 8$

   $\sigma$ (5600) $= 15.624$

Perhatikan kembali definis fungsi sigma , yaitu jika n suatu bilangan bulat positif,maka

$$\sigma(n) = \sum_{d|n} \mathrm{d}$$

Pada rumus ini, d menjalani semua pembagi bulat positif dari n. mengingat $\frac{d}{n}$ merupakan pembagi bulat positif dari n pula, maka rumus dapat ditulis sebagai :

$$\sigma(n) = \sum_{d|n} \frac{d}{n}$$

$$\sigma(n) = n \sum_{d|n} \frac{1}{d}$$

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}$$

Hal ini dikatakan bahwa $\frac{\sigma(n)}{n}$ merupakan jumlah kebalikan dari pembagi-pembagi bulat positif dari n.

**Contoh 7.12**

1. Semua pembagi bilangan bulat positif dari 18 adalah 1, 2, 3, 6, 9 dan 18. Maka σ (18) = 39. Jumlah kebalikan pembagi – pembagi bilangan bulat positif dari 18 adalah

$$\sum_{d|18} \frac{1}{d} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{9} + \frac{1}{18}$$

$$\sum_{d|18} \frac{1}{d} = \frac{18 + 9 + 6 + 3 + 2 + 1}{18}$$

$$\sum_{d|18} \frac{1}{d} = \frac{39}{18}$$

Jadi, Jumlah kebalikan pembagi – pembagi bilangan bulat positif dari 18 adalah $\frac{39}{18}$

2. Periksalah bahwa, $\sum_{d|12} \frac{1}{d} = \frac{7}{3}$ $\sum_{d|11} \frac{1}{d} = \frac{12}{3}$ $\sum_{d|5} \frac{1}{d} = \frac{6}{5}$

**Catatan:**

Jika p suatu bilangan prima maka $\sum_{d|p^3} \frac{1}{d} = \frac{\mathrm{p}^4-1}{\mathrm{p}^3(\mathrm{p}-1)}$

**Teorema 7.4**

Fungsi $\tau$ dan $\sigma$ masing – masing adalah fungsi ganda

Bukti:

Misalkan m dan n adalah bilangan – bilangan bulat positif dan (m, n) = 1. Bentuk – bentuk kanonik dari m dan n berturut – turut adalah

$$m = p_1^{a_1}\, p_2^{a_2} \ldots p_r^{a_r} \text{ dan } n = q_1^{b_1}\, q_2^{b_2} \ldots q_t^{b_t}$$

Karena (m, n) = 1 maka bilangan – bilangan prima $p_i$ dan $q_i$ berbeda. Jadi bentuk kanonik dari mn adalah:

$$mn = p_1^{a_1}\, p_2^{a_2} \ldots\, p_r^{a_r}.\, q_1^{b_1}\, q_2^{b_2} \ldots q_t^{b_t}$$

Menggunakan teorema 7.1 maka diperoleh

Apabila bentuk kanonik dari bilangan bulat n adalah $n = p_1^{a_1}, p_2^{a_2}, p_3^{a_3} \ldots\, p_a^{a_k}$,maka:

$\tau(mn)$ = [($a_1$ + 1) ($a_2$ + 1) … ($a_r$ + 1). [ ($b_1$ + 1) ($b_2$ + 1) … ($b_t$ + 1).

$\boldsymbol{\tau(mn) = \tau(m).\tau(n)}$

Menggunakan teorema 7.3 maka diperoleh

$$\sigma(mn) = \left[\frac{p_1^{a_1}-1}{p_1-1} \ldots \frac{p_r^{a_r}-1}{p_r-1}\right]\left[\frac{q_1^{b_1}-1}{q_1-1} \ldots \frac{q_t^{b_t}-1}{q_t-1}\right]$$

**Teorema 7.5**

Jika f suatu fungsi ganda dan F didefinisikan oleh $F(n) = \sum_{d|n} \mathrm{f(d)}$ maka F merupakan fungsi ganda

**Pembuktian:**

Misalkan m dan n adalah bilangan – bilangan positif yang saling prima maka

$$F(mn) = \sum_{d|mn} \mathrm{f(d)} = \sum_{\substack{d_1|mn \\ d_2|mn}} \mathrm{f}\,(d_1 d_2)$$

Hal ini disebabkan setiap pembagi d dari mn dapat ditulis sebagai hasilkali dari suatu pembagi $d_1$ dari m dan suatu pembagi $d_2$ dari n dengan $(d_1 d_2) = 1$. Karena $f$ suatu fungsi ganda maka $\mathrm{f}(d_1 d_2) = \mathrm{f}(d_1).f(d_2)$ jadi

$$F(mn) = \sum_{\substack{d_1|mn \\ d_2|mn}} \mathrm{f}(d_1 d_2)$$

$$F(mn) = \sum_{\substack{d_1|mn \\ d_2|mn}} \mathrm{f}(d_1).f(d_2)$$

$$F(mn) = \left( \sum_{d_1|m} \mathrm{f}(d_1) \left( \sum_{d_2|m} \mathrm{f}(d_2) \right) \right)$$

$$F(mn) = F(m).F(n)$$

**Contoh 7.13**

1. Buktikan apakah $\tau(mn) = \tau(m).\tau(n)$ jika m = 2 dan dan n = 3

   Penyelesaian:

   $\tau(2.3) = \tau(2).\tau(3)$

   $\tau(6) = \tau(2).\tau(3)$

   $4 = 2.2$

   $4 = 4$

Jadi, karena (2, 3) = 1 maka berlaku $\tau(mn) = \tau(m).\tau(n)$

2. Buktikan apakah $\tau(mn) = \tau(m).\tau(n)$ jika m = 6 dan dan n = 9

   Penyelesaian:

   $\tau(6.9) = \tau(6).\tau(9)$

   $\tau(54) = \tau(6).\tau(9)$

   $8 = 4.3$

   $8 \neq 12$

   Jadi, karena (6, 9) ≠ 1 maka berlaku tidak berlaku $\tau(mn) = \tau(m).\tau(n)$

3. Buktikan apakah $\sigma(mn) = \sigma(m).\sigma(n)$ jika m = 2 dan dan n = 3

   Penyelesaian:

   $\sigma(2.3) = \sigma(2).\sigma(3)$

   $\sigma(6) = \tau(2).\tau(3)$

   $12 = 3.4$

   $12 = 412$

Jadi, karena (2, 3) = 1 maka berlaku $\sigma(mn) = \sigma(m).\sigma(n)$

4. Buktikan apakah $\sigma(mn) = \sigma(m).\sigma(n)$ jika m = 6 dan dan n = 9

   Penyelesaian:

   $\sigma(6.9) = \sigma(6).\sigma(9)$

   $\sigma(54) = \sigma(6).\sigma(9)$

   $120 = 12.13$

   $120 \neq 156$

   Jadi, karena (6, 9) ≠ 1 maka berlaku tidak berlaku $\sigma(mn) = \sigma(m).\sigma(n)$

## C. Fungsi Mobius ($\mu = m\mu$)

Fungsi Mobius dilambangkan sebagai μ(n), merupakan fungsi perkalian dalam teori bilangan. Diperkenalkan oleh seorang matematikawan Jerman bernama August Ferdinand Möbius pada tahun 1832.

Dengan catatan:

a. Bilangan bebas kuadrat adalah bilangan yang tidak memiliki faktor suatu bilangan kuadrat. Contoh: 2, 3, 5, 6, 7, 10, 11, 13, 15, 17, 21, dsb.
b. Bilangan tak bebas kuadrat adalah bilangan yang memiliki faktor suatu bilangan kudrat. Contoh: 4, 8, 12, 16, 18, 20, 24, 27 dsb

**Definisi 7.3 Fungsi Mobius**

Misalkan n bilangan bulat positif

a. $\mu(n) = 1$ , jika n = 1
b. $\mu(n) = 0$ , $jika\ p^2 | n$, untuk suatu bilangan prima p. Dalam hal ini (n) adalah bilangan tak bebas kuadrat yaitu bilangan yang memiliki faktor suatu bilangan kuadrat.
c. $\mu(n) = (-1)^k$ , $n = p_1, p_2, \ldots p_k\ dengan\ p_1$ bilangan prima yang berbeda. Dalam hal ini (n) adalah bilangan tak bebas kuadrat yaitu bilangan yang memiliki faktor suatu bilangan kuadrat.

**Contoh 7.14 fungsi mobius**

1. $\mu(1) = 1$
2. $\mu(2) = -1$
3. $\mu(3) = -1$
4. $\mu(4) = (2)^2 = 0$
5. $\mu(5) = \mu\,(2^2.3) = 0$
6. $\mu(35) = \mu\,(7.5) = (-1)^2 = 1$

**Teorema 7.6**

fungsi μ adalah suatu fungsi ganda

pembuktian

Jika (m, n) = 1maka $\mu\,(mn) = \mu(m).\mu(n)$

1) Jika p suatu bilangan prima dan $p^2|m$ atau $p^2|n$, maka $p^2|mn$ sehingga $\mu\,(mn) = 0 = \mu(m).\mu(n)$
2) Jika m dan n adalah bilangan – bilangan bebas kuadrat, misalnya $m = p_1,\ p_2, \dots\ p_r$ dan $n = q_1,\ q_2, \dots\ q_t$ dengan $p_i$ dan $q_j$ adalah bilangan – bilangan prima yang berbeda. Maka

   $\mu\,(mn) = (p_1,\ p_2, \dots\ p_r\ .q_1,\ q_2, \dots\ q_t) = (-1)^{r+t}$

   $\mu\,(mn) = (-1)^{r+t}$

   $\mu\,(mn) = (-1)^r.(-1)^t$

   $\mu\,(mn) = \mu(m).\mu(n)$

Jadi μ adalah fungsi ganda

**Contoh 7.15**

semua faktor bilangan bulat positif dari 12 adalah 1, 2, 3, 4, 6, 12. Hitunglah jumlah semua nilai fungsi μ untuk semua faktor dari 12 yaitu:

$$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \ \mu(4) + \ \mu(6) + \ \mu(12)$$

$$\sum_{d|12} \mu(d) = 1 + (-1) + (-1) + \ 0 + \ 1 + 0$$

$$\sum_{d|12} \mu(d) = 0$$

**Teorema 7.7**

Untuk setiap bilangan bulat positif n, berlaku

$$\sum_{d|n} \mu(\mathrm{d}) = 1, Jika\ n = 1$$

$$\sum_{d|n} \mu(\mathrm{d}) = 0, Jika\ n > 1$$

Dengan d suatu bilangan bulat positif

Pembuktian

Misalkan suatu bilangan bulat n > 1 dan didefinisikan bahwa

$$F(n) = \sum_{d|n} \mu(d)$$

Jika n = $p^k$ dengan p suatu bilangan prima dan k suatu bilangan bulat positif maka semua faktor bulat positif dari n adalah $1, p, p^2, \ldots p^k$ sehingga

$$F(n) = \sum_{d|a} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k)$$

$$F(n) = \sum_{d|a} \mu(d) = 1 + (-1) + 0 + \cdots + 0 = 0$$

Mengingat μ suatu fungsi ganda dan memperhatikan teorema 7.5. Maka F merupakan fungsi ganda pula. Selanjutnya apabila bentuk kanonik dari n adalah

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{a_r}$$

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \ldots F(p_r^{a_r})$$

**Contoh 7.16**

1. Tentukan nilai dari $\sum_{d|12} \mu(d)$!

Penyelesaian:

Faktor bilangan 12 adalah 1, 2, 3, 4, 6 dan 12

| 12 | |
|---|---|
| 1 | 12 |
| 2 | 6 |
| 3 | 4 |

$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$

$\sum_{d|12} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(2^2) + \mu(2.3) + \mu(2^2.3)$

$\sum_{d|12} \mu(d) = 1 + (-1) + (-1) + (0) + (-1^2) + 0$

$\sum_{d|12} \mu(d) = 1 - 1 - 1 + 0 + 1 + 0$

$\sum_{d|12} \mu(d) = 0$

2. Tentukan nilai dari $\sum_{d|64} \mu(d)$!

Penyelesaian:

Faktor bilangan 64 adalah 1, 2, 4, 8, 16, 32, 64

| 64 | |
|---|---|
| 1 | 64 |
| 2 | 32 |

| | |
|---|---|
| 4 | 16 |
| 8 | 8 |

$\sum_{d|64} \mu(d) = \mu(1) + \mu(2) + \mu(4) + \mu(8) + \mu(16) + \mu(32) + \mu(64)$

$\sum_{d|64} \mu(d) = \mu(1) + \mu(2) + \mu(2^2) + \mu(2^3) + \mu(2^4) + \mu(2^5) + \mu(2^6)$

$\sum_{d|64} \mu(d) = 1 + (-1) + 0 + 0 + 0 + 0 + 0$

$\sum_{d|64} \mu(d) = 1 - 1 - 1 + 0 + 1 + 0$

$\sum_{d|64} \mu(d) = 0$

3. Tentukan nilai dari $\sum_{d|98} \mu(d)$!

Penyelesaian:

Faktor bilangan 98 adalah 1, 2, 7, 14, 49, 98

| 98 | |
|---|---|
| 1 | 98 |
| 2 | 49 |
| 7 | 14 |

$\sum_{d|98} \mu(d) = \mu(1) + \mu(2) + \mu(7) + \mu(14) + \mu(49) + \mu(98)$

$\sum_{d|98} \mu(d) = \mu(1) + \mu(2) + \mu(7) + \mu(2.7) + \mu(7^2) + \mu(2^2.7)$

$\sum_{d|98} \mu(d) = 1 + (-1) + (-1) + (-1)^2 + 0 + 0$

$\sum_{d|98} \mu(d) = 0$

**Teorema 7.8 (Rumus Invers Mobius)**

Misalkan F dan f adalah dua fungsi aritmetik yang dihubungkan dengan rumus

$$F(n) = \sum_{d|n} f(d)$$

Untuk setiap bilangan bulat positif n maka:

$$f(n) = \sum_{d|n} \mu(d)\, F(\frac{n}{d})$$

**Contoh 7.17**

Jika diketahui fungsi f (x) = $x^2 + 1$ dan $n = 6$. Tentukan nilai F (6) dan f (6).

**Penyelesaian:**

a. Mencari nilai F (6) dari fungsi f (x) = $x^2 + 1$ menggunakan rumus:

$$F(n) = \sum_{d|n} f(d)$$

F (6) artinya n = 6 maka diperoleh nilai d (faktor bilangan) yaitu 1, 2, 3, dan 6. Sehingga F (6) dapat ditulis:

F (6) = $f$ (1)+ $f$ (2)+ $f$ (3)+ $f$ (6)

F (6) = 2 + 5 + 10 + 37 = 54

Jadi nilai F (6) adalah 54

b. Mencari nilai F (6) dari fungsi f (x) = $x^2 + 1$ menggunakan rumus:

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$$

$f$ (6) = $\mu(1)\, F\left(\frac{6}{1}\right) + \mu(2)\, F\left(\frac{6}{2}\right) + \mu(3)\, F\left(\frac{6}{3}\right) + \mu(6) F\left(\frac{6}{6}\right)$

$f$ (6) = $\mu(1)\, F(6) + \mu(2)\, F(3) + \mu(3)\, F(2) + \mu(6) F(1)$

$f$ (6) = $(1).54 + (-1).12 + (-1).7 + 1.2$

$f$ (6) = $54 - 12 - 7 + 2$

$f$ (6) = 37

Jadi nilai $f$ (6) adalah 37

**Contoh 7.18**

Jika diketahui fungsi f (x) = $x^2 - 2x - 3$ dan $n = 10$. Tentukan nilai F (10) dan f (10).

Penyelesaian:

a. Mencari nilai F (10) dari fungsi f (x) = $x^2 - 2x - 3$ menggunakan rumus:

$$F(n) = \sum_{d|n} f(d)$$

F (10) artinya n = 10 maka diperoleh nilai d (faktor bilangan) yaitu 1, 2, 5, dan 10. Sehingga F (10) dapat ditulis:

F (10) = $f$ (1) + $f$ (2)+ $f$ (5)+ $f$ (10)

F (10) = $(-4)$+ $(-3)$+ $12 + 77$

F (10) = 82

Jadi nilai F (10) adalah 82

b. Mencari nilai F (10) dari fungsi f (x) = $x^2 - 2x - 3$ menggunakan rumus:

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)$$

$f$ (10) = $\mu(1)\, F\left(\frac{10}{1}\right) + \mu(2)\, F\left(\frac{10}{2}\right) + \mu(5)\, F\left(\frac{10}{5}\right) + \mu(10) F\left(\frac{10}{10}\right)$

$f$ (10) = $\mu(1)\, F(10) + \mu(2)\, F(5) + \mu(5)\, F(2) + \mu(10) F(1)$

$f\ (10) = 1.82 + (-1).8 + (-1)(-7) + 1.(-4)$

$f\ (10) = 77$

Jadi nilai $f\ (10)$ adalah 77

# BAB VIII

## FUNGSI ∅ ($PHI$) dan Teorema Euler

**Definisi 8.1**

Sistem residu sederhana modulo m adalah himpunan semua bilangan bulat positif $r_i$ yang memenuhi $(r_i, m) = 1\ dengan\ r_i \neq r_j\ (mod\ m)\ untuk\ i \neq j$

**Contoh 8.1**

1. Himpunan {0, 1, 2, 3, 4, 5, 6, 7 dan 8} adalah himpunan semua residu terkecil modulo 9. Apabila dipilih unsur yang saling prima dengan 9 yaitu: {1, 2, 4, 5, 7,8} berjumlah 6. Sehingga fungsi ∅ untuk 9 adalah 6 atau di tulis $\emptyset\ (9) = 6$
2. Himpunan {0, 1, 2, 3, 4, 5, 6, dan 7} adalah himpunan semua residu terkecil modulo 8. Apabila dipilih unsur yang saling prima dengan 8 yaitu: {1, 3, 5, 7} berjumlah 4. Sehingga fungsi ∅ untuk 8 adalah 4 atau di tulis $\emptyset\ (8) = 4$
3. Himpunan {0, 1, 2, 3, 4} adalah himpunan semua residu terkecil modulo 5. Apabila dipilih unsur yang saling prima dengan 5 yaitu: {1, 2, 3, 4} berjumlah 4. Sehingga fungsi ∅ untuk 5 adalah 4 atau di tulis $\emptyset\ (5) = 4$

**Latihan 8.1**

1. $\emptyset\ (5) = \cdots$ 2. $\emptyset\ (24) = \cdots$
3. $\emptyset\ (18) = \cdots$ 4. $\emptyset\ (21) = \cdots$

**Definisi 8.2**

Misalkan m adalah suatu bilangan positif maka $\emptyset\ (\mathrm{m})$ adalah banyaknya elemen dari himpunan residu sederhana modulo m.

Hal ini juga dapat dikatakan $\emptyset\ (\mathrm{m})$ adalah banyaknya bilangan bulat positif yang kurang dari m dan saling prima dengan m, $\emptyset\ (\mathrm{m})$ sering disebut indicator m.

**Contoh 8.2**

1. Himpunan residu sederhana modulo 30 adalah {1, 7, 11, 13, 17, 19, 23, 29}. Banyaknya elemen dari himpunan ini adalah 8 maka dapat dikatakan bahwa $\emptyset\ (30) = 8$.
2. Himpunan residu sederhana modulo 7 adalah {1, 2, 3, 4, 5, 6}. Banyaknya elemen dari himpunan ini adalah 8 maka dapat dikatakan bahwa $\emptyset\ (6) = 1$.

**Latihan 8.2**

1. $\emptyset\ (15) = \cdots$ 2. $\emptyset\ (32) = \cdots$
3. $\emptyset\ (17) = \cdots$ 4. $\emptyset\ (23) = \cdots$

**Teorema 8.1**

Apabila p suatu bilangan prima dan k suatu bilangan bulat positif maka

$$\emptyset\,(p^k) = p^{k-1}(p-1)$$

**Pembuktian:**

Ketika $p$ adalah bilangan prima, setiap bilangan bulat positif kurang dari $p^k$ yang tidak relatif prima dengan $p^k$ harus memiliki faktor $p$ dalam faktorisasinya. Oleh karena itu, perlu mencari berapa banyak bilangan bulat positif kurang dari $p^k$ yang tidak relatif prima dengan $p^k$

Dalam hal ini, setiap kelipatan $p^k$ kurang dari $p^k$ tidak relatif prima dengan $p^k$ karena memiliki faktor $p$ yang sama. Ada $p^{k-1}$kelipatan $p$ kurang dari $p^k$ (yaitu p, 2p, 3p, …, $p^{k-1}p$).

Jadi, untuk menghitung $\emptyset\,(p^k)$ dapat diuraikan sebagai berikut:

$\emptyset\,(p^k) = p^k - j$umlah bilangan yang tidak relatif prima dengan $p^k$

$\emptyset\,(p^k) = p^k -$ jumlah kelipatan $p$ kurang dari $p^k$

$\emptyset\,(p^k) = p^k - p^{k-1}$

$\emptyset\,(p^k) = p^{k-1}(p-1)$

Jadi, $\emptyset\,(p^k) = p^{k-1}(p-1)$ terbukti.

**Contoh 8.3**

1. $\emptyset\,(32) = \cdots$

**Penyelesaian:**

Faktorisasi prima dari 32 adalah $2^5$, dapat diketahui p = 2 dan k = 5. Sehingga

$\emptyset\,(p^k) = p^{k-1}(p-1)$

$\emptyset\,(32) = \emptyset\,(2^5) = 2^{5-1}(2-1)$

$\emptyset\,(32) = 2^4.1$

$\emptyset\,(32) = 16$

2. $\emptyset\,(81) = \cdots$

**Penyelesaian:**

Faktorisasi prima dari 81 adalah $3^4$, dapat diketahui p = 3 dan k = 4. Sehingga

$\emptyset\,(p^k) = p^{k-1}(p-1)$

$\emptyset\,(81) = \emptyset\,(3^4) = 3^{4-1}(3-1)$

$\emptyset\,(81) = 3^3.2$

$\emptyset\,(81) = 54$

**Latihan 8.3**

1. $\emptyset\,(125) = \cdots$ 2. $\emptyset\,(1024) = \cdots$

3. $\emptyset\,(729) = \cdots$ 4. $\emptyset\,(343) = \cdots$

**Teorema 8.2**

Misalkan a, b, dan c adalah bilangan – bilangan bulat, maka (a, bc) = 1 jika dan hanya jika (a,b) = 1 dan (a.c) = **1**

Pembuktian:

Pertama, asumsikan bahwa (a, bc) = 1. Ini berarti bahwa a dan bc saling prima, yaitu tidak memiliki faktor prima yang sama. Karena (a, bc) = 1, berarti tidak ada faktor prima yang sama antara a dan bc. Jika ada faktor prima yang sama antara a dan b, atau a dan c, maka akan menjadi faktor prima yang sama antara a dan bc. Oleh karena itu, dapat kita simpulkan bahwa (a, b) = 1 dan (a, c) = 1. jika (a, b) = 1 dan (a, c) = 1, maka (a, bc) = 1. Diketahui bahwa (a, b) = 1, yang berarti a dan b saling prima. Artinya, tidak ada faktor prima yang sama antara a dan b. Demikian pula, (a, c) = 1, berarti a dan c saling prima dan tidak ada faktor prima yang sama antara a dan c.

Kedua misalkan p adalah suatu faktor prima dari a. Karena a dan b saling prima, p tidak dapat menjadi faktor prima dari b. Dengan demikian, p harus menjadi faktor prima dari c, sehingga p juga menjadi faktor prima dari bc. Oleh karena itu, tidak ada faktor prima yang sama antara a dan bc, yang berarti (a, bc) = 1.

Berdasarkan penjelasan pertama dan kedua dapat dibuktikan bahwa (a, bc) = 1 jika dan hanya jika (a, b) = 1 dan (a, c) = 1 (terbukti)

**Contoh 8.4**

(5, 12) = 1

Bentuk pertama:

(5,4) = 1 dan (5, 3) = 1

Bentuk kedua:

(5,6) = 1 dan (5, 2) = 1

Bentuk ketiga:

(1,12) = 1 dan (5, 12) = 1

**Teorema 8.3**

$fungsi\ \emptyset$ adalah suatu fungsi ganda

**Pembuktian**

Sifat Perkalian:

Untuk setiap dua bilangan bulat positif m dan n yang relatif prima, ingin ditunjukkan bahwa $\emptyset$ (mn)= $\emptyset$ (m). $\emptyset$ (n).

Misalkan D adalah himpunan semua bilangan bulat positif kurang dari atau sama dengan mn yang relatif prima dengan mn atau jumlah elemen dihimpunan D adalah ∅ (m). ∅ (n).

Jika diamati bahwa untuk setiap bilangan bulat positif kurang dari atau sama dengan m yang relatif prima dengan m, terdapat ∅ (n) bilangan bulat positif kurang dari atau sama dengan mn yang relatif prima dengan mn. Alasannya adalah setiap bilangan bulat positif kurang dari atau sama dengan m yang relatif prima dengan m juga relatif prima dengan mn, dan ada φ(n) bilangan bulat positif kurang dari atau sama dengan n yang relatif prima dengan n.

Jadi, jumlah elemen di himpunan D adalah ∅ (mn)= ∅ (m). ∅ (n). Dengan demikian, fungsi φ memenuhi sifat perkalian.

**Contoh 8.5**

1. ∅ (30) = …

**Penyelesaian:**

**Sifat Perkalian**

$\emptyset\,(30) = \emptyset\,(5.6)$

$\emptyset\,(30) = \emptyset\,(5).\emptyset\,(6)$

$\emptyset\,(30) = 4.2$

$\emptyset\,(30) = 8$

Jadi nilai dari ∅ (30) menggunakan sifat penjumlahan dan perkalian adalah 8

2. ∅ (36) = …

**Penyelesaian:**

**Sifat perkalian**

$\emptyset\,(36) = \emptyset\,(4.9)$

$\emptyset\,(36) = \emptyset\,(4).\emptyset\,(9)$

$\emptyset\,(36) = 2.6$

$\emptyset\,(36) = 12$

Jadi nilai dari ∅ (36) menggunakan sifat penjumlahan dan perkalian adalah 12

**Teorema 8.4**

Jika n suatu bilangan bulat positif yang mempunyai bentuk kanonik $P_1^{a_1-1}, P_2^{a_2-1} \ldots P_k^{a_k-1}$ maka

$$\emptyset\,(n) = P_1^{a_1-1}(P_1 - 1)\, P_2^{a_2-1}(P_2 - 1) \ldots\, P_k^{a_k-1}(P_1 - 1)$$

**Pembuktian:**

Karena $n = P_1^{a_1}, P_2^{a_2} \ldots P_k^{a_k}$ dengan p adalah bilangan – bilangan prima yang berbeda untuk i = 1, 2, …, k

$\emptyset\,(n) = P_1^{a_1}, P_2^{a_2} \ldots P_k^{a_k}$

$\emptyset\,(n) = \emptyset\,(P_1^{a_1}, P_2^{a_2} \ldots P_k^{a_k})$

$\emptyset\,(n) = \emptyset\,\left(P_1^{a_1}\right) \emptyset\,(P_2^{a_2}) \ldots \emptyset\,(P_k^{a_k})$

Dengan menggunakan bentuk pada teorema 8.1 $\emptyset\,(p^k) = p^{k-1}(p-1)$ maka

$$\emptyset\,(n) = P_1^{a_1-1}(P_1-1)\,P_2^{a_2-1}(P_2-1) \ldots P_k^{a_k-1}(P_k-1) \quad \text{terbukti}$$

Untuk memudahkan dalam menyelesaikan $\emptyset\,(n)$ dapat digunakan rumus berikut:

$$\emptyset\,(n) = n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_k}\right)$$

**Contoh 8.6**

1. $\emptyset\,(360) = \cdots$

Penyelesaian:

| 360 | |
|---|---|
| 2 | 180 |
| 2 | 90 |
| 2 | 45 |
| 3 | 15 |
| 3 | 5 |

**Cara Pertama**

$\emptyset\,(n) = P_1^{a_1-1}(P_1-1)\,P_2^{a_2-1}(P_2-1) \ldots P_k^{a_k-1}(P_k-1)$

Faktorisasi bilangan 360 adalah $2^3.3^2.5$ maka dapat diketahui

$P_1 = 2 \quad P_2 = 3$ dan $P_3 = 5$

$a_1 = 3 \quad a_2 = 2$ *dan* $a_3 = 1$

$\emptyset\,(36) = \emptyset(2^3.3^2.5)$

$\emptyset\,(36) = \emptyset(2^3)\ \emptyset(3^2)\ \emptyset\,(5)$

$\emptyset\,(36) = 2^{3-1}.(2-1).\ 3^{2-1}.(3-1).\ 5^{1-1}.(5-1)$

$\emptyset\,(36) = 2^2.1.\ 3^1.2.\ 5^0.4$

$\emptyset\,(36) = 4.1.3.\ 2.1.4$

$\emptyset\,(36) = 96$

Jadi, $\emptyset\,(36)\ adalah\ 96$

**Cara Kedua**

$\emptyset\,(n) = n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_k}\right)$

Faktorisasi bilangan 360 adalah $2^3.3^2.5$ maka dapat diketahui

n = 360 $P_1 = 2$ , $P_2 = 3$ dan $P_3 = 5$

$$\emptyset\,(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$\emptyset\,(360) = 360\,.\frac{1}{2}.\frac{2}{3}.\frac{4}{5}$$

$$\emptyset\,(360) = \frac{2880}{30}$$

$$\emptyset\,(360) = 96$$

**2.** $\emptyset\,(45) = \cdots$

**Penyelesaian:**

| 45 | |
|---|---|
| 3 | 15 |
| 3 | 5 |

**Cara Pertama**

$$\emptyset\,(n) = P_1^{a_1-1}(P_1-1)\,P_2^{a_2-1}(P_2-1)\ldots\,P_k^{a_k-1}(P_k-1)$$

Faktorisasi bilangan 45 adalah $3^2.5$ maka dapat diketahui

$P_1 = 3 \quad P_2 = 5$

$a_1 = 2 \quad a_2 = 1$

$$\emptyset\,(45) = \emptyset(3^2.5)$$

$$\emptyset\,(45) = \emptyset\,(3^2)\,\emptyset\,(5)$$

$$\emptyset\,(45) = \,3^{2-1}.(3-1).\,5^{1-1}.(5-1)$$

$$\emptyset\,(45) = \,3^1.2.\,5^0.4$$

$$\emptyset\,(45) = 3.2.1.4$$

$$\emptyset\,(45) = 24$$

Jadi, $\emptyset\,(45)$ adalah 24

**Cara Kedua**

$$\emptyset\,(n) = n\,\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_k}\right)$$

Faktorisasi bilangan 45 adalah $3^2.5$ maka dapat diketahui

n = 45 $P_1 = 3 \quad P_2 = 5$

$$\emptyset\,(45) = 45\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$\emptyset\,(45) = 45\,.\frac{2}{3}.\frac{4}{5}$

$\emptyset\,(45) = \frac{2880}{15}$

$\emptyset\,(45) = 24$

**Latihan 8.4**

1. $\emptyset\,(420) = \cdots$ 2. $\emptyset\,(400) = \cdots$

3. $\emptyset\,(720) = \cdots$ 4. $\emptyset\,(1260) = \cdots$

**Teorema 8.5**

Untuk setiap bilangan bulat positif n > 2 maka $\emptyset\,(n)$ suatu bilangan genap.

**Pembuktian:**

Berikut ini contoh – contoh $nilai\ \emptyset\,(n)$ untuk n > 2

$\emptyset\,(3) = 2,\ \emptyset\,(5) = 2,\ \emptyset\,(6) = 2\ ,\ \emptyset\,(7) = 6$ dan seterusnya. Apakah nilai – nilai $\emptyset\,(n)$ tersebut ada yang ganjil? Misalkan n merupakan perpangkatan dari 2, misalkan $n = 2^k$ dengan k > 2 maka

$$\emptyset\,(n) = \emptyset\ (2^k) = 2^{k-1}(2-1) = 2^{k-1}$$

Tampak disini bahwa $\emptyset\ (2^k)$ suatu bilangan genap. Sekarang ambil sebarang bilangan bulat positif n > 2. Apabila n suatu bilangan prima ganjil, maka $\emptyset\,(n) = n - 1$. Jadi $\emptyset\,(n)$ bilangan genap. Dan apabila n suatu bilangan komposit. Maka n mempunyai faktor prima bilangan ganjil p, misalnya $n = p^k m$ dengan $(p^k, m) = 1$ sehingga

$$\emptyset\,(n) = \emptyset\,(p^k, m)\,\emptyset(\mathrm{m}) = p^{k-1}(p-1)\emptyset(\mathrm{m})$$

Karena p bilangan prima ganjil, maka p – 1 suatu bilangan genap, sehingga $p^{k-1}(p-1)\,\emptyset(\mathrm{m})$ suatu bilangan genap pula. Jadi, $\emptyset\,(n)$ suatu bilangan genap.

**Teorema 8.6**

Untuk setiap bilangan bulat positif n, maka $\sum_{t|n}\ \emptyset(\mathrm{t}) = n$

**Pembuktian:**

Perhatikan bilangan – bilangan bulat positif: 1, 2, 3, 4, … n. letakkan bilangan ini dalam hmpunan $C_t$ dengan t|n, yaitu bilangan – bilangan itu yang dengan n, FPB nya sama dengan t. Dengan kata lain, $\mathrm{m} \in C_t$ jika dan hanya jika (m, n) = t. Sedangkan (m,n) = t jika dan hanya jika $\left(\frac{\mathrm{m}}{t}, \frac{\mathrm{n}}{t}\right) = 1$. Menurut definisi fungsi $\emptyset$ euler, banyaknya elemen dalam $C_t$ adalah $\emptyset\left(\frac{\mathrm{n}}{t}\right)$. Maka banyaknya elemen dari gabungan semua himpunan $C_t$ adalah $\sum_{t|n}\ \emptyset\left(\frac{\mathrm{n}}{t}\right)$, mengingat setiap bilangan 1, 2, 3, …, n hanya terdapat dalam tepat satu himpunan dari $C_t$ maka

$$\sum_{t|n} \emptyset(t) = \sum_{t|n} \emptyset\left(\frac{n}{t}\right) = n$$

**Contoh 8.7**

1. $\sum_{t|12} \emptyset(t) = \cdots$

Penyelesaian:

Faktor dari bilangan 12 adalah 1, 2, 3, 4, 6, dan 12.

| 12 | |
|---|---|
| 1 | 12 |
| 2 | 6 |
| 3 | 4 |

$$\sum_{t|12} \emptyset(t) = \emptyset(1) + \emptyset(2) + \emptyset(3) + \emptyset(4) + \emptyset(6) + \emptyset(12)$$

$$\sum_{t|12} \emptyset(t) = 1 + 1 + 2 + 2 + 2 + 4$$

$$\sum_{t|12} \emptyset(t) = 12$$

Jadi $\sum_{t|12} \emptyset(t) = 12$ atau $\sum_{t|n} \emptyset(t) = n$ terbukti

Keterangan:

$\emptyset(1) = 1 \qquad \emptyset(2) = 1 \qquad \emptyset(3) = 2$

$\emptyset(4) = \emptyset(2^2) = 2\,(2-1) = 2.1 = 2$

$\emptyset(6) = \emptyset(2\,)\,\emptyset(3) = 1\,.\,2 = 2$

$\emptyset(12) = \emptyset(3).\emptyset(4) = 2.2 = 4$

2. $\sum_{t|18} \emptyset(t) = \cdots$

**Penyelesaian:**

Faktor dari bilangan 18 adalah 1, 2, 3, 6, 9, dan 18

| 18 | |
|---|---|
| 1 | 18 |
| 2 | 9 |
| 3 | 6 |

$$\sum_{t|18} \emptyset(t) = \emptyset(1) + \emptyset(2) + \emptyset(3) + \emptyset(6) + \emptyset(9) + \emptyset(18)$$

$$\sum_{t|18} \emptyset(t) = 1 + 1 + 2 + 2 + 6 + 6$$

$$\sum_{t|18} \emptyset(t) = 18$$

**Jadi** $\sum_{t|18} \emptyset(t) = 18$ atau $\sum_{t|n} \emptyset(t) = n$ terbukti

**Keterangan:**

$\emptyset(1) = 1 \qquad \emptyset(2) = 1 \qquad \emptyset(3) = 2$

$\emptyset(6) = \emptyset(2)\ \emptyset(3) = 1 . 2 = 2$

$\emptyset(9) = \emptyset(3^2) = 3\ (3 - 1) = 3. 2 = 6$

$\emptyset(18) = \emptyset(2). \emptyset(9) = 1.6 = 6$

**Teorema 8.7**

Teorema Residu Sisa atau Teorema Keberadaan Residu Sisa. Teorema ini menyatakan bahwa jika a dan m adalah dua bilangan bulat positif dengan (a,m) = 1 , maka residu sisa modulo m dari a kali setiap bilangan bulat positif yang kurang dari m yang saling prima dengan m adalah suatu permutasi dari residu sisa modulo m dari bilangan-bilangan tersebut.

**Pembuktian:**

Untuk membuktikan teorema ini, perlu mengenal beberapa definisi terlebih dahulu.

**Definisi 8.3**

a) a $\equiv$ b (mod m) berarti a kongruen dengan b modulo m, yaitu a dan b memiliki residu sisa yang sama saat dibagi dengan m.
b) (a,m) menyatakan FPB (Faktor Persekutuan Terbesar) antara a dan m.

Dalam bukti teorema ini, akan menggunakan beberapa hasil dan sifat yang sudah diketahui, seperti sifat-sifat FPB dan sifat-sifat kongruensi modulo.

**Pembuktian:**

Misalkan $r_1, r_2, r_3$ ... $r_{\emptyset(m)}$ adalah bilangan-bilangan bulat positif kurang dari m yang saling prima dengan m. Dalam bukti ini, akan menggunakan notasi $R_i$ untuk menyatakan residu sisa modulo m dari bilangan $ar_i$

Langkah 1:

Karena (a, m) = 1, maka setiap bilangan ariari juga saling prima dengan m (disebutkan dalam teorema). Dengan kata lain, ($ar_i$, m) =1 untuk setiap i.

Langkah 2:

Karena $r_i$ saling prima dengan m, maka ($r_i$, m) =1 untuk setiap i. Dalam hal ini, juga dapat menggunakan sifat kongruensi modulo yang menyatakan bahwa jika a $\equiv$ b (mod m) dan (b, m) = 1 maka (a, m) = 1.

Langkah 3:

akan membuktikan bahwa $R_i$ juga merupakan suatu permutasi dari $r_i$. Dalam bukti ini, akan menggunakan metode pembuktian secara kontradiksi.

Anggaplah terdapat dua indeks i dan j dengan $1 \leq i < j \leq \emptyset(m)$ sedemikian sehingga $R_i$ = $R_j$. Dengan kata lain, residu sisa modulo m dari $ar_i$ sama dengan residu sisa modulo m dari $ar_j$.

Ini berarti $ar_i \equiv ar_j$ (mod m) Jika dikurangi kedua sisi dengan a, diperoleh $r_i \equiv r_j$ (mod m). Namun, $r_i$ dan $r_j$ adalah bilangan-bilangan bulat positif kurang dari m yang saling prima dengan m, yang berarti mereka tidak dapat memiliki residu sisa yang sama modulo m. Ini adalah kontradiksi dengan asumsi sebelumnya. Jadi, kesimpulan dari langkah ini adalah bahwa $R_i$ adalah suatu permutasi dari $R_i$ untuk setiap i. Dengan demikian, teorema ini terbukti.

**Contoh 8.8**

Carilah residu terkecil dari

a. $11^6$ (mod 9)

**Penyelesaian:**

Bilangan – bilangan 1, 2, 4, 5, 7, 8 masing – masing adalah saling prima terhadap 9. Apabila setiap bilangan tersebut dikalikan 11 diperoleh 11, 22, 44, 55, 77, 88. Selanjutnya jika bilangan – bilangan itu dicari residu terkecil modulo 9 maka di peroleh

$$11 \equiv 2 \pmod 9$$
$$22 \equiv 4 \pmod 9$$
$$44 \equiv 8 \pmod 9$$
$$55 \equiv 1 \pmod 9$$
$$77 \equiv 5 \pmod 9$$
$$88 \equiv 7 \pmod 9$$

Tampak bahwa residu terkecil modulo 9 dari 11, 22, 44, 55, 77, 88 berturut – turut 2, 4, 8, 1, 5 dan 7 yang merupakan suatu permutasi dari 1, 2, 4, 5, 7, 8.

b. $5^6$ (mod 14)

**Penyelesaian:**

Bilangan – bilangan 1, 3, 5, 9, 11, 13 masing – masing adalah saling prima terhadap 14. Apabila setiap bilangan tersebut dikalikan 5 diperoleh 5, 15, 25, 45, 64. Selanjutnya jika bilangan – bilangan itu dicari residu terkecil modulo 14 maka di peroleh

$$5 \equiv 5 \pmod{14}$$
$$15 \equiv 1 \pmod{14}$$
$$25 \equiv 11 \pmod{14}$$
$$45 \equiv 3 \pmod{14}$$
$$55 \equiv 13 \pmod{14}$$
$$65 \equiv 9 \pmod{14}$$

Tampak bahwa residu terkecil modulo 14 dari 15, 45, 5, 65, 25, 55 berturut – turut 5, 1, 11, 3, 13, 9 yang merupakan suatu permutasi dari 1, 3, 5, 9, 11, 13.

**Latihan 8.5**

Carilah residu terkecil dari

1. $3^{12} \pmod{13}$
2. $6^{19} \pmod{19}$
3. $5^{16} \pmod{17}$

**Teorema 8.8**

Jika m suatu bilangan bulat positif dan (a, m) = 1 maka $a^{\emptyset(m)} \equiv 1 \ (mod\ m)$

**Pembuktian:**

Misalkan $r_1, r_2, r_3 \ldots r_{\emptyset(m)}$ adalah bilangan-bilangan bulat positif yang kurang dari m dan masing – masing prima dengan m. menurut teorema 8.7, (a, m) = 1. Maka residu – residu terkecil modulo m dari $ar_1, ar_2, ar_3 \ldots ar_{\emptyset(m)}$ adalah suatu permutasi dari $r_1, r_2, r_3 \ldots r_{\emptyset(m)}$ sehingga diperoleh

$$ar_1, ar_2, ar_3 \ldots ar_{\emptyset(m)} \equiv r_1, r_2, r_3 \ldots r_{\emptyset(m)}$$
$$a^{\emptyset(m)}\, r_1\, r_2\, r_3 \ldots r_{\emptyset(m)} \equiv r_1, r_2, r_3 \ldots r_{\emptyset(m)}$$

Karena $r_1, r_2, r_3 \ldots r_{\emptyset(m)}$ masing – masing prima relatif dengan m, maka hasilkali bilangan – bilangan itu saling prima dengan m pula. Sehingga dapat menghilangkan $r_1, r_2, r_3 \ldots r_{\emptyset(m)}$ dari kekongruenan terakhir dan diperoleh $a^{\emptyset(m)} \equiv 1 \ (mod\ m)$ (terbukti)

**Contoh 8.9**

1. Buktikan $11^6 \equiv 1 \pmod{9}$ ?

**Penyelesaian:**

Bilangan – bilangan 1, 2, 4, 5, 7, 8 masing – masing adalah saling prima terhadap 9. Apabila setiap bilangan tersebut dikalikan 11 diperoleh 11, 22, 44, 55, 77, 88. Selanjutnya jika bilangan – bilangan itu dicari residu terkecil modulo 9 maka di peroleh

$$11 \equiv 2 \pmod 9$$
$$22 \equiv 4 \pmod 9$$
$$44 \equiv 8 \pmod 9$$
$$55 \equiv 1 \pmod 9$$
$$77 \equiv 5 \pmod 9$$
$$88 \equiv 7 \pmod 9$$

Tampak bahwa residu terkecil modulo 9 dari 11, 22, 44, 55, 77, 88 berturut – turut 2, 4, 8, 1, 5 dan 7 yang merupakan suatu permutasi dari 1, 2, 4, 5, 7, 8. Selanjutnya jika ruas - ruas dari 6 kekongruenan tersebut dikalikan, akan diperoleh

11, 22, 44, 55, 77, 88 $\equiv 1, 2, 4, 5, 7, 8 \pmod 9$

$11^6\ (1, 2, 4, 5, 7, 8\ )$ $\equiv 1, 2, 4, 5, 7, 8 \pmod 9$

$11^6$ $\equiv 1 \pmod 9$ terbukti

2. Buktikan $14^6 \equiv 1 \pmod{14}$ ?

**Penyelesaian:**

Bilangan – bilangan 1, 3, 5, 9, 11, 13 masing – masing adalah saling prima terhadap 14. Apabila setiap bilangan tersebut dikalikan 5 diperoleh 5, 15, 25, 45, 64. Selanjutnya jika bilangan – bilangan itu dicari residu terkecil modulo 14 maka di peroleh

$$5 \equiv 5 \pmod{14}$$
$$15 \equiv 1 \pmod{14}$$
$$25 \equiv 11 \pmod{14}$$
$$45 \equiv 3 \pmod{14}$$
$$55 \equiv 13 \pmod{14}$$
$$65 \equiv 9 \pmod{14}$$

Tampak bahwa residu terkecil modulo 14 dari 15, 45, 5, 65, 25, 55 berturut – turut 5, 1, 11, 3, 13, 9 yang merupakan suatu permutasi dari 1, 3, 5, 9, 11, 13. Selanjutnya jika ruas - ruas dari 6 kekongruenan tersebut dikalikan, akan diperoleh

15, 45, 5, 65, 25, 55 $\equiv 1, 3, 5, 9, 11, 13 \pmod{14}$

$14^6\ (1, 3, 5, 9, 11, 13)$ $\equiv 1, 3, 5, 9, 11, 13 \pmod{14}$

$14^6$ $\equiv 1 \pmod{14}$ terbukti

3. Tentukan sisa pembagian $26^6$ oleh 15?

**Penyelesaian:**

Karena (26, 15) = 1 maka $\emptyset(15) = 8$

Maka $26^8 \equiv 1\ (mod\ 15)$ Akibatnya

$26^8 \equiv 26\ (26)^8\ (mod\ 15)$

$26^8 \equiv 11.(1\ )(mod\ 15)$

$26^8 \equiv 11\ (mod\ 15)$

$jadi, 26^6$ di bagi 15 bersisa 11

**Latihan 8.5**

**Buktikan:**

1. $3^{12} \equiv 1\ (\text{mod } 13)$
2. $6^{19} \equiv 1\ (\text{mod } 19)$
3. $5^{16} \equiv 1(\text{mod } 17)$

Perhatikan bahwa teorema Euler ini merupakan generalisasi dari teorema fermat. Sebab jika p suatu bilangan prima, maka $\emptyset\ (\text{p}) = \text{p} - 1$ sehingga jika (a, p) = 1 maka $a^{\emptyset(\text{p})} = a^{(\text{p}-1)} \equiv 1\ (mod\ p)$ (teorema fermat).

Pada teorema euler untuk menentukan invers modulo m dari suatu bilangan bulat a, asalkan (a,m) = 1. Menurut teorema Euler, jika (a, m) = 1 sehingga

$$a\ a^{\emptyset(\text{m})-1} \equiv 1\ (mod\ m)$$

$a^{\emptyset(\text{m})-1}$ merupakan suatu invers a modulo m.

Dengan invers a modulo m ini, dapat menyelesaikan suatu perkongruenan linier $ax \equiv b\ (mod\ m)$ dengan (a, m) = 1 sebagai berikut:

$$ax \equiv b\ (mod\ m)$$
$$a^{\emptyset(\text{m})-1}ax \equiv a^{\emptyset(\text{m})-1}\ b\ (mod\ m)$$
$$x \equiv a^{\emptyset(\text{m})-1}\ b\ (mod\ m)$$

**Contoh 8.10**

1. Tentukan invers 2 mod 15

**Penyelesaian:**

Karena $\emptyset(15) = 8$ maka

$$2.\ 2^{8-1} \equiv 1\ (mod\ 15)$$
$$2.\ 2^7 \equiv 16\ (mod\ 15)$$
$$2^7 \equiv 8\ (mod\ 15)$$

2. Selesaikan perkongruenan $3x \equiv 7\ (mod\ 10)$

**Penyelesaian:**

Diketaui: a = 3, b = 7 dan $\emptyset(10) = 4$ maka

$$a^{\emptyset(\mathrm{m})-1}ax \equiv a^{\emptyset(\mathrm{m})-1}\ b\ (mod\ m)$$

$$3^{4-1}\ 3x \equiv 3^{4-1}\ 7\ (mod\ 10)$$

$$3^3\ x \equiv 3^3\ 7\ (mod\ 10)$$

$$x \equiv 3^3\ 7\ (mod\ 10)$$

$$x \equiv 189\ (mod\ 10)$$

$$x \equiv 9\ (mod\ 10)$$

3. Tentukan dua angka terakhir dari hasil perpangkatan $77^{561}$

**Penyelesaian:**

$\emptyset(100) = \emptyset(2^2.5^2) = 2\ (2-1).\ 5\ (5-1) = 40$ karena (100, 77) = 1 Maka dapat dituliskan menjadi $77^{40} \equiv 1\ (mod\ 100)$.

$$77^{561} \equiv\ 77.(77)^{560}\ (mod\ 100)$$

$$77^{561} \equiv\ 77.(77^{40})^{14}(mod\ 100)$$

$$77^{561} \equiv\ 77.(1)^{14}(mod\ 100)$$

$$77^{561} \equiv\ 77\ (mod\ 100)$$

Jadi dua digit dari hasil perpangkatan $77^{561}$ adalah 77

4. Tentukan dua angka terakhir dari hasil perpangkatan $3^{256}$

**Penyelesaian:**

$\emptyset(100) = \emptyset(2^2.5^2) = 2\ (2-1).\ 5\ (5-1) = 40$ karena (100, 3) = 1 Maka dapat dituliskan menjadi $3^{40} \equiv 1\ (mod\ 100)$.

256 = 6. 40 + 16

$3^{256} \equiv\ (3^{40})^6.(3)^{16}(mod\ 100)$

$3^{256} \equiv\ (1)^6.(3)^{16}(mod\ 100)$

$3^{256} \equiv\ (3)^{16}(mod\ 100)$

$3^{256} \equiv\ (3^4)^4(mod\ 100)$

$3^{256} \equiv\ (81)^4(mod\ 100)$ 81 – 100 = 19

$3^{256} \equiv\ (-19)^4(mod\ 100)$

$3^{256} \equiv\ (-19^2)^2(mod\ 100)$

$3^{256} \equiv\ (361)^2(mod\ 100)$ 361 – 100 = 61

$3^{256} \equiv\ (61)^2(mod\ 100)$

$3^{256} \equiv\ (-39)^2(mod\ 100)$ 61 – 100 = 39

$3^{256} \equiv 1521 \ (mod\ 100)$ 1521 – 1000 = 21

$3^{256} \equiv 21 \ (mod\ 100)$

**Latihan 8.6**

Tentukan dua digit terakhir dari $3^{1234}$ dan $13^{218}$

# BAB IX

## AKAR PRIMITIF DAN INDEKS

### A. Order Bilangan Bulat Positif

Berdasarkan Teorema Euler, yaitu: jika $(a, m) = 1$ maka $a^{\phi(m)} \equiv 1 \ (mod\ m)$. Akan tetapi sering kali, ada pangkat bulat positif dari a lebih kecil dari $\phi(m)$ yang kongruen modulo $m$ dengan 1. Sebagai contoh, menurut Teorema Euler, $2^{\phi(7)} = 2^6 \equiv 1 \ (mod\ 7)$, akan tetapi $2^3 \equiv 1 \ (mod\ 7)$ dan tidak ada bilangan bulat positif yang lebih kecil dari 3, untuk memangkatkan 2 akan kongruen modulo 7 dengan 1. Hal ini berkenaan dengan konsep order suatu bilangan bulat yang definisinya diberikan berikut ini.

**Definisi 9.1**

Misalkan suatu bilangan bulat positif $m > 1$ dan $(a, m) = 1$. Order dari $a$ modulo $m$ adalah suatu bilangan bulat positif terkecil. Misalnya $t$, sedemikian $a^t \equiv 1 \ (mod\ m)$ .

"Order $a$ modulo $m$" diberi simbol "$ord_m a$".

**Contoh 9.1**

Perhatikan residu – residu terkecil dari perpangkatan bulat positif modulo 7, pada tabel 9.1 berikut ini:

**Tabel 9.1**

**Residu – residu terkecil dari perpangkatan bulat positif modulo 7**

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 1 | 2 | 4 | 1 |
| 3 | 2 | 6 | 4 | 5 | 1 |
| 4 | 2 | 1 | 4 | 2 | 1 |
| 5 | 4 | 6 | 2 | 3 | 1 |
| 6 | 1 | 6 | 1 | 6 | 1 |

Tampak pada tabel 9.1 bahwa:

$1^1 \equiv 1 \ (mod\ 7), maka\ ord_7 1 = 1$

$2^3 \equiv 1\ (mod\ 7), maka\ ord_7 2 = 3$

$3^6 \equiv 1\ (mod\ 7), maka\ ord_7 3 = 6$

$4^3 \equiv 1\ (mod\ 7), maka\ ord_7 4 = 3$

$5^6 \equiv 1\ (mod\ 7), maka\ ord_7 5 = 6$

$6^2 \equiv 1\ (mod\ 7), maka\ ord_7 6 = 2$

Berapakah order dari 10 $(mod\ 7)$. Karena $10 \equiv 3\ (mod\ 7)$ maka $10^6 \equiv 3^6\ (mod\ 7)$ dan karena $3^6 \equiv 1\ (mod\ 7)$, yaitu $ord_7 3 = 6$ maka $ord_7 10 = 6$ pula. `

Pada definisi 9.1 tersebut perlu ditekankan bahwa order dari $a\ (mod\ m)$ hanya ada, jika syarat $(a, m) = 1$ dipenuhi. Sebab, jika $(a, m) \neq 1$ seperti telah diketahui bahwa perkongruenan linier $ax \equiv 1\ (mod\ m)$ tidak mempunyai penyelesaian.

Pada contoh di atas tampak bahwa order dari bilangan - bilangan modulo 7 adalah 1, 2, 3 atau 6 yang masing – masing membagi 6. Hal ini mengarahkan pada teorema berikut ini:

**Teorema 9.1**

Misalkan $(a, m) = 1$ dan order a (mod m) adalah $t$, maka $a^k \equiv 1\ (mod\ m)$ jika dan hanya jika $t|k$

**Pembuktian:**

Karena $ord_m a = t$ berarti $t$ adalah suatu bilangan bulat positif terkecil sedemikian hingga $a^t \equiv 1\ (mod\ m)$. Perhatikan bilangan – bilangan bulat positif $k$ dan $t$ menurut algoritma pembagian, maka ada bilangan – bilangan bulat $q$ dan $r$ sedemikian hingga

$$a^k = a^{qt+r} = (a^t)^q . a^r$$

Karena diketahui bahwa$a^k \equiv 1\ (mod\ m)$ maka

$$a^{qt+r} \equiv 1\ (mod\ m)$$

$$(a^t)^q . a^r \equiv 1\ (mod\ m)$$

$a^r \equiv 1\ (mod\ m)$ sebab $a^r \equiv 1\ (mod\ m)$Karena $0 \leq r < t\ dan\ t$ adalah bilangan bulat positif terkecil sedemikian hingga $a^t \equiv 1\ (mod\ m)$ maka $r = 0$ sehingga $k = qt$ dan diperoleh $t|k$. Sebaliknya, karena $t|k$ maka $k = th$ untuk suatu bilangan bulat $h$. Karena $a^t \equiv 1\ (mod\ m)$ maka $(a^t)^h \equiv 1\ (mod\ m)$ yaitu: $a^k \equiv 1\ (mod\ m)$.

Menurut Teorema Euler, $(a, m) = 1\ a^{\phi(m)} \equiv 1\ (mod\ m)$. Apabila order dari $a\ (mod\ m)$ adalah $t$ maka menurut teorema 9.1, dapat disimpulkan bahwa $t|\phi(m)$*.

Hal ini dinyatakan sebagai akibat berikut ini.

**Akibat 9.1**

Jika $(a, m) = 1$ dan order $a\ (mod\ m)$ adalah $t$ maka $t|\phi(m)$

**Contoh 9.2**

**Hitunglah $ord_{21}5$**

**Penyelesaian:**

Perhatikan bahwa $\phi\ (21) = \phi\ (3.7\ ) = \phi(3)\ \varphi(7)\ = 2.6 = 12.$ Faktor-faktor positif d $\phi(21) = 12$ adalah $1, 2, 3, 4, 6,$ dan $12$, sehingga hanya ini nilai yang mungkin dari $ord_{21}5$. Kemudian, cari $5^d$ modulo $21$ untuk setiap $d$ sampai sisanya menjadi $1$ :

$5^1 \equiv 5\ (mod\ 21)$ $\quad$ $5^2\ \equiv\ 4\ (mod\ 21)$ $\quad$ $5^3 \equiv -1\ (mod\ 21)$

$5^4 \equiv -5\ (mod\ 21)$, tetapi $\quad$ $5^6 \equiv 1\ (mod\ 21)$

Dengan demikian, dapat disimpulkan bahwa$ord_{21}\ 5 = 6$

**Sebagai catatan:**

untuk menghitung $ord_m\ a$, kita harus menghitung $a^k$ modulo $m$ untuk setiap bilangan bulat positif $k \leq \phi(m)$.

**Contoh 9.3**

Perhatikan order – order dari bilangan – bilangan bulat positif modulo 13, pada tabel 9.2 berikut ini dan $\phi(13) = 12$

**Tabel 9.2**

**Order – order dari bilangan – bilangan bulat positif modulo 13**

| Bilangan Bulat | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Orde (Mod 13) | 1 | 12 | 3 | 6 | 4 | 12 | 12 | 4 | 3 | 6 | 12 | 2 |

Perhatikan pada tabel 9.2 order dari bilangan – bilangan bulat positif yang merupakan residu terkecil modulo 13 adalah pembagi dari $\phi(13)$

$$3^0 \equiv 3^3 \equiv 3^6 \equiv 3^9 (mod\ 13) \text{ dan}$$

$$3^1 \equiv 3^4 \equiv 3^7 \equiv 3^{10} (mod\ 13)$$

Pernyataan ini mengarahkan pada teorema berikut ini:

**Teorema 9.2**

Jika $(a,m)=1$ dan order $a\ (mod\ m)$ adalah $k$, maka $a^i \equiv a^j\ (mod\ m)$ jika dan hanya jika $i \equiv j\ (mod\ k)$

**Pembuktian:**

Misalkan $a^i \equiv a^j\ (mod\ m)$ dengan $i \geq j$. Karena $(a,m)=1$ maka $a^{i-j} \equiv 1\ (mod\ m)$. Selanjutnya, karena $ord_m a = k$, Menurut teorema 9.1, karena $k|(i-j)$. Hal ini berarti $i \equiv j\ (mod\ k)$. Sebaliknya, karena $i \equiv j\ (mod\ k)$ maka $i = j + tk$, untuk suatu bilangan bulat $t$. Karena $ord_m a = k$ maka $a^k \equiv 1\ (mod\ m)$. Sehingga:

$$a^i \equiv a^{j+tk}(mod\ m)$$
$$a^i \equiv a^j(a^k)^t(mod\ m)$$
$$a^i \equiv a^j(mod\ m)*$$

Memperhatikan teorema ini, karena $ord_m a = k$, yaitu $k$ adalah suatu bilangan bulat terkecil sedemikian hingga $a^k \equiv 1\ (mod\ m)$, maka bilangan – bilangan bulat positif $a, a^2, a^3, \dots, a^k$ tidak ada yang kongruen $modulo\ m$. Sebab, jika $a^i \equiv a^j (mod\ m)$ dengan $1 \leq i \leq j \leq k$ maka menurut teorema 9.2 $i \equiv j\ (mod\ k)$ yang berarti $i = j$. Hal ini merupakan akibat teorema 9.2 yang dinyatakan berikut ini.

**Akibat 9.2**

Jika $(a,m)=1$ dan order $a\ (mod\ m)\ adalah\ k$, maka bilangan – bilangan bulat positif $a, a^2, a^3, \dots, a^k$ tidak ada yang kongruen $modulo\ m$

Jika diketahui bahwa $ord_m a = k$, berapakah order dari $a^t (mod\ m)$? Misalkan $(k,t)=d$ maka $k = k_1 d$ dan $t = t_1 d$ dengan $(k_1, t_1) = 1$ maka:

$$(a^t)^{k_1} = (a^{t_1 d})^{\frac{k}{d}} = (a^k)^{t_1} \equiv 1\ (mod\ m)$$

Misalkan order dari $a^t (mod\ m)$ adalah r, menurut teorema 9.1 maka $r|k_1$ dan

$$(a^t)^r = a^{tr} \equiv 1\ (mod\ m)$$

Karena order dari $a\ (mod\ m)$ adalah $k$, maka $k|\ tr$. Dengan kata lain, $k_1 d | t_1 dr$ atau $k_1 | t_1 r$

Dan karena $(k_1, t_1) = 1$ maka $k_1 | r$. Selanjutnya, karena $r|k_1$ dan $k_1|r$, maka $k_1 = r$,

sehingga $k_1 = r = \frac{k}{d} = \frac{k}{(k,t)}$

**Teorema 9.3**

Jika $(a,m)=1$ dan order $a\ (mod\ m)\ adalah\ k$, maka Jika order $a\ (mod\ m)$ dengan $t > 0$ adalah $\frac{k}{(t,k)}$

Pada teorema 9.3 tersebut $(t,k)=1$, maka $ord_m a^t = ord_m a$ sebaliknya, jika $ord_m a = ord_m a^t = k$ maka dapat dibuktikan $(t,k)=1$.

Misalkan $(t,k) = d$, maka $\frac{t}{d}$ dan $\frac{k}{d}$ adalah bilangan – bilangan bulat. Order $a\ (mod\ m)$ adalah $k$, maka:

$$a^k \equiv 1\ (mod\ m)$$

$$(a^k)^{\frac{t}{d}} \equiv 1\ (mod\ m)$$

$$(a^t)^{\frac{k}{d}} \equiv 1\ (mod\ m)$$

Karena Order dari $a^t\ (mod\ m)$ adalah $k$ maka $k|\frac{k}{d}$. Hal ini hanya mungkin, apabila $d = 1$, jadi $(t,k) = 1$ *

Hal ini merupakan akibat teorema 9.3 yang dinyatakan berikut ini.

**Akibat 9.3**

Jika $(a,m) = 1$ dan order $a\ (mod\ m)\ adalah\ k$, maka order dari $a^t (mod\ m) adalah\ k$ jika dan hanya jika $(t,k) = 1$.

Perhatikan kembali tabel 9.2, order dari 2 $(mod\ 13)$ adalah 12, sedangkan order dari $2^2$ dan $2^3\ (mod\ 13)$ berturut – turut adalah 6.

Sesuai dengan teorema 9.3, hal tersebut mudah diperiksa bahwa

$$ord_{13}2^2 = \frac{ord_{13}2}{(2, ord_{13}2)} = \frac{12}{(2,12)} = 6$$

$$ord_{13}2^3 = \frac{ord_{13}2}{(3, ord_{13}2)} = \frac{12}{(3,12)} = 4$$

Mengingat dari akibat 9.3 tersebut, maka perpangkatan bulat positif dari 2 yang mempunyai order 12 adalah $2^5, 2^7, 2^{11}$. Sedangkan $2^5 \equiv 6\ (mod\ 13), 2^7 \equiv 11\ (mod\ 13)$. Selanjutnya, 2, 6, 7, dan 11 masing – masing yang mempunyai order 12 = $\phi(13)$ dan disebut *akar – akar primitif* dari 13. Akar – akar primitif dari suatu bilangan bulat didefinisikan sebagai berikut:

**Definisi 9.2**

Jika $(a,m) = 1$ dan order $a\ modulo\ m\ adalah\ \phi(m)$ maka $a$ dinamakan *akar – akar primitif dari* $m$.

Dengan kata lain, bilangan bulat positif $m$ mempunyai *akar primitif* $a$, apabila $a^{\phi(m)} \equiv 1\ (mod\ m)$ asalkan $a^k \neq 1\ (mod\ m)$, untuk semua bilangan bulat positif $k < \phi(m)$. Selanjutnya, kita mudah untuk memeriksa bahwa 3 adalah akar – akar primitif dari 7, karena $\phi(7) = 6$ dan

$$3^1 \equiv 3\ (mod\ 7)$$

$$3^2 \equiv 2\ (mod\ 7)$$

$$3^3 \equiv 6\ (mod\ 7)$$

$$3^4 \equiv 4\ (mod\ 7)$$
$$3^5 \equiv 5\ (mod\ 7)$$
$$3^6 \equiv 1\ (mod\ 7)$$

Apabila $p$ suatu bilangan prima dan $(a, p) = 1$, maka perkongruenan linier $ax \equiv 1\ (mod\ p)$ selalu mempunyai solusi. Mengingat Teorema Euler, $a^{p-1} \equiv 1\ (mod\ p)$, maka solusinya adalah residu terkecil modulo $p$ yaitu: $ap^{-2}$. Hal ini berarti setiap bilangan prima mesti mempunyai akar primitif. Sedangkan untuk bilangan bulat positif $n$ yang bukan bilangan prima belum tentu mempunyai akar primitif.

**Contoh 9.4**

Akar – akar primitif dari 9 adalah 2 dan 5, karena $\phi(9) = 6$ dan $ord_9 2 = ord_9 5 = 6$. Tetapi 8 tidak mempunyai akar primitif, sebab $\phi(8) = 4$ dan $3^2 \equiv 1\ (mod\ 8), 5^2 \equiv 1\ (mod\ 8)\ dan\ 7^2 \equiv 1\ (mod\ 8)$

**Teorema 9.4**

Misalkan $(a, m) = 1$ dan $c_1, c_2, \dots, c_{\phi(m)}$ adalah bilangan – bilangan bulat positif yang kurang dari $m$ dan saling prima dengan $m$. Apabila $a$ adalah akar primitif dari $m$, maka $a^1, a^2, \dots, a^{\phi(m)}$ berturut – turut kongruen modulo $m$ dengan permutasi dari $c_1, c_2, \dots, c_{\phi(m)}$

**Pembuktian:**

karena $(a, m) = 1$ maka setiap perpangkatan bulat positif dari $a$ juga saling prima dengan $m$ yaitu: $a^1, a^2, \dots, a^{\phi(m)}$ masing – masing saling prima dengan $m$. Karena $c_1, c_2, \dots, c_{\phi(m)}$ adalah bilangan – bilangan bulat positif yang kurang dari $m$ dan saling prima dengan $m$, maka untuk membuktikan teorema tersebut cukup menunjukkan bahwa tidak ada dua suku dari $a^1, a^2, \dots, a^{\phi(m)}$ yang kongruen modulo $m$

$$a^i \equiv a^j (mod\ m) \text{ untuk } 0 < j \leq i \leq \phi(m)$$
$$a^{i-j} \equiv 1\ (mod\ m)$$

Karena $a$ ialah akar primitif dari $m$, bearti order $a\ (mod\ m)$ adalah $\phi(m)$. Dan karena $0 \leq i - j \leq \phi(m)$, maka kekongruenan terakhir itu mungkin apabila $i - j = 0$, sehingga $i = j$. Hal ini berarti bahwa tidak ada dua suku dari $a^1, a^2, \dots, a^{\phi(m)}$ yang kongruen modulo $m$.*

**Contoh 9.5**

Akar – akar primitif dari 9 adalah 2 dan $\phi(9) = 6$, maka $2^6 \equiv 1\ (mod\ 9)$ dan $2^t \not\equiv 1\ (mod\ 9)$, untuk $1 \leq t < 6$ yaitu: $2^1 \equiv 2\ (mod\ 9), 2^1 \equiv 2\ (mod\ 9), 2^2 \equiv 4\ (mod\ 9), 2^3 \equiv 8\ (mod\ 9)$, $2^4 \equiv 7\ (mod\ 9)$ dan $2^5 \equiv 5\ (mod\ 9)$. Atau dengan kata lain, $\text{ord}_9 2 = 6 = \phi(9)$. Berapakah

$\text{ord}_9 2^5$? Karena $(2^5)^6 \equiv 1\ (mod\ 9)$ maka $\text{ord}_9\ 2^5 = 6 = \phi(9)$ jadi $2^5$ juga merupakan akar primitif dari 9.

Perhatikan bahwa himpunan residu sederhana modulo 9 adalah {1, 2, 4, 5, 7, 8} dan elemen – elemen himpunan ini berturut – turut kongruen modulo 9 dengan elemen – elemen himpunan $\{2^6, 2^1, 2^2, 2^5, 2^4, 2^3\}$, memperhatikan himpunan terakhir ini, maka akar primitif yang lain dari 9 adalah $2^5 \equiv 5(mod\ 9)$. Jadi akar – akar primitif dari 9 adalah 2 dan 5. Contoh ini memberikan ilustrasi pada akibat dari teorema 9.4 berikut ini.

**Akibat 9.4.**

Misalkan $a$ adalah suatu akar primitif $m$, maka $a^t$ suatu akar primitif dari $m$ pula jika dan hanya jika $\big(t, \phi(m)\big) = 1$

**Pembuktian:**

Karena $a^t$ adalah suatu akar primitif $m$, maka $\text{ord}_\text{m}\ a^t = \phi(m) =. \text{ord}_\text{m}$ jika dan hanya jika $\big(t, \phi(m)\big) = 1$, sesuai dengan akibat 3.

Berapakah banyaknya akar – akar dari 13? Jika dilihat pada tabel 9.2 . Maka akar – akar primitif dari 13 adalah 2, 6, 7, dan 11. Jadi banyaknya akar – akar primitif dari 13 adalah 4 (empat). Ingat bahwa $\phi(13) = 12$ dan $\phi(12) = 4$, sehingga banyaknya akar primitif dari 13 adalah $\phi\phi(13) = 4$. Memperhatikan teorema 9.4 dan akibat 9.4 diperoleh berikut ini.

**Teorema 9.5**

Apabila bilangan bulat positif $m$ dmempunyai akar primitif, maka banyaknya akar primitif dari $m$ adalah $\phi(\phi(m))$

**Pembuktian:**

Misalkan akar primitif dari $m$ adalah $a$, maka teorema 9.4, akar - akar primitif yang lain dapat dicari dari himpunan $\{a^1, a^2, \dots, a^{\phi(m)}\}$, yaitu $a^k$ dengan $1 \le k \le \phi(m)$ yang berorder $\phi(m)$. Hal ini diperoleh, apabila $\big(k, \phi(m)\big) = 1$. Banyaknya bilangan bulat positif $k$, dengan $1 \le k \le \phi(m)$ yang memenuhi $\big(k, \phi(m)\big) = 1$ adalah $\phi(\phi(m))$. Jadi banyaknya akar primitif dari $m$ adalah $\phi\big(\phi(m)\big)$. *

**Contoh 9.6**

Sebuah akar primitif dari 17 adalah 3, sebab order 3 $(mod\ 17)$ adalah $16 = \phi(17)$. Akar - akar primitif dari 17 lainnya adalah $3^3, 3^5, 3^7, 3^{11}, 3^{12}, 3^{15}$ (ingat eksponen – eksponen tersebut saling prima dengan 16) yang berturut – turut kongruen modulo 17 dengan 10, 5, 11, 14, 7, 12, 6. Jadi banyaknya akar primitif dari 17 adalah 8, dan $\phi\big(\phi(17)\big) = \phi(16) = 8$

## B. Akar Primitif

Pengertian akar primitif dari suatu bilangan positif $m$ yang telah dipelajari sebelumnya. Selanjutnya, akan mempelajari keberadaan akar - akar primitif untuk bilangan – bilangan bulat, khususnya bilangan perkongruenan polinomial. Misalnya $f(x)$ suatu polynomial dengan koefisien bulat. Suatu bilangan bulat $c$ adalah suatu akar dari $f(x)$ dari modulo $m$, jika $f(c) \equiv 0\ (mod\ m)$. Selanjutnya, dapat ditunjukkan bahwa setiap bilangan bulat yang kongruen modulo $m$ dengan $c$ juga merupakan akar dari $f(x)$

**Contoh 9.7**

(1) Perkongruenan $f(x) = x^2 + x + 1 \equiv 0\ (mod\ 7)$, mempunyai dua solusi yang tidak kongruen modulo 7, yaitu $x \equiv 2\ (mod\ 7)$ dan $x \equiv 4\ (mod\ 7)$

(2) Perkongruenan $g(x) = x^2 + 2\ \equiv 0\ (mod\ 2)$ tidak memiliki solusi modulo 2.

(3) Sesuai dengan teorema Fermat, jika $p$ suatu bilangan prima, maka $h(x) = x^{p-1} - 1 \equiv 0\ (mod\ p)$, mempunyai $p - 1$ solusi yang tidak kongruen modulo $p$, yaitu: $1, 2, 3, \ldots\ , p - 1\ (mod\ p)$

**Teorema 9.6** (Teorema Lagrange)

Jika $p$ suatu bilangan prima dan $f$ adalah suatu polynomial berderajat $n$, maka perkongruenan $f(x) \equiv 0\ (mod\ p)$ mempunyai sebanyak – banyaknya $n$ solusi.

**Pembuktian:**

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ dengan $a_n \not\equiv 0\ (mod\ p)$

Teorema akan dibuktikan dengan induksi matematika pada n, yaitu derajat dari $f(x)$

Untuk $n = 1$, maka

$$f(x) = a_1 x + a_0 \equiv 0\ (mod\ p)$$

$$f(x) = a_1 x \equiv -a_0 (mod\ p)$$

Karena $(a_1, p) = 1$ maka perkongruenan liniear ini mempunyai tepat satu solusi. Jadi teorema benar untuk n = 1*.

Selanjutnya, diasumsikan bahwa teorema benar untuk $n = k - 1$ yaitu, polynomial $f$ berderajat $(k - 1)$ solusi. Akan ditunjukkan bahwa untuk polynomial $f$ berderajat $k$, $f(x) \equiv 0\ (mod\ p)$ mempunyai sebanyak – banyaknya $k$ solusi. Untuk itu, cukup menunjukkan bahwa $f(x) \equiv 0\ (mod\ p)$ tidak mempunyai solusi atau mempunyai satu solusi. Jika $f(x) \equiv 0\ (mod\ p)$ tidak mempunyai solusi, maka teorema tersebut terbukti.

Selanjutnya, jika $f(x) \equiv 0\ (mod\ p)$ mempunyai sekurang – kurang satu solusi, misalnya $a$, maka $f(a) \equiv 0\ (mod\ p)$ dan $a$ adalah suatu residu terkecil modulo $p$.

Jika $f(x)$ dibagi dengan $(x - a)$, maka diperoleh:

$$f(x) = (x - a)\, q(x) + r$$

Suku banyak $q(x)$ berderajat $k - 1$ dengan koefisien bulat dan $r$ suatu bilangan bulat pula. Substitusi $x = a$, pada $f(x) \equiv 0\ (mod\ p)$ dan pada $f(x) = (x - a)\, q(x) + r$ diperoleh:

$$0 \equiv f(a) = (a - a)\, q(a) + r\ (mod\ p)$$

$$r \equiv 0\ (mod\ p)$$

Sehingga $$f(x) = (x - a)\, q(x) (mod\ p)$$

Misalkan $b$ adalah penyelesaian lain dengan $b \not\equiv a\ (mod\ p)$ dari $f(x) \equiv 0\ (mod\ p)$, maka

$$0 \equiv f(b) = (b - a)\, q(b)\ (mod\ p)$$

Karena $p$ prima dan $(b - a) \not\equiv 0\ (mod\ p)$, maka $q(b) \equiv 0 (mod\ p)$. Hal ini dapat dikatakan bahwa suatu solusi dari $f(x) \equiv 0\ (mod\ p)$ yang berbeda dengan $a$ merupakan penyelesaian dari $q(x) \equiv 0\ (mod\ p)$, polynomial $q(x)$ mempunyai sebanyak – banyaknya $(k - 1)$ sehingga $f(x) \equiv 0\ (mod\ p)$ tidak mempunyai lebih dari $k$ solusi.

Perlu digaris bawahi teorema 9.6 hanya benar, apabila modulonya suatu bilangan prima. Sebab, jika modulonya tidak prima, maka teorema tersebut tidak benar.

Misalnya $x^2 + x \equiv 0\ (mod\ 6)$ mempunyai solusi 4 yaitu: 0, 2, 3 dan 5. Meskipun ruas kiri dari perkongruenan tersebut suatu polinom berderajat dua.

**Teorema 9.7**

Jika $p$ suatu bilangan prima dan $d \mid p - 1$, maka perkongruenan $x^d - 1 \equiv 0\ (mod\ p)$ mempunyai tepat $d$ solusi

**Pembuktian:**

Menurut teorema Fermat, jika $p$ prima dari $(a, p) = 1$, maka $a^{p-1} \equiv 1\ (mod\ p)$. Ini berarti perkongruenan $x^{p-1} - 1 \equiv 0\ (mod\ p)$ mempunyai tepat $(p - 1)$ solusi, yaitu:

$$1, 2, 3, \dots, p - 1$$

Misalkan bahwa $d|(p - 1)$, maka:

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + 1)$$

$$x^{p-1} - 1 = (x^d - 1)\, f(x)$$

Menurut teorema 9.6, $f(x) \equiv 0\ (mod\ p)$ mempunyai sebanyak – banyaknya $(p - 1 - d)$ solusi. Misalkan $x = a$ suatu solusi dari $x^{p-1} - 1 \equiv 0\ (mod\ p)$ yang bukan solusi $f(x) \equiv 0\ (mod\ p)$, maka $a$ suatu solusi dari $x^d - 1 \equiv 0\ (mod\ p)$. Sebab

$$0 \equiv a^{p-1} - 1 \equiv (a^d - 1)\, f(a)\ (mod\ p)$$

Karena $p$ prima dan $p \nmid f(a)$, maka $p|\ (a^d - 1)$. Jadi $a^d - 1 \equiv 0\ (mod\ p)$ mempunyai sekurang – kurangnya $p - 1 - (p - 1 - d) = d$ solusi *

Sekarang perhatikan bilangan prima 13 dan $\phi(13) = 12$. Dibentuk $\psi(d) =$ banyaknya bilangan bulat positif $k$ yang kurang dari 13 dan berorder $d$ dengan $d|12$.

Untuk modulo 13 ini,

1 berorder 1;

3 dan 9 masing – masing berorder 3;

4 dan 10 masing – masing berorder 6;

5 dan 8 masing – masing berorder 4;

2, 6, 7 dan 11 masing – masing berorder 12, dan

12 beroder 2.

Sehingga

$$\sum_{d|12} \psi(d) = \psi(1) + \psi(2) + \psi(3) + \psi(4) + \psi(6) + \psi(12)$$

$$\sum_{d|12} \psi(d) = 1 + 1 + 2 + 2 + 2 + 4$$

$$\sum_{d|12} \psi(d) = 12$$

Perhatikan juga bahwa

$\psi(1) = 1 = \phi(1)$ $\psi(4) = 2 = \phi(4)$

$\psi(2) = 1 = \phi(2)$ $\psi(6) = 2 = \phi(6)$

$\psi(3) = 2 = \phi(3)$ $\psi(12) = 4 = \phi(12)$

Contoh ini memberikan ilustrasi untuk teorema berikut ini.

**Teorema 9.8**

Jika $p$ suatu bilangan prima dan $d \mid (p-1)$, maka ada tepat $\phi(d)$ bilangan bulat positif kurang dari $p$ yang berorder $d$ modulo $p$

**Pembuktian:**

Dibentuk fungsi $\psi(d)$, yaitu banyaknya bilangan bulat positif kurang dari $p$ yang berorder $d$ modulo $p$. Karena setiap bilangan bulat positif kurang dari $p$ selalu beroder $d$ dengan $d| p-1$, maka

$$\sum_{d|p-1} \psi(d) = p - 1$$

Padahal telah mengetahui bahwa $\sum_{d|p-1} \phi\,(d) = p - 1$, maka harus menunjukkan bahwa $\psi(d) = \phi\,(d)$

Ambil sembarang $d$, yaitu pembagi dari $p-1$ sedemikian hingga $\psi(d) > 0$, maka ada suatu bilangan bulat positif $a$ yang berorder $d$, sehingga barisan:

$$a, a^2, a^3, \dots, a^d$$

Tidak memiliki dua suku yang kongruen modulo $p$ dan masing – masing memenuhi perkongruen

$$x^d \equiv 1 \ (mod\ p),$$

Sebab $(a^k)^d \equiv (a^d)^k \equiv 1 \ (mod\ p),$ dengan $1 \leq k \leq d$

Menurut teorema 9.6, perkongruenan tersebut tepat $d$ solusi. Selanjutnya, suatu bilangan bulat positif yang berorder $d$ modulo $p$ mesti kongruen modulo $p$ dengan satu bilangan $a, a^2, a^3, \dots, a^d$. Dan hanya sebanyak $\phi\ (d)$ dari perpangkatan $a$ tersebut yang berorder $d$, yaitu $a^k$ dengan $(k, d) = 1$. Jadi banyaknya bilangan bulat positif yang kurang dari $p$ dan berorder $d$ modulo $p$ adalah $\phi\ (d)$. Sehingga $\psi(d) = \phi\ (d)$

Apabila pada teorema 8.7, $d = p - 1$, maka diperoleh akibat dari teorema itu sebagai berikut:

**Akibat 9.5**

Setiap bilangan prima $p$ mempunyai sebanyak $\phi(p-1)$ akar primitif.

**Contoh 9.8**

Tentukan akar – akar primitif dari 31 dan tentukan pula bilangan – bilangan bulat positif yang kurang dari 31 yang berorder 6 modulo 31.

**Penyelesaian:**

Banyaknya akar primitif dari 31 $\phi\big(\phi(31)\big) = \phi(30) = 8$.

Karena $2^5 \equiv 1 \ (mod\ 31)$, maka 2 bukan akar primitif dari 31. Mari mencoba memangkatkan 3 dengan eksponen bulat positif yang tidak lebih dari 15, karena order dari 3 mesti membagi $\phi(31) = 30$, maka perhitungannya dilakukan sebagai berikut.

$3^{15} \equiv (27)^5 \equiv (-4)^5 \equiv (-64)(16) \equiv -2\ (16) \equiv -1 \not\equiv 1 \ (mod\ 31)$

Karena $3^{15} \not\equiv 1 \ (mod\ 31)$ dan $3^k \not\equiv 1 \ (mod\ 31)$ untuk $1 \leq k \leq 15$, maka order dari 3 mesti lebih dari 15. Dan karena order 3 mesti membagi $\phi(31) = 30$, maka dapat ditarik kesimpulan bahwa order 3 (mod 31) adalah 30. Jadi 3 adalah suatu akar primitif dari 31. Akar – akar primitif dari 31 yang lain adalah $3^k$ dengan $(k, 30) = 1$, yaitu:

$$3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23} \text{ dan } 3^{29}$$

Yang berturut – turut kongruen mod 31 dengan

$$17, 13, 24, 22, 12, 11 \text{ dan } 21$$

Karena 3 adalah akar primitif 31, maka setiap bilangan bulat positif yang kurang dari 31 dapat dinyatakan dalam bentuk $3^k$ dengan $1 \leq k \leq 30$. Selanjutnya menurut teorema 9.3, maka

order dari $3^k$adalah $\frac{30}{(k,30)}$. Sehingga $3^k$ yang berorder 6, apabila $(k, 30) = 5$, yaitu $k = 5$ atau $k = 25$. Jadi $3^5$ dan $3^{25}$ masing – masing berorder 6 (mod 31).

Dengan perhitungan berikut ini dapat diketahui residu terkecilnya.

$3^5 \equiv (27)(9) \equiv (-4)(9) \equiv -36 \equiv 26\ (mod\ 31)$

$3^{25} \equiv (3^5)^5 \equiv (26)^5 \equiv (-5)^5 \equiv (-125)(25) \equiv (-1)(25) \equiv 6\ (mod\ 31)$

Banyaknya bilangan bulat positif yang kurang dari 31 dan berorder 6 adalah $\phi(6) = 2$, yaitu 6 dan 26.

Akibat 9.5 menyatakan bahwa suatu prima $p$ mempunyai sebanyak $\phi(p-1)$. Akar primitif. Apakah suatu bilangan komposit mempunyai primitif? Akar – akar primitif dari 9 adalah 2 dan 5, tetapi 8 mempunyai akar primitif.

Sekarang perhatikan $2^k$ dengan $k \geq 3$, maka $\phi(2^k) = 2^{k-1}$. Akan ditunjukkan bahwa untuk sembarang bilangan ganjil $a$ dengan $(a, 2^k) = 1$, maka:

$$a^{2^{k-2}} \equiv 1\ (mod\ 2^k) \text{ dengan } 2^{k-2} = \frac{\phi(2^k)}{2} \text{ dan } k \geq 3.$$

**Pembuktian:**

(1) Diberikan bahwa $2^{k-2} = \frac{\phi(2^k)}{2}$ dan $k \geq 3$. Perlu dicatat bahwa $\phi(n)$ adalah fungsi totien Euler yang menghitung jumlah bilangan bulat positif yang relatif prima dengan $n$ yang lebih kecil dari n itu sendiri.

(2) asumsikan bahwa $a$ dan $2^k$saling prima, artinya$(a, 2^k) = 1$.

(3) Karena $a$ dan $2^k$saling prima, maka $a$ juga saling prima dengan 2, karena $2^k$merupakan kelipatan dari 2.

(4) Dengan asumsi tersebut, berdasarkan teorema Euler, bahwa $a^{\phi(2^k)} \equiv \equiv 1\ (mod\ 2^k)$.

(5) Substitusi $\phi(2^k) = 2^{k-1}$. Pada persamaan tersebut, maka di dapatkan

$$a^{(2^{(k-1)})} \equiv 1\ (mod\ 2^k)$$

(6) Karena $2^{(k-2)} = \frac{(\phi(2^k))}{2}$ didapatkan

$$2^{(k-1)} = 2.2^{(k-2)}$$

(7) Dengan mengganti persamaan tersebut pada Langkah (5) dapatkan

$$a^{(2.2^{(k-2)})} \equiv 1\ (mod\ 2^k)$$

(8) Dengan membagi kedua sisi persamaan dengan $a^2$, didapatkan $a^{(2^{(k-2)})} \equiv 1\ (mod\ 2^k)$

(9) Dengan demikian, telah dibuktikan bahwa $a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$ ketika $a$ dan $2^k$ saling prima.

(10) Terakhir, jika $a$ dan $2^k$tidak saling prima, maka bisa menyederhanakan $a^x$ menjadi $\left(\frac{a}{g}\right)^x$, di mana $g = (a, 2^k)$. Kemudian didapatkan $\left(\frac{a}{g}\right)^{(2^{(k-2)})} \equiv 1\ (mod\ 2^k)$. Karena $a$ dan $2^k$ saling prima, maka $\frac{a}{g}$ juga saling prima dengan $2^k$. *

Akan ditunjukan $2^k$ tidak mempunyai akar primitif dengan induksi matematik. Misalnya: Untuk setiap bilangan asli $k \geq 3$. Jika $k = 3$, maka diperoleh kekongruenan $a^2 \equiv 1\ (mod\ 8)$ untuk yang benar $a = 1, 3, 5, dan\ 7$, yaitu:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1\ (mod\ 8)$$

Jadi benar bahwa $2^3$tidak mempunyai akar primitif

**Teorema 9.9**

Untuk $k \geq 3$, bilangan bulat $2^k$ tidak mempunyai akar primitif.

pembuktian:

diasumsikan kekogruenan benar untuk suatu bilangan bulat $k$ yang lebih besar dari 3, yaitu:

$a^{2^{k-2}} \equiv 1\ (mod\ 2^k)$

Kekogruenan ini ekuivalen dengan

$a^{2^{k-2}} = 1 + 2^k\ m$ dengan $m$ suatu bilangan bulat

Jika kedua ruas dikuadratkan, maka diperoleh:

$$a^{2^{k-1}} = 1 + 2^{k+1}\ m + \ 2^{2k}\ \ m^2$$

$$a^{2^{k-1}} = 1 + 2^{k+1}\ (m + \ 2^{k-1}\ \ m^2)$$

$$a^{2^{k-1}} \equiv 1\ (mod\ 2^{k+1})$$

Jadi kekongruenan juga benar untuk $k + 1$, sehingga kekongruenan benar untuk semua bilangan bulat $k \geq 3$ *

**Contoh 9.9**

Karena $\phi(16) = 8$ dan $3^4 \equiv 11^4 \equiv 5^4 \equiv 13^4 \equiv 1\ (mod\ 16)$, $7^2 \equiv 9^2 \equiv 15^2 \equiv 1\ (mod\ 16)$, maka tidak ada bilangan bulat positif yang kurang dari 16 dan yang saling prima dengan 16 yang berorder 8, sehingga 16 tidak mempunyai akar primitif.

**Teorema 9.10**

Jika bilangan – bilangan bulat $m > 2$ dan $n > 2$ dengan $(m, n) = 1$, maka $mn$ tidak mempunyai akar primitif.

Ambil sembarang bilangan bulat positif $a$ dengan $(a, mn) = 1$, maka $(a, m) = 1$ dan $(a, n) = 1$. Misalnya $[\phi(m),\ \phi(n)] = h$ dan $[\phi(m),\ \phi(n)] = d$ karena $\phi(m)$ dan $\phi(n)$ masing – masing bilangan genap

$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}$

Karena $(a, m) = 1$ maka teorema Euler $a^{\phi(m)} \equiv 1\ (mod\ m)$, selanjutnya

$$a^h = a^{\frac{\phi(m)\phi(n)}{d}} = \left(a^{\phi(m)}\right)^{\frac{\phi(n)}{d}} \equiv 1^{\frac{\phi(n)}{d}} \equiv 1\ (mod\ m)$$

Dengan cara yang sama dapat diperoleh bahwa $a^h \equiv 1\ (mod\ n)$ karena $(m, n) = 1,\ a^h \equiv 1\ (mod\ m)$ dan $a^h \equiv 1\ (mod\ n)$, maka $a^h \equiv 1\ (mod\ mn)$

Karena $h \leq \frac{\phi(mn)}{d}$ dan $(a, mn) = 1$, maka order dari $a$ modulo $mn$ tidak lebih dari $\frac{1}{2}\phi(mn)$. Hal ini berarti $mn$ tidak mempunyai akar primitif.

**Contoh 9.10**

(1) Himpunan residu sederhana modulo 15 adalah {1, 2, 4, 7, 8, 11, 13, 14} dan $\phi(15) = 8$. Karena $2^4 \equiv 7^4 \equiv 8^4 \equiv 13^4 \equiv 1\ (mod\ 15)$ dan $4^2 \equiv 11^2 \equiv 14^2 \equiv 1\ (mod\ 15)$, maka 15 tidak mempunyai akar primitif.

(2) Himpunan residu sederhana modulo 20 adalah {1, 3, 7, 9, 11, 13, 17, 19} dan $\phi(20) = 8$. Karena $3^4 \equiv 7^4 \equiv 13^4 \equiv 17^4 \equiv 1\ (mod\ 20)$ dan $9^2 \equiv 11^2 \equiv 19^2 \equiv 1\ (mod\ 20)$, maka 20 tidak mempunyai akar primitif

(3) Himpunan residu sederhana modulo 24 adalah {1, 5, 7, 11, 13, 17, 19, 23} dan $\phi(24) = 8$. Karena $5^2 \equiv 7^2 \equiv 11^2 \equiv 13^2 \equiv 17^2 \equiv 19^2 \equiv 23^2 \equiv 1\ (mod\ 24)$, maka 24 tidak mempunyai akar primitif

Keadaan khusus dari teorema 9.10 tersebut, apabila $m$ dan $n$ merupakan dua bilangan prima ganjil atau $m = 2^r$ dengan $r \geq 2$ dan $n = p^k$ dengan $p$ suatu bilangan prima ganjil. Hal ini dinyatakan sebagai akibar dari teorema berikut.

**Akibat 9.6**

Bilangan – bilangan positif $n$ tidak mempunyai akar primitif, apabila

(i) $n$ tterbagi oleh dua bilangan prima ganjil dan

(ii) $n = 2^r p^k$ dengan $r \geq 2$ dengan $p$ suatu bilangan prima ganjil

Memperhatikan dua teorema terakhir dan akibatnya tersebut, maka penyelidikan akar primitif untuk bilangan – bilangan komposit $2, 4,\ p^k$ dan $2p^k$ dengan $p$ suatu bilangan prima ganjil. Untuk penyelidikan akar – akar primitif dari bilangan – bilangan tersebut, perhatikan lemma – lemma berikut ini.

**Lemma 1:**

Jika $p$ suatu bilangan prima ganjil, maka $p$ mempunyai suatu akar primitif $r$ sedemikian hingga $r^{p-1} \not\equiv 1\ (mod\ p^2)$

Pembuktian:

Bilangan prima ganjil $p$ mesti mempunyai akar primitif . Pilih satu akar primitifnya, misalnya $r$

Andaikan bahwa $r^{p-1} \not\equiv 1 \ (mod \ p^2)$

Jika $r$ diganti $r + p = t$ yang juga merupakan akar primitif dari $p$, maka dengan menggunakan teorema Binomial diperoleh:

$$t^{p-1} \equiv (r + p)^{p-1}$$

$$t^{p-1} \equiv r^{p-1} + (p-1)\, p\ r^{p-2} (mod \ p^2)$$

$$t^{p-1} \equiv 1 - p\, r^{p-2} (mod \ p^2)$$

Jadi $$t^{p-1} \not\equiv 1 \ (mod \ p^2)$$

Karena $r$ suatu akar primitif dari $p$, berarti $(r, p) = 1$, maka $p \nmid r^{p-2}$. Jadi $t^{p-1} \not\equiv 1 \ (mod \ p^2)$. Hal ini bertentangan dengan pengandaian bahwa $t$ adalah akar primitif dari $p$. Pada bukti lemma 1 tersebut. Jika $t^{p-1} \equiv 1 \ (mod \ p^2)$ maka $r^{p-2} \equiv 0 \ (mod \ p^2)$. Hal ini tidak mungkin, karena $p \nmid r$ (ingat bahwa r adalah akar primitif dari $p$).

Jadi $orde_{p^2}\ t = p\ (p-1) = \phi\ (p^2)$, sehingga $t = r + p$ adalah akar primitif dari $p^2$. Hal ini dinyatakan sebagai akibat lemma 1 berikut:

**Akibat 9.7**

Jika $p$ suatu bilangan prima ganjil, maka $p^2$ mempunyai akar primitif. Apabila $r$ suatu akar primitif dari $p$, maka $r + p$ adalah suatu akar primitif dari $p^2$

**Pembuktian:**

Jika $r$ suatu akar primitif dari $p$, maka order dari $r \ (mod \ p^2)$ adalah $p - 1$ atau $p\ (p-1) = \phi(p^2)$. Dengan bukti pada lemma 1 tersebut menunjukkan bahwa jika $r$ berorder $p - 1 \ (mod\ p^2)$ maka $r + p$ adalah suatu akar primitif dari $p^2$

**Lemma 2:**

Misakan $p$ suatu bilangan prima ganjil dan $r$ suatu akar primitif dari $p$ sedemikian hingga $r^{p-1} \not\equiv 1 \ (mod \ p^2)$, maka untuk setiap bilangan bulat $k \leq 2$, berlaku:

$$r^{p^{k-2}(p-1)} \not\equiv 1 \ (mod \ p^k)$$

**Pembuktian:**

Akan dibuktikan dengan induksi matematik pada bilangan bulat $k \geq 2$. Dari ketentuan menunjukkan bahwa kekongruenan tersebut benar untuk k = 2.

Selanjutnya harus ditunjukkan bahwa kekongruenan benar untuk suatu bilangan bulat $k$ yang lebih besar dari 2 dan harus ditunjukkan benar untuk $k + 1$

$(r, p^{k-1}) = (r, p^k) = 1,$ maka menurut teorema Euler bahwa

$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \ (mod \ p^{k-1})$

$r^{p^{k-2}(p-1)} = 1 + mp^{k-1}$ untuk suatu bilangan bulat $m$

Sesuai dengan asumsi bahwa $p \nmid m$. Jika kedua ruas dipangkatkan $p$, maka diperoleh:

$$r^{p^{k-1}(p-1)} = (1 + mp^{k-1})^p$$

$$r^{p^{k-1}(p-1)} \equiv 1 + mp^k (mod \ p^{k+1})$$

Karena $p \nmid m$, maka:

$$r^{p^{k-1}(p-1)} \not\equiv 1 + (mod \ p^{k+1})$$

Jadi kekongruenan benar untuk $k + 1$, sehingga kekongruenan tersebut benar untuk setiap bilangan bulat positif $k \geq 2$

Selanjutnya berdasarkan dua lemma tersebut dapat ditunjukkan bahwa perpangkatan bulat positif dari suatu bilangan prima ganjil mempunyai akar primitif dari suatu bilangan prima ganjil mempunyai akar primitif seperti dinyaatakan dalam teorema berikut:

**Teorema 9.11**

Jika $p$ suatu bilangan prima ganjil dan bilangan bulat $k \geq 1$ maka $p^k$ mempunyai akar primitif.

**Pembuktian:**

Berdasarkan lemma di atas, sehingga dapat memilih suatu akar primitif $r$ dari $p$ dan misalkan order $r \ (mod \ p^k)$ adalah $n$.

Sesuai dengan teorema 9.10, maka $n$ mesti membagi $\phi(p^k) = p^{k-1} \ (p - 1)$. Karena $r^n \equiv 1 \ (mod \ p^k)$, maka $r^n \equiv 1 \ (mod \ p)$, sehingga $p - 1 | \ n$. Sebagai konsekuensinya maka $n = p^m \ (p - 1)$ dengan $0 \leq m \leq k - 1$. Apabila $n \neq p^m \ (p - 1)$, maka $p^{k-2} \ (p - 1)$ dapat dibagi oleh $n$ berarti

$$r^{p^{k-2}(p-1)} \equiv 1 \ (mod \ p^k)$$

Hal ini kontradiksi dengan lemma 2.

Jadi $n = p^m \ (p - 1)$ dan $r$ adalah akar primitif dari $p^k$

**Teorema 9.12**

Jika $p$ suatu bilangan prima ganjil dan suatu bilangan bulat $k \geq 1$, maka $2p^k$ mempunyai akar primitif

**Pembuktian**:

Menurut teorema 9.11, $p^k$ mempunyai akar primitif, misalnya $r$. Jika mengasumsikan bahwa $r$ suatu bilangan ganjil, sebab jika $r$ genap, maka $r + p^k$ adalah suatu bilangan ganjil yang merupakan akar primitif dari $p^k$ pula. Maka $(r, 2p^k) = 1$

Misalkan order dari $r \ (mod \ 2p^k)$ adalah $n$, maka $n$ mesti membagi $\phi(2p^k)$.

$$\phi(2p^k) = \phi(2)\,\phi(p^k) = \phi(p^k)$$

Dan karena $r^n \equiv (mod\ 2p^k)$, maka $r^n \equiv 1\ (mod\ p^k)$, sehingga $\phi(p^k)|n$. Karena order dari $r\ (mod\ 2p^k)$ adalah $n$, maka $n|\phi(2p^k)$

Jadi $n = \phi(2p^k)$, yang berarti $r$ adalah akar primitif dari $2p^k$

**Contoh 9.11**

Bilangan prima 5 mempunyai $\phi\big(\phi(5)\big) = 2$ akar primitif, yaitu 2 dan 3.

Karena

$2^{5-1} \equiv 16 \not\equiv 1\ (mod\ 25)$ dan $3^{5-1} \equiv 81 \equiv 6 \not\equiv 1\ (mod\ 25)$

Maka 2 dan 3 merupakan akar – akar primitif dari $5^2$

Menurut teorema 9.11, 2 dan 3 juga merupakan akar – akar primitif $5^k$ dengan $k \geq 1$, sedangkan menurut teorema 9.12, 3 merupakan suatu akar primitif dari semua bilangan berbentuk $2.5^k$ dengan $k \geq 1$.

Dari teorema – teorema yang telah dipelajari pada bagian ini, maka dapat disimpulkan bahwa bilangan asli yang lebih besar dari 1 mempunyai akar primitif jika dan hanya jika bilangan asli itu adalah 2, 4, $p^t$ dan $2p^t$, dengan $p$ suatu bilangan prima ganjil dan $t$ suatu bilangan asli.

**Tabel 9.3**

**Daftar Akar Primitif Terkecil Dari Bilangan Prima Yang Kurang Dari 102**

| Prima | Akar Primitif Terkecil | Prima | Akar Primitif Terkecil |
|---|---|---|---|
| 2 | 1 | 43 | 3 |
| 3 | 2 | 47 | 5 |
| 5 | 2 | 53 | 2 |
| 7 | 3 | 59 | 2 |
| 11 | 2 | 61 | 2 |
| 13 | 2 | 67 | 2 |
| 17 | 3 | 71 | 7 |
| 19 | 2 | 73 | 5 |
| 23 | 5 | 79 | 3 |
| 29 | 2 | 83 | 2 |
| 31 | 3 | 89 | 3 |
| 37 | 2 | 97 | 5 |
| 41 | 6 | 101 | 2 |

## C. Aritmetik Indeks

Suatu konsep yang mirip dengan konsep logaritma diberikan contoh konsep indeks dalam Teori Bilangan. Perhatikan contoh berikut ini.

Salah satu akar primitif dari 11 adalah 2, maka setiap bilangan asli kurang dari 11 dan saling prima dengan 11, dapat dinyatakan sebagai perpangkatan bulat positif dari 2 yaitu:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Berturut – turut dapat dinyatakan sebagai

$2^{10}, 2^{1}, 2^{8}, 2^{2}, 2^{4}, 2^{9}, 2^{7}, 2^{3}, 2^{6}$, dan $2^{5}(mod\ 11)$, Selanjutnya 4 disebut indeks dari 5 untuk basis 2 modulo 11 dan pada $9 \equiv 2^{6}\ (mod\ 11)$, 6 disebut indeks dari 9 untuk basis 2 modulo 11.

Secara formal konsep indeks didefinisikan sebagai berikut:

**Definisi 9.3:**

Misalkan $r$ suatu akar primitif dari $m$. Jika $(a, m) = 1$, maka bilangan bulat positif terkecil $k$ sedemikian hingga $a \equiv r^{k}\ (mod\ m)$ disebut indeks dari $a$ untuk basis $r$ modulo $m$. Indeks dari $a$ pada basis $r$ modulo $m$ ditulis "$ind_r\ a\ (mod\ m)$"

Dari definisi tersebut dapat diketahui bahwa $1 \leq ind_r\ a \leq \phi(m)$ dan $r^{ind_r a} \equiv a\ (mod\ m)$. Notasi $ind_r a$ tidak berarti, apabila tidak dipenuhi $(a, m) = 1$. Pada contoh di atas, yaitu 2 adalah suatu akar primitif dari 11, maka

$ind_2\ 1 = 10$ $ind_2\ 2 = 1$ $ind_2\ 3 = 8$ $ind_2\ 4 = 2$

$ind_2\ 5 = 4$ $ind_2\ 6 = 9$ $ind_2\ 7 = 7$ $ind_2\ 8 = 3$

$ind_2\ 9 = 6$ $ind_2\ 10 = 5$

Dengar akar primitif lain dari 11, misalnya 7, maka diperoleh daftar dari nilai indeks yang berbeda, yaitu:

$ind_7\ 1 = 10$ $ind_7\ 2 = 3$ $ind_7\ 3 = 4$ $ind_7\ 4 = 6$

$ind_7\ 5 = 2$ $ind_7\ 6 = 7$ $ind_7\ 7 = 1$ $ind_7\ 8 = 9$

$ind_7\ 9 = 8$ $ind_7\ 10 = 5$

Misalkan $r$ suatu akar primitif dari $m$ dan $a \equiv b\ (mod\ m)$ dengan $(a, m) = (b, m) = 1$, maka

$$r^{ind_r a} \equiv a\ (mod\ m) \text{ dan } r^{ind_r b} \equiv b\ (mod\ m)$$

Sehingga

$$r^{ind_r a} \equiv r^{ind_r b} (mod\ m)$$

Jadi kongruenan dapat disimpulkan bahwa

$$ind_r\ a \equiv ind_r\ b\ (mod\ (\phi(m))$$

Dengan memperhatikan definisi 9.3 maka $ind_r\, a = ind_r\, b$. Karena konsep indeks mempunyai kemiripan konsep logaritma, maka teoremanya pun juga ada kemiripan.

**Teorema 9.13**

Jika $r$ suatu akar primitif dari $m$ dan $ind_r\, a$ mempunyai indeks dari $a\ (mod\ m)$ untuk basis $r$ maka:

(i) $ind_r\, ab \equiv ind_r\, a + ind_r\, b\ (mod\ (\phi(m))$

(ii) $ind_r\, a^k \equiv k\ ind_r\ (mod\ (\phi(m))$ untuk bilangan bulat positif $k$

(iii) $ind_r\, 1 \equiv 0(mod\ (\phi(m))$ dan $ind_r\, r \equiv 1(mod\ (\phi(m))$

**Pembuktian:**

(i) Menurut definisi 9.3, $r^{ind_r a} \equiv a\ (mod\ m)$ dan $r^{ind_r b} \equiv b\ (mod\ m)$. Apabila ruas – ruas kedua kekongruenan tersebut dikalikan, maka diperoleh $r^{\,ind_r\, a + ind_r\, b} \equiv ab(mod\ m)$ maka $r^{\,ind_r\, a + ind_r\, b} \equiv b\ (mod\ m)$. Selanjutnya dapat disimpulkan bahwa:

$$ind_r\, a + \ ind_r\, b \equiv ind_r\ (ab)\ (\phi(m))$$

(ii) Mengingat definisi 9.3, $r^{ind_r\, a^k} \equiv a^k\ (mod\ m)$, sehingga

$$r^{ind_r\, a^k} \equiv r^{k\ ind_r\, a}\ (mod\ m)$$

Jadi $ind_r\, a^k \equiv k\ ind_r\, a\ (mod(\phi(m))$

(iii) Mengingat bahwa $ind_r\, a^k \equiv k\ ind_r\, a\ (mod(\phi(m))$ maka

$ind_r\, 1 = ind_r\, a^0 \equiv 0\ ind_r\, a\ \equiv 0\ (mod(\phi(m))$

Karena $r^{ind\, r} \equiv r\ (mod\ m)$, maka $ind\, r \equiv 1\ (mod(\phi(m))$

**Contoh 9.12**

Perhatikan bilangan bulat modulo 7. Salah satu akar primirif dari 7 adalah 5 dan $\phi(7) = 6$. Karena

$ind_5 2 = 4$ dan $ind_5 3 = 5$, maka sesuai dengan teorema 9.13 bagian (ii) memperoleh bahwa:

$$ind_5\, 6 = \ ind_5\ (2.3) = \ ind_5 2 + \ ind_5 3 = 4 + 5 \equiv 3\ (mod\ 6)$$

Hal ini sesuai karena $5^3 \equiv 6\ (mod\ 7)$ yang berarti $ind_5\, 6 = 3$. Dari teorema 9.13 bagian (ii) memberikan $ind_5\, 3^4 \equiv 4\ ind_5\, 3 \equiv 4.5 \equiv 2\ (mod\ 6)$. Apabila dihitung secara langsung diperoleh

$ind_5\, 3^4 \equiv ind_5\, 81 \equiv ind_5\, 4 = 2$ (ingat bahwa $81 \equiv 4\ (mod\ 7)$ dan $5^2 \equiv 4\ (mod\ 7)$

Teori indeks dapat digunakan untuk menyelesaikan beberapa tipe dari perkongruenan. Perhatikan perkongruenan $x^k \equiv a\ (mod\ m)$, dengan $m$ suatu bilangan bulat positif yang mempunyai akar primitif $r$ dan $(a, m) = 1$. Maka dengan teorema 9.13 (i) dan (ii), perkongruenan tersebut dirubah menjadi perkongruenan linier

$$ind_r\, x^k \equiv\ ind_r\, a\ (mod\ (\phi(m))$$
$$k\ ind_r\, x \equiv\ ind_r\, a\ (mod\ (\phi(m))$$

Jika $\big(r, \phi(m)\big) = d$ dengan $d|\ ind_r\, a,$ maka perkongruenan ini mempunyai $d$ solusi untuk $ind_r\, x$ sehingga perkongruenan semula mempunyai $d$ solusi pula. Dan apabila $d \nmid\ ind_r\, a,$ maka perkongruenan linier tidak mempunyai solusi.

Khusus untuk $k = 2$ dan $m$ suatu bilangan prima ganjil. Karena $(2, m-1) = 2,$ maka perkongruenan $x^2 \equiv a\ (mod\ m)$ mempunyai solusi jika dan hanya jika $2 \mid ind\ a$. Apabila syarat ini dipenuhi, maka perkongruenan kuadrat tersebut mempunyai tepat dua solusi. Jika $r$ suatu akar primitif dari $m$, maka $r^k$ untuk $k = 1, 2, 3, \dots,\ m-1$, adalah suatu permutasi dari $k = 1, 2, 3, \dots,\ m-1$. Sehingga $x^2 \equiv a\ (mod\ m)$ dapat diselesaikan (mempunyai solusi) apabila $a$ sama dengan perpangkatan genap dari $r$, jadi ada $\frac{1}{2}(m-1)$ pilihan untuk $a$

**Contoh 9.13**

Selesaikan $4x^9 \equiv 7\ (mod\ 13)$

Penyelesaian:

Langkah pertama membuat tabel indeks untuk suatu akar primitif dari 13. Dipilih salah satu akar primitif dari 13, yaitu 2. Hitung perpangkatan bulat positif dari 2 (mod 13) sebagai berikut:

$2^1 \equiv 2\ (mod\ 13)$ $\quad 2^2 \equiv 4\ (mod\ 13)$ $\quad 2^3 \equiv 8\ (mod\ 13)$

$2^4 \equiv 3\ (mod\ 13)$ $\quad 2^5 \equiv 6\ (mod\ 13)$ $\quad 2^6 \equiv 12\ (mod\ 13)$

$2^7 \equiv 11\ (mod\ 13)$ $\quad 2^8 \equiv 9\ (mod\ 13)$ $\quad 2^9 \equiv 5\ (mod\ 13)$

$2^{10} \equiv 10\ (mod\ 13)$ $\quad 2^{11} \equiv 7\ (mod\ 13)$ $\quad 2^{12} \equiv 1\ (mod\ 13)$

Dari perpangkatan ini dapat disusun tabel indeks sebagai berikut:

| a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_2\ a$ | 12 | 1 | 4 | 2 | 9 | 5 | 11 | 3 | 8 | 10 | 7 | 6 |

Perkongruenan linier $4x^9 \equiv 7\ (mod\ 13)$ mempunyai solusi jika dan hanya jika

$ind_2\ (4x^9) \equiv ind_2 7\ (mod\ 12)$ $\quad$ ingat $\phi(13) = 12$

$ind_2 4 + 9\ ind_2 x \equiv ind_2 7\ (mod\ 12)$

$2 + 9\ ind_2 x \equiv 11\ (mod\ 12)$

$9\ ind_2 x \equiv 9\ (mod\ 12)$

$ind_2 x \equiv 1\ (mod\ 4)$

Jadi, $ind_2\, x \equiv 1, 5$ atau 9 (mod 13)

Selanjutnya, dengan memperhatikan tabel indeks, juga akan terlihat bahwa perkongruenan $4x^9 \equiv 7\ (mod\ 13)$ mempunyai tiga solusi, yaitu:

$x \equiv 2, 6, dan\ 5\ (mod\ 13)$

Jika memilih akar primitif dari 13 yang lain, maka akan diperoleh tabel indeks yang berbeda pula. 13 mempunyai $\phi(\phi(13)) = 4$, akar primitif yaitu $2, 6, 11, dan\ 7$. Jika memilih akar primitif dari 13 yang lainnya, misalnya 6, maka dengan cara seperti di atas, maka akan diperoleh tabel indeks sebagai berikut:

| a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_6\ a$ | 12 | 5 | 8 | 10 | 9 | 1 | 7 | 3 | 4 | 2 | 11 | 6 |

Perkongruenan tabel ini, maka perkongruenan $4x^9 \equiv 7\ (mod\ 13)$ ekuivalen dengan

$ind_6\ (4x^9) \equiv ind_6 7\ (mod\ 12)$

$ind_6 4 + 9\ ind_6 x \equiv ind_6 7\ (mod\ 12)$

$10 + 9\ ind_6 x \equiv 7\ (mod\ 12)$

$9\ ind_6 x \equiv 9\ (mod\ 12)$

$ind_6 x \equiv 1\ (mod\ 4)$

$ind_6 x = 1, 5$ atau 9

$x \equiv 2, 6, dan\ 5\ (mod\ 13)$

**Contoh 9.14**

Selesaikan perkongruenan

(i) $16x^{12} \equiv 11\ (mod\ 17)$

(ii) $7^x \equiv 6\ (mod\ 17)$

**Penyelesaian:**

Ambil salah satu akar primitif dari 17. Misalnya 3 dan dibuat tabel indeks untuk bilangan – bilangan bulat positif kurang dari 17 untuk basis 3.

| a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_3\ a$ | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |

(i) Ambil indeks pada kekongruenan untuk basis 3 modulo 17, sehingga diperoleh suatu kekongruenan modulo $\phi(17) = 16$

$ind_3\ 6x^{12} \equiv ind_3 11\ (mod\ 16)$

$ind_3\ 6\ +\ ind_3\ x^{12} \equiv 7\ (mod\ 16)$

$15\ +\ 12\ ind_3\ x\ \equiv 7\ (mod\ 16)$

$12\ ind_3\ x\ \equiv 8\ (mod\ 16)$

$3\ ind_3\ x\ \equiv 2\ (mod\ 4)$

$ind_3\ x\ \equiv 2\ (mod\ 4)$

Jadi $ind_3\ x\ \equiv 2, 6, 10, atau\ 14\ (mod\ 16)$

Sehingga $x \equiv 9, 15\ , 8\ dan\ 2\ (mod\ 17)$

(ii) Ambil indeks pada kekongruenan untuk basis 3 modulo 17, sehingga diperoleh suatu kekongruenan modulo $\phi(17) = 16$

$ind_3\ 7^x \equiv ind_3 6\ (mod\ 16)$

$x\ ind_3\ 7\ \equiv 15\ (mod\ 16)$

$11x\ \equiv 15\ (mod\ 16)$

$x\ \equiv 13\ (mod\ 16)$

dari contoh penyelesaian dapat dirumuskan sebagai kriteria penyelesaian suatu perkongruenan yang dinyatakan sebagai teorema berikut ini.

**Teorema 9.14**

Misalkan $m$ suatu bilangan bulat positif yang mempunyai akar primitif dan misalkan $(a, m) = 1$, maka perkongruenan $x^k \equiv a\ (mod\ m)$ mempunyai solusi jika dan hanya jika

$a^{\frac{\phi(m)}{d}} \equiv a\ (mod\ m)$ dengan $d = (k, \phi(m))$

Jika perkongruenan $x^k \equiv a\ (mod\ m)$ mempunyai solusi, maka terdapat $d$ solusi modulo $m$.

**Pembuktian:**

Misalkan $r$ adalah suatu akar primitif dari $m$, maka dari perkongruenan

$$x^k \equiv a\ (mod\ m)$$

Diperoleh

$$k\ ind_r\ x \equiv ind_r\ a\ \left(mod\ \phi(m)\right) \ldots \text{ (i)}$$

Karena $d = (k, \phi(m))$ dan jika $d \nmid ind_r\ a$, maka perkongruenan (i) mempunyai $d$ solusi modulo $\phi(m)$. Jika $d | ind_r\ a$ jika dan hanya jika $\frac{\phi(m)}{d} ind_r\ a \equiv 0\ \left(mod\ \phi(m)\right)$. Kekongruenan terakhir ini benar jika dan hanya jika

$$a^{\frac{\phi(m)}{d}} \equiv a\ (mod\ m)$$

**Akibat 9.8 (Euler)**

Misalkan $p$ suatu bilangan prima, dan $(a, p) = 1$, maka perkongruenan $x^k \equiv a\ (mod\ p)$ mempunyai solusi jika dan hanya jika $a^{\frac{p-1}{d}} \equiv 1 (mod\ p)\ dengan\ d = (k, p-1)$

**Contoh 9.15**

Selesaikan perkongruenan

(i) $x^3 \equiv 4\ (mod\ 13)$

(ii) $x^3 \equiv 5\ (mod\ 13)$

Penyelesaian:

(i) $x^3 \equiv 4\ (mod\ 13)$, terlihat $d = (3,\ \phi(13)) = (3, 12)$ dan $\frac{\phi(13)}{d} = \frac{12}{3} = 4$, karena $4^4 \equiv 9 \not\equiv 1\ (mod\ 13)$, maka menurut teorema 9.14. Perkongruenan $x^3 \equiv 4\ (mod\ 13)$ tidak mempunyai solusi

(ii) karena $5^4 \equiv 1\ (mod\ 13)$, maka Perkongruenan $x^3 \equiv 5\ (mod\ 13)$ tidak mempunyai solusi

dan diselesaikan sebagai berikut:

$$x^3 \equiv 5\ (mod\ 13)$$

$$ind_2\ x^3 \equiv ind_2\ 5\ (mod\ 12)$$

$$3\ ind_2\ x \equiv 9\ (mod\ 12)$$

$$ind_2\ x \equiv 3\ (mod\ 4)$$

$$ind_2\ x = 3{,}7\ atau\ 11$$

$$x \equiv 8, 11\ atau\ 7\ (mod\ 13)$$

# BAB X

## KONGRUENSI KUADRATIS

Perhatikan bentuk umum kogruensi kuadratis berikut ini.

$$ax^2 + bx + c \equiv 0 \ (mod\ p)\ .$$

Dengan $a = 0$, $p$ adalah suatu bilangan prima ganjil, dan $(a,p) = 1,$ keadaan $(a,p) = 1$ mengakibatkan adanya suatu kongruensi linier:

$$ak \equiv 1 \ (mod\ p)$$

Mempunyai satu penyelesaian sebab $(a,p) = 1|1$. Dengan demikian $a$ mempunyai invers perkalian (multiplikatif) $a^{-1} \equiv k \ (mod\ p)$ sehingga $ak \equiv 1 \ (mod\ p)$, sehingga kongruensi kuadratis dapat disederhanakan menjadi:

$$ax^2 + bx + c \equiv 0 \ (mod\ p)$$
$$akx^2 + bkx + ck \equiv 0 \ (mod\ p)$$
$$1.x^2 + bkx + ck \equiv 0 \ (mod\ p)$$
$$x^2 + bkx + ck \equiv 0 \ (mod\ p)$$

Dengan memilih $q = bk$ dan $r = ck$, maka $x^2 + bkx + ck \equiv 0 \ (mod\ p)$ maka dapat dinyatakan dengan;

$$x^2 + qx + r \ \equiv 0 \ (mod\ p)\ *$$

**Contoh 10.1**

Kongruensi kuadratis $4x^2 - 9x + 5 \equiv 0 \ (mod\ 17)$ menunjukkan bahwa $a = 4 \neq 0$, $p = 17$ dan $(a,p) = 1$, serta inversi perkalian 4 adalah $k = 13$. Sebab $4.13 = 52 \equiv 1 \ (mod\ 17)$, sehingga : $4.13 \equiv 1 \ (mod\ 17)$.

Dengan demikian koefisien $a = 4$ dapat direduksi menjadi 1 setelah dikalikan dengan k = 13.

$$4x^2 - 9x + 5 \equiv 0 \ (mod\ 17)$$
$$4.13x^2 - 9.13\ x + 5.13 \equiv 0 \ (mod\ 17)$$
$$52x^2 - 117\ x + 65 \equiv 0 \ (mod\ 17)$$
$$x^2 + 2x + 14 \equiv 0 \ (mod\ 17)$$

**Contoh 10.2**

Kongruensi kuadratis $5x^2 + 4x + 17 \equiv 0 \ (mod\ 13)$ menunjukkan bahwa $a = 5 \neq 0, p = 13$ dan $(a,p) = 1$, serta inversi perkalian 5 adalah $k = 8$. Sebab $5.8 = 40 \equiv 1 \ (mod\ 13)$, sehingga : $5.8 \equiv 1 \ (mod\ 13)$.

Dengan demikian koefisien $a = 5$ dapat direduksi menjadi 1 setelah dikalikan dengan k = 8.

$$5x^2 + 4x + 17 \equiv 0 \ (mod\ 13)$$

$$5.8x^2 + 4.8\,x + 17.8 \equiv 0 \ (mod\ 13)$$

$$40x^2 + 32\,x + 136 \equiv 0 \ (mod\ 13)$$

$$x^2 + 6x + 6 \equiv 0 \ (mod\ 13)$$

Kongruensi Dalam Bentuk Kuadrat Sempurna

$$x^2 + qx + r \ \equiv 0 \ (mod\ p)$$

Dengan keadaan p adalah suatu bilangan prima ganjil, dan 2 adalah bilangan prima genap, maka dapat ditentukan bahwa $(2, p) = 1|1$ , sehingga ada suatu bilangan bulat $m$ yang memenuhi:

$$2m \equiv 1 \ (mod\ p)$$

Ini berarti bahwa bilangan bulat $m$ merupakan invers perkalian 2 modulo $m$, dan adanya $m$ dapat digunakan untuk menentukan penyelesaian:

$$x^2 + qx + r \ \equiv 0 \ (mod\ p)$$

dengan jalan mengusahakan menjadi bentuk kuadrat sempuma:

$$x^2 + qx + r \ \equiv 0 \ (mod\ p)$$

$$x^2 + q.1x + r \ \equiv 0 \ (mod\ p)$$

$$x^2 + q.2mx + r \ \equiv 0 \ (mod\ p)$$

$$x^2 + q.2mx + [(qm)^2 - (qm)^2] + r \ \equiv 0 \ (mod\ p)$$

$$[x^2 + q.2mx + (qm)^2] - (qm)^2 + r \ \equiv 0 \ (mod\ p)$$

$$[x + (qm)]^2 \equiv [(qm)^2 - r] \ (mod\ p)$$

Misalkan $y = x + qm$ dan $k = (qm)^2 - r$, maka hasil terakhir dapat dinyatakan sebagai:

$$y^2 \equiv k \ (mod\ p)$$

Dengan demikian kongruensi semula dapat diubah menjadi kongruensi dalam bentuk kuadrat sempurna, dan selesaian kongruensi kuadratis ditentukan oleh keadaan $k$ dan $p$.

**Contoh 10.3**

Selesaikan kongruensi $4x^2 - 9x + 5 \equiv 0 \ (mod\ 17)$ dapat diperoleh dengan cara mengubah kongruensi semula sehingga diperoleh kongruensi dalam bentuk kuadrat kuadrat sempuma.

$$4x^2 - 9x + 5 \equiv 0 \ (mod\ 17)$$

$$4.13x^2 - 9.13\,x + 5.13 \equiv 0 \ (mod\ 17),\ 13 \text{ adalah invers 4 modulo } 17$$

$$52x^2 - 117\,x + 65 \equiv 0 \ (mod\ 17)$$

$$x^2 + 2x + 14 \equiv 0 \ (mod\ 17)$$

$$x^2 + 2.1x + 14 \equiv 0 \ (mod\ 17)$$

$$x^2 + 2.(2.9)x + (2.9)^2 - (2.9)^2 + 14 \equiv 0 \ (mod\ 17)$$

$$x^2 + 2.18x + (18)^2 - (18)^2 + 14 \equiv 0\ (mod\ 17)$$

Karena $x^2 + 2.18x + (18)^2 = \ (x + 18)^2$ maka

$$(x + 18)^2 \equiv (18)^2 - 14\ (mod\ 17) \equiv 1^2 - 14\ (mod\ 17)) \equiv -13\ (mod\ 17))$$
$$\equiv 4\ (mod\ 17)$$

Karena $18 \equiv 1\ (mod\ 17)$ maka

$(x + 1)^2 \equiv 4\ (mod\ 17)$ maka $(x + 1) \equiv 2\ (mod\ 17)$ atau $(x + 1) \equiv -2\ (mod\ 17)$

Jadi $x \equiv 1\ (mod\ 17)$ atau $x \equiv -3\ (mod\ 17) = 14\ (mod\ 17)$

**Contoh 10.4**

Selesaikan kongruensi $3x^2 + 5x - 4 \equiv 0\ (mod\ 7)$ dapat diperoleh dengan cara mengubah kongruensi semula sehingga diperoleh kongruensi dalam bentuk kuadrat kuadrat sempuma.

$$3x^2 + 5x - 4 \equiv 0\ (mod\ 7)$$

$$3.5x^2 + 5.5\ x - 4.5 \equiv 0\ (mod\ 17),\ 5 \text{ adalah invers 3 modulo 7}$$

$$15x^2 + 25\ x - 20 \equiv 0\ (mod\ 7)$$

$$x^2 + 4x + 1 \equiv 0\ (mod\ 7)$$

$$x^2 + 4.1x - 20 \equiv 0\ (mod\ 7)$$

$$x^2 + 4.\ (2.4)x + (2.4)^2 - (2.4)^2 - 20 \equiv 0\ (mod\ 7)$$

$$x^2 + 2.8x + (2.8)^2 - (2.8)^2 - 6 \equiv 0\ (mod\ 7)$$

Karena $x^2 + 2.8x + (2.8)^2 = \ (x + 16)^2$ maka

$(x + 16)^2 \equiv (16)^2 + 6\ (mod\ 7) \equiv 2^2 + 6\ (mod\ 7)) \equiv 10\ (mod\ 7)) \equiv 3\ (mod\ 7)$

Karena $16 \equiv 2\ (mod\ 7)$ maka $(x + 2)^2 \equiv 3\ (mod\ 7)$ atau $y^2 \equiv 3\ (mod\ 7)$ dengan $y = x + 2$

Kongruensi tidak mempunyai selesaian karena tidak ada $y = 0, 1, 2, 3, 4, 5, \text{dan } 6$ yang memenuhi

**Teorema 10.1**

Misalkan $p$ suatu bilangan prima ganjil dan $(a, p) = 1$, maka perkogruenan $x^2 \equiv a\ (mod\ p)$ tidak mempunyai solusi atau mempunyai tepat dua solusi.

**Pembuktian:**

Misalkan $p$ suatu bilangan prima ganjil dan $(a, p) = 1$, dan $x^2 \equiv a\ (mod\ p)$ mempunyai solusi, misalnya $x_0$, maka $-x_0$ juga merupakan solusi pula, sebab $(-x_0)^2 \equiv x_0^2 \equiv a(mod\ p)$, sebab andaikan $x_0 \equiv -x_0\ (mod\ p)$, maka $2\ x_0 \equiv 0\ (mod\ p)$. Hal ini tidak mungkin karena $p$ prima ganjil dan $p \nmid x_0$ (karena $x_0^2 \equiv a(mod\ p)$ dan $p \nmid a$).

Perkongruenan $x_0^2 \equiv a\ (mod\ p)$ mempunyai tepat dua solusi, sebab jika ada solusi lain, misalnya $x_0$ dan $x_1$, maka $x_0^2 \equiv x_1^2 \equiv a(mod\ p)$ sehingga $x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv$

0 $(mod\ p)$. Ini berarti $p|(x_0 - x_1)$ atau $p|(x_0 + x_1)$, yaitu $x_0 \equiv -x_1(mod\ p)$ atau $x_0 \equiv x_1(mod\ p)$

**Contoh 10.5**

Selesaikan $x^2 \equiv 5\ (mod\ 11)$ dan $x^2 \equiv 11\ (mod\ 19)$

**Penyelesaian:**

$x^2 \equiv 5\ (mod\ 11)$ adalah $x \equiv 4\ (mod\ 11)$ atau $x \equiv -4\ (mod\ 11) \equiv 7\ (mod\ 11)$

$x^2 \equiv 11\ (mod\ 19)$ adalah $x \equiv 7\ (mod\ 19)$ atau $x \equiv -7\ (mod\ 19) \equiv 12\ (mod\ 19)$

**Definisi 10.1**

Misalkan $m$ suatu bilangan positif, bilangan bulat $a$ disebut residu kuadratik dari $m$, apabila $(a, m) = 1$ dan perkongruenan $x^2 \equiv a\ (mod\ m)$ mempunyai solusi. Jika perkongruenan $x^2 \equiv a\ (mod\ p)$ tidak mempunyai solusi, maka $a$ disebut non residu kuadratik dari $m$.

**Contoh 10.6**

Kongurensi $x^2 \equiv k\ (mod\ 7)$ mempunyai penyelesaian:

$x = 1$ dan $x = 6$ jika $k = 1$

$x = 2$ dan $x = 4$ jika $k = 2$

$x = 3$ dan $x = 5$ jika $k = 4$

Dan tidak mempunyai penyelesaian jika $k = 3$, $k = 5$ atau $k = 6$

Jadi, residu kuadratis modulo 7 adalah 1, 2, dan 4 sedangkan nonresidu kuadratis modulo 7 adalah 3, 5, dan 6.

**Contoh 10.7**

residu – residu kuadratik dari modulo 11 adalah $1, 3, 4, 5$ dan 9 karena

$x^2 \equiv 1\ (mod\ 11)$ mempunyai penyelesaian, yaitu: $x = 1$ atau $x = 10$

$x^2 \equiv 3\ (mod\ 11)$ mempunyai penyelesaian, yaitu: $x = 5$ atau $x = 6$

$x^2 \equiv 4\ (mod\ 11)$ mempunyai penyelesaian, yaitu: $x = 2$ atau $x = 9$

$x^2 \equiv 5\ (mod\ 11)$ mempunyai penyelesaian, yaitu: $x = 4$ atau $x = 7$

$x^2 \equiv 9\ (mod\ 11)$ mempunyai penyelesaian, yaitu: $x = 3$ atau $x = 8$

Bukan residu kuadratik dari modulo 11 adalah $2, 6, 7, 8$ dan 10 karena:

$x^2 \equiv 2\ (mod\ 11)$ tidak mempunyai penyelesaian

$x^2 \equiv 6\ (mod\ 11)$ tidak mempunyai penyelesaian

$x^2 \equiv 7\ (mod\ 11)$ tidak mempunyai penyelesaian

$x^2 \equiv 8\ (mod\ 11)$ tidak mempunyai penyelesaian

$x^2 \equiv 10\ (mod\ 11)$ tidak mempunyai penyelesaian

**Teorema 10.2**

Misalkan $p$ suatu bilangan prima ganjil maka untuk $\{1, 2, 3, \dots, (p-1)\}$ terdapat sebanyak $\frac{1}{2}(p-1)$ residu kuadratik dari $p$ dan sebanyak $\frac{1}{2}(p-1)$ non residu kuadratik dari $p$. Residu – residu kuadratik merupakan unsur dari kelas residu yang memuat bilangan – bilangan:

$$1^2, 2^2, 3^2, \dots \left[\frac{1}{2}(p-1)\right]^2$$

**Pembuktian:**

Untuk menentukan residu kuadratik dari $p$ diantara bilangan – bilangan bulat $1, 2, 3, \dots, (p-1)$ dihitung residu positif terkecil modulo $p$ dari kuadrat bilangan – bilangan $1, 2, 3, \dots, (p-1)$. Karena $(p-1)$ bilangan kuadrat dan karena pengkoruenan $x^2 \equiv a \ (mod\ p)$ tidak mempunyai solusi atau mempunyai dua solusi, maka mesti terdapat sebanyak $\frac{1}{2}(p-1)$ residu kuadratik dari $p$ diantara $1, 2, 3, \dots, (p-1)$. Sedangkan sebanyak $(p-1) - \frac{1}{2}(p-1) = \frac{1}{2}(p-1)$ lainnya merupakan non residu kuadratik dari $p$

**Contoh 10.8**

**Cari semua residu kuadratis Modulo $p$**

a. $p = 13$

b. $p = 19$

**Penyelesaian:**

a. Semua residu kuadratis modulo 13 terdapat di dalam kelas residu yang ditunjukkan oleh:

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2$$

Atau ditunjukkan oleh residu positif terkecil dari $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$:

$$1, 4, 9, 3, 12, 10$$

$1^2 \equiv 12^2 \equiv 1 \ (mod\ 13)$ karena 144 = 11. 13 = 143 + 1

$2^2 \equiv 11^2 \equiv 4 \ (mod\ 13)$

$3^2 \equiv 10^2 \equiv 9 \ (mod\ 13)$ .

$4^2 \equiv 9^2 \equiv 3 \ (mod\ 13)$ .

$5^2 \equiv 8^2 \equiv 12 \ (mod\ 13)$

$6^2 \equiv 7^2 \equiv 10 \ (mod\ 13)$ .

b. Semua residu kuadratis modulo 19 terdapat di dalam kelas residu yang ditunjukkan oleh:

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2$$

Atau ditunjukkan oleh residu positif terkecil dari $1^2, 2^2, 3^2, 4^2, 5^2, 7^2, 8^2, 9^2$:

$$1, 4, 9, 16, 6, 17, 11, 7, 5$$

**Definisi 10.2**

Misalkan $p$ suatu bilangan prima ganjil dan $(a,p)=1$, symbol Legendre $\left(\frac{a}{p}\right)$ didefinisikan oleh

$$\left(\frac{a}{p}\right)=\begin{cases}1, \text{jika a suatu residu kuadratik dari p}\\ -1, \text{jika a suatu nonresidu kuadratik dari p}\end{cases}$$

**Catatan:**

Nama simbol ini diberikan untuk menghormati orang yang pertama menggunakan, yaitu Adrien – Marie Legendre ( 1752 – 1830) bangsa perancis.

**Contoh:**

Untuk $p=11$ maka

$$\left(\frac{1}{11}\right)=\left(\frac{3}{11}\right)=\left(\frac{4}{11}\right)=\left(\frac{5}{11}\right)=\left(\frac{9}{11}\right)=1$$

Karena residu – residu kuadratik dari modulo 11 adalah $1,3,4,5$ dan $9$

$$\left(\frac{2}{11}\right)=\left(\frac{6}{11}\right)=\left(\frac{7}{11}\right)=\left(\frac{8}{11}\right)=\left(\frac{10}{11}\right)=-1$$

Bukan residu kuadratik dari modulo 11 adalah $2,6,7,8$ dan $10$

**Contoh 10.9**

Untuk $p=5$ dapat ditentukan bahwa:

$a=1,2,3,4$ sehingga (1,5), (2,5) (3,5) dan (4, 5) = 1

$\left(\frac{1}{5}\right)=1$ sebab 1 adalah suatu residu kuadratis modulo 5, yaitu: $x^2\equiv 1\ (mod\ 5)$ dapat diselesaikan dengan $x\equiv 1\ (mod\ 5)$ atau $x\equiv 4\ (mod\ 5)$

$\left(\frac{4}{5}\right)=1$ sebab 4 adalah suatu residu kuadratis modulo 5, yaitu: $x^2\equiv 4\ (mod\ 5)$ dapat diselesaikan dengan $x\equiv 2\ (mod\ 5)$ atau $x\equiv 3\ (mod\ 5)$

$\left(\frac{2}{5}\right)=-1$ sebab 2 adalah suatu residu kuadratis modulo 5, yaitu: $x^2\equiv 2\ (mod\ 5)$ tidak dapat diselesaikan

$\left(\frac{3}{5}\right)=-1$ sebab 3 adalah suatu residu kuadratis modulo 5, yaitu: $x^2\equiv 3\ (mod\ 5)$ tidak dapat diselesaikan

**Teorema 10.3 (Kriteria Euler)**

Jika $p$ suatu bilangan ganjl dan $(a,p)=1$ maka

$$\left(\frac{a}{p}\right)\equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$$

**Pembuktian:**

Misalkan $p$ suatu bilangan prima ganjil, $(a,p)=1$ dan $x^2 \equiv a\ (mod\ p)$ mempunyai solusi, misalnya $x_0 = -x_0$ maka $\left(\frac{a}{p}\right) = 1$. Dengan teorema Fermat diperoleh

$$a^{\frac{1}{2}(p-1)} = x_0^{2\frac{1}{2}(p-1)} = x_0^{p-1} \equiv 1\ (mod\ p)$$

Jadi, jika $\left(\frac{a}{p}\right) = 1$ maka $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$ *

Selanjutnya, jika $\left(\frac{a}{p}\right) = -1$ maka perkongruenan $x^2 \equiv a\ (mod\ p)$ tidak mempunyai solusi. Menurut teorema 10.12 pada materi "kekongruenan" untuk setiap bilangan bulat $i$ dengan $1 \leq i \leq (p-1)$, maka ada dengan tunggal bilangan bulat $j$ sedemikian hingga $ij \equiv a\ (mod\ p)$. Karena perkongruenan $x^2 \equiv a\ (mod\ p)$ tidak mempunyai solusi, maka $i \neq j$. Oleh karena itu, dapat dikelompokkan bilangan – bilangan $1, 2, 3, \ldots, (p-1)$ menjadi $\frac{1}{2}(p-1)$ pasangan yang masing – masing hasilkalinya kongruen dengan $a\ (mod\ p)$. Jika $\frac{1}{2}(p-1)$ kekongruenan tersebut dikalikan, maka diperoleh bahwa

$$(p-1)!\ \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$$

Selanjutnya, menurut teorema Wilson, yaitu $(p-1)!\ \equiv\ -1\ (mod\ p)$ diperoleh bahwa

$$-1\ \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)\ **$$

Dapat disimpulkan bahwa

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$$

**Contoh 10.10**

Ditentukan $x^2 \equiv 3\ (mod\ 7)$ tidak mempunyai penyelesaian, akan ditunjukan bahwa $\left(\frac{3}{7}\right) = -1$

**Penyelesaian:**

Bilangan bulat $1, 2, 3, 4, 5, \text{dan } 6$ dapat dipasang – pasangkan dalam bentuk pekalian $ij \equiv 3\ (mod\ 7)$ yaitu:

$1.3 \equiv 3 \equiv 3\ (mod\ 7)$

$2.5 \equiv 10 \equiv 3\ (mod\ 7)$

$4.6 \equiv 24 \equiv 3\ (mod\ 7)$

Sehingga

$1.2.3.4.5.6 \equiv 3^{\frac{1}{2}(7-1)}\ (mod\ 7)$

$6! \equiv 3^3\ (mod\ 7)$ atau bisa d tuliskan menjadi

$-1 \equiv 27\ (mod\ 7)$

Jadi, $\left(\frac{3}{7}\right) = -1$ *

**Contoh 10.11**

Selesaikan

$x^2 \equiv 5\ (mod\ 23)$

**Penyelesaian:**

$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$

$\left(\frac{5}{23}\right) = 5^{\frac{1}{2}(23-1)} = 5^{11} \equiv 5^2.5^2.5^2.5^2.5 \equiv 2.2.2.2.2.5\ (mod 23)$

$\equiv 32.5\ (mod 23) \equiv 9.5(mod 23) \equiv 45\ (mod\ 23) \equiv -1\ (mod\ 23)$

Karena $\left(\frac{5}{23}\right) = -1$ maka kongruensi tidak mempunyai penyelesaian

**Teorema 10.4 (Beberapa sifat dari symbol Legendre)**

Misalkan $p$ suatu bilangan prima ganjil, $a$ dan $b$ bilangan – bilangan bulat yang tidak terbagi oleh $p$, maka:

(i) Jika $a \equiv b\ (mod\ p)$ maka $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$

(iii) $\left(\frac{a^2}{p}\right) = 1$

**Pembuktian:**

(i) Jika $a \equiv b\ (mod\ p)$, maka $x^2 \equiv a\ (mod\ p)$ mempunyai solusi jika dan hanya jika $x^2 \equiv b\ (mod\ p)$ mempunyai solusi. Jadi $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) Menurut kriteria Euler $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p), \left(\frac{b}{p}\right) \equiv b^{\frac{1}{2}(p-1)}\ (mod\ p)$ dan $\left(\frac{ab}{p}\right) \equiv ab^{\frac{1}{2}(p-1)}\ (mod\ p)$, Jadi:

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{1}{2}(p-1)}b^{\frac{1}{2}(p-1)}\ (mod\ p)$

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv (ab)^{\frac{1}{2}(p-1)}\ (mod\ p)$

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right)$

Karena nilai simbol Legendre hanya mungkin $\pm 1$, maka dapat disimpulkan bahwa $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$

(iii) Karena $\left(\frac{a}{p}\right) = \pm 1$ maka menurut (ii) maka diperoleh bahwa

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$$

Bagian (ii) Teorema 10.4 dapat diartikan sebagai berikut:

1) Hasilkali dua residu kuadratik dari suatu bilangan prima adalah suatu residu kuadratik dari hasilkali bilangan – bilangan prima tersebut.
2) Hasilkali dua nonresidu kuadratik dari suatu bilangan prima adalah suatu residu kuadratik dari hasilkali bilangan – bilangan prima tersebut.
3) Hasilkali dua residu kuadratik dan nonresidu kuadratik dari suatu bilangan prima adalah suatu nonresidu kuadratik dari hasilkali bilangan prima tersebut.
4) Dan juga memperhatikan bagian (iii) dapat disimpulkan bahwa $\left(\frac{a^2}{p}\right) = (\frac{a}{p})^2 = 1$

**Contoh 10.12**

Tunjukkan apakah masing – masing kongruensi berikut dapati diselesaikan:

(a) $x^2 \equiv 3\ (mod\ 41)$

(b) $x^2 + 1 \equiv 0\ (mod\ 127)$

**Penyelesaian:**

(a) $\left(\frac{3}{41}\right) \equiv 3^{\frac{1}{2}(41-1)}\ (mod\ 41) \equiv 3^{20}\ (mod\ 41) \equiv (3^4)^5 (mod\ 41) \equiv (81^2)^5 (mod\ 41)$

$\equiv (-1)^5 (mod\ 41) \equiv (-1)(mod\ 41)$

Karena $\left(\frac{3}{41}\right) = -1$, maka $x^2 \equiv 3\ (mod\ 41)$ tidak dapat diselesaikan

(b) $x^2 + 1 \equiv 0\ (mod\ 127)$ maka $x^2 \equiv -1\ (mod\ 127)$

$\left(\frac{-1}{127}\right) \equiv (-1)^{\frac{1}{2}(127-1)}(\ mod\ 127) \equiv (-1)^{63}(\ mod\ 127) \equiv -1\ mod(127)$

$\left(\frac{-1}{127}\right) \equiv -1,$ maka kongruensi $x^2 + 1 \equiv 0\ (mod\ 127)$ tidak mempunyai penyelesian.

**Teorema 10.5**

Misalkan $p$ suatu bilangan prima ganjil maka

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{p} \equiv 1\ (mod\ 4) \\ -1, \text{p} \equiv 3\ (mod\ 4) \end{cases}$$

**Pembuktian:**

Suatu bilangan prima ganjil $p$ dapat dinyatakan dengan $4n + 1$ atau $4n + 3$ dengan $n$ suatu bilangan asli. Dengan kata lain, $p \equiv 1\ (mod\ 4)$ atau $p \equiv 3\ (mod\ 4)$.

Jika $p \equiv 1\ (mod\ 4)$, yaitu: $p = 4n + 1,$ untuk suatu bilangan bulat $n$ maka $(-1)^{\frac{1}{2}(p-1)} = (-1)^{2n} = 1$. Dan karena $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)}\ (mod\ p)$ maka $\left(\frac{-1}{p}\right) = 1$ *

Jika $p \equiv 3\ (mod\ 4)$, yaitu: $p = 4n + 3$, untuk suatu bilangan bulat $n$ maka $(-1)^{\frac{1}{2}(p-1)} = (-1)^{2n+1} = -1$. Dan karena $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{1}{2}(p-1)}\ (mod\ p)$ maka $\left(\frac{-1}{p}\right) = -1$ *

**Contoh 10.13**

Kongruensi kuadratis $x^2 \equiv -1\ (mod\ 11)$, tidak mempunyai penyelesaian sebab $11 \equiv -1\ (mod\ 11)$ sehingga $\left(\frac{-1}{11}\right) = -1$

**Contoh 10.14**

Kongruensi kuadratis $x^2 \equiv -1\ (mod\ 29)$, dapat diselesaikan sebab $29 \equiv 1\ (mod\ 4)$ sehingga $\left(\frac{-1}{29}\right) = \pm 1$. Untuk memperoleh penyelesaian, perlu menambah $-1$ dengan $29k$ yang mana $k = 1,2,3,\ldots$ sehingga diperoleh suatu bilangan kuadrat. Dengan demikian kongruensi dapat diubah menjadi:

$x^2 \equiv -1\ (mod\ 29) \equiv (-1 + 29k) \equiv (-1 + 29.10)(mod\ 29) \equiv 289\ (mod\ 29)$

Sehingga $x^2 - 289 \equiv 0\ (mod\ 29)$, $(x - 17)(x + 17) \equiv 0\ (mod\ 29)$. Jadi kongruensi adalah

$x \equiv 17\ (mod\ 29)$ atau $x \equiv 12\ (mod\ 29)$

**Teorema 10.6 (Lemma Gauss)**

Misalkan $p$ suatu bilangan prima ganjil maka $(a, p) = 1$. Jika $k$ adalah banyaknya residu positif terkecil dari bilangan – bilangan $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a$ lebih besar dari $\frac{1}{2}p$, maka $\left(\frac{a}{p}\right) = (-1)^k$

Pembuktian:

Misalkan $u_1, u_2, u_3, \ldots u_k$ adalah residu – residu positif terkecil yang lebih besar dari $\frac{1}{2}p$ dari $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a$.

Misalkan $v_1, v_2, v_3, \ldots v_t$ adalah residu – residu positif terkecil yang lebih kecil dari $\frac{1}{2}p$ dari $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)$.

Karena $(ja, p) = 1$. Untuk semua $j$ dengan $1 \leq j \leq \frac{1}{2}(p-1)$, residu – residu positif terkecil itu berada dalam $\{1, 2, 3, \ldots, (p-1)\}$.

Akan ditunjukkan bahwa himpunan $\{p - u_1,\ p - u_2,\ p - u_3, \ldots, p - u_k, v_1, v_2, v_3, \ldots v_t\} = \{1, 2, 3, \ldots, \frac{1}{2}(p-1)$ hanya berbeda urutannya. Untuk ini cukup ditunjukkan bahwa tidak ada dua elemen pada himpunan pertama yang kongruen modulo $p$, karena himpunan tersebut mempunyai tepat $\frac{1}{2}(p-1)$ elemen yang semuanya tidak lebih besar dari $\frac{1}{2}(p-1)$.

Tidak ada dua $u_i$ yang kongruen modulo $p$ dan tidak ada dua $v_j$ yang kongruen modulo $p$. Sebab, jika $ma \equiv na\ (mod\ p)$, dengan $1 \leq m, n \leq \frac{1}{2}(p-1)$ dan karena $p \nmid a$, maka $m \equiv n\ (mod\ p)$. Hal ini tidak mungkin.

Selanjutnya $p - u_i \not\equiv v_j\ (mod\ p)$, sebab jika $p - ma \equiv na\ (mod\ p)$ atau $-m \equiv n\ (mod\ p)$. Hal ini juga tidak mungkin, karena $1 \leq m, n \leq \frac{1}{2}(p-1)$.

Jadi $\{p-u_1,\ p-u_2,\ p-u_3, \dots, p-u_k, v_1, v_2, v_3, \dots v_t\} = \{1, 2, 3, \dots, \frac{1}{2}(p-1)$ yang hanya berbeda urutannya, sehingga diperoleh bahwa:

$$\{p-u_1,\ p-u_2,\ p-u_3, \dots, p-u_k, v_1, v_2, v_3, \dots v_t\} \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p)$$

$$(-1)^k u_1, u_2, u_3, \dots u_k v_1, v_2, v_3, \dots v_t \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Tetapi karena $u_1, u_2, u_3, \dots u_k v_1, v_2, v_3, \dots v_t$ adalah residu – residu terkecil positif dari $a, 2a, 3a, \dots, \frac{1}{2}(p-1)$ maka diperoleh bahwa:

$$u_1, u_2, u_3, \dots u_k v_1, v_2, v_3, \dots v_t \equiv a.2a.3a.\dots, \frac{1}{2}(p-1)(mod\ p)$$

$$u_1, u_2, u_3, \dots u_k v_1, v_2, v_3, \dots v_t \equiv a^{\frac{1}{2}(p-1)}\left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Sehingga diperoleh:

$$(-1)^k a^{\frac{1}{2}(p-1)}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Karena $\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$, maka pengkongruenan terakhir itu menjadi:

$$(-1)^k a^{\frac{1}{2}(p-1)}\left(\frac{p-1}{2}\right)! \equiv 1\ (mod\ p)$$

$$a^{\frac{1}{2}(p-1)}\left(\frac{p-1}{2}\right)! \equiv (-1)^k\ (mod\ p)$$

Dan karena menurut kriteria Euler, yaitu: $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}\ (mod\ p)$ maka diperoleh bahwa

$$\left(\frac{a}{p}\right) \equiv (-1)^k\ (mod\ p)\ *$$

**Contoh 10.15**

Kongruensi kuadratis $x^2 \equiv 7\ (mod\ 13)$ akan diselidiki menggunakan Lemma Gauss, buat barisan $7k$ dengan $k = 1, 2, \dots, \left(\frac{13-1}{2}\right)$ atau $k = 1, 2, \dots, 6$ diperoleh $7, 14, 21, 28, 35$ dan $42$ dan dalam modulo 13 diperoleh barisan residu positif terkecil 7, 1, 8, 2, 9, 3 sehingga dapat

dikelompokkan menjadi barisan residu positif terkecil lebih dari $\left(\frac{13-1}{2}\right) = 6$ yaitu: $7, 8, 9$ dan barisan residu positif terkecil kurang dari $\left(\frac{13-1}{2}\right) = 6$ yaitu: 1, 2, 3. Dengan demikian:

$u_1 = 7 \equiv 7\ (mod\ 13), u_2 = 8 \equiv 21\ (mod\ 13)\ u_3 = 9 \equiv 35\ (mod\ 13)$

$v_1 = 1 \equiv 14\ (mod\ 13), u_2 = 2 \equiv 28\ (mod\ 13)\ u_3 = 3 \equiv 42\ (mod\ 13)$

Sehingga:

$u_1.u_2.u_3.v_1.v_2.v_3 \equiv 7.21.35.14.28.42\ (mod\ 13) \equiv 7^6.1.2.3.4.5.6\ (mod\ 13)$

Sekarang buat barisan $p - u_1, p - u_2, p - u_3.v_1.v_2.v_3$ diperoleh $6, 5, 4, 1, 2, 3$ yang mana tidak memuat dua suku yang kongruen

$$(-1)^k a^{\frac{1}{2}(p-1)}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!\ (mod\ p)$$

$$(-1)^3 7^{\frac{1}{2}(13-1)}\left(\frac{13-1}{2}\right)! \equiv \left(\frac{13-1}{2}\right)!\ (mod\ 13)$$

$$(-1)^3 7^6 6! \equiv 6!\ (mod\ 13)$$

$7^6 \equiv -1\ (mod\ 13)$, berarti $\left(\frac{7}{13}\right) \equiv 7^6 (mod\ 13) \equiv -1\ (mod\ 13)$

Jadi, kongruen $x^2 \equiv 7 (mod\ 13)$ tidak mempunyai penyelesaian

**Contoh 10.16**

Misalkan akan ditentukan $\left(\frac{9}{17}\right)$. Residu terkecil modulo 17 dari suku – suku barisan $9, 18, 27, 36, 45, 54, 36, 72$ berturut – turut adalah $9, 1, 10, 2, 11, 3, 12, 4$. Karena terdapat empat residu terkecil yang lebih dari $\frac{17}{2}$, maka menurut lemma Gauss diperoleh $\left(\frac{9}{17}\right) \equiv (-1)^4 = 1$

**Teorema 10.7**

Jika $p$ suatu bilangan prima ganjil, $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{1}{8}(p^2-1)}$ dengan kata lain, 2 adalah residu kuadratik dari semua bilangan prima $p \equiv \pm 1\ (mod\ 8)$ atau 2 adalah nonresidue dari semua prima berbentuk $p \equiv \pm 1\ (mod\ 8)$

**Pembuktian:**

Menurut Lemma Gauss, jika $k$ adalah banyaknya residu positif terkecil dari barisan bulat $1.2,\ 2.2, 2.2, 3.3, \ldots, \frac{1}{2}(p-1).2$ yang lebih dari $\frac{1}{2}p$, maka $\frac{2}{p} = (-1)^k$. Karena semua suku dalam barisan tersebut kurang dari $p$, maka akan menentukan banyaknya residu positif terkecil modulo $p$ dari suku barisan tersebut yang kurang dari $\frac{1}{2}p$. Selanjutnya dengan Lemma Gauss diperoleh bahwa

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left(\frac{p}{4}\right)}$$

Sesuai dengan teoremanya, maka perlu menunjukkan bahwa

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) \equiv \frac{1}{8}(p^2-1)(mod\ 2)$$

Untuk menunjukkan ini, perlu memperhatikan kelas kongruensi dari $p$ modulo 8, sebab kedua ruas kekongruenan itu hanya bergantung pada kelas kekongruenan dari $p$ dari modulo 8.

Perhatikan ruas kanannya, yaitu: $\frac{p^2-1}{8}$

Jika $p \equiv \pm 1\ (mod\ 8)$, maka $p = 8k \pm 1$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k \equiv 0(mod\ 2)$$

Jika $p \equiv \pm 3\ (mod\ 8)$, maka $p = 8k \pm 3$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1 \equiv 1(mod\ 2)$$

Sekarang perhatikan ruas kirinya, $\frac{p-1}{2} - \left(\frac{p}{4}\right)$

Jika $p \equiv 1\ (mod\ 8)$, maka $p = 8k + 1$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) = 4k - \left[2k + \frac{1}{4}\right] = 2k \equiv 0\ (mod\ 2)$$

Jika $p \equiv 7\ (mod\ 8)$, maka $p = 8k + 7$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) = 4k + 3 - \left[2k + \frac{7}{4}\right] = 2k + 2 \equiv 0\ (mod\ 2)$$

Jika $p \equiv 3\ (mod\ 8)$, maka $p = 8k + 3$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) = 4k + 3 - \left[2k + \frac{7}{4}\right] = 2k + 1 \equiv 1\ (mod\ 2)$$

Jika $p \equiv 5\ (mod\ 8)$, maka $p = 8k + 5$ dengan $k$ suatu bilangan bulat, sehingga

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) = 4k + 2 - \left[2k + \frac{5}{4}\right] = 2k + 1 \equiv 1\ (mod\ 2)$$

Dengan membandingkan kelas – kelas kekongruenan modulo 2 dan $\frac{p-1}{2} - \left(\frac{p}{4}\right)$ dan $\frac{p^2-1}{8}$.

Untuk empat kemungkinan kelas kekongruenan dari $p$ modulo 8 tersebut, maka disimpulkan bahwa

$$\frac{p-1}{2} - \left(\frac{p}{4}\right) \equiv \frac{1}{8}(p^2-1)(mod\ 2)$$

Jadi untuk setiap bilangan prima ganjil $p$, berlaku:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$$

Memperhatikan perhitungan dari kelas – kelas kongruensi dari $\frac{p^2-1}{8}(mod\ 2)$ pada pembuktian tersebut, maka akan diperoleh bahwa $\left(\frac{2}{p}\right) = 1$, jika $p \equiv \pm 1\ (mod\ 8)$ sedangkan $\left(\frac{2}{p}\right) = -1$, jika $p \equiv \pm 3\ (mod\ 8)$ *

**Contoh 10.17 (Sifat – Sifat Legendre)**

(i) $\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right) = \left(\frac{2}{23}\right) = \left(\frac{2}{31}\right) = 1$

$\left(\frac{2}{7}\right) = 1$, karena $7 \equiv -1\ (mod\ 8)$ 8. 1 – 1 = 7

$\left(\frac{2}{17}\right) = 1$, karena $17 \equiv 1\ (mod\ 8)$ 8. 2 + 1 = 17

$\left(\frac{2}{23}\right) = 1$, karena $23 \equiv -1\ (mod\ 8)$ 8.3 - 1 = 23

$\left(\frac{2}{31}\right) = 1$, karena $31 \equiv -1\ (mod\ 8)$ 8.4 – 1 = 31

(ii) $\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{19}\right) = \left(\frac{2}{29}\right) = -1$

$\left(\frac{2}{3}\right) = -1$, karena $3 \equiv 3\ (mod\ 8)$ 8.0 + 3 = 3

$\left(\frac{2}{5}\right) = -1$, karena $5 \equiv -3\ (mod\ 8)$ 8. 1 - 3 = 5

$\left(\frac{2}{11}\right) = -1$, karena $11 \equiv 3\ (mod\ 8)$ 8.1 + 3 = 11

$\left(\frac{2}{13}\right) = -1$, karena $13 \equiv -3\ (mod\ 8)$ 8.2 – 3 = 13

$\left(\frac{2}{19}\right) = -1$, karena $19 \equiv 3\ (mod\ 8)$ 8.2 + 3 = 19

$\left(\frac{2}{29}\right) = -1$, karena $29 \equiv -3\ (mod\ 8)$ 8.4 – 3 = 31

**Contoh 10.18 (Menentukan Nilai Simbol Legendre)**

(i) Karena $317 \equiv 9\ (mod\ 11)$ dan memperhatikan Teorema 10.4. Maka $\left(\frac{317}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)^2 = 1$

(ii) Karena $89 \equiv -2\ (mod\ 13)$ dan memperhatikan Teorema 10.4. Maka $\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right).\left(\frac{2}{13}\right)$. Karena $13 \equiv 1\ (mod\ 4)$ dan memperhatikan Teorema 10.5, maka $\left(\frac{-1}{13}\right) = 1$ Karena $13 \equiv -3\ (mod\ 8)$ dan memperhatikan Teorema 10.7, maka $\left(\frac{-2}{13}\right) = -1$. Jadi $\left(\frac{89}{13}\right) = -1$

Misalkan $n = pq$ dengan $p$ dan $q$ adalah bilangan – bilangan prima ganjil yang berbeda dan misalkan bahwa $x^2 \equiv a\ (mod\ n)$, dengan $0 < a < n$ mempunyai solusi $x = x_0$.

Akan dibuktikan ada empat solusi yang tidak kongruen modulo $n$ atau $a$ mempunyai empat akar kuadrat yang tidak kongruen modulo $n$.

**Pembuktian:**

Misalkan $x_0 \equiv x_1(mod\ p), 0 < x_1 < p$ dan $x_0 \equiv x_2(mod\ p), 0 < x_2 < q$ maka perkongruenan $x^2 \equiv a\ (mod\ p)$ mempunyai dua solusi yang tidak kongruen modulo $p$, misalnya $x \equiv x_1(mod\ p)$ dan $x \equiv p - x_1(mod\ p)$, mirip dengan ini, maka perkongruenan $x^2 \equiv a\ (mod\ q)$ mempunyai dua solusi yang tidak kongruen modulo $q$, misalnya $x \equiv x_2(mod\ q)$ dan $x \equiv q - x_2(mod\ q)$.

Dari Teorema Sisa Cina, terdapat empat solusi yang tidak kongruen dari perkongruenan $x^2 \equiv a\ (mod\ n)$. Empat solusi ini merupakan solusi tunggal modulo $pq$ dari empat sistem perkongruenan, yaitu:

(i) $\begin{cases} x \equiv x_1(mod\ p) \\ x \equiv x_2(mod\ q) \end{cases}$

(ii) $\begin{cases} x \equiv p - x_1(mod\ p) \\ x \equiv x_2(mod\ q) \end{cases}$

(iii) $\begin{cases} x \equiv x_1(mod\ p) \\ x \equiv q - x_2(mod\ q) \end{cases}$

(iv) $\begin{cases} x \equiv p - x_1(mod\ p) \\ x \equiv q - x_2(mod\ q) \end{cases}$

Misalnya Solusi dari (i) dan (ii) berturut – turut adalah x dan $y$. Solusi dari (iii) dan (iv) berturut – turut $n - y$ dan $n - x$

Jika $p \equiv q \equiv 3(mod\ 4)$, solusi dari $x^2 \equiv a\ (mod\ p)$ dan dari $x^2 \equiv a\ (mod\ q)$ berturut – turut adalah $x \equiv \pm\, a^{\frac{p+1}{4}}(mod\ p)$ dan $x \equiv \pm\, a^{\frac{q+1}{4}}(mod\ q)$. Dengan kriteria Euler, diketahui bahwa $a^{\frac{p+1}{2}} = \left(\frac{a}{p}\right) = 1\ \ (mod\ p)$ dan $a^{\frac{q-1}{2}} = \left(\frac{a}{q}\right) = 1\ \ (mod\ q)$. (Asumsi bahwa $x^2 \equiv a\ (mod\ pq)$ mempunyai solusi kuadratik dari $p$ maupun $q$).

Jadi,

$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}}.a \equiv a\ (mod\ p)$ dan $\left(a^{\frac{q+1}{4}}\right)^2 = a^{\frac{q+1}{2}} = a^{\frac{q+1}{2}}.a \equiv a\ (mod\ q)$

**Contoh 10.19**

Misalkan perkongruenan $x^2 \equiv 860\ (mod\ 11021)$ mempunyai solusi. Karena 11021 = 103. 107, maka akan mendapat empat solusinya, penyelesaian perkongruenan – perkongruenan sebagai berikut:

$$x^2 \equiv 860 \equiv 36\ (mod\ 103) \text{ dan } x^2 \equiv 860 \equiv 4\ (mod\ 107)$$

Solusi dari perkongruenan – perkongruenan berturut – turut itu adalah:

$$x^2 \equiv \pm 36^{\frac{103+1}{4}} (mod\ p) \equiv \pm 36^{26} \equiv \pm 6\ (mod\ 103)$$

Dan

$$x^2 \equiv \pm 4^{\frac{107+1}{4}} (mod\ p) \equiv \pm 4^{27} \equiv \pm 2\ (mod\ 107)$$

Dengan menggunakan Teorema Sisa Cina diperoleh $x \equiv \pm 212, \pm 109\ \ (mod\ 11021)$ yang merupakan solusi dari empat sistem perkongruenan yang dibentuk oleh empat kemungkinan pilihan tanda sistem perkongruenan.

$x \equiv \pm 6\ (mod\ 103)$ dan $x \equiv \pm 2\ (mod\ 107)$

Misalkan $p$ suatu bilangan prima ganjil, maka $\frac{p-1}{2}$ suatu bilangan genap, bila $x \equiv \pm 1\ (mod\ 4)$ dan $\frac{p-1}{2}$ suatu bilangan ganjil, bila $p \equiv 3\ (mod\ 4)$. Sehingga, jika $p$ dan $q$ dua prima ganjil, maka $\frac{p-1}{2}\frac{q-1}{2}$ adalah genap, jika $p \equiv 1\ (mod\ 4)$ atau $q \equiv 1\ (mod\ 4)$ dan $\frac{p-1}{2}\frac{q-1}{2}$ adalah ganjil jika $p \equiv 3\ (mod\ 4)$ atau $q \equiv 3\ (mod\ 4)$.

Menurut Aturan kebalikan Kuadratik yang akan diberikan kemudian, diperoleh:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, \text{jika p} \equiv 1\ (mod\ 4) \text{ atau q} \equiv 1\ (mod\ 4) \\ -1, \text{jika p} \equiv 1\ (mod\ 4) \text{ atau q} \equiv 1\ (mod\ 4) \end{cases}$$

Karena nilai – nilai yang mungkin dari $\left(\frac{p}{q}\right) dan \left(\frac{q}{p}\right)$ hanya $\pm 1$, maka:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), \text{jika p} \equiv 1\ (mod\ 4) \text{ atau q} \equiv 1\ (mod\ 4) \\ -\left(\frac{q}{p}\right), \text{jika p} \equiv 1\ (mod\ 4) \text{ atau q} \equiv 1\ (mod\ 4) \end{cases}$$

Hal ini berarti bahwa jika $p$ dan $q$ bilangan prima ganjil, maka:

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ apabila p $\equiv 1\ (mod\ 4)$ atau q $\equiv 1\ (mod\ 4)$ dan

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ apabila p $\equiv 3\ (mod\ 4)$ atau q $\equiv 3\ (mod\ 4)$

**Contoh 10. 20**

$p = 13$ dan $q = 17$. Karena $13 \equiv 17 \equiv 1 (mod\ 4)$, maka $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. Selanjutnya, sesuai dengan sifat Legendre $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$. Dan karena $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$, maka $\left(\frac{13}{17}\right) = 1$

**Contoh 10.21**

$p = 7$ dan $q = 19$. Karena $7 \equiv 19 \equiv 3\ (mod\ 4)$, maka $\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right)$. Selanjutnya, sesuai dengan sifat Legendre $\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right)$. karena $5 \equiv 1\ (mod\ 4)$ maka $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right).\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$. (Sesuai Teorema 10.6). Jadi $\left(\frac{7}{19}\right) = 1$

**Contoh 10.22**

Tentukan nilai dari $\left(\frac{713}{1009}\right)$ degan suatu bilangan prima.

**Penyelesaian:**

Karena $713 = 23.31$ maka $\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$.

Selanjutnya, karena $1009 \equiv 1\ (mod\ 4)$ maka $\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right)$ dan $\left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right)$

$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2 5}{23}\right) = \left(\frac{2}{23}\right)^2 \left(\frac{5}{23}\right) = \left(\frac{5}{23}\right)$ karena $5 \equiv 1\ (mod\ 4), \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) =$

$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$ Jadi, $\left(\frac{23}{1009}\right) = -1$

$\left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right)$, karena $17.5 \equiv 1\ (mod\ 4), \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2.7}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) =$

$\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$ Jadi, $\left(\frac{1009}{31}\right) = -1$

Kesimpulan $\left(\frac{713}{1009}\right) = (-1).(-1) = 1$

**Teorema 10.8**

Jika $k$ adalah suatu bilagan bulat ganjil, $p$ adalah suatu bilangan prima ganjil $(a, p) = 1$ dan

$\mathrm{T(a,p)} = \sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{ja}{p}\right]$ maka $\left(\frac{\mathrm{a}}{\mathrm{p}}\right) = (-1)^{T(a,p)}$

Pembuktian:

Misalkan $u_1, u_2, u_3, \ldots u_k$ adalah residu – residu positif terkecil yang lebih besar dari $\frac{1}{2}p$ dari $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)a$. Misalkan pula $v_1, v_2, v_3, \ldots v_t$ adalah residu – residu positif terkecil yang lebih dari $\frac{1}{2}p$ dari $a, 2a, 3a, \ldots, \frac{1}{2}(p-1)$. Sesuai dengan algoritma pembagian untuk $p$ dan $ja$, maka:

$$ja = p\left[\frac{ja}{p}\right] + sisa$$

Sisa ini sama dengan salah satu dari $u_i$ dan $v_j$. Menjumlahkan $\frac{1}{2}(p-1)$ persamaan tersebut, maka diperoleh:

$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \mathrm{ja} = \sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} p\left[\frac{ja}{p}\right] + \sum_{i=1}^{\mathrm{k}} u_i + \sum_{j=1}^{\mathrm{t}} v_j \ldots$ (1)

Seperti pada pembuktian lemma Gauss, bahwa barisan bilangan bulat $p - u_1, p - u_2, p - u_3, p - u_k, v_1, v_2, v_3, \ldots v_t$ sama dengan barisan bulat $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ pada suatu urutan. Sehingga penjumlahan dari semua bilangan bulat ini diperoleh:

$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \mathrm{j} = \sum_{j=1}^{\mathrm{k}}(p - u_j) + \sum_{j=1}^{\mathrm{t}} v_j = ps - \sum_{j=1}^{\mathrm{k}} u_j + \sum_{j=1}^{\mathrm{t}} v_j \ldots$ (2)

Apabila ruas – ruas dari (1) dikurangi ruas – ruas dari (2), maka di peroleh

$$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \mathrm{ja} - \sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \mathrm{j} = \sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} p\left[\frac{ja}{p}\right] - ps + 2\sum_{i=1}^{\mathrm{k}} u_i$$

Karena $T(a,p) = \sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} p\left[\frac{ja}{p}\right]$

$$(a-1)\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \mathrm{j} = p\,T(a,p) - ps + 2\sum_{j=1}^{\mathrm{k}} u_j$$

Karena $a$ dan $p$ bilangan ganjil, maka kesamaan ini dalam modulo 2 ditulis sebagai

$$0 \equiv T(a,p) - s\ (md\ 2)$$

$$T(a,p) \equiv s\ (md\ 2)$$

Menurut Lemma Gauss $\left(\frac{a}{p}\right) = (-1)^s$. Dan karena $(-1)^s = (-1)^{T(a,p)}$ maka

$$\left(\frac{\mathrm{a}}{\mathrm{p}}\right) = (-1)^{T(a,p)}\ *$$

**Contoh 10.23**

Untuk menentukan nilai $\left(\frac{7}{11}\right)$ dengan menggunakan teorema 10.8 dihitung jumlahan

**Penyelesaian:**

$\left(\frac{7}{11}\right)$ artinya $a = 7$ dan $\mathrm{p} = 11$ maka

$$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{ja}{p}\right] = \sum_{j=1}^{\frac{1}{2}(11-1)} \left[\frac{7j}{11}\right] = \sum_{j=1}^{5} \left[\frac{7j}{11}\right]$$

$$\sum_{j=1}^{5} \left[\frac{7j}{11}\right] = \left[\frac{7.1}{11}\right] + \left[\frac{7.2}{11}\right] + \left[\frac{7.3}{11}\right] + \left[\frac{7.4}{11}\right] + \left[\frac{7.5}{11}\right]$$

$$\sum_{j=1}^{5} \left[\frac{7j}{11}\right] = \left[\frac{7}{11}\right] + \left[\frac{14}{11}\right] + \left[\frac{21}{11}\right] + \left[\frac{28}{11}\right] + \left[\frac{35}{11}\right]$$

$$\sum_{j=1}^{5} \left[\frac{7j}{11}\right] = 0 + 1 + 1 + 2 + 3$$

$$\sum_{j=1}^{5} \left[\frac{7j}{11}\right] = 7$$

Jadi, $\left(\frac{7}{11}\right) = (-1)^7 = -1$

Dengan cara yang sama dapat ditentukan $\left(\frac{11}{7}\right)$ sebagai berikut:

$\left(\frac{11}{7}\right)$ artinya $a = 11$ dan p $= 7$ maka

$$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{ja}{p}\right] = \sum_{j=1}^{\frac{1}{2}(7-1)} \left[\frac{11j}{7}\right] = \sum_{j=1}^{3} \left[\frac{11j}{7}\right]$$

$$\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = \left[\frac{11.1}{7}\right] + \left[\frac{11.2}{7}\right] + \left[\frac{11.3}{7}\right]$$

$$\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = \left[\frac{11}{7}\right] + \left[\frac{22}{7}\right] + \left[\frac{33}{7}\right]$$

$$\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = 1 + 3 + 4$$

$$\sum_{j=1}^{3} \left[\frac{11j}{7}\right] = 8$$

Jadi, $\left(\frac{11}{7}\right) = (-1)^8 = 1$

**Teorema 10.9**

Misalkan $p$ dan $q$ bilangan prima ganjil, maka $(a, p) = 1$ dan

$$\left(\frac{\mathrm{p}}{\mathrm{q}}\right)\left(\frac{\mathrm{q}}{\mathrm{p}}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

**Pembuktian:**

Perhatikan pasangan bilangan – bilangan bulat $(x, y)$ dengan $1 \le x \le \frac{1}{2}(p-1)$ dan $1 \le y \le \frac{1}{2}(q-1)$ maka terdapat $\frac{p-1}{2}\frac{q-1}{2}$ pasangan. Bagi pasangan – pasangan ini dalam dua kelompok berdasarkan besarnya $qx$ dan py

Perhatikan bahwa $qx \neq$ py untuk semua pasangan. Sebab, Andaikan $qx =$ py maka $q \mid$ py, sehingga $q \mid$ p atau $q \mid$ y. Akan tetapi, karena $p$ dan $q$ bilangan – bilangan prima yang berbeda, maka $q \nmid$ p, dan karena $1 \le y \le \frac{1}{2}(q-1)$, maka $q \nmid$ y.

Banyaknya pasangan $(x, y)$ dengan $1 \le x \le \frac{1}{2}(p-1)$ , $1 \le y \le \frac{1}{2}(q-1)$ dan $qx >$ py sama dengan banyaknya pasangan $(x, y)$ dengan $1 \le x \le \frac{1}{2}(p-1)$ , $1 \le y \le \frac{qx}{p}$. Sebab, setiap nilai bilangan bulat $x$ dengan $1 \le x \le \frac{1}{2}(p-1)$ ada $\left[\frac{qx}{p}\right]$ bilangan bulat yang memenuhi $1 \le y \le \frac{qx}{p}$. Jadi banyaknya semua pasangan $(x, y)$ dengan $1 \le x \le \frac{1}{2}(p-1)$ , $1 \le y \le \frac{1}{2}(q-1)$ dan $qx >$ py adalah $\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{qj}{p}\right]$

Banyaknya pasangan $(x, y)$ dengan $1 \leq x \leq \frac{1}{2}(p-1)$ , $1 \leq y \leq \frac{1}{2}(q-1)$ dan $qx <$ py sama dengan banyaknya pasangan $(x, y)$ dengan $1 \leq y \leq \frac{1}{2}(q-1), 1 \leq x \leq \frac{py}{q}$. Sebab setiap nilai bilangan bulat $y$ dengan $1 \leq y \leq \frac{1}{2}(q-1)$ ada $\left[\frac{py}{q}\right]$ bilangan bulat $x$ yang memenuhi $1 \leq x \leq \frac{py}{q}$. Jadi banyaknya semua pasangan $(x, y)$ dengan $1 \leq x \leq \frac{1}{2}(p-1)$ , $1 \leq y \leq \frac{1}{2}(q-1)$ dan $qx <$ py adalah $\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{pj}{q}\right]$

Mengingat banyaknya semua pasangan adalah $\frac{p-1}{2}.\frac{q-1}{2}$,

$\sum_{j=1}^{\frac{1}{2}(\mathrm{p}-1)} \left[\frac{qj}{q}\right] + \sum_{j=1}^{\frac{1}{2}(\mathrm{q}-1)} \left[\frac{pj}{q}\right] = \frac{p-1}{2}.\frac{q-1}{2}$ atau $T(q,p) + T(p,q) = \frac{p-1}{2}.\frac{q-1}{2}$

Jadi

$(-1)^{T(q,p)+T(p,q)} = (-1)^{T(q,p)}\,(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$

Karena menurut lemma Gauss $\left[\frac{q}{p}\right] = (-1)^{T(q,p)}$ dan $\left[\frac{p}{q}\right] = (-1)^{T(p,q)}$ maka:

$$\left(\frac{\mathrm{p}}{\mathrm{q}}\right)\left(\frac{\mathrm{q}}{\mathrm{p}}\right) = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}} \quad *$$

Satu diantara kegunaan dari aturan kebalikan kuadratik adalah untuk membuktikan keabsahan tes keprimaan dari bilangan Fermat.

## DAFTAR PUSTAKA


Apostol, Tom M. 1983. *Introduction to Analytic Number Theory*. New York: John Wiley & Sons

Burton, David M. 1986. *Elementary Number Theory Revised Printing*. Boston: Allyn and Bacon. Inc.

Dudley, Underwood. 19689. *Elementary Number Theory*. San Francisco: W.H. Freeman and Company.

Munir, R. 2004. *Bahan Kuliah ke-3: Teori Bilangan (Number Theory).* Bandung: Departemen Teknik Informatika ITB

Shapiro, Harold N. 1995. *Introduction Number Theory*. New York: Springer – Verlag.

Sukirman. 2006. *Pengantar Teori Bilangan*. Yogyakarta: Hanggar Kreator

Roses, Kenneth H. 1993. *Elementary Number Theory and Its Applications.* Edisi ketiga. New York: Addision – Wesley Publishing Company.