ISBN 978-623-198-458-6

TEORI BILANGAN

Penulis:

- Samuel Urath
- Yunita Oktavia Wulandari
- Rifka Agustianti
- Hetty Elfina
- Titik Pitriani Muslimin
- Haerudin
- Ahmad Choirul Anam
- Nanang
- Azmidar
- Prida N. L. Taneo

TEORI BILANGAN

Samuel Urath
Yunita Oktavia Wulandari
Rifka Agustianti
Hetty Elfina
Titik Pitriani Muslimin
Haerudin
Ahmad Choirul Anam
Nanang
Azmidar
Prida N. L. Taneo

PT GLOBAL EKSEKUTIF TEKNOLOGI

TEORI BILANGAN

Penulis :
Samuel Urath
Yunita Oktavia Wulandari
Rifka Agustianti
Hetty Elfina
Titik Pitriani Muslimin
Haerudin
Ahmad Choirul Anam
Nanang
Azmidar
Prida N. L. Taneo

ISBN : 978-623-198-458-6

Editor : Ari Yanto, M.Pd.
Nurfathzi Jhonez, S.Pd.
Penyunting: Yuliatri Novita, M.Hum.
Desain Sampul dan Tata Letak : Tri Putri Wahyuni, S.Pd.
Penerbit : PT GLOBAL EKSEKUTIF TEKNOLOGI
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jl. Pasir Sebelah No. 30 RT 002 RW 001
Kelurahan Pasie Nan Tigo Kecamatan Koto Tangah
Padang Sumatera Barat
Website : www.globaleksekutifteknologi.co.id
Email : globaleksekutifteknologi@gmail.com

Cetakan pertama, Juli 2023

KATA PENGANTAR

Dengan mengucapkan puji syukur kehadirat Allah SWT, atas limpahan rahmat dan hidayahNya, maka Penulisan Buku dengan judul Teori Bilangan dapat diselesaikan dengan baik atas kerjasama tim penulis. Buku ini berisikan tentang induksi matematika, teorema binomia, keterbagian pada bilangan bulat, sistem bilangan, bilangan prima dan faktorisasi tunggal, kekongruenan dan aplikasinya, pengkongruenan linier, algoritma euclid, fungsi φ, teorema euler, akar primitive dan indeks, fungsi tangga.

Buku ini masih banyak kekurangan dalam penyusunannya. Oleh karena itu, kami sangat mengaharapkan kritik dan saran demi perbaikan dan kesempurnaan buku ini selanjutnya. Kami mengucapkan terima kasih kepada berbagai pihak yang telah membantu dalam proses penyelesaian Buku ini. Semoga Buku ini dapat menjadi sumber referensi dan literatur yang mudah dipahami.

Padang, Juli 2023
Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
INDUKSI MATEMATIKA, TEOREMA BINOMIAL

Oleh Samuel Urath

1.1 Induksi Matematika

Suatu alat berharga untuk membuktikan hasil-hasil yang terkait dengan bilangan bulat Z baik bulat positif Z^+dan bulat negatif Z^-atau hubungan tertentu yang dapat diperluas berlaku untuk semua bilangan asli N adalah Induksi matematika. Hasil-hasil tersebut tentang penjumlahan, perkalian dan hubungan tertentu dapat berupa kesamaan, ketidaksamaan, keterbagian atau diferensial. Induksi Matematika juga merupakan salah satu metode dengan penalaran deduktif untuk pembuktian dari berbagai teorema yang merupakan bagian dari Teori Bilangan serta dalam bidang matematika terkait. Menurut (Sukirman, 2016) Induksi Matematika adalah salah satu argumentasi pembuktian suatu teorema atau pernyataan matematika yang semesta pembicaraannya himpunan bilangan bulat atau lebih khusus himpunan bilangan asli. Induksi matematika menggunakan notasi jumlah (*summation*) dan notasi kali (*products*). Notasi-notasi ini bermanfaat untuk menyederhanakan tulisan menjadi lebih ringkas dan mudah untuk dipahami.

1.1.1 Notasi Jumlah dan Notasi Kali

Notasi jumlah digunakan untuk menuliskan penjumlahan bilangan secara singkat yang dilambangkan dengan Σ dibaca sigma penjumlahan. Notasi kali digunakan untuk menuliskan

perkalian bilangan secara singkat yang dilambangkan dengan Π dibaca sigma perkalian, kedua notasi tersebut didefenisikan sebagai berikut:

$$\sum_{i=1}^{r} X_i = X_1 + X_2 + \cdots + X_r \text{ untuk notasi jumlah dan}$$

$$\prod_{i=1}^{r} X_i = X_1 . X_2 \ldots X_r \text{ untuk notasi kali}$$

Huruf i dari indeks pada bentuk diatas disebut variabel *dummy* karena dapat berubah sesuai dengan himpunan bilangannya. Indeks i = 1 adalah batas bawah atau *lower limit* dan i = r adalah batas atas atau *upper limit*. Catatan: indeks jumlah atau kali tidak wajib dimulai dari bilangan bulat 1 namun dapat juga dimulai dari bilangan bulat bukan 1 dengan ketentuan batas bawah lebih kecil dari batas atas.

Contoh 1:

Tentukanlah hasil jumlah dan hasil kali berikut:

1. $\sum_{i=1}^{4} i$ 2. $\sum_{i=3}^{6} (3i - 1)$ 3. $\prod_{i=1}^{4} i^2$ 4. $\prod_{i=3}^{3} 2^i$

Solusi 1:

1. $\sum_{i=1}^{4} i = 1 + 2 + 3 + 4 = 10$

2. $\sum_{i=3}^{6} (3i - 1) = (3(3) - 1) + (3(4) - 1) + (3(5) - 1) + (3(6) - 1)$

$= 8 + 11 + 14 + 17$

$= 10$

3. $\prod_{i=1}^{4} i^2 = 1^2 . 2^2 . 3^2 . 4^2$

$= 1 . 4 . 9 . 16 = 576$

4. $\prod_{i=3}^{5} 2^i = 2^3 . 2^4 . 2^5$

$= 8 . 16 . 32 = 4096$

Sifat 1

sifat notasi jumlah:

a. $\sum_{i=r}^{s} tx_i = t \sum_{i=r}^{s} x_i$

b. $\sum_{i=r}^{s} (x_i + y_i) = \sum_{i=r}^{s} x_i + \sum_{i=r}^{s} y_i$

c. $\sum_{i=a}^{b} \sum_{j=c}^{d} x_i y_j = \left(\sum_{i=a}^{b} x_i \right) \left(\sum_{j=c}^{d} y_j \right)$

d. $\sum_{i=a}^{b} \sum_{j=c}^{d} x_i y_j = \sum_{j=c}^{d} \sum_{i=a}^{b} x_i y_j$

Bukti Sifat 1

a. $\sum_{i=r}^{s} tx_i = tx_r + tx_{r+1} + \cdots + tx_s = t(x_r + x_{r+1} + \cdots + x_s) = t\sum_{i=r}^{s} x_i$ ■

b. $\sum_{i=r}^{s} (x_i + y_i) = (x_r + y_r) + (x_{r+1} + y_{r+1}) + \cdots + (x_s + y_s)$

$$= (x_r + x_{r+1} + \cdots + x_s) + (y_r + y_{r+1} + \cdots + y_s)$$

$$= \sum_{i=r}^{s} x_i + \sum_{i=r}^{s} y_i \text{ ■}$$

Bukti c dan d untuk Latihan.

Contoh 2:

Tentukanlah hasil jumlah dan hasil kali berikut berdasarkan sifat 1:

1. $\sum_{i=2}^{4} 3i$ 2. $\sum_{i=1}^{2}\sum_{j=3}^{4} ij$

Solusi 2:

1. $$\sum_{i=2}^{4} 3i = 3\sum_{i=2}^{4} i \qquad \text{(sifat 1a)}$$

$$3(2) + 3(3) + 3(4) = 3(2 + 3 + 4)$$

$$6 + 9 + 12 = 3(9)$$

$$27 = 27$$

2. $$\sum_{i=1}^{2}\sum_{j=3}^{4} ij = \left(\sum_{i=1}^{2} i\right)\left(\sum_{j=3}^{4} j\right) \qquad \text{(sifat 1c)}$$

$$\sum_{i=1}^{2} i(3+4) = (1+2)(3+4)$$

$$\sum_{i=1}^{2} 7i = (3)(7)$$

$$7(1+2) = (3)(7)$$

$$7(3) = (3)(7)$$

$$21 = 21$$

1.1.2 Prinsip Induksi Matematika

Telah dijelaskan diatas bahwa salah satu argumentasi pembuktian suatu pernyataan matematika yang semesta pembicaraannya himpunan bilangan bulat yang dilambangkan dengan Z atau lebih khusus pada bilangan asli yang dilambangkan dengan N adalah induksi matematika. Misalkan terdapat pernyataan matematika berikut:

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1), \forall\, n \in N$$

Terhadap pernyataan matematika diatas, benarkah pernyataan tersebut? Untuk menjawab pernyataan tersebut maka dapat mencoba dengan mensubstitusikan n dalam pernyataan tersebut dengan sembarang bilangan asli N.

Jika $n = 1$ maka $1 = \frac{1}{2}1(1+1) = \frac{1}{2}(2)$ atau $1 = 1$ bernilai benar

Jika $n = 2$ maka $1 + 2 = \frac{1}{2}2(2+1) = \frac{1}{2}(6)$ atau $3 = 3$ bernilai benar

Jika $n = 3$ maka $1 + 2 + 3 = \frac{1}{2}3(3+1) = \frac{1}{2}(12)$ atau $6 = 6$ juga bernilai benar dan seterusnya.

Jika pengerjaan diatas dilanjutkan dengan bilangan asli selain diatas maka pasti pernyataan tersebut mempunyai nilai benar. Apakah dengan mensubstitusikan n pada pernyataan diatas

sebagai contoh sehingga diperoleh pernyataan yang nilainya benar sudah dapat membuktikan kebenaran pernyataan tersebut? dalam matematika, pemberian beberapa contoh seperti di atas belum sepenuhnya memberikan nilai kebenaran dari pernyataan yang berlaku pada himpunan semestanya. Himpunan semesta pada pernyataan di atas adalah himpunan semua bilangan asli N. Selanjutnya dapat memberikan contoh untuk tiap bilangan asli N pada pernyataan tersebut dan jika masing-masing memperoleh pernyataan yang benar maka hal tersebut dapat merupakan bukti kebenaran dari pernyataan itu. Akan tetapi, hal ini tidak efisien dan tidak mungkin kita lakukan karena banyaknya himpunan bilangan asli N ada tak berhingga.

Salah satu cara pemecahan masalah di atas adalah dengan memandang ruas pertama dari pernyataan itu sebagai deret aritmetika dengan suku pertama a = 1, bedanya b = 1, suku terakhirnya ialah $U_n = n$ dan memiliki n buah suku. Maka, jumlah deret itu adalah:

$$\begin{aligned} S_n &= \frac{1}{2}n(a + U_n) \\ &= \frac{1}{2}n(1 + n) \\ &= \frac{1}{2}n(n + 1) \end{aligned}$$

$\frac{1}{2}n(n + 1)$ adalah merupakan ruas kanan dari pernyataan matematika yang dibuktikan.

Metode lain untuk membuktikan pernyataan matematika tersebut diatas adalah dengan prinsip induksi matematika, jika ada sebuah pernyataan P(n) akan dibuktikan benar untuk setiap n bilangan bulat positif (Hasan B, 2021). Pembuktian tersebut dikerjakan dengan tiga prosedur berikut:

1. Buktikan kebenaran pernyataan tersebut untuk $n = 1$ atau tunjukan bahwa P(1) benar.
2. Andaikan benar pernyataan tersebut untuk $n = k$, dengan $k \in N$ atau andaikan bahwa P(k) benar.

3. Selanjutnya buktikan benar pernyataan tersebut untuk $n = k + 1$ atau tunjukan bahwa $P(k + 1)$ benar.

Jika prosedur 1, 2 dan 3 dapat ditunjukkan kebenarannya maka dapat disimpulkan bahwa P(n) benar untuk setiap bilangan asli n. Karena prosedur 1, yaitu P(1) benar dan karena prosedur 2 maka P(2) benar. Selanjutnya karena P(2) benar, menurut prosedur 2 maka P(3) juga benar. Menurut prosedur 2 lagi maka P(4) juga benar dan seterusnya sehingga P(n) benar. Prosedur 1 di atas sering disebut basis atau dasar induksi dan prosedur 2 disebut langkah induksi.
Selanjutnya akan dibuktikan contoh diatas dengan menggunakan prinsip induksi matematika berikut:

Contoh 3:
Buktikan bahwa $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1), \forall\, n \in N$

Bukti 3:
Misalkan P(n): $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1)$

Prosedur 1
Untuk $n = 1$, $1 = \frac{1}{2}1(1 + 1) = \frac{1}{2}(2) = 1$, P(1) benar

Prosedur 2
Andaikan $n = k$, P(k): $1 + 2 + 3 + \cdots + k = \frac{1}{2}k(k + 1)$ benar untuk suatu bilangan asli k.

Prosedur 3
Selanjutnya harus ditunjukan bahwa $n = k + 1$, $P(k + 1)$ benar
$1 + 2 + 3 + \cdots + k + (k + 1) = \frac{1}{2}(k + 1)(k + 1 + 1)$

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

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

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

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

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

Jadi $1 + 2 + 3 + \cdots + k + (k+1) = \frac{1}{2}(k+1)(k+1+1)$, berarti $P(k+1)$ benar

Sehingga $P(n)$ benar $\forall\ n \in N$.

Contoh 4:

Buktikan untuk semua $n \in Z^+$ dan $n \geq 6, 4n < n^2 - 7$

Bukti 4:

Misalkan $P(n)$: $4n < n^2 - 7, n \geq 6$

Prosedur 1

Karena $n \geq 6$, maka

Untuk $n = 6$, $6 < 6^2 - 7$, $P(1)$ benar

Prosedur 2

Andaikan $n = k$, $P(k)$: $4k < k^2 - 7$ benar untuk $k \geq 6$.

Prosedur 3

Selanjutnya harus ditunjukan bahwa $n = k + 1$, $P(k+1)$ benar

$4(k+1) < (k+1)^2 - 7$

$4(k+1) = (4k+4) < (k^2 - 7) + 4$

$(4k+4) < (k^2 - 7) + 13$, sebab $4 < 13$

$(4k+4) < (k^2 - 7) + (2k+1)$, sebab $(2k+1) \geq 13$

untuk $n \geq 6$

$(4k+4) < (k+1)^2 - 7$

Jadi $(4k+4) < (k+1)^2 - 7$, berarti $P(k+1)$ benar

Sehingga $P(n)$ benar untuk semua $n \geq 6$.

1.2 Teorema Binomial

Sebelum membahas lebih jauh tentang teorema binomial, maka kita mengingat kembali konsep kombinasi dari sejumlah r objek yang diambil dari n objek. Banyaknya kombinasi tersebut $r \leq n$ adalah:

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

Contoh 5:
Diberikan tiga kotak berisi satu bola merah dan satu bola putih untuk setiap kotak. Dari kotak-kotak tersebut diambil satu bola sehingga total tiga bola yang diambil. Tentukanlah:

1. Banyaknya cara pengambilan 3 bola tersebut agar terambil semua bola merah.
2. Banyaknya cara pengambilan 3 bola tersebut agar terambil 2 bola merah.
3. Banyaknya cara pengambilan 3 bola tersebut agar terambil 1 bola merah.
4. Banyaknya cara pengambilan 3 bola tersebut agar tidak terambil bola merah.

Solusi 5:

1. Banyaknya cara pengambilan 3 bola tersebut, agar terambil semua bola merah.
$$\frac{3!}{(3-3)!\, 3!} = \frac{3!}{0!\, 3!} = 1$$
Jadi ada 1 cara agar terambil bola merah semua.
2. Banyaknya cara pengambilan 3 bola tersebut agar terambil 2 bola merah.
$$\frac{3!}{(3-2)!\, 2!} = \frac{3!}{1!\, 2!} = 3$$
Jadi ada 3 cara agar terambil 2 bola merah.

3. Banyaknya cara pengambilan 3 bola tersebut agar terambil 1 bola merah.

$$\frac{3!}{(3-1)!\,1!} = \frac{3!}{2!\,1!} = 3$$

Jadi ada 3 cara agar terambil 1 bola merah.

4. Banyaknya cara pengambilan 3 bola tersebut agar tidak terambil bola merah.

$$\frac{3!}{(3-0)!\,1!} = \frac{3!}{3!\,1!} = 1$$

Jadi ada 1 cara agar tidak terambil bola merah.

Contoh 5 diatas 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 di atas terdiri dari 3 faktor dan masing-masing faktor berturut-turut diambil dari faktor pertama, faktor kedua dan faktor ketiga dari ruas pertama. Memperhatikan Contoh 5 di atas maka

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

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

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

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

pada kesamaan terakhir itu jika suku-suku sejenisnya dioperasikan maka akan diperoleh:

$$(\mathrm{m}+\mathrm{p})^3 = m^3 + 3m^2p + 3mp^2 + p^3$$

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:

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

Periksalah kebenaran kesamaan-kesamaan di bawah ini dengan menggunakan argumentasi yang mirip dengan ilustrasi diatas.

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

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

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

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

Kesamaan tersebut adalah merupakan dugaan karena khususnya kesamaan terakhir diperoleh dengan penalaran induktif. Maka perlu dibuktikan kebenarannya. Kita akan membuktikan kebenarannya, tetapi kita perlu mendahuluinya dengan memanfaatkan rumus kombinasi.

Dari rumus kombinasi di atas, yaitu:

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

kita dapat memahami bahwa

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

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

Teorema 1.

Jika r ≤ n maka $\binom{n}{r} = \binom{n}{n-r}$

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

Teorema 2.

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

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

Bukti:

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

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

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

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

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

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

Setelah terbukti maka dilanjutkan dengan pembuktian kebenaran penjabaran suku dua berpangkat n di atas dengan memilih a = 1 dan x = a yang akan menemukan sebuah teorema yang disebut Teorema Binomial.

Teorema 3. (Teorema Binomial)

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

$\forall\, n \in N$

Bukti:

Membuktikan Terema 3 diatas dengan menggunakan induksi matematika.

Misalkan,

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

Prosedur 1

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

Prosedur 2

Andaikan $n = k,\ P(k)$:

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

benar untuk suatu bilangan asli k.

Prosedur 3

Selanjutnya harus ditunjukan bahwa $n = k+1$, $P(k+1)$ benar

$$\begin{aligned}(1+a)^{k+1} &= (1+a)^k(1+a)^1 \\ &= \left[\binom{k}{0} + \binom{k}{1}a + \binom{k}{2}a^2 + \binom{k}{3}a^3 + \cdots + \binom{k}{k}a^k\right](1+a) \\ &= \binom{k}{0}\left[\binom{k}{0} + \binom{k}{1}\right]a + \left[\binom{k}{1} + \binom{k}{2}\right]a^2 + \cdots + \left[\binom{k}{k-1} + \binom{k}{k}\right]a^k + \binom{k}{k}a^{k+1} \\ &= \binom{k+1}{0} + \binom{k+1}{1}a + \binom{k+1}{2}a^2 + \cdots + \binom{k+1}{k}a^k + \binom{k+1}{k+1}a^{k+1}\end{aligned}$$

Jadi $P(k+1)$ benar

Sehingga P(n) benar ∀ n ∈ N.
Koefisien-koefisien a pada ruas kanan teorema 3 disebut koefisien binomial.

Contoh 6:
Koefisien x^9 dari penjabaran $(1 + x)^{12}$ adalah?

Solusi 6:

$$\binom{12}{9} = \frac{12 \,.\, 11 \,.\, 10}{1 \,.\, 2 \,.\, 3} = 660$$

Apabila pada teorema binomial diatas $a = 1$, maka:

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

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

sehingga diperolah teorema berikut ini.

Teorema 4.

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

Perhatikan penurunan rumus berikut:

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

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

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

Hasilnya dinyatakan dengan teorema berikut:

Teorema 5.
Jika n, m dan k bilangan-bilangan asli dengan n > k > m maka

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

Contoh 7:
Sebuah organisasi terdiri dari 15 orang anggota. Organisasi tersebut ingin membentuk pengurus yang terdiri 5 orang. Pengurus inti terdiri dari 2 orang. Tentukan banyaknya pilihan pengurus dari perkumpulan tersebut.

Solusi 7:
$$\binom{15}{5}\binom{5}{2} = \frac{15\,.\,14\,.\,13.\,12\,.\,11}{1\,.\,2\,.\,3\,.\,4\,.\,5} = 30030$$

DAFTAR PUSTAKA

Basri Hasan. 2021. Teori Bilangan. Purbalingga: CV. Eureka Media Aksara.

Sukirman. 2016. Teori Bilangan. Tangerang Selatan: Universitas Terbuka.

BAB 2
KETERBAGIAN PADA BILANGAN BULAT

Oleh Yunita Oktavia Wulandari

2.1 Keterbagian

Semesta pembicaraan dalam teori bilangan ini adalah himpunan semua bilangan bulat yang dinyatakan dengan huruf-huruf latin kecil seperti a, b, c, dan sebagainya. Salah satu hal penting yang dipelajari dalam teori bilangan adalah tentang keterbagian bilangan bulat (Musthofa, 2011) .

Definisi 1 Keterbagian Bilangan Bulat

Untuk setiap bilangan bulat a dan b, maka dikatakan a membagi b jika terdapat suatu bilangan bulat c sedemikian sehingga $b = ac$ (Schroeder, 1989; Handayani and Yulina, 2015; Correlat and Test, 2019).

Notasi:

Jika a membagi b dituliskan $a \mid b$ dan jika a tidak membagi b dituliskan $a \nmid b$.

Jika a membagi b berarti a merupakan pembagi atau faktor dari b.

Untuk lebih jelasnya dapat dilihat di Tabel 2.1 berikut.

Tabel 2.1 Notasi dan Cara Membaca Keterbagian

Notasi	Dibaca
$a \mid b$	a membagi b
	a faktor dari b
	b habis dibagi a
	b kelipatan dari a
$a \nmid b$	a tidak membagi b
	a bukan faktor dari b
	b tidak habis dibagi a
	b bukan kelipatan dari a

Catatan: Notasi " $a \mid b$ " berbeda dengan "a/b" atau "$a \div b$"

"$a \mid b$" berarti bahwa a membagi b

"a/b" atau "$a \div b$" berarti a dibagi b

Contoh

1. $2 \mid 6$ benar karena terdapat $3 \in \mathbb{Z}$ sedemikian sehingga $6 = 2.3$
2. $3 \nmid 5$ benar karena tidak ada bilangan bulat a sedemikian sehingga $5 = 3a$.
3. $-3 \mid 6$ benar karena terdapat $-2 \in \mathbb{Z}$ sedemikian sehingga $6 = (-3)(-2)$.
4. $0 \mid 0$ benar karena terdapat $7 \in \mathbb{Z}$ sedemikian sehingga $0 = 7.0$

Teorema 1. Sifat-Sifat Dasar Keterbagian

Jika $m, n, p, q, k \in \mathbb{Z}$ dan $m \neq 0$, maka

a. $m \mid 0,\ 1 \mid n,$ dan $n \mid n$
b. Jika $m \mid 1$, maka $m = 1$ atau $m = -1$
c. Jika $m \mid n$ dan $n \mid k$, maka $m \mid k$
d. Jika $m \mid n$ dan $k \mid r$, maka $mk \mid nr$
e. Jika $m \mid n$ dan $n \mid m$, maka $m = \pm n$
f. Jika $m \mid p$ dan $m \mid q$, maka $m \mid p + q$
g. Jika $m \mid n$ dan $m \mid k$, maka $m = un \pm vk, \forall u, v \in \mathbb{Z}$
(Hardy and Wright, 1960; Sukirman, 2017)

Bukti

a. (i) Akan ditunjukkan bahwa $m \mid 0$.
Ambil sebarang $m \in \mathbb{Z}$, maka terdapat $0 \in \mathbb{Z}$, sehingga $m.0 = 0$. Jadi terbukti bahwa $m \mid 0$.
(ii) Akan ditunjukkan bahwa $1 \mid n$.
Ambil sebarang $n \in \mathbb{Z}$, maka terdapat $1 \in \mathbb{Z}$, sehingga $1.n = n$. Jadi terbukti bahwa $1 \mid n$.

(iii) Buktikan sebagai latihan.

b. Jika $m \mid 1$, maka $m = 1$ atau $m = -1$
Bukti
Perhatikan $m \mid 1$ berarti ada $\frac{1}{m} \in \mathbb{Z}$ sedemikian sehingga $1 = m(\frac{1}{m})$.
$\frac{1}{m} \in \mathbb{Z}$ berarti $m = 1$ atau $m = -1$.
Jadi terbukti jika Jika $m \mid 1$, maka $m = 1$ atau $m = -1$.

c. Jika $m \mid n$ dan $n \mid k$, maka $m \mid k$
Bukti
Diketahui: $m \mid n$ dan $n \mid k$

Akan ditunjukkan bahwa $m \mid k$.
Perhatikan
$m \mid n$ maka $n = m.a$, untuk suatu $a \in \mathbb{Z}$
$n \mid k$ maka $k = n.b$, untuk suatu $b \in \mathbb{Z}$
$k = n.b = (m.a)b = m.(ab)$, $ab \in \mathbb{Z}$ ... sifat tertutup $\mathbb{Z}$
Karena $k = m(ab)$ dan $ab \in \mathbb{Z}$ maka $m \mid k$.
Jadi terbukti jika $m \mid n$ dan $n \mid k$, maka $m \mid k$.

d. Jika $m \mid n$ dan $k \mid r$, maka $mk \mid nr$
Bukti
Diketahui: $m \mid n$ dan $k \mid r$
Akan ditunjukkan bahwa $mk \mid nr$.
Perhatikan
$m \mid n$ maka $n = m.a$, untuk suatu $a \in \mathbb{Z}$
$k \mid r$ maka $r = k.b$, untuk suatu $b \in \mathbb{Z}$
$n.r = (ma)(k.b)$
$= m.a.k.b$
$= m.k.a.b$ ... sifat komutatif bilangan bulat
$= m.k.(ab)$
Karena $n.r = m.k.(ab)$ dan $ab \in \mathbb{Z}$ maka $mk \mid nr$.
Jadi terbukti jika $m \mid n$ dan $k \mid r$, maka $mk \mid nr$.

e. Jika $m \mid n$ dan $n \mid m$, maka $m = \pm n$.
Bukti
Diketahui: $m \mid n$ dan $n \mid m$
Akan ditunjukkan bahwa $m = \pm n$.
Perhatikan
$m \mid n$ maka $n = m.a$, untuk suatu $a \in \mathbb{Z}$
$n \mid m$ maka $m = n.b$, untuk suatu $b \in \mathbb{Z}$
$m = n.b$
$= m.(a.b)$
$m.1 = m(ab)$ maka $ab = 1$
Karena $a, b \in \mathbb{Z}$, dan $ab = 1$ maka ada dua kemungkinan yaitu $a = -1$ dan $b = -1$ atau $a = 1$ dan $b = 1$.
Untuk $b = -1$, maka $m = n.b = n(-1) = -n$

Untuk $b = 1$, maka $m = n.b = n(1) = n$.
Jadi terbukti bahwa jika $m \mid n$ dan $n \mid m$, maka $m = \pm n$.

f. Jika $m \mid p$ dan $m \mid q$, maka $m \mid p + q$.
Diketahui: $m \mid p$ dan $m \mid q$
Akan ditunjukkan bahwa $m \mid p + q$.
Perhatikan
$m \mid p$ maka $p = m.a$, untuk suatu $a \in \mathbb{Z}$
$m \mid q$ maka $q = m.b$, untuk suatu $b \in \mathbb{Z}$
$p + q = m.a + m.b$
$= m(a + b)$, $a + b \in \mathbb{Z}$ ... sifat tertutup $\mathbb{Z}$
Karena $p + q = m(a + b)$ dan $a + b \in \mathbb{Z}$, maka $m \mid p + q$.
Jadi terbukti bahwa jika $m \mid p$ dan $m \mid q$, maka $m \mid p + q$.

g. Buktikan sebagai latihan.

Contoh

1. Buktikan jika x genap, maka $x^2 + 2x + 4$ habis dibagi oleh 4.
Bukti
x genap, maka $2 \mid x$
Perhatikan
$2 \mid x$ dan $2 \mid x$, maka berdasarkan teorema 2.1 bagian d didapatkan $2.2 \mid x.x \rightarrow 2 \mid x$, maka berdasarkan teorema 2.1 bagian d didapatkan $2.2 \mid x.x \rightarrow 4 \mid x^2$ ...(i)
$2 \mid 2$ dan $2 \mid x$, maka berdasarkan teorema 2.1 bagian d didapatkan $2.2 \mid 2.x \rightarrow 4 \mid 2x$ ...(ii)

Jelas bahwa $4 \mid 4$ ...(iii)

Karena (i), (ii), (iii), maka berdasarkan Teorema 2.1 bagian f didapatkan $4 \mid x^2 + 2x + 4$.
Jadi, terbukti jika x genap, maka $x^2 + 2x + 4$ habis dibagi oleh 4 (Correlat and Test, 2019).

2. Jika 3 | $a + 4b$ tunjukkan bahwa 3 | $(10a + b)$

   Penyelesaian

   Perhatikan 3 | $a + 4b$ maka 3 | $a + b + 3b$

   Karena 3 | $a + b + 3b$ dan 3 | $3b$ maka 3 | $a + b$

   $10a + b = 9a + a + b$

   Jelas bahwa 3 | $9a$ karena $9a = 3(6a)$ untuk suatu $6a \in \mathbb{Z}$.

   Karena 3 | $9a$ dan 3 | $a + b$, maka 3 |$9a + a + b$.

   Jadi terbukti jika 3 | $a + 4b$ maka 3 | $(10a + b)$.

2.2 Ciri-Ciri Bilangan Habis Dibagi

Berikut merupakan ciri-ciri bilangan habis dibagi.

1. Keterbagian oleh 2

   Suatu bilangan habis dibagi 2, jika n digit terakhirnya dapat dibagi oleh 2.

   Bukti

   Misalkan diberikan bilangan $a = a_n a_{n-1} \dots a_3 a_2 a_1 a_0$

   Perhatikan

   $a = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 1000a_3 + 100a_2 + 10a_1 + a_0$

   $= 2(10^{n-1}.5a_n + 10^{n-2}.5a_{n-1} + \cdots + 10^2.5a_3 + 10.5a_2 + 5a_1) + a_0$

   Karena $2 \mid 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 1000a_3 + 100a_2 + 10a_1$

   dan supaya a habis dibagi 2, maka haruslah $2 \mid a_0$.

   Jadi terbukti jika suatu bilangan habis dibagi 2, jika n digit terakhirnya dapat dibagi oleh 2.

   Contoh

   a. Apakah 1234567898 habis dibagi 2?

      Iya karena digit terakhirnya 8 dan $2 \mid 8$, maka $2 \mid 1234567898$.

   b. Apakah 2345678943 habis dibagi 2?

      Tidak karena digit terakhirnya 3, tetapi $2 \nmid 3$, sehingga $2 \nmid 2345678943$.

2. Keterbagian oleh 3

   Suatu bilangan habis dibagi 3 jika jumlah semua digitnya habis dibagi 3.

   Buktikan sebagai latihan.

   Contoh

   a. Apakah 1234567998 habis dibagi 3?

      Iya, perhatikan $1 + 2 + 3 + 4 + 5 + 6 + 7 + 9 + 9 + 8 = 54$

      $3 \mid 54$ maka $3 \mid 1234567998$.

      Coba cek dengan menggunakan kalkulator apakah benar 1234567998 habis dibagi 3.

   b. Apakah 1234567883 habis dibagi 3?

      Tidak, perhatikan $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 8 + 3 = 47$, akan tetapi $3 \nmid 47$.

      Sehingga $3 \nmid 1234567883$.

      Coba cek menggunakan kalkulator.

3. Keterbagian oleh 4

   Suatu bilangan habis dibagi 4 jika dua digit terakhirnya habis dibagi 4.

   Buktikan sebagai latihan.

   Contoh

   a. Apakah 1234567996 habis dibagi 4?

      Iya, dua digit terahir dari 1234567996 adalah 96. Perhatikan $4 \mid 96$ karena ada $24 \in \mathbb{Z}$ sehingga $96 = 4(24)$. Oleh karena itu, $4 \mid 1234567996$.

      Coba cek menggunakan kalkulator apakah 1234567996 habis dibagi 4.

   b. Apakah 1234567934 habis dibagi 4?

      Tidak, dua digit terahir dari 1234567934 adalah 34. Perhatikan $4 \nmid 34$ karena tidak ada $a \in \mathbb{Z}$ sehingga $34 = 4(a)$. Oleh karena itu, $4 \nmid 1234567934$.

Coba cek menggunakan kalkulator apakah 1234567934 habis dibagi 4.

4. Keterbagian oleh 5
   Suatu bilangan habis dibagi 5 jika digit terakhirnya 0 atau 5.
   Buktikan sebagai latihan.
   Contoh
   a. Apakah 1234567995 habis dibagi 5?
      Iya, digit terahir dari 1234567995 adalah 5. Oleh karena itu, $5 \mid 1234567995$.
      Coba cek menggunakan kalkulator apakah 1234567995 habis dibagi 5.
   b. Apakah 1234567934 habis dibagi 5?
      Tidak, digit terahir dari 1234567934 adalah 4. Oleh karena itu, $5 \nmid 1234567934$.
      Coba cek menggunakan kalkulator apakah 1234567934 habis dibagi 5.

5. Keterbagian oleh 6
   Suatu bilangan habis dibagi 6 jika bilangan tersebut habis dibagi 2 dan 3.
   Buktikan sebagai latihan.
   Contoh
   Apakah 1234567998 habis dibagi 6?
   Iya, perhatikan $1 + 2 + 3 + 4 + 5 + 6 + 7 + 9 + 9 + 8 = 54$
   $3 \mid 54$ maka $3 \mid 1234567998$.
   Digit terakhir 1234567998 adalah 8 dan $2 \mid 8$, maka $2 \mid 1234567998$.
   Karena $2 \mid 1234567998$ dan $3 \mid 1234567998$ maka $6 \mid 1234567998$.
   Coba cek dengan menggunakan kalkulator apakah benar 1234567998 habis dibagi 6.

6. Keterbagian oleh 8

   Suatu bilangan habis dibagi 8 jika tiga digit terakhirnya habis dibagi 8.

   Buktikan sebagai latihan.

   Contoh

   Apakah 1234567984 habis dibagi 8?

   Iya, tiga digit terahir dari 1234567984 adalah 984. Perhatikan $8 \mid 984$ karena ada $123 \in \mathbb{Z}$ sehingga $984 = 8(123)$. Oleh karena itu, $8 \mid 1234567984$.

   Coba cek menggunakan kalkulator apakah 1234567984 habis dibagi 8.

7. Keterbagian oleh 9

   Suatu bilangan habis dibagi 9 jika jumlah semua digitnya habis dibagi 9.

   Buktikan sebagai latihan.

   Contoh

   a. Apakah 1234567998 habis dibagi 9?

      Iya, perhatikan $1 + 2 + 3 + 4 + 5 + 6 + 7 + 9 + 9 + 8 = 54$

      $9 \mid 54$ maka $9 \mid 1234567998$.

      Coba cek dengan menggunakan kalkulator apakah benar 1234567998 habis dibagi 9.

   b. Apakah 1234567883 habis dibagi 9?

      Tidak, perhatikan $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 8 + 3 = 47$, akan tetapi $9 \nmid 47$.

      Sehingga $9 \nmid 1234567883$.

      Coba cek menggunakan kalkulator.

8. Keterbagian oleh 10

   Suatu bilangan habis dibagi 10 jika digit terakhirnya adalah 0.

   Buktikan sebagai latihan.

Contoh

a. Apakah 1234567990 habis dibagi 10?
   Iya, perhatikan digit terakhir dari 1234567990 adalah 0. Maka 10 |1234567990.
   Coba cek dengan menggunakan kalkulator apakah benar 1234567990 habis dibagi 10.
b. Apakah 1234567883 habis dibagi 10?
   Tidak, perhatikan digit terakhir dari 1234567990 adalah 3. Maka 10 ∤ 1234567883.
   Coba cek dengan menggunakan kalkulator.

Latihan Soal

1. Tunjukkan bahwa $2 \mid n^3 + 5n$,untuk suatu $n \in \mathbb{N}$.
2. Bilangan enam digit $a1989b$ habis dibagi oleh 72. Tentukan nilai a dan b.
3. Apakah 987654321 habis dibagi 27? Jelaskan jawaban Saudara.
4. Tentukan apakah bilangan 6512347998 habis dibagi oleh:
   a. Bilangan 2
   b. Bilangan 3
   c. Bilangan 4
   d. Bilangan 5
   e. Bilangan 6
   f. Bilangan 8
   g. Bilangan 9
   h. Bilangan 10

   Jelaskan jawaban Saudara.

DAFTAR PUSTAKA

Correlat, G. S. and Test, L. M. (2019) :'1', 1 - 1 - بابسأ طابترلاا تياذلا(c), pp. 1–13.

Handayani, R. and Yulina (2015) *Teori Bilangan*, *Paper Knowledge . Toward a Media History of Documents*.

Hardy, G. H. . and Wright, E. M. (1960) 'An theory introduction'.

Schroeder, M. R. (1989) 'Number theory', *IEEE Potentials*, 8(3), pp. 14–17. doi: 10.1109/45.41531.

BAB 3
SISTEM BILANGAN

Oleh Rifka Agustianti

3.1 Jenis-jenis Sistem Bilangan

Sistem bilangan ialah kaidah ataupun lambang yang dipakai dalam menguraikan serangkaian hal dengan spesifik. Berikut ini jenis-jenis sistem bilangan, sebagai berikut (Nengsih and Samosir, 2020) :

1. Sistem Bilangan Biner (basis 2) merupakan sebuah kaidah ataupun teknik membilangan sebuah bilangan melalui penggunaan dua lambang angka yakni '0' serta '1'
2. Sistem bilangan desimal (basis 10) merupakan sebuah kaidah ataupun teknik membilangan sebuah bilangan melalui penggunaan sepuluh lambang angka yakni '0' ,'1', '2','3','4','5','6','7','8' serta '9'
3. Sistem bilangan oktal (basis 8) merupakan sebuah kaidah ataupun teknik membilangan sebuah bilangan melalui penggunaan delapan lambang angka yakni '0' ,'1', '2', '3', '4','5','6', serta '7'
4. Sistem bilangan heksadesimal (basis 16) merupakan sebuah kaidah ataupun teknik membilangan sebuah bilangan melalui penggunaan 16 variasi lambang angka dan huruf yakni '0' ,'1', '2', '3', '4', '5', '6', '7', '8','9','A','B', 'C','D','E', dan 'F' dimana 'A' sama dengan 10, 'B' sama dengan 11, dan seterusnya

3.2 Konversi Sistem Bilangan

Berbagai jenis sistem bilangan dapat dikonversi dari sistem bilangan yang satu ke sistem bilangan lainnya. Berikut ini disajikan Teknik mengubah sistem bilangan biner, oktal, serta heksadesimal ke sistem bilangan desimal dan sebaliknya melalui teknik menjumlahkan hasil dari perkalian bilangan dengan basis bilangan yang dipangkatkan 0,1,2, dan seterusnya diawali dari sebelah kanan

3.2.1 Konversi Sistem Bilangan Biner ke Desimal

Teknik mengubah sistem bilangan biner ke desimal yaitu dengan menjumlahkan hasil dari perkalian bilangan dengan basis 2 yang dipangkatkan 0, 1, 2, dan seterusnya dimulai dari kanan.

Contoh 1 :

$1010011_{(2)}$ = . . . $_{(10)}$

$$1010011_{(2)} = 1.2^0 + 1.2^1 + 0.2^2 + 0.2^3 + 1.2^4 + 0.2^5 + 1.2^6$$

$$= 1 + 2 + 0 + 0 + 16 + 0 + 64 = 83$$

Sehingga, $1010011_{(2)} = 83_{(10)}$

3.2.2 Konversi Sistem Bilangan Oktal ke Desimal

Teknik mengubah sistem bilangan oktal ke desimal yaitu dengan menjumlahkan hasil dari perkalian bilangan dengan basis 8 yang dipangkatkan 0, 1, 2, dan seterusnya dimulai dari kanan

Contoh 2 :

$3174_{(8)}$ = . . . $_{(10)}$

$$3174_{(8)} = 4.8^0 + 7.8^1 + 1.8^2 + 3.8^3$$

$$= 4 + 56 + 64 + 1536 = 1660$$

Sehingga, $3174_{(8)} = 1660_{(10)}$

3.2.3 Konversi Sistem Bilangan Heksadesimal ke Desimal

Teknik mengubah sistem bilangan heksadesimal ke desimal yaitu dengan menjumlahkan hasil dari perkalian bilangan dengan basis 16 yang dipangkatkan 0, 1, 2, dan seterusnya dimulai dari kanan

Contoh 3 :

$2AF3_{(16)} = \ldots_{(10)}$

$2AF3_{(16)} = 3.16^0 + 15.16^1 + 10.16^2 + 2.16^3$

$= 3 + 240 + 2560 + 8192 = 10995$

$2AF3_{(16)} = 10995_{(10)}$

3.2.4 Konversi Sistem Bilangan Desimal ke Biner

Teknik mengubah sistem bilangan desimal ke biner ialah melalui pembagian bilangan desimal dengan 2 serta menyimpan sisa bagi tiap pembagian sehingga hasil pembagiannya kurang dari 2. Hasil dari konversi tersebut merupakan susunan sisa pembagian dari yang paling terakhir sampai paling dahulu.

Contoh 4 :

$75_{(10)} = \ldots_{(2)}$

$75 : 2 = 37$ sisa 1

$37 : 2 = 18$ sisa 1

$18 : 2 = 9$ sisa 0

$9 : 2 = 4$ sisa 1

$4 : 2 = 2$ sisa 0

$2 : 2 = 1$ sisa 0

$1 : 2 = 0$ sisa 1

Sehingga, $75_{(10)} = 1001011_{(2)}$

3.2.5 Konversi Sistem Bilangan Desimal ke Oktal

Teknik mengubah sistem bilangan desimal ke oktal ialah melalui pembagian bilangan desimal dengan 8 serta menyimpan sisa bagi tiap pembagian sehingga hasil pembagiannya kurang dari 8. Hasil dari konversi tersebut merupakan susunan sisa pembagian dari yang paling terakhir sampai paling dahulu.

Contoh 5 :

$1059_{(10)} = . \ . \ . _{(8)}$

$1059 : 8 = 132$ sisa 3

$132 : 8 = 16$ sisa 4

$16 : 8 = 2$ sisa 0

$2 : 8 = 0$ sisa 2

Sehingga, $1059_{(10)} = 2043_{(8)}$

3.2.6 Konversi Sistem Bilangan Desimal ke Heksadesimal

Teknik mengubah sistem bilangan desimal ke heksadesimal ialah melalui pembagian bilangan desimal dengan 16 serta menyimpan sisa bagi tiap pembagian sehingga hasil pembagiannya kurang dari 16. Hasil dari konversi tersebut merupakan susunan sisa pembagian dari yang paling terakhir sampai paling dahulu.

Contoh 6 :

$10846_{(10)}$ = . . . $_{(16)}$

$10846 : 16 = 677$ sisa 14 (E)

$677 : 16 = 42$ sisa 5

$42 : 16 = 2$ sisa 10 (A)

$2 : 16 = 0$ sisa 2

Sehingga, $10846_{(10)} = 2A5E_{(16)}$

3.2.7 Konversi Sistem Bilangan Selain Desimal

Teknik mengubah sistem bilangan selain desimal yakni mengubah sistem bilangan tersebut ke sistem bilangan desimal terlebih dahulu, misalnya konversi sistem bilangan biner ke oktal, maka sistem bilangan biner diubah dulu ke desimal kemudian ubah ke oktal dengan mengikuti kaidah konversi perkalian dan pembagian di atas.

Contoh 7 : Konversi sistem bilangan biner ke oktal

$101011_{(2)}$ = . . . $_{(8)}$

$$101011_{(2)} = 1.2^0 + 1.2^1 + 0.2^2 + 1.2^3 + 0.2^4 + 1.2^5$$

$$= 1 + 2 + 0 + 8 + 0 + 32 = 43_{(10)}$$

$43 : 8 = 5$ sisa 3

$5 : 8 = 0$ sisa 5

$43_{(10)} = 53_{(8)}$

Sehingga, $101011_{(2)} = 53_{(8)}$

Contoh 8 : Konversi sistem bilangan oktal ke heksadesimal

$776_{(8)}$ = . . . (16)

$776_{(8)} = 6.8^0 + 7.8^1 + 7.8^2$

$= 6 + 56 + 448 = 510_{(10)}$

$510 : 16 = 31$ sisa 14 (E)

$31 : 16 = 1$ sisa 15 (F)

$1 : 16 = 0$ sisa 1

$510_{(10)} = 1FE_{(16)}$

Sehingga, $776_{(8)} = 1FE_{(16)}$

Contoh 9 : Konversi sistem bilangan heksadesimal ke biner

$3F_{(16)}$ = . . . (2)

$3F_{(16)} = 15.16^0 + 3.16^1$

$= 15 + 48 = 63_{(10)}$

$63 : 2 = 31$ sisa 1

$31 : 2 = 15$ sisa 1

$15 : 2 = 7$ sisa 1

$7 : 2 = 3$ sisa 1

$3 : 2 = 1$ sisa 1

$1 : 2 = 0$ sisa 1

$63_{(10)} = 111111_{(2)}$

Sehingga, $3F_{(16)} = 111111$ (2)

3.3 Operasi Penjumlahan dan Pengurangan Sistem Bilangan

3.3.1 Operasi Penjumlahan dan Pengurangan Sistem Bilangan Biner

Pada operasi penjumlahan dan pengurangan sistem bilangan biner berlaku kaidah berikut :

Tabel 3.1 Kaidah Penjumlahan dan Pengurangan Sistem Bilangan Biner

Penjumlahan	Pengurangan
$0 + 0 = 0$	$0 - 0 = 0$
$0 + 1 = 1$	$1 - 0 = 1$
$1 + 0 = 1$	$1 - 1 = 0$
$1 + 1 = 0, carry\ 1$	$0 - 1 = 1, borrow\ 1$

Sumber : (Nengsih and Samosir, 2020)

Contoh 10 :

$0101_{(2)} + 0100_{(2)} = \cdots$

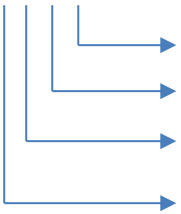
Penyelesaian dari soal di atas dapat diselesaikan melalui teknik bersusun pendek dengan menggunakan kaidah di atas di mulai dari angka yang paling kanan, seperti berikut.

0 1 0 1

0 1 0 0

_____+

1 0 0 1



$1 + 0 = 1$

$0 + 0 = 0$

$1 + 1 = 0, carry\ 1$ ke angka sebelah kirinya

$1 + 0 + 0 = 1$

Contoh 11 :

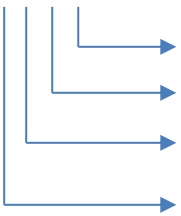
$1001_{(2)} - 0100_{(2)} = \cdots$

1 0 0 1

0 1 0 0

_____-

0 1 0 1



$1 - 0 = 1$

$0 - 0 = 0$

$0 - 1 = 1, borrow\ 1$ dari angka sebelah kirinya

$1 - 1 - 0 = 0$

3.3.2 Operasi Penjumlahan dan Pengurangan Sistem Bilangan Oktal

Pada operasi jumlah bilangan oktal, operasikan dengan berurut berawal dari angka paling kanan. Untuk dua angka yang dijumlah, bila hasil pengoperasiannya melebihi 7 maka akan muncul *carry* 1 yang akan disertakan operasinya dengan angka

di sebelah kirinya, lalu hasil operasi jumlahnya dikurangkan 8 yang akan ditaruh sebagai hasil operasi penjumlahan oktal.

Contoh 12 :

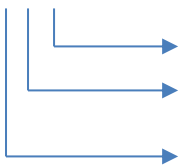
$243_{(8)} + 56_{(8)} = \cdots$

2 4 3

  5 6

_____+

3 2 1



$3 + 6 = 9\ carry\ 1\ (9 - 8) = 1$

$1 + 4 + 5 = 10\ carry\ 1\ (10 - 8) = 2$

$1 + 2 = 3$

Sementara pada operasi pengurangan bilangan oktal melalui pengurangan secara berurut berawal pada angka paling kanan. Bila angka yang dikurangkan lebih besar, maka hasilnya ditaruh sebagai hasil pengurangan oktal, namun bila angka yang dikurangkan lebih kecil, maka muncul *borrow* (pinjam) 1 dari angka di sebelah kirinya. Jika pada bilangan desimal, angka 1 yang dipinjamkan berbobot 10 maka pada bilangan oktal angka 1 ini berbobot 8.

Contoh 13 :

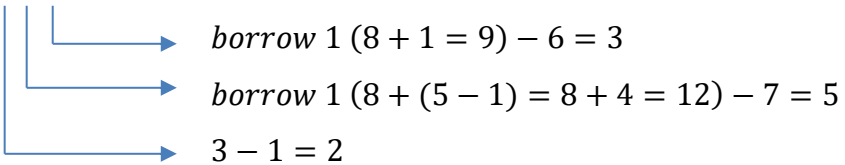
$351_{(8)} - 76_{(8)} = \cdots$

3 5 1

  7 6

_____-

2 5 3



3.3.3 Operasi Penjumlahan dan Pengurangan Sistem Bilangan Heksadesimal

Kaidah yang digunakan dalam operasi penjumlahan serta pengurangan sistem bilangan heksadesimal sama seperti kaidah pada sistem bilangan oktal. Perbedaannya ialah jika angka 1 yang dipinjam pada bilangan oktal berbobot 8, sedangkan pada sistem bilangan heksadesimal berbobot 16

Contoh 14 :

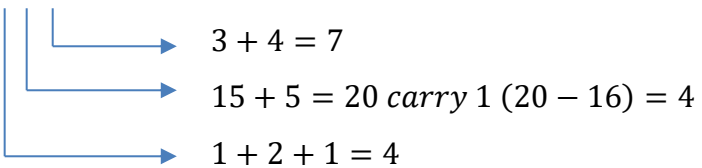
$2F3_{(16)} + 154_{(16)} = \cdots$

2 F 3

1 5 4

_____+

4 4 7



Contoh 15 :

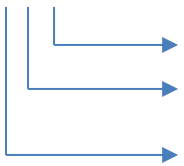
$43A_{(16)} - 76_{(16)} = \cdots$

4 3 A

7 6

_____-

3 C 4



$10 - 6 = 4$

borrow $1\ (16 + 3 = 19) - 7 = 12$ (C)

$4 - 1 = 3$

DAFTAR PUSTAKA

Nengsih, Y. G. and Samosir, K. (2020) *Matematika Diskrit*. Surabaya: CV. Jakad Media Publishing.

BAB 4
BILANGAN PRIMA DAN FAKTORISASI TUNGGAL

Oleh Hetty Elfina

4.1 Bilangan Prima

Definisi .1.

Suatu bilangan bulat $p > 1$ dinamakan bilangan prima jika hanya memiliki pembagi p dan 1. Bilangan prima tidak mempunyai pembagi selain 1 dan dirinya sendiri.

Angka 1 bukan merupakan bilangan prima. Bilangan prima paling kecil yaitu 2 dan merupakan bilangan genap. Bilangan prima yang lainnya yaitu 3, 5, 7, 11, 13, 17, ... yang merupakan bilangan ganjil. Tidak semua bilangan ganjil tersebut merupakan bilangan prima, seperti angka 15 yang merupakan angka ganjil namun bukan angka prima. Bilangan diluar prima seperti 4, 6, 8, 9, 10, 12, ... disebut bilangan komposit. Jika n komposit maka dapat dinyatakan dengan $n = ab$ dengan $a, b \in Z, 1 < a < n$, $1 < b < n$.
(Hernadi, 2018)

Jika terdapat dua bilangan positif yang saling prima maka disebut dengan relatif prima atau koprima dimana FPB dari dua bilangan tersebut sama dengan 1. Bila $a_1, a_2, \dots, a_n$ adalah bilangan bulat positif hingga $(a_1, a_2, \dots, a_n) = 1$ maka $a_1, a_2, \dots, a_n$ merupakan saling prima. Namun jika $(a_k, a_l) = 1$ untuk setiap $k, l = 1, 2, 3, \dots, n$ dengan $k \neq l$ maka bilangan $a_1, a_2, \dots, a_n$ dikatakan saling prima dua-dua atau saling prima sepasang demi sepasang.

Contoh :
FPB $(4, 7, 9) = 1$ maka 4, 7, 9 disebut dengan tiga bilangan yang saling prima dan saling prima sepasang demi sepasang, sebab $(4,7) = (4,9) = (7,9) = 1$
(Sukirman, 2016)

Teorema 1.1.
Andaikan p bilangan prima dan g,h suatu bilangan bulat, maka berlaku
(i) p membagi g. Jika tidak maka g dan p merupakan koprima
(ii) Misalkan p membagi gh maka p membagi g atau p membagi h.

Pembuktian :
(i) FPB (g, p) harus pembagi positif p, sehingga hasilnya 1 atau p. Jika FPB (g,p) = p maka p pembagi g. Jika tidak maka FPB (g, p) = 1 yang artinya g dan p koprima.
(ii) Jika p tidak membagi g maka FPB (g, p) = 1. Melalui identitas Bezout, diperoleh $m, n \in Z$ sehingga $1 = gm + pn$. Mengakibatkan $h = gmh + pnh$ dan karena $p|h$ sehingga $p|gmh$ dan menjadi $p|pnh$. Dapat disimpulkan bahwa $p|h = gmh + pnh$.

Akibat 1.1.
Andaikan p prima dan q membagi $g_1 \dots g_n$ maka p mambagi g_i pada i dengan $1 \leq i \leq n$
Pembuktian :
Dengan menggunakan induksi matematika. Untuk $n = 1$ maka $p|g_1$ sehingga $p|g_1$. Untuk $n = k$ maka $p|g_1 \dots g_k$ sehingga $p|g_i$ untuk $1 \leq i \leq k$. Untuk $n = k + 1$, diubah menjadi $g = g_1 \dots g_k$ dan $h = g_{k+1}$. Berdasarkan teorema 1 (ii), $p|g$ atau $p|h$. Jika $p|g$ terjadi maka $p|g_i$ untuk $1 \leq i \leq k$. Jika $p|h$ terjadi maka $p|g_{k+1}$. Jadi $p|g_i$ untuk $1 \leq i \leq k + 1$. Hal ini berlaku untuk $n = k + 1$.

Teorema 1.2. (Fundamental Aritmatika)

Pada setiap bilangan bulat $n > 1$ bisa dibuat dalam perkalian bilangan prima berpangkat, seperti

$$n = p_1^{e_1} \dots p_k^{e_k}$$

Dengan $p_1, \dots, p_k$ bilangan prima yang berlainan dan $e_1, \dots, e_k$ bilangan bulat positif. Representasi ini tunggal dan tidak berkaitan pada permutasi faktornya.

Pembuktian :

Akan diperlihatkan hasilnya dengan menggunakan induksi. Ketika $n = 2$, maka $n = 2^1$ dengan $p_1 = 2, e_1 = 1$. Seandainya teorema berlaku pada semua bilangan bulat k, $1 < k < n$ dengan k sebagai perkalian bilangan berpangkat. Pada bilangan n, jika n merupakan prima maka $n = n^1$. Namun jika n bilangan komposit maka $n = ab$ dengan $1 < a, b < n$. Karena a dan b bisa dibuat menjadi perkalian bilangan berpangkat, sehingga n juga demikian. Terbuktilah bahwa setiap $n > 1$ bisa dibuat menjadi perkalian bilangan prima berpangkat.

Kemudian akan perlihatkan bahwa representasi tunggal. Misalnya terdapat dua representasi :

$$n = p_1 \dots p_m = q_1 \dots q_t \qquad (*)$$

Terdapat peluang bahwa faktor prima yang sama dan bisa diatur ulang menjadi

$$p_1 \le p_2 \le \dots \le p_m \text{ dan } q_1 \le \dots \le q_t, m \le t \qquad (**)$$

Karena $p_1 | n$ maka dari akibat 1 yaitu $p_1 | q_j$ untuk $j = 1,2, \dots, t$. Dari (**) diperoleh $p_1 \ge q_1$ dan $q_1 \ge p_1$ sehingga $p_1 = q_1$. Untuk persamaan (*) dapat diperoleh bentuk

$$p_2 \dots p_m = q_2 \dots q_t$$

Menggunakan alasan yang sama dengan yang diatas maka diperoleh $p_2 = q_2$ dan

$$p_3 \dots p_m = q_3 \dots q_t$$

Jika $m < t$ maka diperoleh hasil akhir $1 = q_{m+1} \dots q_t$

Hasil ini kontradiksi dengan $q_j > 1$. Jadi seharusnya $m = t$ dan $p_1 = q_1, p_2 = q_2, p_m = q_m$.

Teorema 1.3.

Jika m tidak merupakan bilangan kuadrat sempurna, maka $\sqrt{m}$ merupakan bilangan irrasional.

Pembuktian :

Dengan menggunakan kontraposisi yakni andaikan $\sqrt{m}$ rasional sehingga m adalah kuadrat sempurna. Jika $\sqrt{m}$ rasional maka dapat diubah menjadi $\sqrt{m} = \frac{a}{b}$ dengan a,b bilangan bulat positif. Lalu kedua ruas dikuadratkan sehingga menjadi

$$m = \frac{a^2}{b^2}$$

Misal a,b memiliki faktorisasi prima seperti :

$$a = p_1^{e_1} \dots p_k^{e_k} \text{ dan } b = p_1^{f_1} \dots p_k^{f_k};\ e_i, f_i \geq 0$$

Maka

$$m = \frac{a^2}{b^2} = \frac{p_1^{2e_1} \dots p_k^{2e_k}}{p_1^{2f_1} \dots p_k^{2f_k}} = \left(p_1^{e_1 - f_1} \dots p_k^{e_k - f_k}\right)^2$$

Ini berarti m bilangan kuadrat sempurna.

Teorema 1.4.

Terdapat takhingga banyak bilangan prima

Pembuktian :

Digunakan dengan kontradiksi. Andaikan banyak bilangan prima berhingga, dengan bilangan-bilangannya $p_1, p_2, \dots, p_k$. Misalkan

$$m = (p_1 \dots p_k) + 1$$

Karena $m > 1$ dan sesuai dengan Teorema Fundamental Aritmatika maka m dapat dibagi suatu bilangan prima p. Artinya p harus dipilih dari salah satu $p_1, p_2, \dots, p_k$ dan didapatkan

$$p|p_1 \dots p_k \text{ dan } p|m \Rightarrow p|m - p_1 \dots p_k = 1$$

Hasil tersebut bertentangan karena $p > 1$ menyebabkan $p|1$ tidak memenuhi.

(Hernadi, 2018)

Teorema 1.5.

Untuk setiap bilangan komposit n, diperoleh bilangan prima p sehingga $p|n$ dan $p \leq \sqrt{n}$. Jika tidak terdapat bilangan prima p yang bisa membagi n dengan $p \leq \sqrt{n}$, maka n merupakan bilangan prima.

Contoh :

Selidiki apakah bilangan dibawah ini merupakan bilangan prima atau majemuk

a) 223
b) 187

Penyelesaian :

a) Bilangan prima dari $\sqrt{223}$ yaitu 2, 3, 5, 7, 11, 13. Karena tidak terdapat bilangan yang bisa membagi 223, maka 223 merupakan bilangan prima
b) Bilangan prima dari $\sqrt{187}$ adalah 2, 3, 5, 7, 11, 13. Karena $11|187$ maka 187 merupakan bilangan komposit.

(Vahlia, 2021)

Teorema 1.6.

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

Pembuktian :

Pilih sembarang bilangan bulat positif $n > 1$. Jika n merupakan bilangan prima maka $n|n$. Bila n suatu bilangan komposit, n memiliki faktor bulat positif selain 1 dan n sendiri, contohnya e_1, yakni $e_1|n$. Sehingga akan terdapat bilangan bulat positif n_1 dengan

$$n = e_1 n_1, 1 < n_1 < n$$

Bila n_1 suatu bilangan prima maka $n_1|n$ sehingga teorema terbukti. Namun, bila n_1 bilangan komposit, n_1 memiliki faktor bulat positif selain 1 dan n_1 misal e_2 sehingga $e_2|n_1$. Terdapat bilangan bulat positif n_2 sedemikian sehingga

$$n_1 = e_2 n_2 \text{ dengan } 1 < n_2 < n_1$$

Bila n_2 suatu bilangan prima maka $n_2|n_1$. Karena $n_1|n$ maka $n_2|n_1$ dan n terbagi oleh bilangan prima n_2 maka teorema terbukti. Namun, bila n_2 bilangan komposit, n_2 memiliki faktor bulat positif selain 1 dan n_2 misal e_3 sehingga $e_3|n_2$. Terdapat bilangan bulat positif n_3 sedemikian sehingga

$$n_2 = e_3 n_3 \text{ dengan } 1 < n_3 < n_2$$

Proses pembuktian di atas dapat dilanjutkan sehingga diperoleh

$$n, n_1, n_2, \ldots \text{ dengan } n > n_1 > n_2 > \cdots > 1$$

Hasil penguraian faktor komposit akan selesai pada faktor prima sebab faktor tersebut selalu memiliki nilai lebih kecil dari bilangan yang difaktorkan dan selalu memiliki nilai lebih besar dari 1.
(Sukirman, 2016)

4.2 Bilangan Fermat dan Prima Mersenne

Pada bilangan prima $3, 5, 7, 17, 31, \ldots$memiliki bentuk $2^n \pm 1$. Contohnya $3 = 2^2 - 1; 5 = 2^2 + 1; 7 = 2^3 - 1$, dan lain-lain. Namun ada bilangan dalam bentuk $2^n \pm 1$ yang bukan merupakan bilangan prima, misal $33 = 2^5 + 1$ bukan bilangan prima.

Teorema 2.1.

Andaikan $2^m + 1$ bilangan prima maka $m = 2^n$ pada bilangan bulat $n \geq 0$.

Pembuktian :

Teorema ditunjukkan dengan kontraposisi. Diketahui m bukan pangkat dari 2, maka $m = 2^n q$ dengan $q > 1$ ganjil. Fungsi $f(t) = t^q + 1$ mempunyai nilai nol di $t = -1$ karena q ganjil.

$$t^q + 1 = (t + 1)(t^{q-1} - t^{q-2} + t^{q-3} - \cdots - t + 1)$$

Jadi $t + 1$ merupakan faktor sejati dari $t^q + 1$. Misal $t = x^{2^n}$, didapatkan

$$g(x) = f\left(x^{2^n}\right) = \left(x^{2^n}\right)^q + 1 = x^{2^n q} + 1 = x^m + 1$$

Ketika $x = 2$ diperoleh $2^{2^n} + 1$ merupakan faktor sejati dari $g(2) = x^m + 1$ menyebabkan $x^m + 1$ bukan prima.

Hasil dari $F_n = 2^{2^n} + 1$ dinamakan bilangan **Fermat** dan bilangan Fermat yang prima dinamakan bilangan **prima Fermat**. Konjektur Fermat menyatakan bahwa F_n prima untuk setiap $n > 0$. Contohnya saat $n = 0, 1, 2, 3, 4$ maka $F_n = 3, 5, 17, 257, 65537$ merupakan bilangan prima. Namun ketika $n = 5$ maka $F_5 = 4294976297 = 641 \times 6700417$ bukan bilangan prima. Meskipun ada bilangan yang bukan bilangan Fermat prima tetapi setiap pasang bilangan Fermat adalah koprima.

Bilangan yang memiliki bentuk $2^p - 1$ dengan p bilangan prima dinamakan bilangan **Mersenne** dan bilangan yang prima dinamakan bilangan **prima Mersenne**. Pada bilanga prima $p = 2, 3, 5, 7$ maka $M_p = 3, 7, 31, 127$ merupakan bilangan prima. Namun untuk $n = 11$ maka hasilnya $M_{11} = 2047 = 23 \times 89$ dan bukan bilangan prima.
(Hernadi, 2018)

4.3 Faktorisasi Tunggal

Pemfaktoran suatu bilangan bulat positif pada faktor prima disebut dengan faktorisasi tunggal.

Teorema 3.1.

Memfaktorkan suatu bilangan bulat positif yang lebih besar dari 1 pada faktor prima adalah tunggal, kecuali susunan faktornya.

Pembuktian :

Ambil sembarang bilangan bulat positif $n > 1$. Ketika n suatu bilangan prima, maka n merupakan faktornya sendiri. Ketika n suatu bilangan komposit dan misalkan pemfaktoran n pada faktor prima bukan yang tunggal, seperti

$$n = p_1 p_2 \dots p_t \text{ dan } n = q_1 q_2 \dots q_r$$

dengan p_i dan q_j merupakan bilangan prima untuk $i = 1,2,3,\dots,t$ dan $j = 1,2,3,\dots,r$ lalu $p_1 \geq p_2 \geq p_3 \geq \cdots \geq p_t$ dan $q_1 \geq q_2 \geq q_3 \geq \cdots \geq q_r$ dan $t \leq r$. Karena $n = p_1 p_2 \dots p_t$ sehingga $p_1 | n$ dan $p_1 | q_1 q_2 q_3 \dots q_r$. Berdasarkan perluasan teorema 1.1 (ii), $p_1 = q_k$ untuk k dengan $1 \leq k \leq r$. Karena $q_1 \geq q_2 \geq q_3 \geq \cdots \geq q_r$ maka $p_1 \leq q_1$.

Karena $n = q_1 q_2 \dots q_r$ maka $q_1 | n$ dan $q_1 | p_1 p_2 \dots p_t$. Berdasarkan perluasan teorema 1.1 (ii) $q_1 = p_m$ untuk m dengan $1 \leq m \leq t$. Karena $p_1 \geq p_2 \geq p_3 \geq \cdots \geq p_t$ maka $q_1 \leq p_1$. Sebab $p_1 \leq q_1$ dan $q_1 \leq p_1$ maka $p_1 = q_1$. Pada hasil permisalan diatas dapat diambil kesimpulan bahwa $p_2 p_3 \dots p_t = q_2 q_3 \dots q_r$. Saat pembuktian di atas dilanjutkan maka akan diperoleh

$$p_2 = q_2 \text{ sehingga } p_3 p_4 \dots p_t = q_3 q_4 \dots q_r$$
$$p_3 = q_3 \text{ sehingga } p_4 p_5 \dots p_t = q_4 q_5 \dots q_r$$

dan seterusnya

Bila $t = r$, maka pembuktian berhenti pada $p_t = q_r$ dan teorema terbukti. Namun bila $t < r$, maka

$$1 = q_{t+1} q_{t+2} q_{t+3} \dots q_r$$

Hasil yang diperoleh ini mustahil karena $q_{t+1} q_{t+2} q_{t+3} \dots q_r$ merupakan bilangan prima, oleh sebab itu sudah seharusnya $t = r$ menghasilkan $p_1 = q_1, p_2 = q_2, p_3 = q_3, p_t = q_r$.

Maka dapat diambil kesimpulan bahwa bilangan bulat positif *n* hanya bisa dihasilkan pada hasil kali faktor prima secara tunggal.

Euclides membuktikan bahwa banyaknya bilangan prima adalah tak hingga. Misal $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$ merupakan urutan bilangan prima dan misalkan p_n diambil untuk bilangan prima terbesar

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

dengan $N > 1$, berdasarkan teorema 1.6, *N* bisa dibagi bilangan prima menyebabkan *N* dapat dibagi oleh sedikitnya satu bilangan prima pada $p_1, p_2, p_3, \dots, p_n$. Misal bilangan prima p_k dengan $1 \leq k \leq n$ yang membagi *N*, yaitu $p_k | N$.

$N = p_1 p_2 \dots p_n + 1$, dengan $p_k | N$ dan $p_k | p_1 p_2 p_3 \dots p_n$, maka $p_k | 1$

Hasil yang diperoleh salah sebab p_k merupakan bilangan prima. Oleh sebab itu, permisalan bernilai salah. Hasil yang benar yaitu banyaknya bilangan prima adalah tak hingga.

Teorema 3.2.

Pada suatu barisan bilangan prima, andaikan p_n sebagai bilangan prima ke *n* maka $p_n \leq 2^{2^{n-1}}$

Pembuktian :

Dalam pembuktian digunakan induksi matematika. Saat $n = 1$ didapat $p_1 \leq 2^{2^{n-1}}$, yaitu $p_1 \leq 2$. Hasil tersebut bernilai benar sebab bilangan prima pertama yaitu 2.

Andaikan $n = k$ bernilai benar yaitu $p_k \leq 2^{2^{k-1}}$. Akan ditunjukkan juga akan bernilai benar untuk $n = k + 1$ yakni $p_{k+1} \leq 2^{2^k}$

Penjabarannya sebagai berikut

$$p_{k+1} \leq p_1 p_2 p_3 \dots p_k + 1$$
$$p_{k+1} \leq 2\ 2^2\ 2^{2^2}\ 2^{2^3} \dots 2^{2^{k-1}} + 1$$
$$p_{k+1} \leq 2^{1+2+2^2+2^3+\cdots+2^{k-1}} + 1$$

$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = 2^k - 1$ merupakan deret geometri dengan rasio 2, menyebabkan

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

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

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

Berdasarkan pembuktian di atas, maka teorema bernilai benar.

Berdasarkan teorema diatas, bilangan prima ke $(n + 1)$ yaitu $p_{n+1} \leq 2^{2^n}$. Oleh sebab itu, banyaknya bilangan prima yang lebih kecil dari 2^{2^n} tidak kurang dari $(n + 1)$. Jadi untuk $n \geq 1$ terdapat paling sedikit $n + 1$ bilangan prima yang lebih kecil dari 2^{2^n}.

(Sukirman, 2016)

DAFTAR PUSTAKA

Hernadi, J. 2018. *Teori Bilangan.* [Online] Available at: https://www.academia.edu/8123313/BAB_2_BILANGAN_PRIMA [Accessed 28 04 2023].

Sukirman. 2016. *Teori Bilangan.* Banten : Universitas Terbuka

Vahlia, Ira. 2021. *Modul Teori Bilangan.* Lampung : Universitas Muhammadiyah Metro

BAB 5
KEKONGRUENAN DAN APLIKASINYA

Oleh Titik Pitriani Muslimin

5.1 Pendahuluan

Pada kegiatan-kegiatan belajar terdahulu, kita telah mempelajari konsep keterbagian dan sifat-sifatnya. Konsep dan sifat-sifat keterbagian itu dapat dipelajari lebih mendalam dengan relasi kekongruenan. Dengan menggunakan konsep kekongruenan, kita dapat menelaah sifat-sifat keterbagian tersebut lebih luas dan mendalam sehingga lebih nampak manfaatnya. Namun demikian untuk mempelajari keongruenan dan sifat-sifatnya ini diperlukan penguasaan konsep dan sifat-sifat keterbagian (Tiro, M.A., dkk., 2008).

Beberapa kegunaan kekongruenan akan dipelajari dalam modul ini, misalnya untuk menjelaskan ciri terbagi habis dari beberapa bilangan, koreksi sembilan yaitu menguji kebenaran suatu hasil penjumlahan, pengurangan, perkalian, dan pembagian bilangan-bilangan bulat. Dengan konsep kekongruenan, kita lebih mudah dan cepat untuk menentukan sisa berapa pembagian bilangan-bilangan bulat.

5.2 Kekongruenan

Pada bab ini akan dibahas mengenai kekongruenan dengan memaparkan definisi, contoh, kemudian teorema-teoremanya.

Sama halnya dengan persamaan pada materi aljabar, kajian utama pada kongruensi adalah mencari nilai bilangan-bilangan bulat yang memenuhi $f(x) \equiv 0(mod\ 0)$. Kalimat

terbuka yang menggunakan relasi kekongruenan disebut pengkongruenan. Jika suatu pengkongruenan variabelnya berpangkat tertinggi satu disebut pengkongruenan linier atau kongruensi linier.

Definisi. 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 (ditulis $a \equiv b$ (mod m)) jika m membagi habis ($a - b$). Atau $a \equiv b$ (mod m) jika a dan b memberikan sisa yang sama bila dibagi oleh m (Tiro, M.A., dkk., 2008).

Contoh 1.

a. 38 mod 5 = 3 dan 13 mod 5 = 3, maka kita katakan 38 ≡ 13 (mod 5) (baca: 38 kongruen dengan 13 dalam modulo 5).
b. Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b$ (mod m) jika m habis membagi $a - b$.
c. Jika a tidak kongruen dengan b dalam modulus m, maka ditulis $a \not\equiv b$ (mod m)
d. $25 \equiv 1$ (mod 4) sebab (25-1) terbagi 4
e. $31 \neq 5$ (mod 6) sebab (31-5) tidak terbagi 6

Definisi kekongruenan diatas dapat ditulis bahwa:

$$jika\ m > 0\ maka\ m|(a - b)\ jika\ dan\ hanya\ jika\ a \equiv b$$

Dari defenisi 1 diatas kita dapat tuliskan bahwa jika m>0 dan m|(a-b) maka terdapat bilangan bulat r sedemikian sehingga (a-b)=mr. Jadi $a \equiv b\ (mod\ m)$ dapat dinyatakan dalam selisih antara a dan b yang merupakan kelipatan dari m atau a-b = mr. Akan tetapi, karena a-b=mr memiliki makna yang sama dengan a=mr+b yaitu a sama dengan b ditambah kelipatan m, maka diperoleh definisi bahwa:

$a \equiv b\ (mod\ m)$ jika dan hanya jika ada bilangan bulat r sedemikian sehingga a=mr+b.

Contoh 2.

a. $41 \equiv 2\ (mod\ 13)$ sama artinya dengan 41 = 13(3)+2
b. $17 \equiv 3\ (mod\ 7)$ sama artinya dengan 17 = 7(2)+3
c. $26 \equiv 4\ (mod\ 11)$ sama artinya dengan 26 = 11(2)+4

Teorema 1.

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

Teorema tersebut dapat dibuktikan kebenarannya yakni sebagai berikut:

a$\equiv b\ (mod\ m) \leftrightarrow \exists\ r\ \rightarrow a = mr + b$. Jika a dan m adalah bilangan bulat dimana m>0, maka a dapat dinyatakan sebagai a=mq+k dengan 0<k<m. hal ini berarti bahwa a-k=mq, atau sama dengan a=k(mod m). Sebab 0<k<m, maka ada m nuah pilihan untk k uaiyu 0,1,2,3,4,…,(m-1). Jadi setiap bilangan bulat akan kongruen dengan modulo m dan tepat satu diantara 0,1,2,3,…,(m-1).

Berdasarkan teorema diatas maka didapat definisi sebagai berikut:

"Pada a $\equiv k(mod\ m) dengan\ 0 \leq k < m$, maka k disebut sisaan terkecil dari a modulo m. Sedangkan untuk kekongruenan himpunan {0,1,2,3,…,(m-1)} disebut himpunan sisaan positif terkecil modulo m" (Kartasasmita, B., 1982).

Contoh 3.

a. $71 \equiv 2(\text{mod } 3)$ karena 2 adalah sisaan terkecil dari 71 mdulo 3

b. $34 \equiv 4 \pmod 5$ karena 4 adalah sisaan terkecil dari 34 modulo 5
c. $12 \equiv 2 \pmod 5$ karena 2 adalah sisaan terkecil dari 12 modulo 5
d. {0,1,2,3,4} adalah himpunan sisaan terkecil modulo 5
e. {0,1,2,3,4, 5} adalah himpunan sisaan terkecil modulo 6

Teorema 2

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

Untuk membuktikan teorema diatas maka pertama yang harus dibuktikan adalah jika $a \equiv b \pmod m$ maka a dan b memiliki sisa yang sama jika dibagi dengan m. Seandainya $a \equiv b \pmod m$ maka $a \equiv k \pmod m$ dan $b \equiv k \pmod m$, dimana k adalah sisaan terkecil modulo m. Karena $a \equiv k \pmod m$ berarti berlaku $a = mq + k$ untuk suatu q. Hal ini berarti a dan b memiliki sisa yang sama yaitu k, jika dibagi m.

Selanjutnya akan dibuktikan bahwa jika a dan b memiliki sisa yang sama jika dibagi denga m maka $a \equiv b \pmod m$. misalkan a memiliki sisa k jika dibagi m, berarti $a=mq+k$ dan b memiliki sisa k jika dibagi m maka $b=mr+k$. Berdasarkan kedua persamaan tersebut maka diperoleh bahwa $a-b=m(q-r)$ berarti $m|(a-b)$ atau $a \equiv b \pmod m$.

Jadi menurut teorema tersebut jika $n \equiv 7 \pmod 8$ memiliki arti yang sama dengan $n=17+8k$ untuk suatu bilangan bulat k dan n dibagi 8 bersisa 7.

Contoh 4.

$10 \equiv \pmod 4$ mempunyai arti yang sama dengan $10=4k+2$ untuk suatu bilngan bulat $k=2$ dan 10 dibagi 4 bersisa 2.

Definisi 2.

Himpunan bilangan bulat n_1, n_2,n_3,..., n_r disebut sistem sisaan lengkap modulu m jika dan hanya jika setiap bilangan bulat adalah kongruen modulo m dengan satu dan hanya satu diantara n_1, n_2,n_3,..., atau n_r (Sukarman, H., 2001).

Contoh 5.

a. Himpunan {11, 12, 13, 14, 15} adalah suatu sistem sisaan lengkap modulo 5 karena $11 \equiv 1 (\text{mod } 5)$, $12 \equiv 2 (\text{mod } 5)$, $13 \equiv 3 (\text{mod } 5)$, $14 \equiv 4 (\text{mod } 5)$, dan $15 \equiv 0 (\text{mod } 5)$.
b. Himpunan {8, 33, 46, 63} adalah suatu sistem sisaan lengkap modulo 4 karena $8 \equiv 0 (\text{mod } 4)$, $33 \equiv 1 (\text{mod } 4)$, $46 \equiv 2 (\text{mod } 4)$, $63 \equiv 3 (\text{mod } 4)$
c. Himpunan {0,1,2,3,4} merupakan suatu sistem sisaan lengkap modulo 5, sekaligus sebagai himpunan sisaan terkecil modulo 5.

Kekongruenan pada modulo bilangan bulat positif memberikan padanan dengan suatu bilangan bulat a dengan bialngan bualat b. Karena merupakan padanan maka kekongruenan modulo merupakan suatu relasi yang merupakan relasi ekuivalen seperti halnya relasi kesamaan. Adapun sifat-sifat relasi kesamaan yakni memiliki sifat refleksi, sifat simetris, dan sifat transitif.

Berikut diberikan suatu teorema tentang kekongruenan modulo bilangan bulat positif m adalah suatu relasi ekuivalen pada himpunan bilangan bulat (Sukirman, 1987).

Teorema 3.

Untuk bilangan bulat positif dan a,b, dan c bilangan bulat, maka berlaku:

1) Sifat refleksi yakni a ≡a(mod m)
2) Sifat simetris yakni a≡b(mod m) jika dan hanya jika b≡a(mod m)
3) Sifat transitif yakni jika a ≡ b(mod m) dan b ≡ c(mod m) maka a ≡ c(mod m).

Teorema 4.

Jika a ≡ b(mod m) dan c ≡ d(mod m) maka (a±c) ≡ $\{(b \pm d\}(mod\ m)$

Penurunan teorema 4 diatas dinyatakan dalam teorema berikut.

Teorema 5.

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

Pembuktian teorema tersebut sebagai berikut:

> Asumsikan $a \equiv b(mod\ m)$ berarti a = ms + b untuk suatu bilangan bulat s. Demikian juga jika $c \equiv d(mod\ m)$ berarti $c = mt + d$ untuk suatu bilangan bulat t. jika kedua ruas persamaan pertama dikalikan x dan kedua ruas persamaan kedua dikalikan y maka diperoleh :
>
> $ax = msx + bx\ dan\ cy = mty + dy$.

Dengan menjumlahkan kedua persamaan maka diperoleh:

$ax + cy = (msx + bx) + (mty + dy)$

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

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

Hasil penjumlahan ini berarti bahwa: $m|\{(ax + cy) - (bx + dy)\}\ atau\ ax + cy \equiv (bx + dy)(mod\ m)$.

Jadi terbukti benar untuk teorema tersebut.

Teorema 6

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

Pembuktian teorema tersebut sebagai berikut:

Akan diasumsikan $a \equiv b(mod\ m) dan\ c \equiv d(mod\ m)$. Berdasarkan definisi 1 bahwa $m|(a - b) dan\ m|(c - d)$. Hal ini berarti terdapat suatu bilangan bulat s, sehingga $(a - b) = ms\ atau\ a = ms + b$. Dan terdapat suatu bilangan bulat t sedemikian sehingga $(c - d) = mt\ atau\ c = mt + d$. Kemudian kedua persamaan diperkalikan sehingga diperoleh,

$ac = (ms + b)(mt + d) \leftrightarrow ac = bd + m(mst + sd + bt)$. Ini berarti bahwa $ac \equiv bd(mod\ m)$. Maka teorema 6 terbukti benar.

Teorema 7.

Jika $a \equiv b(mod\ m)$ maka $ka \equiv kb(mod\ m)$ untuk suatu k bilangan bulat sembarang.

Pembuktian teorema tersebut sebagai berikut:

Ambil $a \equiv b(mod\ m)$ maka menurut definisi 1 diperoleh $m|(a-b)$. Karena $m|(a-b)$ maka menurut teorema keterbagian diperoleh m|k(a-b) atau m|(ka-kb) untuk sembarang k suatu bilangan bulat. Sesuai definisi bahwa jika m suatu bulangan positifmaka a kongruen dengan b modulo m jika dan hanya jika m membagi (a-b), hal ini berarti bahwa $ka \equiv kb(mod\ m)$. Sehingga teorema tersebut terbukti kebenarannya.

Teorema 8.

Jika $a \equiv b(mod\ m)$ maka $ka \equiv kb(mod\ km)$ untuk suatu bilangan bulat k sebarang.

Pembuktian teorema tersebut sebagai berikut:

Pertama-tama diasumsikan $a \equiv b(mod\ m)$, sehingga berdasarka definisi kekongruenan dimana m membagi habis (a-b) atau $m|(a-b)$, maka ada y anggota bilangan bulat Z sedemikian sehingga (a-b)=my atau k(a-b)=kmy. Berdasarkan sifat aosiatif maka diperoleh ka-kb = (km)y. Sehingga berdasarkan definisi keterbagian maka diperoleh bahwa km|(ka-kb), sedemikian sehingga pastilah $ka \equiv kb(mod\ km)$ sesuai dengan definisi dari kekongruenan.

Teorema 9.

Jika $a \equiv b(mod\ m) dan\ terdapat\ n \in Z, dimana\ n|m\ maka\ a \equiv b(mod\ n) untuk\ setiap\ a.b \in Z$.

Pembuktian teorema tersebut sebagai berikut:

Langkah pertama kita hipotetsiskan bahwa $a \equiv b(mod\ m)$. Sesuai definisi dari kekongruenan maka m|(a-b). karena diketahui bahwa n|m dan m|(a-b) maka berdasarkan teorema dari keterbagian diperoleh bahwa n juga membagi habis (a-b)

atau n|(a-b). berdasarkan hal tersebut maka terbukti bahwa $a \equiv b \ (mod \ n)$.

Teorema 10.

Jika $a \equiv b(mod\ m), dan\ terdapat\ bilangan\ bulat\ positif\ n, maka\ a^n \equiv b^n(mod\ m)$.

Selanjutnya jika terdapat dua bilangan bulat p dan q yang keduanya kongruen dengan modulo m, maka kemungkinan juga bisa kongruen dengan modulo suatu bilangan lainnya. Jika d>0 dan d membagi habis m sedangkan $p \equiv q(mod\ m)$. Maka m=kd dan p-q = am sehingga p-q=a(kd)=(ak)d atau d membagi habs p-q. dari ilustrasi tersebut diperoleh teorema sebagai berikut.

Teorema 11.

$$Jika\ d|m\ dan\ p \equiv q(mod\ m) maka\ p \equiv q(mod\ d).$$

Dalam persamaan bilangan bulat terdapat sifat penghapusan yakni jika ab-ac dengan a tidak sama dengan 0 maka b=c. Akan tetapi dalam relasi kekongruenan sifat penghapusan tidak sepenuhnya berlaku, hanya berlaku dengan syarat seperti pada teorema berikut.

Teorema 12.

$$Jika\ ac \equiv bc(mod\ m) dan\ (c, m) = 1\ maka\ a \equiv b(mod\ m).$$

Teorema 13.

$Asumsikan\ (c,m) = d, ac \equiv bc(mod\ m)\ jika\ dan\ hanya\ jika\ a \equiv b\left(mod\ \frac{m}{d}\right).$

Contoh 6.

Tentukanlah nilai p yang memenuhi $2p \equiv 4(mod\ 6)$!

Penyelesaian:

Diketahui bahwa $2p \equiv 4(mod\ 6)$, hal ini berarti $2p \equiv 2.2(mod\ 6)$.

Karena (2,6) = 2, maka berdasarkan teorema 13 diatas diperoleh $p \equiv 2(mod\ \frac{6}{2}$ atau $p \equiv 2(mod\ 3)$. Jadi nilai nilai p yang memenuhi persamaan tersebut adalah (3k+2) untuk setiap bilangan bulat k.

5.3 Aplikasi Kekongruenan

Banyak permasalahan yang serupa dengan permasalahan kekongruenan yang sering ditemukan dalam kehidupan sehari-hari. Seperti kalender yang disusun mengikuti aturan modulo 7 untuk hari dalam seminggu dan modulo 12 untuk bulan dalam setahun. Contoh lainnya kerja jam tangan yang mengikuti aturan modulo 12 untuk menyatakan jam, dan modulo 60 untuk menyatakan menit. (Tiro, M.A., dkk., 2008).

Salah satu bilanga modulo yang spesial yakni modulo 9, karena setiap bilangan bulat kongruen dengan modulo 9 dengan jumlah angka-angkanya. Selain itu modulo 9 dapat digunakan dlaam menguji kebenaran perkalian dan penjumlahan bilangan bulat.

Perhatikan ilustrasi berikut ini:

10.000-1=9.999 =9 k_4 sehingga 10.000=1(mod 9)

1.000-1=999 =9 k_3 sehingga 1.000=1(mod 9)

100-1=99 =9 k_2 sehingga 100=1(mod 9)

10-1=9 =9 k_1 sehingga 10=1(mod 9)

Berikut ini diberikan contoh bahwa setiap bilangan bulat kongruen modulo 9 dengan jumlah angkanya.

Contoh 7.

$$6724 \equiv \{6000 + 700 + 20 + 4\}(mod\ 9)$$
$$\equiv \{6(1000) + 7(100) + 2(10) + 4\}(mod\ 9)$$
$$\equiv \{6(1) + 7(1) + 2(1) + 4\}(mod\ 9)$$
$$\equiv 19(mod\ 9)$$

Sehingga $6724 \equiv 19(mod\ 9)$

Selanjutnya kita dapat menyederhanakannya lagi menjadi:

$19 \equiv 10 + 9(mod\ 9) \equiv 1 + 9(mod\ 9)$

$19 \equiv 10\ (mod\ 9)$

Jadi dipeoreh hasil akhirnya yakni $6724 \equiv 10(mod\ 9)$

Ada beberapa teorema yang dipaparkan dalam pengaplikasian kekongruenan, diantaranya:

Teorema 1.

"$10^n \equiv 1(mod\ 9) untuk\ n = 0,1,2,3, \ldots$."

Pembuktian teorema 1 sebagai berikut:

Jika n adalah angka semuanya 9 maka $10^n - 1 = 999 \ldots .9\ terbagi\ oleh\ 9. sehingga\ 10^n \equiv 1(mod\ 9)$.

Teorema 2.

"Setiap bilangan bulat kongruen dengan modulo 9 beserta jumlah angka-angkanya."

Jika terdapat persamaan a+b=c. Maka $a + b \equiv c(mod\ 9)$.

Jika $a \equiv m(mod\ 9), b \equiv n(mod\ 9), dan\ c \equiv p(mod\ 9). maka\ dapat\ disimpulkan\ bahwa\ m + n \equiv p(mod\ 9)$.

Contoh 8.

Buktikanlah bahwa 324+224+564=1112!

Penyelesaian:

Akan dibuktikan bahwa 224+324+564=1112

Langkah pertama yakni mencari modulo 9 yang kongruen terhadap angka-angka tersebut (sesuai teorema 2).

$324 \equiv \{3 + 2 + 4\}(mod\ 9) = 9(mod\ 9) = 0(mod\ 9)$

$224 \equiv \{2 + 2 + 4\}(mod\ 9) = 8(mod\ 9)$

$564 \equiv \{5 + 6 + 4\}(mod\ 9) = 15(mod\ 9) = 6(mod\ 9)$

Sehingga $\{324+224+564\} \equiv \{0 + 8 + 6\}(mod\ 9) = 14(mod\ 9) = 5(mod\ 9)$.

Sedangkan $1112 \equiv \{1 + 1 + 1 + 2\}(mod\ 9) = 5(mod\ 9)$.

Karena hasil pengkongruenan pada ruas kiri dan ruas kanan dari persamaan tersebut adalah sama yakni sama-sama kongruen terhadap 5(mod 9), maka hal ini berarti bahwa persamaan 324+224+564=1112 adalah benar.

Contoh 9.

Buktikanlah apakah persamaan berikut ini benar atau salah, 254 x 17 = 4318!

Penyelesaian:

Akan dibuktikan bahwa 254 x 17 = 4318.

Sesuai prinsip teorema 2 diatas, maka:

$254 \equiv \{2 + 5 + 4\}(mod\ 9) = 11(mod\ 9) = \{1 + 1\}(mod\ 9) = 2(mod\ 9)$

$17 \equiv \{1 + 7\}(mod\ 9) = 8(mod\ 9)$

Sehingga diperoleh hasil perkaliannya yakni,(ruas kiri):

$254 \times 17 \equiv 2 \times 8(mod\ 9) = 16(mod\ 9) = 7(mod\ 9).$

Selanjutnya mencari kekongruenan untuk ruas kanan:

$4318 \equiv \{4 + 3 + 1 + 8\}(mod\ 9) = 16(mod\ 9) = 7(mod\ 9).$

Berdasarkan hasil pengkongruenan pada ruas kiri dan kanan yakni sama-sama kongruen terhadap 7(mod 9), maka persamaan 254 x 17 =4318 adalah benar.

Teorema 3.

"Suatu bilangan terbagi oleh 2 jika dan hanya jika angka terakhirnya terbagi oleh 2."

Pembuktian teorema tersebut sebagai berikut:

Jika kita mengambil sebarang n yaitu bilangan yaang dinyatakan dengan $n=a_k a_{k-1} a_{k-2} \ldots a_1 a_0$ dengan $0 \leq a_i \leq 9, untuk\ i = 1,2,3 \ldots k.$

Maka $n = a_k a_{k-1} a_{k-2} \ldots a_1 a_0 = a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \cdots . + a_1 10 \quad + a_0$

Pada persamaan diatas, terlihat bahwa suku pada ruas kanannya habis terbagi oleh dua, maka bilngan terkahir dari n yakni a_0 juga akan terbagi oleh dua. Sehingga dapat disimpulman bahwa suatu bilangan dapat terbagi habis oleh dua jika dan hanya jika bilngan akhir atau angka terakhirnya juga terbagi habis oleh dua.

Selanjutnya dari uraian pembuktian teorema tersebut didapatkan kesimpulan laini yakni suatu bilangan terbagi habis oleh angka empat jika dan hanya jika bilangan atau angka yang dinyatakan oleh dua angka terakhirnya juga terbagi habis oleh angka empat.

Contoh. 10

Bilangan 7.345.316 terbagi oleh angka 4 karena dua angka terkhirnya terbagi oleh 4 (kelipatan 4) yakni 16 terbagi habis oleh 4.

Dengan cara yang sama pula ditemukan bahwa suatu bilangan akan terbagi habis oleh angka delapan jika dan hanya jika bilangan tersebut memiliki tiga angka terkahir yang dapat terbagi habis oleh angka delapan.

Contoh. 11

Bilangan 45.256 adalah bilangan yang dapat dibagi habis oleh angka delapan, karena tiga angka terakhirnya dapat dibagi habis oleh 8 yakni bilangan 256 terbagi habis oleh angka delapan.

DAFTAR PUSTAKA

Kartasasmita,B, 1982. *Pengantar Teori Bilangan,* Bandung: ITB

Sukarman, H. 2001. *Teori Bilangan.* Jakarta: Pusat Penerbitas Universitas Terbuka.

Sukirman, 1987. *Pengantar Teori bilangan*. Yogyakarta: FPMIPA IKIP Yogyakarta.

Tiro, M.A., dkk. 2008. *Pengenalan Teori Bilangan*. Makassar: Andira Publisher.

BAB 6
PENGKONGRUENAN LINIER

Oleh Haerudin

6.1 Kongruensi Linear

Al Jupri, (2022) bahwa Kongruensi linier yang paling sederhana berbentuk $ax \equiv b \pmod m$. Sedangkan solusi dari kongruensi linier tersebut merupakan suatu bilangan bulat x sehingga berlaku $ax \equiv b \pmod m$

Definisi 6.1

Jika $r_1, r_2, r_3, \ldots r_m$ adalah suatu sistem residu lengkap modulo m. Banyaknya selesaian dari kongruensi $f(x) \equiv 0 \pmod m$ adalah banyaknya r_i sehingga $f(r_i) \equiv 0 \pmod m$

Contoh:

1. $f(x) = x^3 + 5x - 4 \equiv 0 \pmod 7$
   Jawab

   Selesaiannya adalah x = 2, karena

   $f(2) = 2^3 + 5(2) - 4 = 14 \equiv 0 \pmod 7$

   Ditulis dengan $x \equiv 2 \pmod 7$.

   Untuk mendapatkan selesaian kongruensi di atas adalah dengan mensubstitusi x dari 0, 1, 2, 3, ..., (m-1).

2. $x^3 - 2x + 6 \equiv 0 \pmod 5$
   Jawab

   Selesaiannya adalah x = 1 dan x = 2, sehingga dinyatakan dengan $f(1) = (1)^3 - 2.1 + 6 \equiv 0 \pmod 5$ dan dengan $f(2) = (2)^3 - 2.2 + 6 \equiv 0 \pmod 5$

Jadi, $x \equiv 1 \pmod 5$ dan $x \equiv 2 \pmod 5$.

Bentuk kongruensi yang paling sederhana adalah kongruensi yang berderajat satu dan disebut dengan kongruensi linear. Jika dalam aljabar kita mengenal persamaan linear yang berbentuk $ax = b$, $a \neq 0$, maka dalam teori bilangan dikenal kongruensi linear yang mempunyai bentuk $ax \equiv b \pmod m$.

Definisi 6.2

Kongruensi sederhana berderajat satu atau yang disebut kongruensi linear mempunyai bentuk umum $ax \equiv b \pmod m$, dengan $a,b,m \in Z$, $a \neq 0$, dan $m > 0$.

Teorema 6.1

Kongruensi linear $ax \equiv b \pmod m$, dengan $a,b,m \in Z$, $a \neq 0$, dan $m > 0$. dapat diselesaikan jika $d = (a,m)$ membagi b. Pada kasus ini memiliki selesaian. Jika $(a,m) = 1$, maka kongruensi linear $ax \equiv b \pmod m$ hanya mempunyai satu selesaian.

Bukti.

Kongruensi linear $ax \equiv b \pmod m$ mempunyai selesaian, berarti $m \mid ax - b$.

Andaikan $d \nmid b$.

$d = (a,b) \rightarrow d \mid a \rightarrow d \mid ax$.

$d \mid ax$. dan $d \nmid b \rightarrow d \nmid ax - b$.

$d = (a,m) \rightarrow d \mid m$.

$d \mid m$ dan $d \nmid b \rightarrow m \nmid ax - b$.

$m \nmid ax - b$ bertentangan dengan $m \mid ax - b$, Jadi $d \mid b$.

Diketahui $d \mid b$ dan $d = (a,m) \rightarrow d \mid a \rightarrow d \mid m$.

$d \mid a$, $d \mid m$, dan $d \mid b \rightarrow \frac{a}{d}, \frac{m}{d}$, dan $\frac{b}{d} \in Z$.

$ax \equiv b \pmod{m} \rightarrow m \mid ax - b.$

$m \mid ax - b$ dan $\frac{a}{d}, \frac{m}{d}, \frac{b}{d} \rightarrow \frac{m}{d} \mid (\frac{ax}{d} - \frac{b}{d})$

$\frac{m}{d} \mid \frac{ax}{d} - \frac{b}{d} \rightarrow \frac{ax}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Misal selesaian kongruensi $\frac{ax}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ adalah $x \equiv x_o$; $x_o < \frac{m}{d}$, maka sebarang selesaiannya berbentuk $x = x_o + k.\frac{m}{d}$, $k \in Z$, yaitu:

$x = x_o + k.\frac{m}{d}$, $x = x_o + k.\frac{2m}{d}$, $x = x_o + k.\frac{3m}{d}$, ... , $x = x_o + k.\frac{(d-1)m}{d}$

.

dimana seluruhnya memenuhi kongruensi dan seluruhnya mempunyai d selesaian.

Jika (a,d) = 1, maka selesaiannya didapat $x = x_o$ yang memenuhi kongruensi dan mempunyai satu selesaian.

Contoh:

1. $7x \equiv 3 \pmod{12}$
   Jawab

   Karena (7,12) = 1, atau 7 dan 12 relatif prima dan $1 \mid 3$ maka $7x \equiv 3 \pmod{12}$, Hanya mempunyai 1 selesaian yaitu $x \equiv 9 \pmod{12}$

2. $6x \equiv 9 \pmod{15}$
   Jawab

Karena (6,15) = 3 atau 6 dan 15 tidak relatif prima dan 3 | 9, maka kongruensi di atas mempunyai 3 selesaian (tidak tunggal).

Selesaian kongruensi linear $6x \equiv 9 \pmod{15}$ adalah

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

3. $12x \equiv 2 \pmod{18}$
   Jawab

   Karena (18,12) = 4 dan $4 \nmid 2$, maka kongruensi $12x \equiv 2 \pmod{18}$ tidak mempunyai selesaian.

4. $144x \equiv 216 \pmod{360}$
   Jawab

   Karena (144,360) = 72 dan $72 \mid 216$, maka kongruensi $144x \equiv 216 \pmod{360}$ mempunyai 72 selesaian.

   Selesaian tersebut adalah $x \equiv 4 \pmod{360}$, $x \equiv 14 \pmod{360}$, ... , $x \equiv 359 \pmod{360}$.

5. Bila kongruensi $144x \equiv 216 \pmod{360}$ disederhanakan dengan menghilangkan faktor d, maka kongruensi menjadi $2x \equiv 3 \pmod{5}$. Kongruensi $2x \equiv 3 \pmod{5}$ hanya mempunyai satu selesaian yaitu $x \equiv 4 \pmod{5}$.

Pada kongruensi $ax \equiv b \pmod{m}$ jika nilai a,b, dan m besar, akan memerlukan penyelesaian yang panjang, sehingga perlu disederhanakan penyelesaian tersebut.

$ax \equiv b \pmod{m} \leftrightarrow m \mid (ax - b) \leftrightarrow (ax-b) = my, y \in Z.$

$ax - b = my \leftrightarrow my + b = ax \leftrightarrow my \equiv -b \pmod{a}$ dan mempunyai selesaian y_o.

Sehingga dari bentuk $my + b = ax$ dapat ditentukan bahwa $my_o + b$ adalah kelipatan dari.

Atau dapat dinyatakan dalam bentuk:

$my_o + b = ax \leftrightarrow x_o = \frac{my_o + b}{a}$

Contoh.

1. Selesaikan kongruensi $7x \equiv 4 \pmod{25}$
   Jawab

   $7x \equiv 4 \pmod{25}$

   $25y \equiv -4 \pmod{7}$

   $4y \equiv -4 \pmod{7}$

   $y \equiv -1 \pmod{7}$

   $y_o = -1$ sehingga $x_o = \frac{25(-1)+4}{7} = -3$

   Selesaian kongruensi linear di atas adalah

   $x \equiv -3 \pmod{25}$

   $x \equiv 22 \pmod{25}$

2. Selesaikan kongruensi $4x \equiv 3 \pmod{49}$
   Jawab

   $4x \equiv 3 \pmod{49}$

   $49y \equiv -3 \pmod{4}$

   $4y \equiv -3 \pmod{4}$

   $y \equiv -3 \pmod{7}$

   $y_o = -3$ sehingga $x_o = \frac{49(-3)+3}{4} = -36$

Selesaikan kongruensi linear di atas adalah

$x \equiv -36 \pmod{49}$

$x \equiv 13 \pmod{25}$

Cara di atas dapat diperluas untuk menentukan selesaian kongruensi linear dengan menentukan nilai y_o dengan mencari z_o, menentukan w_o dengan mencari w_o, menentukan v_o dengan mencari w_o, dan seterusnya.

Contoh

1. Selesaikan kongruensi $82x \equiv 19 \pmod{625}$
   Jawab

   $82x \equiv 19 \pmod{625}$

   $625y \equiv -19 \pmod{82}$

   $51y \equiv -19 \pmod{82}$

   $82z \equiv 19 \pmod{51}$

   $31z \equiv 19 \pmod{82}$

   $51v \equiv -19 \pmod{31}$

   $20v \equiv -19 \pmod{31}$

   $31w \equiv 19 \pmod{20}$

   $11w \equiv 19 \pmod{20}$

$20r \equiv -19 \pmod{11}$

$9r \equiv -19 \pmod{11}$

$9r \equiv 3 \pmod{11}$

$11s \equiv -3 \pmod{9}$

$2s \equiv -3 \pmod{9}$

$9t \equiv 3 \pmod{2}$

$t \equiv 3 \pmod{2}$

Jadi to = 3, sehingga:

$s_o = (9t_o-3)/2 = (27-3)/2 = 12$

$r_o = (11s_o+3)/9 = (132+3)/9 = 15$

$w_o = (20r_o+19)/11 = (300+19)/11 = 29$

$v_o = (31w_o-19)/20 = (899-19)/20 = 44$

$z_o = (51v_o+19)/31 = (2244 +19)/31 = 73$

$y_o = (82z_o-19)/51 = (5986-19)/51 = 117$

$x_o = (625y_o+19)/82 = (73126+19)/82 = 892$

Selesaian kongruensi di atas adalah

$x \equiv 892 \pmod{625}$ atau $x \equiv 267 \pmod{625}$

Teorema 6.2

Jika (a,m) = 1 maka kongruensi linear ax ≡ b (mod m) mempunyai selesaian x = $a^{\phi(m)-1}b$, dimana $\phi(m)$ adalah banyaknya residu didalam sistem residu modulo m tereduksi.

Bukti.

Menurut teorem Euler jika (a,m) = 1 maka $a^{\phi(m)-1} = 1$.

ax ≡ b (mod m)

$a.\ a^{\phi(m)-1}.x \equiv b\ a^{\phi(m)-1}$ (mod m)

$a^{\phi(m)} \equiv b\ a^{\phi(m)-1}$ (mod m)

Karena $a^{\phi(m)} \equiv 1$ (mod m) dan $a^{\phi(m)}\ x \equiv b\ a^{\phi(m)-1}$ (mod m)

Maka $1.x \equiv b\ a^{\phi(m)-1}$ (mod m)

$x \equiv b\ a^{\phi(m)-1}$ (mod m)

$x \equiv a^{\phi(m)-1}\ b$ (mod m)

Contoh

1. Selesaikan 5x ≡ 3 (mod 13)

   Jawab

   Karena (5,13) = 1

   Maka kongruensi linear 5x ≡ 3 (mod 13) mempunyai selesaian

   $x \equiv 3.5^{\phi(13)-1}$ (mod 13)

   $\equiv 3.5^{12-1}$ (mod 13)

   $\equiv 3.(5^2)^5.5$ (mod 13)

$\equiv 3.(-1)^5 \ 5 \pmod{13}$, karena $5^2 \equiv -1 \pmod{13}$

$\equiv 11 \pmod{13}$

6.2 Kongruensi Simultan

Sering kita dituntut secara simultan untuk menentukan selesaian yang memenuhi sejumlah kongruensi. Hal ini berarti dari beberapa kongruensi linear yang akan ditentukan selesaiannya dan memenuhi masing-masing kongruensi linear pembentuknya.

Contoh

1. Diberikan dua kongruensi (kongruensi simultan)
   $x \equiv 3 \pmod{8}$

   $x \equiv 7 \pmod{10}$

   Karena $x \equiv 3 \pmod{8}$, maka $x = 3 + 8t$ ($t \in Z$).

   Selanjutnya $x = 3 + 8t$ disubstitusikan ke $x \equiv 7 \pmod{10}$, maka diperoleh

   $3 + 8t \equiv 7 \pmod{10}$ dan didapat

   $8t \equiv 7-3 \pmod{10}$

   $8t \equiv 4 \pmod{10}$

   Karena $(8,10) = 2$ dan $2 \mid 4$ atau $2 \mid 7-3$, maka kongruensi $8t \equiv 4 \pmod{10}$ mempunyai dua selesaian bilangan bulat modulo 10 yaitu

   $8t \equiv 4 \pmod{10}$

   $4t \equiv 2 \pmod{5}$

   $t \equiv 3 \pmod{5}$

Jadi $t \equiv 3 \pmod 5$ atau $t \equiv 8 \pmod{10}$

Dari $t \equiv 3 \pmod 5$ atau $t = 3 + 5r$ $(r \in Z)$ dan $t \equiv 8 \pmod{10}$ atau $x = 3 + 8t$

Selanjutnya dapat dicari nilai x sebagai berikut:

$x = 3 + 8t$

$= 3 + 8(3+5r)$

$= 3 + 24 + 40r$

$= 27 + 40r$ atau $x \equiv 27 \pmod{40}$ atau $x \equiv 27 \pmod{[8,10]}$

2. Diberikan kongruensi simultan
   $x \equiv 15 \pmod{51}$

   $x \equiv 7 \pmod{42}$

   Selesaian

   Karena $(51,42) = 3$ dan $15 \not\equiv 7 \pmod 3$ atau $3 \nmid 15 - 7$, maka kongruensi simultan di atas tidak mempunyai selesaian.

Teorema 6.3

Kongruensi simultan dari $x \equiv a \pmod m$ dan $x \equiv b \pmod n$

dapat diselesaikan jika

$a \equiv b \pmod{(m,n)}$ dan memiliki selesaian tunggal $x \equiv x_o \pmod{[m,n]}$.

Bukti

Diketahui : $x \equiv a \pmod m$ dan $x \equiv b \pmod n$

Kongruensi pertama $x \equiv a \pmod m \rightarrow x = a + mk, k \in Z$.

Kongruensi kedua harus memenuhi a + mk ≡ b (mod n) atau mk ≡ b-a (mod n)

Menurut teorema sebelumnya mk ≡ b-a (mod n) dapat diselesaikan jika

d | b-a, d = (m,n) atau dengan kata lain kondisi kongruensi a ≡ b (mod (m,n)) harus dipenuhi.

d = (m,n) → d | m dan d | m.

Jika d | m dan d | m maka $\frac{m}{d}, \frac{n}{d}, \frac{(b-a)}{d} \in Z$.

$\frac{m}{d}, \frac{n}{d}, \frac{(b-a)}{d} \in Z$ dan mk ≡ b-a (mod n) mengakibatkan

$\frac{mk}{d} \equiv \frac{(b-a)}{d} \left(\text{mod } \frac{n}{d} \right)$

Dari teorema sebelumnya jika d = (m,n) maka $\left(\frac{m}{d}, \frac{n}{d} \right) = 1$

Jika $\left(\frac{m}{d}, \frac{n}{d} \right) = 1$ dan $\frac{mk}{d} \equiv \frac{(b-a)}{d} \left(\text{mod } \frac{n}{d} \right)$, maka

$\frac{mk}{d} \equiv \frac{(b-a)}{d} \left(\text{mod } \frac{n}{d} \right)$ mempunyai 1 selesaian.

Misalkan selesaian yang dimaksud adalah k = k_o sehingga selesaian kongruensi adalah

k ≡ k_o (mod $\frac{n}{d}$) atau k = k_o + $\frac{n}{d}$ r, r ∈ Z.

Karena x = a = mk dan k = k_o + $\frac{n}{d}$ r, maka

$x = a + mk$

$= a + m\,(k_o + \frac{n}{d} r)$

$= (\, a + m\, k_o + \frac{mn}{d} r)$

$= (\, a + m\, k_o\,) + [m,n].r$; sebab $[m,n](m,n) = m.n$

$= x_o + [m,n]r$, sebab $x_o = (\, a + m\, k_o\,)$

$= x_o \pmod{[m,n]}$

Latihan soal dan jawaban:

1. Tentukan penyelesaian dari $9x + 16y = 35$
   Jawab:

   $9x + 16y = 35$ berarti $16y \equiv 35 \pmod 9$

   $$7y \equiv 35 \pmod 9$$

   $$y \equiv 5 \pmod 9$$

   ini berarti $y = 5 + 9t$ untuk suatu bilangan bulat t.

   kemudian substitusikan $y = 5 + 9t$ pada persamaan $9x + 16y = 35$ sehingga,

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

   $9x + 144t = -45$

   $x + 16t = -5$ sehingga diperoleh $x = -5 - 16t$

   Himpunan penyelesaian dari $9x + 16y = 35$ adalah $\{(x,y) \mid x = -5 - 16t,\ y = 5 + 9t$ dan t bilangan bulat$\}$. Jika $t = 0$ maka $x = -$

5 dan y = 5. Jadi, (-5, 5) merupakan solusi dari persamaan 9x + 16y = 35.

2. Carilah bilangan-bilangan bulat positif x dan y yang memenuhi

3. m

DAFTAR PUSTAKA

Al Jupri. 2022. *Dasar-Dasar Teori Bilangan.* Bandung: Yrama Widya

Sukirman. 2013. *Teori Bilangan*Yogyakarta: UNY Press.

BAB 7
ALGORITMA EUCLID

Oleh Ahmad Choirul Anam

7.1 Pendahuluan

FPB merupakan suatu istilah dalam matematika yang merupakan singkatan dari Faktor Persekutuan Terbesar, atau didalam bahasa inggris disebut sebagai *Greatest Common Divisor* (GCD). Dengan kata lain, bilangan bulat positif terbesar yang membagi dua bilangan disebut sebagai FPB atau GCD (Burton, 2002). Pada saat masih di sekolah menengah, bilangan yang digunakan tidak terlalu besar, sehingga FPB mudah ditemukan. Akan tetapi, bagaimana menemukan FPB jika dua bilangan yang akan digunakan merupakan bilangan yang cukup besar, maka dibutuhkan strategi lain dalam menyelesaikannya.

Matematikawan Yunani yang lahir pada tahun 350 M bernama Euclid dalam bukunya yang berjudul "*Element*" menuliskan suatu metode untuk menemukan pembagi persekutuan terbesar (*greatest common devisor* atau *gcd*) dari dua buah bilangan, dimisalkan *a* dan *b*. Hal ini berarti bahwa pembagi persekutuan terbesar dari dua buah bilangan bulat tak negatif adalah bilangan bulat positif terbesar yang habis membagi kedua bilangan tersebut. Euclid tidak menyebutkan metodenya sebagai algoritma, namun pada abad modern (sekitar tahun 1950) orang – orang menyebut metodenya itu sebagai "algoritma Euclidean" (*Euclid's algorithm*) (Everest, Graham & Ward, 1963).

Misalkan:
Diketahui $a = 80$
$b = 12$
Ditanya:

Pembagi persekutuan terbesar dari bilangan 80 dan 12, bisa juga disimbolkan $gcd(80, 12)$.

Sebelumnya, diuaraikan terlebih dahulu semua faktor pembagi dari masing-masing bilangan.

Semua faktor pembagi dari 80 adalah $1, 2, \mathbf{4}, 5, 8, 10, 16, 20, 40, 80$
Semua faktor pembagi dari 12 adalah $1, 2, \mathbf{4}, 6, 12$

Berdasarkan faktor pembagi yang telah diuraikan, terdapat bilangan yang sama sebagai faktor pembagi pada 80 dan 12 yaitu 4. Maka dapat disimpulkan bahwa $gcd(80, 12) = 4$

7.2 Algoritma Euclid (*Euclid's Algorithm*)

7.2.1 Algoritma

Algoritma adalah metode atau prosedur yang disiapkan untuk menyelesaikan atau memecahkan kesulitan dengan suatu instruksi atau tindakan secara berurutan dan sistematis.

Dewasa ini, perkembangan ilmu pengetahuan dan teknologi mengalami kemajuan yang cukup pesat dengan hasil yang semakin canggih dan kompleks. Salah satu iptek yang paling sering digunakan adalah komputer, kemampuan komputer dalam melakukan perhitungan memang bisa dikatakan lebih cepat dibandingkan manusia pada umumnya. Tetapi komputer tidak dapat menyelesaikan permasalahan dalam perhitungan begitu saja tanpa ada langkah-langkah (algoritma) yang sebelumnya sudah didefinisikan. Berikut

ditunjukkan beberapa pendapat dari ahli terkait definisi algoritma.

a. Algoritma menurut Kani adalah upaya yang digunakan untuk menyelesaikan permasalahan dengan tahapan yang sistematis dan disusun secara logis sebagai upaya untuk menghasilkan *output* tertentu (Munir, 1999).
b. Algoritma menurut Abu Ja'far Muhammad Ibn Musa Al Khawarizmi dalam bukunya Al-Jabr Wa-al Muqabala pada tahun 825 M dikenalkan sebagai algoris dan ritmis. Selanjutnya, algoritma lebih dikenal sebagai bahasa pemrograman dalam komputer yang berarti serangkaian metode terstruktur dan sistematis dalam menyelesaikan permasalahan (Jando, Emanuel & Nani, 2018).
c. Algoritma merupakan kumpulan instruksi atau proses yang dituliskan secara sistematis dan digunakan untuk memecahkan masalah logis dan matematis dengan menggunakan komputer (Sismoro, 2005).

Dengan demikian, Algoritma bisa dikatakan sebagai sekumpulan strategi dalam menyelesaikan permasalahan melalui langkah-langkah yang sistematis dan terstruktur dalam menemukan hasil tertentu, bisa secara manual ataupun menggunakan bantuan komputer.

7.2.2 Algoritma Euclid

Pembagi persekutuan terbesar dari dua bilangan bulat dapat ditemukan dengan mendaftar semua pembagi positifnya, kemudian menentukan bilangan yang menjadi pembagi persekutuan terbesar dari setiap bilangan bulat. Pada kasus dengan bilangan yang besar, maka lebih efisien menggunakan Algoritma Euclid.

Sebelum mengetahui lebih lanjut terkait algoritma euclid, sebaiknya mengetahui terkait algoritma pembagian.

Misalkan a dan b merupakan dua bilangan bulat positif dengan $a > 0$, maka b dibagi oleh a akan menunjukkan hasil bagi dan sisa pembagian.

Teorema 7.1

Jika a dan b bilangan bulat dengan $a > 0$, maka terdapat pasangan bilangan bulat q dan r sedemikian hingga

$$\boldsymbol{a = qb + r} \text{ dengan } \boldsymbol{0 \leq r < b},$$

dimana: q hasil bagi ($quotient$), b pembagi, r sisa, dan a bilangan yang dibagi (*devidend*).

Contoh:

Jika $a = 36$, dan $b = 4$, maka $q = 9$ dan $r = 0$

Jika $a = 133$, dan $b = 21$, maka $q = 6$ dan $r = 7$

Berdasarkan contoh di atas diketahui bahwa terdapat $r = 0$ dan $r = 7$. Menggunakan definisi keterbagian bahwa a dikatakan terbagi oleh b jika dan hanya jika sisa pembagian dari algoritma pembagian sama dengan 0, dapat disimbolkan $b|a$ (a habis terbagi oleh b atau b membagi habis a).

Algoritma Euclid didefinisikan sebagai berikut:

Misalkan a dan b adalah dua bilangan bulat yang akan dicari pembagi persekutuan terbesarnya (gcd). Sebelumnya, disimbolkan bahwa $gcd(|a||b|) = gcd(a, b)$ dan diasumsikan $a \geq b > 0$. Selanjutnya menerapkan algoritma pembagian pada a dan b, diperoleh

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

Jika $r_1 \neq 0$, maka bagi b dengan r_1 sehingga diperoleh q_2 dan r_2 yang memenuhi

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

Selanjutnya, jika $r_2 = 0$ maka proses perhitungan berhenti. Sebaliknya, jika $r_2 \neq 0$ menggunakan cara seperti sebelumnya diperoleh q_3 dan r_3, maka

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

Proses pembagian ini berlanjut sampai mendapatkan sisa pembagian sama dengan 0. Misalkan pada langkah ke $(n+1)$, dimana r_{n-1} dibagi r_n dengan $b > r_1 > r_2 > \cdots > 0$. Maka proses tersebut menghasilkan persamaan berikut:

$$\begin{aligned}
a &= q_1 b + r_1 && 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Berdasarkan proses pembagian di atas, perhatikan pada proses yang menghasilkan sisa tidak sama dengan 0, yaitu r_n. Maka dapat disimpulkan bahwa $gcd(a, b) = r_n$

Teorema 7.2

Jika $a = qb + r$, maka $gcd(a, b) = gcd(b, r)$

Bukti:

Jika $gcd(a, b) = d$, maka dapat dikatakan bahwa $d|a$ dan $d|b$ mengakibatkan $d|(a - qb)$ atau $d|r$ karena $r = a - qb$, sehingga d merupakan pembagi persekutuan dari b dan r. Selanjutnya di sisi lain, jika c merupakan sebarang pembagi persekutuan dari b dan r, maka $c|(qb + r)$ atau $c|a$. Hal ini mengakibatkan c merupakan pembagi persekutuan dari a dan b

dengan $c \leq d$. Dengan demikian, berdasarkan definisi pembagi persekutuan terbesar maka disimpulkan bahwa $d = gcd(a,b) = gcd(b,r)$.

Berdasarkan lemma dan pembuktian di atas, dari suatu sistem persamaan diperoleh bahwa

$$\begin{aligned} gcd(a,b) &= gcd(b,r_1) \\ &= gcd(r_1,r_2) \\ &= \vdots \\ &= gcd(r_{n-1},r_n) \\ &= gcd(r_n,0) \\ &= r_n \end{aligned}$$

Contoh

Tentukan $gcd(272,119)$

Penyelesaian

Menggunakan algoritma pembagian dan informasi terkait algoritma euclid, diketahui

$$a = qb + r \text{ , dengan } a \geq b > 0$$

Berdasarkan soal, $a = 272, b = 119$ diperoleh

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + \mathbf{17} \\ 34 &= 2 \cdot \mathbf{17} + 0 \end{aligned}$$

Dari proses perhitungan di atas, diketahui bahwa sisa yang tidak nol adalah **17**. Hal ini berarti 17 merupakan pembagi persekutuan terbesar dari 272 dan 119 dan dituliskan $gcd(272,119) = 17$.

Pembagi persekutuan terbesar atau biasa dikenal faktor persekutuan terbesar dari a dan b dapat dinyatakan sebagai kombinasi linier dari a dan b yang ditulisa dalam bentuk $ax + by$ dengan x dan y merupakan bilangan-bilangan tertentu. Untuk menentukan nilai x dan y yang memenuhi $gcd(a, b) = ax + by$ yaitu dengan menggunakan substitusi balik dari Algoritma Euclid.

$$r_n = r_{n-2} - q_n r_{n-1}$$

Selanjutnya, menyelesaikan persamaan dengan mengganti r_{n-1}, menjadi

$$\begin{aligned} r_n &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= (1 + q_n q_{n-1})r_{n-2} + (-q_n)r_{n-3} \end{aligned}$$

Berdasarkan proses di atas, r_n menunjukkan kombinasi linier dari r_{n-2} dan r_{n-3}. Melanjutkan substitusi balik dari sistem persamaan tersebut, maka $r_{n-1}, r_{n-2}, \dots, r_2, r_1$ sehingga $r_n = gcd(a, b)$ disebut sebagai kombinasi linier dari a dan b.

Contoh

Hitunglah $gcd(299, 247)$ dan tentukan bilangan – bilangan bulat m dan n yang memenuhi $299m + 247n = (299, 247)$

Penyelesaian

Misalkan $a = 299$ dan $b = 247$, menggunakan Teorema 7.1 dan definisi algoritma euclid maka diperoleh

$$\begin{aligned} 299 &= 1 \cdot 247 + 52 \\ 247 &= 4 \cdot 52 + 39 \\ 52 &= 1 \cdot 39 + \mathbf{13} \\ 39 &= 3 \cdot \mathbf{13} + 0 \end{aligned}$$

Sehingga, $gcd(299, 247) = 13$

Selanjutnya, dengan memperhatikan beberapa persamaan tersebut diperoleh

$$\begin{aligned} 13 &= 52 - 39 \cdot 1 \\ &= 52 - (247 - 4 \cdot 52) \cdot 1 \\ &= 52 \cdot 5 - 247 \\ &= (299 - 247) \cdot 5 - 247 \\ 13 &= 299 \cdot 5 + 247 \cdot (-6) \end{aligned}$$

Sehingga, nilai $m = 5$ dan $n = -6$

Meskipun demikian, nilai m dan n yang memenuhi $299m + 247n = 13$ tidak tunggal, hal ini dikarenakan masih terdapat

$299(5 - 247t) + 247(-6 + 299t) = 13$, untuk setiap bilangan bulat t. Sehingga, nilai yang lainnya adalah $m = 5 - 247t$ dan $n = -6 + 299t$, untuk setiap bilangan bulat t. Dalam hal ini, persamaan $299m + 247n = 13$ dengan m dan n bilangan bulat termasuk dalam Persamaan Linier Diophantus (Dhiopantine).

Gabriel lame (1795 – 1870) merupakan Matematikawan dari Perancis yang membuktikan bahwa banyaknya tahapan atau langkah dalam algoritma euclid paling banyak 5 kali banyaknya digit dari bilangan yang lebih kecil. Misalkan dalam menemukan $gcd(299, 247)$ seperti contoh di atas, bilangan 299 dan 247 memiliki tiga digit, maka langkah algoritma euclid tidak akan lebih dari $5 \cdot 3 = 15$ langkah. Kenyataannya dalam proses tahapan yang sudah dilakukan sebelumnya hanya memerlukan empat langkah saja.

Pada kasus lain, pembagi persekutuan terbesar (FPB atau *gcd*) dapat diperluas bukan hanya dua bilangan tetapi bisa lebih. Misalkan a, b, dan c merupakan bilangan yang tidak nol, maka $gcd(a, b, c) = d$

Contoh

$gcd(39, 42, 54) = 3$ dan $gcd(49, 210, 350) = 7$

Terdapat konsep yang setara dengan pembagi persekutuan terbesar (FPB atau *GCD*) dari dua bilangan bulat, yang lebih dikenal dengan kelipatan persekutuan terkecil (KPK) dalam bahasa inggris dikenal dengan istilah *least common multiple* (LCM).

Definisi 7.1

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

Nol (0) adalah suatu kelipatan persekutuan dari sebarang bilangan-bilangan bulat a dan b. Bilangan-bilangan bulat ab dan $-ab$ masing-masing juga merupakan suatu kelipatan persekutuan dari a dan b. Sehingga, himpunan semua kelipatan persekutuan bulat positif dari a dan b tidak pernah sama dengan himpunan kosong (SUKIRMAN, 2013).

Contoh:

Kelipatan persekutuan dari 6 dan -9

Himpunan semua kelipatan $6 = \{6, 12, 18, 24, . .\}$

Himpunan semua kelipatan $-9 = \{-9, 0, 9, 18, 27, 36, \dots\}$

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

Perlu diperhatikan bahwa himpunan bagian dari suatu himpunan bilangan bulat positif selalu memiliki anggota terkecil. Sehingga KPK atau *lcm* dari setiap dua bilangan bulat selalu ada.

Secara formal, kelipatan persekutuan terkecil (KPK atau lcm) dari dua bilangan bulat didefinisikan sebagai berikut.

Definisi 7.2

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

a) $a|m$ dan $b|m$
b) Jika $a|c$ dan $b|c$ dengan $c > 0$, maka $m \leq c$

Berdasarkan definisi di atas diketahui bahwa kelipatan dari setiap dua bilangan bulat yang tidak nol selalu merupakan suatu bilangan bilat positif. Pada a) syarat itu mengemukakan bahwa setiap dari dua bilangan itu membagi kelipatan persekutuan terkecilnya. Sedangkan pada b) menyatakan bahwa kelipatan persekutuan lainnya tidak lebih kecil dari KPK atau lcm dari dua bilangan itu.

Contoh:

Jika diketahui $lcm(6, 8) = 24$, maka berlaku

$6|24$ dan $8|24$ dan kelipatan persekutuan yang lain, misalnya $48, 72, 96, \ldots$ dan semuanya tidak lebih besar dari 24

Teorema 7.3

Untuk a dan b bilangan bulat positif

$$gcd(a, b) \cdot lcm(a, b) = ab$$

Bukti:

Misalkan $p = gcd(a, b)$ dan ditulis $a = pr, b = ps$ untuk suatu r dan s bilangan bulat. Jika $m = \frac{ab}{p}$, maka $m = as = br$. Persamaan

ini berakibat bahwa m (suatu bilangan positif) sebagai kelipatan persekutuan dari a dan b.

Selanjutnya, misalkan q merupakan bilangan bulat positif yang menjadi kelipatan persekutuan dari a dan b, dapat dikatakan bahwa $q = au = bv$. Seperti yang sudah dijelaskan sebelumnya, terdapat x dan y yang memenuhi $p = ax + by$. Sehingga

$$\begin{aligned}\frac{q}{m} &= \frac{qp}{ab} \\ &= \frac{q(ax+by)}{ab} \\ &= \left(\frac{q}{b}\right)x + \left(\frac{q}{a}\right)y \\ &= vx + uy\end{aligned}$$

Berdasarkan proses persamaan di atas, dinyatakan bahwa $m|c$, sampai dapat disimpulkan bahwa $m \leq c$. Menggunakan definisi kelipatan persekutuan terkecil, maka $m = gcd(a, b)$ dimana

$$lcm(a,b) = \frac{ab}{p} = \frac{ab}{gcd(a,b)}$$

Atau dapat ditulis

$$gcd(a,b) \cdot lcm(a,b) = ab$$

Teorema Akibat 7.3.1

Untuk setiap bilangan positif a dan b, maka $lcm(a,b) = ab$ jika dan hanya jika $gcd(a,b) = 1$

Bukti:

Menggunakan Teorema 7.3 yaitu $gcd(a,b) \cdot lcm(a,b) = ab$, diketahui bahwa proses perhitungan kelipatan persekutuan terkecil dari dua bilangan bulat bergantung pada nilai pembagi persekutuan terbesarnya yang selanjutnya dapat dihitung

menggunakan algoritma euclid. Secara matematis, ditunjukkan bahwa

Jika $lcm(a,b) = ab$, maka $gcd(a,b) = \frac{ab}{ab} = 1$

Jika $gcd(a,b) = 1$, maka $lcm(a,b) = \frac{ab}{1} = ab$

Contoh

Pada contoh sebelumnya yaitu $gcd(299,247) = 13$, menggunakan Teorema Akibat 7.3.1 maka dapat diketahui $lcm(299{,}247)$ yaitu

$$lcm(299,247) = \frac{299 \cdot 247}{13} = 5681$$

Soal Latihan

1. Apabila $gcd(a,b) = d$ buktikan bahwa $d \mid (ax + by)$ untuk setiap bilangan bulat x dan y.
2. Tentukan $gcd(12378, 3054)$ menggunakan proses algoritma Euclid.
3. Seorang petani membeli 100 ekor hewan dengan harga 4000. Harga seekor sapi 120, seekor domba 50 dan seekor kambing 25. Jika petani harus membeli sekurang-kurangnya seekor untuk jenis hewan tersebut, berapa ekor masing-masing hewan yang dibelinya?
4. Tentukanlah kelipatan persekutuan terkecil (KPK atau lcm) dari
   a. $(28, 35)$
   b. $(111, 303)$
   c. $(256, 5040)$
   d. $(343, 999)$
5. Tentukanlah pasangan-pasangan dua bilangan bulat positif a dan b yang memenuhi $gcd(a,b) = 18$ dan $lcm(a,b) = 540$.

DAFTAR PUSTAKA

Burton, D.M. (2002) *Elementary Number Theory*. 5th ed. New York: McGraw-Hill.

Everest, Graham & Ward, T. (1963) *An Introduction to Number Theory*. London: Springer.

Jando, Emanuel & Nani, P.A. (2018) *Algoritma dan Pemrograman dengan Bahasa Java*. Yogyakarta: Penerbit ANDI.

M. Kani, (2020) "Algoritma Dan Bahasa Pemrograman," In Pengantar Algoritma Dan Pemrograman,

Munir, R. (1999) *Algoritma dan Pemrograman*. Bogor: IPB.

Sismoro, H. (2005) *Pengantar logika informatika, algoritma dan pemrograman komputer*. Bogor: Penerbit ANDI.

SUKIRMAN (2013) *TEORI BILANGAN*. Yogyakarta: UNY Press.

BAB 8
Fungsi φ, Teorema Euler

Oleh Nanang

8.1 Fungsi bilangan bulat terbesar

Fungsi bilangan bulat terbesar, atau fungsi kurung siku [ ], sebetulnya bukan fungsi teori bilangan karena wilayahnya (daerah definisinya) .adalah himpunan bilangan real; jelajahnya (daerah nilainya) adalah himpunan bilangan bulat.

Definisi 10-1.

Untuk x bilangan real, [x] menyatakan bilangan bulat terbesar yang lebih kecil, atau sama dengan x:, dengan kata lain, [x] adalah bilangan bulat tunggal yang memenuhi x - 1 < [x] < x.

Contoh. $\left[-\frac{5}{4}\right] = -2$ $\left[\sqrt{2}\right] = 1$ $[\pi] = 3$ $\left[\frac{1}{4}\right] = 0$

Dari Definisi 4 – 20, tiap bilangan real x dapat ditulis

$$x = [x] + \theta$$

dengan $0 \leq \theta < 1$. Sering-sering ini dinamakan bagian pecahan dari x. Juga dari Definisi itu, -[-x] adalah bilangan bulat terkecil yang lebih besar atau sama dengan x.

Berikut ini diajukan sifat-sifat fungsi bilangan bulat terbesar. Bukti-buktinya dapat diperoleh dari Definisi 10-20 dan pembuktian diserahkan kepada para pembaca sebagai latihan. (Periksa Latihan).

Teorema 10-1. Sifat-sifat fungsi bilangan bulat terbesar

Misalkan x dan y bilangan real sebarang. Maka berlaku yang berikut ini.

(i) $[x] < x < [x] + 1$ atau $x - 1 < [x] \leq x$ atau $0 \leq x - [x] < 1$

(ii) $[x] = \sum 1$ untuk $x \geq 0$ dan i bilangan bulat $i \leq i \leq x$

(iii) $[x+m] = [x] + m$ jika m suatu bilangan bulat

(iv) $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$

(v) $[x] + [-x] = \begin{cases} 0; jika\ x\ bilangan\ bulat \\ -1; jika\ x\ bukan\ bilangan\ bulat \end{cases}$

(vi) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$ Jika m suatu bilangan bulat positif

Teorema 10-2. Bilangan bulat terdekat kepada x

Jika x suatu bilangan real, maka berlaku yang berikut ini.

(i) $[x + ½]$ adalah bilangan bulat yang terdekat kepada x. Jika x titik tengah antara dua bilangan bulat maka $[x + ½]$ adalah yang terbesar di antara kedua bilangan bulat itu.

(ii) $-[-x + h]$ adalah bilangan bulat yang terdekat kepada x. Jika x titik tengah antara dua bilangan bulat maka $-[-x + ½]$ adalah yang terkecil di antara kedua bilangan bulat itu.

Bukti:

Di sini diberikan bukti untuk bagian (i) saja. Bukti bagian (ii) dijadikan latihan. Misalkan m bilangan bulat terdekat kepada x.

Maka $m = x + \theta$ dengan $- ½ < \theta \leq ½$, atau $½ > - \theta \_> - ½$

Dari $x = m - \theta$, didapat $[x + ½] = m + [-\theta + ½]$

Tetapi $1 > - \theta + ½ \geq 0$ sehingga $[x +] = m$

Jika x = n_1 + ½ , dengan n_1 bilangan bulat, maka [x + ½] = n_1 + 1

yaitu bilangan bulat berikutnya setelah n_1.

Pandang dua bilangan bulat positif a = 3 dan n = 14 dan perhatikan barisan bilangan 1, 2, 3, ..., 14. Di antara 14 unsur barisan itu tampak bahwa jika masing-masing dibagi 3 maka ada 4 buah unsur yang merupakan bilangan bulat, yaitu 3, 6, 9, 12. Untuk a = 6,misalnya, (hanya ada dua bilangan bulat seperti itu,6 dan 12.

Perhatikan untuk n = 14 dan a = 3, $\left[\frac{n}{a}\right]=\left[\frac{14}{3}\right]=4$ yang merupakan banyaknya bilangan dalam barisan 1, 2, 3, ..., 14 yang terbagi 3. Untuk n = 14 dan a = 6, ada $\left[\frac{14}{6}\right]$ = 2 buah bilangan di antara 1 dan 14 yang terbagi 6.

Misalkan n = 16 dan a = 5 maka ada 3 bilangan bulat di antara 1, 2, 3, ..., 16 yang terbagi 5.

Kita resmikan pola ini ke dalam suatu teorema.

Teorema 10 - 3.

Jika a dan n dua bilangan bulat positif dengan a < n maka $\left[\frac{n}{a}\right]$ adalah banyaknya bilangan bulat di antara 1, 2, 3, ..., n yang terbagi a.

Bukti:

Misalkan a, 2a, 3a, ..., ka semua bilangan bulat positif yang lebih kecil atau sama dengan n, yang masing-masing terbagi a.

Maka ka $\leq$ n < (k + 1) a dan k $\leq \left[\frac{n}{a}\right]$ k + 1. Ini berarti $\left(\frac{n}{e}\right)$ = k.

Banyaknya bilangan bulat di antara 1, 2, 3, ..., n yang terbagi a adalah k buah.

Dari Definisi $\left[\frac{n}{a}\right]$, jika dimisalkan $\left[\frac{n}{a}\right]$ = α maka ini berarti n = α + r dengan 0 < r < a. Dengan pengertian ini kita pandang teorema berikut ini.

Teorema 10-4.

Untuk a dan b bilangan bulat sebarang yang masing-masing positif, berlaku

$$\left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{n}{ab}\right]$$

Bukti:

Andaikan $\left[\frac{n}{a}\right] = \alpha$ dan $\left[\frac{\alpha}{b}\right]$ = β

Maka n = αa + r_1 , 0 $\leq$ r_1 < a dan

a = βb + r_2 , 0 $\leq$ r_2 < b sehingga

n = αab + ar_2 + r_1 dan

$$\left[\frac{n}{ab}\right] = \beta + \left[\frac{ar_2 + r_1}{ab}\right]$$

Tetapi r_1 paling besar sama dengan a - 1 dan r_2 paling besar sama dengan b - 1; jadi ar_2 + r paling besar sama dengan a(b -1) + (a - 1) = ab - 1. Paling kecil r_1 = 0 dan r_2 = 0 sehingga paling kecil ar_2 + r sama dengan a(0) +0 = 0. Jadi 0 $\leq$ ar_2 + r_1 < ab.

Ini berakibat $\left[\frac{ar_2 + r_1}{ab}\right]$ = 0, atau $\left[\frac{n}{ab}\right] = \beta + \left[\frac{\alpha}{b}\right]$. Maka terbukti $\left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{n}{ab}\right]$

Contoh:

Misalkan n = 34, a = 4 dan b = 6

$$\left[\frac{n}{a}\right] = \left[\frac{34}{4}\right] = 8 \qquad \left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{8}{6}\right] = 1$$

$$\left[\frac{n}{ab}\right] = \left[\frac{34}{24}\right] = 1 \neq \left[\frac{\left[\frac{n}{a}\right]}{b}\right]$$

Misalkan n = 34, a = 4 dan b = 9

$$\left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{\left[\frac{34}{b}\right]}{9}\right] = 0 = \left[\frac{34}{36}\right] = \left[\frac{n}{ab}\right]$$

Bagaimana jika a = 2^2 dan b = 2^2, artinya a dan b masing-masing bilangan basit yang berkuasa bilangan bulat positif?

$$\left[\frac{\left[\frac{n}{a}\right]}{b}\right] = \left[\frac{\left[\frac{34}{22}\right]}{23}\right] = \left[\frac{8}{8}\right] = 1 \neq \left[\frac{34}{32}\right] = \left[\frac{34}{(2^2)(2^3)}\right] = \left[\frac{n}{ab}\right]$$

Teorema terdahulu (Teorema 10-4) memungkinkan diturunkannya beberapa teorema akibat yang di bawah ini tanpa semua buktinya.

<u>Teorema 10-5</u>.

Jika p suatu bilangan basit maka

$$\left[\frac{p^{\left[\frac{n}{s}\right]}}{p^t}\right] = \left[\frac{n}{p^{p+t}}\right]$$

Teorema 10-6.

Jika $m = n_1 + n_2 + ... + n_t$ dengan n_i positif untuk i = 1, 2, 3, . . . t, maka

$$\left[\frac{m}{a}\right] \geq \left[\frac{n_1}{a}\right] + \left[\frac{n_2}{a}\right] + ... + \left[\frac{n_t}{a}\right]$$

Bukti:

Misalkan $\left[\frac{n_1}{a}\right] = \alpha_1, \left[\frac{n_2}{a}\right] = \alpha_2, ..., \left[\frac{n_t}{a}\right] = \alpha_t$ ini berarti

$n_1 = \alpha_1 a + r_1 \qquad 0 \leq r_1 < a$

$n_2 = \alpha_2 a + r_2 \qquad 0 \leq r_2 < a$

. .

. .

. .

$n_t = \alpha_t a + r_2 \qquad 0 \leq r_t < a$

Maka

$m = n_1 + n_2 + ... + n_t$ menjadi

$m = (\alpha 1 + \alpha 2 + ... + \alpha_t)a + (r_1 + r_2 + ... + r_t)$

$$\left[\frac{m}{a}\right] = \alpha_1 + \alpha_2 + ... + \alpha_t + \left[\frac{r_1 + r_2 + ... + r_t}{a}\right]$$

Jadi $\left[\frac{m}{a}\right] \geq \left[\frac{n_1}{a}\right] + \left[\frac{n_2}{a}\right] + ... + \left[\frac{n_t}{a}\right]$

Berikut ini diberikan suatu teorema pentingnya merupakan hasil karya Legendre (1752-1833).

Teorema 10-7.

Andaikan p suatu bilangan basit dan n bilangan bulat positif. Maka kuasa (eksponen) k yang tertinggi bagi p yang memenuhi $p^k \mid n!$ adalah

$$k = \sum_{i=1}^{\infty} \left[\frac{n}{p_1} \right]$$

Contoh:

Pandang n = 10 dan 10! = $(2^8)(3^4)(5^2)(7)$ dalam bentuk kanoniknya. Banyaknya faktor 10! yang terbagi 2 adalah $\left[\frac{10}{2} \right] = 5$ dan yang terbagi 2^2 adalah $\left[\frac{10}{2^2} \right] = 2$ yang terbagi 2^3 adalah $\left[\frac{10}{2^3} \right] = 1$

Banyaknya faktor 10! yang terbagi 2^4 adalah $\left[\frac{10}{2^4} \right] = 0$

Menurut teorema di atas, kuasa tertinggi dari 2 untuk 10! adalah $\sum_{i=1}^{3} \left[\frac{10}{2^1} \right] = \left[\frac{10}{2} \right] + \left[\frac{10}{2^2} \right] + \left[\frac{10}{2^3} \right] = 5 + 2 + 1 = 8$. Memang 10! memiliki faktor 2^8 dan 8 merupakan kuasa tertinggi untuk faktor basit 2 dari 10!

Banyaknya faktor 10! yang terbagi 3 adalah $\left[\frac{10}{3} \right] = 3$; yang terbagi 3^2 adalah $\left[\frac{10}{3^2} \right] = 1$. Maka kuasa tertinggi dari 3 untuk 10! Adalah 3 + 1 = 4. Keuntungan teorema ini adalah cepatnya ditentukan kuasa tertinggi faktor basit untuk n!, tanpa menguraikan dulu n! ke dalam bentuk kanoniknya.

Bukti:

Pandang (1)(2)(3) ... (n-l)(n) = n! Kita hendak menentukan kuasa tertinggi dari p yang menjadi suatu faktor basit dari n! Banyaknya faktor untuk n! yang terbagi p adalah $\left[\frac{n}{p}\right]$ buah dan faktor-faktor itu adalah p, 2p, 3p, ..., $\left[\frac{n}{p}\right]$ p. Perkalian faktor-faktor itu menghasilkan (p)(2p)(3p) ... $\left[\frac{n}{p}\right]$ p) yang merupakan faktor dari n! Dari hasil kali (p)(2p)(3p) ... $\left(\left[\frac{n}{p}\right]\right)p$, dengan mengeluarkan p dari titip faktornya, diperoleh $P^{\left\lfloor\frac{n}{p}\right\rfloor}$ yang membagi hasil kali itu, yaitu (p)(2p)(3p) ... $\left(\left[\frac{n}{p}\right]p\right)$ = $p^{\left\lfloor\frac{n}{p}\right\rfloor}$ (1)(2)(3) ... $\left(\left[\frac{n}{p}\right]\right)$.

Kuasa tertinggi p yang membagi n! adalah $\left[\frac{n}{p}\right]$ ditambah dengan kuasa tertinggi p yang membagi (1)(2)(3) ... $\left(\left[\frac{n}{p}\right]\right)$.

Dalam barisan bilangan 1, 2, 3, ..., $\left[\frac{n}{p}\right]$, bilangan bulat terbesar yang merupakan kelipatan p adalah

$$\left[\frac{\frac{n}{p}}{p}\right]p = \left[\frac{n}{p^2}\right]p \qquad \text{(Teorema 10-5)}$$

Ini artinya ada $\left[\frac{n}{p^2}\right]$ buah kelipatan p dalam barisan bilangan tadi.

Dari hasil kali (1)(2)(3) ... $\left(\frac{n}{p}\right)$ dapat dikeluarkan faktor $p^{\left[\frac{n}{p^2}\right]}$

Maka

$$(p)(2p)(3p)\ldots\left(\left[\frac{n}{p}\right]p\right) = p^{\left[\frac{n}{p}\right]}p^{\left[\frac{n}{p^2}\right]}(1)\,(2)\,(3)\ldots\ldots\left(\left[\frac{n}{p^2}\right]\right)$$

Kuasa tertinggi p yang membagi n! adalah $\left[\frac{n}{p}\right]$ ditambah dengan $\left[\frac{n}{p^2}\right]$ ditambah dengan kuasa tertinggi p yang membagi (1) (2) (3) .... $\left(\left[\frac{n}{p^2}\right]\right)$.

Jalan pikiran ini dapat diteruskan

$$(p)(2p)(3p)\ldots\left(\left[\frac{n}{p}P\right]\right) = p^{\left[\frac{n}{p}\right]}p^{\left[\frac{n}{p^2}\right]}p^{\left[\frac{n}{p^3}\right]}(1)\,(2)\,(3)\ldots\left(\left[\frac{n}{p^3}\right]\right)$$

$$= p^{\left[\frac{n}{p}\right]}p^{\left[\frac{n}{p^2}\right]}p^{\left[\frac{n}{p^3}\right]}p^{\left[\frac{n}{p^4}\right]}(1)\,(2)\,(3)\ldots\left(\left[\frac{n}{p^4}\right]\right)$$

Pada suatu ketika akan diperoleh $p^3 \le n \le p^{n+1}$ yang menghasilkan $\left[\frac{n}{p^3}\right] \neq 0$ tetapi $\left[\frac{n}{p^{3+1}}\right] = 0$.

Jadi kuasa k tertinggi untuk p yang memenuhi p^k |n! adalah

k = $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]\ldots+\left[\frac{n}{p^3}\right]=\sum_{i=1}^{s}\left[\frac{n}{i}\right]$. Tetapi karena untuk i s $\left[\frac{n}{p^1}\right]=0$ maka ditulis k = $\sum_{i=1}^{s}\left[\frac{n}{p^i}\right]$.

Dari Teorema 10-7 di atas. jumlah total p membagi n! adalah $k=\sum_{i=1}^{\infty}\left[\frac{n}{p_1}\right]$. Ini acapkali diberikan dalam bentuk persamaan yang biasanya disebut rumus Legendra :

$$n!=\prod_{p\le n} p^{\sum_{I=1}^{\infty}\left[\frac{n}{p^i}\right]}$$

Contoh:

Terapan Teorema 10-7 adalah pada soal seperti yang berikut ini. Pada penulisan 20! berapa buah nolkah mengakhiri penulisan bilangan itu? Ini artinya kita harus tahu berapa kalikah 10 menjadi pembagi 20! Untuk ini 20! dibagi oleh 2 berapa kali dan juga dibagi oleh 5 berapa kali; kemudian dari dua bilangan yang diperoleh, diambil yang paling rendah.

Dengan Teorema 10-7, 2 membagi 20! sebanyak 18 kali.

$$\left[\frac{20}{2}\right]+\left[\frac{20}{2^2}\right]+\left[\frac{20}{2^3}\right]+\left[\frac{20}{2^4}\right]=10+5+2+1=18$$

(Perhatikan $\left[\frac{20}{2^5}\right]=0$; begitu juga $\left[\frac{20}{2^i}\right]=0$ untuk i bilangan bulat positif > 5).

Dengan teorema yang sama» 5 membagi 20! sebanyak 4 kali

$$\left[\frac{20}{5}\right]+\left[\frac{20}{5^2}\right]+\ldots=4+0+\ldots=4$$

Ini berarti kuasa tertinggi untuk 5 dalam 20! adalah 4. Jika memang ada 2 dalam 20! (memang ada) maka 20! mengandung faktor 10 .

Maka ini berarti bahwa 20! berakhir dengan 4 buah nol.

Teorema 10-8 berikut ini sebenarnya dapat dibuktikan dengan cara lain tetapi di sini dibuktikan dengan menerapkan Teorema 10-7.

Teorema 10-8.

Andaikan n dan r bilangan bulat positif dan 1 < r < n. Maka

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

merupakan suatu bilangan bulat.

Bukti:

Dari Teorema 10-1, Bagian iv, [x] + [y] ≥ [x + y] untuk dua bilangan real sebarang x dan y.

Pandang r!(n - r)! Perhatikan bahwa n = r + (n - r).

Untuk tiap faktor basit p untuk r! (n - r)!,

Jika tiap suku dijumlahkan menurut indeks k, maka

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{n}{p^k}\right] + \left[\frac{n-r}{p^k}\right] \qquad k = 1, 2$$

Ruas kiri dari (*) adalah kuasa tertinggi untuk p yang membagi n! Ruas kanan dari (*) adalah kuasa tertinggi untuk p yang membagi r!(n - r)! Maka dalam bilangan $\frac{n!}{r!(-r)!}$, pada pembilangnya paling kurang p muncul sama banyaknya dengan ia muncul pada penyebutnya.

Tetapi ini berlaku juga untuk faktor basit lain, misalnya q, yang membagi r!(n - r)! Maka r! (n - r)! Maka r! (n – r)! membagi n!

Kalau begitu, $\frac{n!}{r!(-r)!}$ adalah suatu bilangan bulat.

Teorema 10-9.

Misalkan r suatu bilangan bulat positif. Maka hasil kali r buah bilangan positif berurutan sebarang, dapat dibagi r!

Bukti:

Pandang barisan bilangan bulat positif menurun r buah bilangan yang mulai dari n,

$$n, n-1, n-2, ..., n - (r - l)$$

Hasil kali bilangan-bilangan itu adalah

$$(n) (n - l) (n - 2) ... (n – r + 1)$$

Ini dapat ditulis $n(n - l) (n - 2) ... (n – r + 1) = \frac{n!}{r!(-r)!}$ r!

Dari Teorema 10-8, $\frac{n!}{r!(-r)!}$ adalah bilangan bulat.

Jadi ini berakibat bahwa r! membagi (n) (n - l) (n - 2) ... (n – r + 1)

Teorema 10-10.

Andaikan f dan F dua fungsi teori bilangan yang dihubungkan dengan rumus

$$F(n) = \sum_{d \mid n} f(d)$$

Maka untuk sebarang bilangan bulat positif m, berlaku

$$\sum_{n-1}^{m} F(n) = \sum_{n-1}^{m} F(k)\left(\frac{m}{k}\right)$$

Bukti:

Dari F(n) = $\sum_{d \mid n}$ f(d) dapat diperoleh $\sum_{n=1}^{m} F(n) = \sum_{n=1}^{m}\sum_{d|n} f(d)$

Andaikan ada suatu bilangan bulat k yang membagi m dengan k ≤ m maka f(k) akan muncul dalam jumlah $\sum_{d \mid n}$ f(d) jika dan hanya jika k suatu pembagi n. Karena tiap n memiliki n itu sendiri sebagai salah satu pembaginya. Maka f(k) muncul paling kurang satu kali dalam $\sum_{n=1}^{\infty}\sum_{d|n} f(d)$.

Yang perlu dihitung adalah berapa banyak jumlah $\sum_{d|n} f(d)$ yang mengandung f(k) seperti yang dimaksud. Untuk ini cukup dihitung berapa buah kelipatan k terdapat di antara 1, 2, ..., m, yaitu $\left(\frac{m}{k}\right)$ buah. Maka untuk tiap k yang memenuhi 1 ≤ k ≤ m, f(k) merupakan suatu suku dalam $\sum_{d \mid n}$ untuk $\left(\frac{m}{k}\right)$ buah bilangan bulat positif yang lebih kecil atau sama dengan m.

Maka $\sum_{n=1}^{m}\sum_{d|n} f(d) = \sum_{n=1}^{m}\sum_{d|n}\left(\frac{m}{k}\right)$

Teorema 10-10 menurunkan langsung dua teorema berikut ini.

<u>Teorema 10-11</u>.

Untuk m suatu bilangan bulat positif, berlaku $\sum_{n=1}^{m}\sum_{d|n} f(d) = \sum_{k=1}^{m} f(k)\left(\frac{m}{k}\right)$

Pembuktian dapat dikerjakan sebagai latihan

Teorema 10-12.

Untuk m suatu bilangan bulat positif, berlaku $\sum_{n=1}^{m}\sigma(n)=\sum_{n=1}^{m}n\left(\frac{m}{k}\right)$

Pembuktian dapat dikerjakan sebagai latihan.

Contoh:

Pandang m = 8

$$\sum_{n-1}^{8}\tau(n)= \tau(1)+\tau(2)+\tau(3)+\tau(4)+\tau(5)+\tau(6)+\tau(7)+\tau(8)$$

$$= 1 + 2 + 2 + 3 + 2 + 4 + 2 + 4 = 20$$

$$\sum_{n-1}^{8}\left(\frac{8}{n}\right)=[8]+[4]+\left(\frac{8}{3}\right)+[2]+\left(\frac{8}{5}\right)+\left(\frac{8}{6}\right)+\left(\frac{8}{7}\right)+[1]$$

$$= 8+4+2+2+1+1+1+1= 20$$

$$\sum_{n-1}^{8}\tau(n)=\sum_{n-1}^{8}\left(\frac{8}{n}\right)=20$$

$$\sum_{n-1}^{8}\sigma(n)=\sigma(1)+\sigma(2)+\sigma(3)+\sigma(4)+\sigma(5)+\sigma(6)+\sigma(7)+\sigma(8)$$

$$= 1 + 3 + 4 + 7 + 6 + 12 + 8 + 15 = 56$$

$$\sum_{n-1}^{8}\sigma(n)=\sigma(1)+\sigma(2)+\sigma(3)+\sigma(4)+\sigma(5)+\sigma(6)+\sigma(7)+\sigma(8)$$

$$= 8 + 8 + 6 + 8 + 5 + 6 + 7 + 8 = 56$$

$$\sum_{n-1}^{8}\sigma(n)=\sum_{n-1}^{8}n\left(\frac{8}{n}\right)=56$$

Jika Teorema 10-1 dan 10-12 merupakan suatu interaksi antara fungsi - fungsi [ ] dengan τ dan [ ] dengan σ, maka yang berikut ini suatu interaksi antara fungsi [ ] dan fungsi-μ Moebius.

Teorema 10-13.

Untuk m suatu bilangan bulat positif, berlaku

$$\sum_{n-1}^{m} \mu(n)\left(\frac{m}{n}\right) = 1$$

Bukti:

Pembuktian teorema ini memerlukan suatu teorema terdahulu yang menunjukkan

$$\sum_{d_1 \mid 1} \mu(d_1) + \sum_{d_2 \mid 2} \mu(d_2) + ... + \sum_{d_m \mid m} \mu(d_{m1})$$

Baik dijadikan latihan saja.

Contoh:

Misalkan m = 12 dan n = 5

$$\sum_{n=1}^{12} \mu(n)\left(\frac{12}{n}\right) = \mu(1)\ (12) + \mu(2)\ (6) + \mu(3)(4) + \mu(4)(3) + \mu(5)(2)$$
$$+ \mu(6)(2) + \mu(7)(1) + \mu(8)(1) + \mu(9(1) + \mu\ (10)(1)$$
$$+ \mu(11)(1) + \mu(12)\ (1) =$$
$$12 - 6 - 4 + 0 - 2 + 2 - 1 + 0 + 0 + 1 - 1 + 0 = 1$$

8.2 Fungsi Ø(fi) Euler

Selain fungsi-fungsi aritmetika (fungsi teori bilangan) τ, σ dari μ dan λ terdahulu, ada satu lagi fungsi yang menarik, yaitu fungsi Ø (fi) Euler yang dibahas berikut ini. Fungsi Ø ini adalah

fungsi ganda dan ia banyak berguna dalam pembuktian teorema-teorema kekongruenan modulo m. Fungsi Ø ini dapat dibataskan dengan pengertian sistem residu modulo m, yaitu dari pandangan kekongruenan modulo m, atau dengan cara lain.

Definisi 10-2.

Sistem residu sederhana (yang disederhanakan) modulo m adalah himpunan bilangan-bilangan bulat r_1 yang memenuhi $(r_i,m) = 1$ dengan $r_1 \neq rj \pmod m$ untuk $i \neq j$. Untuk tiap bilangan bulat x yang basit terhadap m ada unsur r. dalam himpunan itu sehingga $x = r. \pmod m$.

Contoh:

1. Pandang modulo 9.
   {l, 2, 3, 4, 5, 6, 7, 8, 9} merupakan suatu sistem residu lengkap modulo 9. Di antara unsur-unsur sistem residu itu, 1, 2, 4, 5, 7 dan 8 masing-masing adalah basit terhadap 9. Maka {1, 2, 3, 5, 7, 8} merupakan suatu sistem residu sederhana modulo 9. Suatu sistem residu sederhana modulo 9 yang lain adalah {10, -7, 22, -2, 8}.
2. Untuk modulo 6, {1,5} adalah sistem residu sederhana modulo 6.

Definisi 10-3.

Fungsi Ø Euler untuk bilangan bulat $n \geq 1$, Ø(n) menyatakan banyaknya bilangan bulat positif k yang lebih kecil daripada n tetapi basit terhadap n, yaitu (k , n) = 1.

Dengan Definisi ini maka Ø(l) = 1 karena (1 , 1) = 1

Definisi 10-4.

Fungsi Ø Euler adalah banyaknya unsur sistem residu sederhana modulo m; Ø(m) sama dengan kekardinalan sistem residu sederhana modulo m.

Contoh:
Kita hendak menentukan Ø(9).

Dengan Definisi 10-35, kita pandang barisan bilangan 1, 2, 3, 4, 5, 6, 7, 8, 9 dan kita temukan bahwa ada 6 bilangan yaitu 1, 2, 4, 5, 7, 8 yang masing-masing basit terhadap 9.

Maka Ø(9) = 6.

Dengan Definisi 10-36, kita tentukan dulu bahwa {1, 2, 4, 5, 7, 8} sistem residu sederhana modulo 9. Karena banyaknya unsur dalam sistem itu adalah 6, maka Ø(9) = 6.

Catatan. Ø(n) sering juga disebut indikator n

Dari contoh terdahulu, Ø(9) = 6; dapat dikatakan bahwa indikator 9 adalah 6.

Jika p bilangan basit maka dari pengamatan Ø(p) = p-1; atau dikatakan indikator p adalah p-1.

Teorema 10-14.

Jika p bilangan basit dan k bilangan bulat positif maka

$$Ø(p^k) = p^k - p^{k-1} = p^k \left(1-\frac{1}{2}\right) = p^{k-1}(p-1)$$

Bukti.

Pandang barisan bilangan

1, 2, 3, ... p, p + 1, p + 2, ... 2p, ..., p

Tiap bilangan dalam barisan bilangan itu akan basit terhadap p atau merupakan kelipatan p.

Dalam barisan itu, p muncul $\left(\frac{p^k}{p}\right)$ kali atau p^{k-1} kali. Ini berarti ada P^{k-1} buah bilangan dalam barisan tadi yang kelipatan p sehingga ada $p^k - p^{k-1}$ buah bilangan basit terhadap p.

Maka $\emptyset(p^k) = pk - {}^{pk-}1 = {}^{pk-}1\ (p - 1) = p^k\ (1 - \frac{1}{p})$ seperti yang dinyatakan teorema ini.

Contoh

Ambil p = 3 bilangan basit

Maka $\emptyset(3) = \emptyset(3^2) = 3^{2-1}(3 - l) = (3)(2) = 6$. Terdahulu telah dihitung (dengan cara lain) bahwa $\emptyset(9) = 6$.

Perhatikan bahwa untuk k = 1, teorema ini memberikan $\emptyset(p) = p - 1$. Ini dapat juga disimak dengan memandang sistem residu sederhana modulo p, p bilangan basit.

Teorema 10-15.

Untuk p bilangan basit, $\emptyset(p) = p - 1$.

Lema 10-1.

Diberikan bilangan-bilangan bulat a, b, c. Maka (a, b, c)= jika dan hanya jika (a, b) = 1 dan (a,c) = 1.

Bukti:

Misalkan (a,b, c) = 1 dan (a,b) = d

Ini artinya d|a dan d|b sehingga d|bc. Maka (a, be) $\geq$ d. Tetapi (a,bc) = 1 maka d = 1. Dengan cara berfikir yang sama, (a,c) = 1 Misalkan (a,c) = 1 = (a,b), dan (a,bc) = $d_1 > 1$. Maka ada bilangan basit $p|d_1$. Karena $d_1|bc$ maka p|bc sehingga p|b atau p|c; juga $d_1|a$ memberikan p|a. Maka (a,b) $\geq$ p tetapi (a,b) = 1 dan juga (a,c) $\geq$ p tetapi (a,c) = 1 sehingga haruslah p = 1 yang mustahil

karena p bilangan basit, p ≥ 2. Ini berarti d_1 tidak memiliki faktor basit, atau d, = 1.

Teorema 10-16.

Fungsi Ø Euler adalah fungsi ganda. Dengan kata lain, jika (a,b) = 1 maka Ø (ab) = Ø (a) Ø (b).

Bukti:

Kita susun m = ab buah bilangan dari 1 hingga ab dalam bentuk susunan berikut ini, yaitu b buah baris yang masing-masing terdiri dari a buah unsur

1	2	3	....	k	....
a+1	z+2	a+3	....	a+k	....
2a-4-l	2a+2	2a+3	....	2a+k	....

.
.
.

(b – 1) a + 1 (b - l) a + 2 (b - l) a + 3 ... (b - l) a + k ... ba

Perhatikan baris pertama, yaitu barisan bilangan 1, 2, 3, ..., a Dalam barisan ini ada Ø(a) buah bilangan yang basit terhadap a. Perhatikan unsur k dalam barisan 1, 2, 3, ..., a dan kolom yang dikepalai k. Tiap unsur dalam kolom ini berbentuk sa + k ≡ k (mod a) Jika k dan a memiliki pembagi yang sama, maka tiap unsur kolom ini memiliki pembagi yang sama dengan a.

Jika k basit terhadap a maka tiap unsur kolom ini akan basit terhadap a. Banyaknya k yang basit terhadap a ini telah ditunjukkan ada (a) buah. Maka ada Ø(a) buah kolom bilangan, antara 1 dan ab, yang basit terhadap a, Dari antara Ø(a) buah kolom bilangan itu, berapa buah basit terhadap Perhatikan barisan bilangan dalam kolom yang dikepalai k, dengan (k,a) = 1, yaitu k, a+k, 2a+k, ... (b-l) a k. Tidak ada dua bilangan dalam

barisan b buah bilangan bulat itu yang saling kongruen modulo b. Misalkan ada dua yang kongruen modulo b. Maka

$$sa + k \equiv ta + k \pmod{b}$$

$$(t - s)\, a = 0 \pmod{b}$$

Tetapi (a, b) = 1, atau b tak membagi a. Maka: $t - s = 0 \pmod{b}$

Dari susunan bilangan dalam bentuk bujur sangkar tadi, $0 < s < b$ dan $0 < t < b$ sehingga $t - s = 0 \pmod{b}$ hanya bisa terjadi jika t = s. Namun demikian, jika $s = t \pmod{b}$ maka (s,b) = 1 jika dan hanya jika (t,b) = 1. ini artinya bilangan-bilangan k, a + k, 2a + k, ... (b - l) a + k masing-masing kongruen modulo b terhadap 0, 1, 2, ..., b - 1 dalam suatu urutan tertentu. Jika dalam barisan 0, 1, 2, ..., b - 1 ada 4 > (b) buah bilangan yang basit terhadap b maka dalam barisan k, a + k, 2a + k, ..., (b - l) a + k pun ada Ø (b) buah bilangan yang basit terhadap b. Telah ditunjukkan bahwa barisan yang seperti yang terakhir ini ada Ø (a) buah banyaknya.

Dari banyaknya ab buah bilangan bulat dalam susunan siku empat ukuran a kali b di awal pembuktian, yang basit terhadap a dan sekaligus terhadap b, adalah Ø (a) Ø (b) buah.

Teorema 10–17.

Andaikan bilangan bulat n > 1 memiliki bentuk kanonik

$$n = P_1^{K_1} P_{21}^{K_2} \ldots\ldots P_r^{K_{1r}}$$

Maka

$$\phi(n) = \left(P_1^{K_1} - P_1^{K_1^{-1}}\right)\left(P_2^{K_2} - P_2^{K_2^{-1}}\right)\ldots\left(P_r^{K_r} + P_r^{K_r}\right)$$

$$= n\,(1 - 1/P_1)\,(1 - 1/P_2)\ldots(1 - 1/P_r)$$

$$= P_1^{k_1^{-1}} P_2^{k_2^{-1}} \ldots P_r^{k_r^{-1}} (P_1 - 1)(P_2 - 1)\ldots(P_r - 1)$$

Bukti:

$\phi(n) = \phi\left(P_1^{k_1^{-1}} P_2^{k_2^{-1}} \ldots P_r^{k_r^{-1}}\right)$, tetapi karena Ø adalah fungsi gana dan $(P_1, P_j) = 1$ (Teorema 10–10) maka

$$\phi(n) = \phi\left(P_1^{k_1^{-1}} P_2^{k_2^{-1}} \ldots P_r^{k_r^{-1}}\right)$$

Dengan Teorema 10-17 diperoleh

$$\phi(n) = P_1^{K_1}\left(P_1^{-1}\right)P_2^{K_2^{-1}} P_2^{-1} \ldots P_r^{K_{r^{-1}}}\left(P_r^{-1}\right)$$

$$= P_1^{K_{1^{-1}}} P_2^{K_2^{-1}} \ldots P_r^{K_{r^{-1}}}\left(P_2^{-1}\right)\left(P_2^{-1}\right)\ldots\left(P_r - 1\right)$$

$$= n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_r}\right)$$

Contoh :

Ambil m = 9000 = $2^3 . 3^2 . 5^3$

Ø(9000) = Ø ($2^3 . 3^2 . 5^3$) = Ø(2^3) Ø(3^2) Ø(5^2) =

$2^{3-1}(2-1) . 3^{2-1}(3-1) . 5^{3-1}(5-1)$

Ø(9000) = (4) (1) (3) (2) (25) (4) = 2400

Banyaknya bilangan antara 1 dan 9000 yang basit

a) terhadap 2 dan 5 adalah (9000) $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$ = 3600

b) terhadap 3 adalah (9000) $\left(1-\frac{1}{3}\right)$ = 6000

c) terhadap 2, 3 dan 5 adalah (9000) $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$ = 2400

Teorema 10–18.

Untuk bilangan bulat n > 2, Ø(n) adalah bilangan bulat genap.

Bukti:

Misalkan n = 2^k dengan k ≥ 2 bilangan bulat.

Maka Ø(n) = Ø(2^k) = 2^k (l - $\left(1-\frac{1}{2}\right) = 2^{k-1}$. Ini suatu bilangan bulat genap.

Misalkan n bukan bilangan 2 dengan kuasa tertentu; katakanlah n = p^hm dengan h ≥ 1 dan p bilangan basit ganjil sehingga (p^h, m) = 1 Maka Ø(n) = Ø(p^h,m) = Ø(p^hm) Ø(m) = p (p-l)(J)(m)

Karena p - 1 bilangan bulat genap maka Ø(n) genap.

DAFTAR PUSTAKA

Jones, Gareth A and J. Mary Jones. (2005). *Elementary Number Theory*, Spring-Verlag, London.

Redmond, D. (1996). *Number Theory*. New York: Marcel Dekker.

Rosen, Kenneth h. (2000). *Elementary Number theory and Its Application*, four edition. Massachussetts: Addison Wesley.

Sukirman. (2016). *Teori Bilangan*. Jakarta: Universitas Terbuka.

Sukirman. (2000). *Pengantar Teori Bilangan*, Universitas Negeri Yogyakarta: Press Yogya.

Tung, Khoe Yao. (2008). *Memahami Teori BIlangan dengan Mudah dan Menarik*. Jakarta: PT Gramedia Widiasarana Indonesia.

BAB 9
AKAR PRIMITIVE DAN INDEKS

Oleh Azmidar

9.1 Tingkat suatu bilangan bulat modulo n

Sebelum membahas tentang akar primitive, marilah kita mengingat terlebih dahulu tentang teorema Euler, yaitu jika $(b, n) = 1$ maka $b^{\phi(n)} \equiv 1 \pmod{n}$. Namun, tidak jarang ada kepangkatan bulat positif dari b yang lebih kecil dari $\phi(n)$ dan kongruen modulo m dengan 1 (Rosen, 2005). Misalnya, berdasarkan teorema Euler, diketahui bahwa $2^{\phi(5)} = 2^8 \equiv 1 \pmod{5}$. Akan tetapi, kita ketahui juga bahwasanya $2^4 \equiv 1 \pmod{5}$ dan tidak ada lagi bilangan bulat positif kurang dari 4 yang digunakan untuk memangkatkan 2 agar hasilnya kongruen dengan 1 modulo 5. Ini adalah sebuah contoh pengertian dari tingkat dari 2 modulo 5. Secara formal, diberikan definisi di bawah ini.

Definisi 1. tingkat suatu bilangan bulat modulo n

Misalkan suatu bilangan bulat $n > 1$dan $(b, n) = 1$. Tingkat dari b modulo n adalah suatu bilangan bulat positif terkecil r sedemikian hingga $b^r \equiv 1 \pmod{n}$ (Burton, 2010).

Tingkat dari b modulo n dituliskan dengan simbol $\text{ord}_n b$

Contoh 1.

Untuk menentukan tingkat 4 modulo 11, kita menentukan pangkat bulat positif terkecil dari 4 yang sisa bagi terkecilnya sama dengan 1. Oleh karenanya, pertama-tama yang harus dilakukan adalah menentukan sisa bagi-sisa bagi terkecil modulo 11 dari kepangkatan bulat positif dari 4, yaitu:

$4^1 \equiv 4 \pmod{11}$; $4^2 \equiv 5 \pmod{11}$; $4^3 \equiv 9 \pmod{11}$

$4^4 \equiv 3 \pmod{11}$; $\mathbf{4^5 \equiv 1 \pmod{11}}$; $4^6 \equiv 4 \pmod{11}$

Jadi, $\text{ord}_{11}4 = 5$

Dengan cara yang sama, untuk menentukan tingkat 5 modulo 11, kita menentukan sisa bagi terkecil modulo 11 dari kepangkatan bulat positif dari 5 seperti di bawah ini.

$5^1 \equiv 5 \pmod{11}$; $5^2 \equiv 3 \pmod{11}$; $5^3 \equiv 4 \pmod{11}$

$5^4 \equiv 9 \pmod{11}$; $\mathbf{5^5 \equiv 1 \pmod{11}}$; $5^6 \equiv 5 \pmod{11}$

Jadi, $\text{ord}_{11}5 = 5$

Contoh 2.

Cermati sisa bagi terkecil dari kepangkatan bulat positif *b* modulo 11 pada tabel 9.1 di bawah ini.

Tabel 9.1. Sisa bagi dari suatu bilangan positif *b* modulo 11

b	b^2	b^3	b^4	b^5	b^6	b^7	b^8	b^9	b^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

Pada tabel 9.1 terlihat bahwa $\text{ord}_{11}1 = 1, \text{ord}_{11}2 = 10$ sebab 10 merupakan bilangan bulat positif terkecil sedemikian hingga $2^{10} \equiv 1 \pmod{11}$. Demikian halnya dengan $\text{ord}_{11}3 = 5$ sebab 5 merupakan bilangan bulat positif terkecil sedemikian hingga

$3^5 \equiv 1 \pmod{11}$. Selanjutnya, teliti kembali tabel 11.1, akan didapati: $\text{ord}_{11}4 = 5$, $\text{ord}_{11}5 = 5$, $\text{ord}_{11}6 = 10$, $\text{ord}_{11}7 = 10$, $\text{ord}_{11}8 = 10$, $\text{ord}_{11}9 = 5$, dan $\text{ord}_{11}10 = 2$.

Berapakah tingkat dari 13 (mod 11)?

Karena $13 \equiv 2 \pmod{11}$ maka $13^{10} \equiv 2^{10} \pmod{11}$ dan oleh karena $2^{10} \equiv 1 \pmod{11}$, yaitu $\text{ord}_{11}2 = 10$, maka $\text{ord}_{11}13 = 10$ juga.

Pada definisi 1. tentang tingkat, perlu ditekankan bahwa tingkat dari $b \pmod{n}$ hanya ada jika memenuhi syarat $(b, n) = 1$. Jika $(b, n) \neq 1$, seperti yang telah dipahami bersama bahwa kekongruenan linear $bx \equiv 1 \pmod{n}$ tidak memiliki penyelesaian (Rosen, 2005).

Pada contoh tersebut, tampak bahwa tingkat dari bilangan-bilangan bulat positif b modulo 11 selalu membagi $\phi(11) = 10$, yaitu tingkat b mod 11, yaitu 1, 2, 5, dan 10 yang masing-masing membagi 10. Hal ini membawa kita pada teorema berikut ini.

Teorema 1.

Misalkan $(b, n) = 1$ dan tingkat $b \pmod{n}$ adalah r maka $b^s \equiv 1 \pmod{n}$ jika dan hanya jika $r \mid s$.

Bukti

Tingkat $b \pmod{n}$ adalah r, hal ini berarti r adalah suatu bilangan bulat positif terkecil sedemikian hingga $b^r \equiv 1 \pmod{n}$.

Perhatikan bilangan-bilangan bulat positif r dan s. Berdasarkan aturan pembagian, terdapat bilangan-bilangan bulat u dan v sedemikian hingga $s = ru + v$ dengan $0 \leq v < r$ sehingga didapatkan:

$$b^s = b^{ru+v} = (b^r)^u b^v$$

Karena diketahui bahwa $b^s \equiv 1 \pmod{n}$ maka

$$(b^r)^u b^v \equiv 1 \pmod{n}$$

$$b^v \equiv 1 \pmod{n} \text{ sebab } b^r \equiv 1 \pmod{n}$$

Karena $0 \leq v < r$ dan r merupakan bilangan bulat positif terkecil sedemikian hingga $b^r \equiv 1 \pmod{n}$ maka $r = 0$. Oleh karena itu, $s = ru$ dan didapatkan $r \mid s$.

Begitupun sebaliknya, karena $r \mid s$ maka $s = rh$ untuk suatu bilangan bulat h. Karena $b^r \equiv 1 \pmod{n}$ maka $(b^r)^h \equiv 1 \pmod{n}$, yaitu $b^s \equiv 1 \pmod{n}$.

Merujuk pada Teorema Euler, yaitu jika $(b, n) = 1$ maka $b^{\phi(n)} \equiv 1 \pmod{n}$. Seandainya tingkat dari $b \pmod{n}$ adalah r, berdasarkan Teorema 1. dapat disimpulkan bahwa $r \mid \phi(n)$.

Akibat

Jika $(b, n) = 1$ dan tingkat $b \pmod{n}$ adalah r , maka $r \mid \phi(n)$.

Contoh 3.

Perhatikan tingkat dari beberapa bilangan bulat positif modulo 11 pada tabel 9.2.

Tabel 9.2 Tingkat bilangan-nilangan positif modulo 11

Bilangan bulat	1	2	3	4	5	6	7	8	9	10
tingkat	1	10	5	5	5	10	10	10	5	2

Cermati Tabel 9.2, tingkat dari bilangan-bilangan bulat positif yang merupakan sisa bagi terkecil modulo 11 adalah pembagi dari $\phi(11)$.

Perhatikan juga bahwa

$$3^1 \equiv 3 \pmod{11} \; ; \; 3^6 \equiv 3 \pmod{11}$$

$$3^2 \equiv 9 \pmod{11} \; ; \; 3^7 \equiv 9 \pmod{11}$$

$$3^3 \equiv 5 \pmod{11} \; ; \; 3^8 \equiv 5 \pmod{11}$$

Teorema 2.

Jika $(b, n) = 1$ dan tingkat $b \pmod{n}$ adalah s maka $b^i \equiv b^j \pmod{n}$ jika dan hanya jika $i \equiv j \pmod{s}$ (Burton, 2010)

Bukti

Misalkan $b^i \equiv b^j \pmod{n}$ dengan $i \geq j$. Karena $(b, n) = 1$ maka diperoleh $b^{i-j} \equiv 1 \pmod{n}$. Berikutnya, karena tingkat $b \, (mod \, n)$ adalah s, menurut teorema 1. maka $s \mid (i - j)$. Ini berarti bahwa $i \equiv j \pmod{s}$.

Sebaliknya, karena $i \equiv j \pmod{s}$ maka $i = j + rs$ untuk suatu bilangan bulat r. Tingkat $b \pmod{n}$ adalah s, berarti $b^s \equiv 1 \pmod{n}$ sehingga diperoleh berikut ini.

$$b^i \equiv b^{j+rs} \pmod{n}$$

$$b^i \equiv \left(b^j\right)(b^r)^s \pmod{n}$$

$$b^i \equiv \left(b^j\right) \pmod{n}$$

Perhatikan kembali teorema 2. di atas, karena tingkat $b \pmod{n}$ adalah s, dimana s merupakan suatu bilangn bulat positif terkecil sedemikian hingga $b^s \equiv 1 \pmod{n}$, tidak ada bilangan bulat positif $b, b^2, b^3, b^4, \ldots, b^s$ yang kongruen modulo n. Ini disebabkan oleh $b^i \equiv b^j \pmod{n}$ dengan $1 \leq i \leq j \leq s$, berdasarkan teorema 2., $i \equiv j \pmod{s}$ yang berakibat $i = j$.

Akibat

Jika $(b, n) = 1$ dan tingkat $b \pmod n$ adalah s maka tidak ada bilangan-bilangan bulat positif $b, b^2, b^3, b^4, \dots, b^s$ yang kongruen dengan modulo n.

Jika diketahui tingkat $b \pmod n$ adalah s, berapakah tingkat dari $b^r \pmod n$? Misalkan $(s, r) = d$ dan $s = s_1 d$ dan $r = r_1 d$ dengan $(s_1, r_1) = 1$ sehingga diperoleh:

$$(b^r)^{s_1} = (b^{r_1 d})^{\frac{s}{d}} = (b^r)^{s_1} \equiv 1 (\mathrm{mod}\, n)$$

Misalkan tingkat dari $b^r \pmod n$ adalah t, berdasarkan teorema 11.1.4 maka $t \mid s_1$ dan $(b^r)^t = b^{rt} \equiv 1 (\mathrm{mod}\, n)$.

Karena tingkat dari $b \pmod n$ adalah s maka $s \mid rt$. Atau bisa juga dituliskan dengan $s_1 d \mid r_1 dt$ atau $s_1 \mid r_1 t$. Karena $(s_1, r_1) = 1$ maka $s_1 \mid t$. Selanjutnya, karena $t \mid s_1$ dan $s_1 \mid t$, maka $s_1 = r$ sehingga $s_1 = r = \frac{s}{d} = \frac{s}{(s,\ r)}$.

Pemaparan d atas merupakan bukti dari teorema 3. berikut.

Teorema 3.

Jika $(b, n) = 1$ dan tingkat $b \pmod n$ adalah s maka tingkat dari $b^r \pmod n$ dengan $r > 0$ adalah $\frac{s}{(s,\ r)}$.

Pada teorema 3., jika $(r, s) = 1$ maka tingkat dari $b^r \pmod n$ sama dengan tingkat pada $b \pmod n$. Demikian pula, jika tingkat $b \pmod n$ adalah s dan tingkat dari $b^r \pmod n$ adalah s pula, kita bisa menunjukkan bahwa (r, s) = 1. Andaikan $(r, s) = d$ maka $\frac{r}{d}$ dan $\frac{s}{d}$ dan d suatu bilangan bulat. Tingkat $b \pmod n$ adalah s maka:

$$b^s \equiv 1 \pmod n$$

$$(b^s)^{\frac{1}{d}} \equiv 1 (\mathrm{mod}\, n)$$

$$(b^r)^{\frac{s}{d}} \equiv 1(\text{mod } n)$$

Oleh sebab tingkat dari $b^r \pmod n$ adalah s, maka $s \mid \frac{s}{d}$. Ini akan mungkin terjadi hanya jika $d = 1$. Jadi $(r, s) = 1$.

Akibat

Jika $(b, n) = 1$ dan tingkat $b \ (mod\ n)$ adalah s maka tingkat dari $b^r \pmod n$ adalah s juga jika dan hanya jika $(r, s) = 1$.

Amati kembali tabel 9.2, tingkat dari 2 (mod 11) adalah 10, tingkat dari 2^2 (mod 11) adalah 5, sedangkan tingkat dari 2^3 (mod 11) adalah 10. Berdasarkan teorema 11.1.7 kita dapat memeriksa bahwa

$$\text{ord}_{11}2^2 = \frac{\text{ord}_{11}2}{(2, \text{ord}_{11}2)} = \frac{10}{(2,10)} = 5$$

9.2 Akar Primitif

Ingat kembali akibat dari teorema 3., kepangkatan bulat positif dari 2 yang memiliki tingkat 10 modulo 11 adalah $2^6, 2^7$, dan 2^8. Di lain sisi, $2^6 \equiv 9 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$, dan $2^8 \equiv 3 \pmod{11}$. Jadi tingkat dari 2 (mod 11), 6 (mod 11), 7 (mod 11) dan 8 (mod 11) masing-masing adalah 10 dan $\phi(11) = 10$. Berikutnya, 2, 6, 7, dan 8 masing-masing dikenal sebagai akar-akar primitif dari 11.

Definisi 2.

Jika $(b, n) = 1$ dan tingkat dari b modulo n adalah $\phi(n)$ maka b disebut sebagai akar primitif dari n.

Bilangan bulat positif n memiliki akar primitif b jika $b^{\phi(n)} \equiv 1(\text{mod } n)$ dengan syarat $b^s \not\equiv 1(\text{mod } n)$ untuk setiap bilangan bulat positif $s < \phi(n)$. Ini memudahkan kita dalam menyelidiki

bahwa 5 adalah akar-akar primitif dari 11 karena $\phi(11) = 10$ dan $5^1 \equiv 5 \pmod{11}$; $5^2 \equiv 3 \pmod{11}$; $5^3 \equiv 4 \pmod{11}$; $5^4 \equiv 9 \pmod{11}$; $5^5 \equiv 1 \pmod{11}$ dan $5^6 \equiv 5 \pmod{11}$.

Jika q sebuah bilangan prima dan $(b, q) = 1$, kekongruenan linear $bx \equiv 1 (\text{mod q})$ selalu memiliki penyelesaian. Ingat bahwa $b^{q-1} \equiv 1 \pmod{q}$ sehingga penyelesaiannya adalah sisa bagi terkecil modulo q dari b^{q-2}.

Dapat disimpulkan bahwa akar primitif pasti dimiliki oleh setiap bilangan prima. Namun, akar primitif belum pasti dimiliki oleh bilangan bulat positif n yang non prima.

Contoh 1.

Akar primitif pada 7 ialah 3 sebab $\phi(7) = 6$, dan tingkat dari masing-masing 2 (mod 7) dan 4 (mod 7) ialah 3. Tapi 4 tidak memiliki akar primitif karena $\phi(4) = 3$ dan $3^2 \equiv 1 \pmod{4}$; $5^2 \equiv 1 \pmod{4}$; $7^2 \equiv 1 \pmod{4}$ dan $9^2 \equiv 1 \pmod{4}$.

Teorema 4.

Andaikan $(b, n) = 1$ dan $z_1, z_2, z_3, \dots, z_{\phi(n)}$ adalah bilangan yang saling prima dengan n dan juga merupakan bilangan bulat positif kurang dari n. Jika b merupakan akar primitif dari n maka $b^1, b^2, b^3, \dots, b^{\phi(n)}$ masing-masing kongruen dengan modulo n menggunakan suatu permutasi dari $z_1, z_2, z_3, \dots, z_{\phi(n)}$.

Bukti

Sebab $(b, n) = 1$, tiap pangkat bulat positif dari b ($b^1, b^2, b^3, \dots, b^{\phi(n)}$) akan saling prima dengan n. Karena $z_1, z_2, z_3, \dots, z_{\phi(n)}$ suatu bilangan bulat positif kurang dari n serta saling prima terhadap n, maka untuk melakukan pembuktian terhadap teorema 4., cukup dengan menunjukkan bahwa tidak terdapat dua suku pada $b^1, b^2, b^3, \dots, b^{\phi(n)}$ yang kongruen dengan modulo n.

Misal:

$$b^i \equiv b^j \pmod{n} \text{ untuk } 0 < i \text{ dan } j \leq \phi(n)$$

$$b^{i-j} \equiv 1 \pmod{n}$$

Sebab b merupakan akar primitif dari n, maka $\phi(n)$ merupakan tingkat $b \pmod{n}$. Sebab $0 < i$ dan $j \leq \phi(n)$, sifat kongruen tersebut hanya terjadi jika $i - j = 0$ sehingga $i = j$. Ini menunjukkan bahwa tidak terdapat dua suku pada b^1, $b^2, b^3, \ldots, b^{\phi(n)}$ yang kongruen modulo n.

Contoh 2.

Akar primitif dari 7 ialah 3 dan $\phi(7) = 6$ karena $3^6 \equiv 1 \pmod{7}$ sementara $3^1 \equiv 3 \pmod{7}$; $3^2 \equiv 2 \pmod{7}$; $3^3 \equiv 6 \pmod{7}$; $3^4 \equiv 4 \pmod{7}$; dan $3^5 \equiv 5 \pmod{7}$.

Amati bahwa himpunan sisa bagi sederhana dari modulo 7 adalah $\{1, 2, 3, 4, 5, 6\}$. Anggota-anggota himpunan tersebut kongruen dengan modulo 7 dengan anggota-anggota himpunan berikut:

$$\{3^6, 3^2, 3^1, 3^4, 3^5, 3^3\}.$$

Ada berapa akar primitif dari 11?

Perhatikan kembali tabel 9.2, akar-akar primitif dari 11 adalah 2, 6, 7, 8. Sehingga, akar primitif dari 11 sebanyak 4. Ingat bahwa $\phi(11) = 10$ dan $\phi(10) = 4$ jadi akar primitif dari 11 ialah sebanyak $\phi(\phi(11)) = 4$.

Teorema 5.

Jika bilangan bulat positif n memiliki akar primitif, maka banyaknya akar primitif dari n ialah $\phi(\phi(n))$.

Bukti

Andaikan b adalah akar primitif dari n, berdasarkan teorema 5. maka akar primitif lainnya dapat ditentukan dari himpunan $\{b^1, b^2, b^3, \dots, b^{\phi(n)}\}$, yakni b^s dengan $1 \leq s \leq \phi(n)$ yang bertingkat $\phi(n)$. Ini didapatkan jika $(s, \phi(n)) = 1$. Bilangan bulat positif sebanyak s dengan $1 \leq s \leq \phi(n)$ yang memenuhi $(s, \phi(n)) = 1$ ialah $\phi(\phi(n))$. Oleh karena itu, akar-akar primitif dari n ialah sebanyak $\phi(\phi(11))$.

Contoh 3.

Salah satu akar primitif dari 17 adalah 3 karena $ord_{17}3 = 16$ dan $\phi(17) = 16$. Akar-akar primitif lainnya dari 17 ialah $3^1, 3^5, 3^{15}, 3^{11}, 3^3, 3^7, 3^{13}, 3^9$ (pangkat-pangkat tersebut saling prima dengan 16) secara berturut-turut kongruen modulo 17 dengan $3, 5, 6, 7, 10, 11, 12, 14$. Jadi, akar primitif dari 17 sebanyak 8 dan $\phi(\phi(17)) = \phi(16) = 8$.

Selanjutnya akan kita bahas mengenai eksistensi akar-akar primitif pada bilangan prima. Akan dimulai dengan memperlihatkan banyaknya penyelesaian kekongruenan polinomial.

Teorema 6.

Andaikan q sebuah bilangan prima dan h merupakan polinomial yang berderajat m, kekongruenan $h(x) \equiv 0 \pmod{q}$ memiliki m penyelesaian.

Bukti

Andaikan polinomial h berderajat m berbentuk:

$h(x) = b_m x^m + b_m x^m + \cdots + b_1 x + b_0$ dengan $b_m \not\equiv 0 \pmod{q}$

teorema di atas akan dibuktikan menggunakan induksi matematika pada derajat $h(x)$ yaitu m.

Untuk $m = 1$ Maka $h(x) = b_1 x + b_0 \equiv 0 \pmod{q}$

$$b_1 x \equiv -b_0 \pmod{q}$$

Sebab $(b_1, q) = 1$, kekongruenan linear tersebut memiliki satu penyelesaian. Akibatnya, teorema benar untuk $m = 1$.

Andaikan teorema benar untuk $m = s - 1$, yakni polinomial h berderajat $(s-1)$ dengan penyelesaian sebanyak $(s-1)$. Kita akan menunjukkan bahwa pada polinomial h berderajat m sehingga $h(x) \equiv 0 \pmod{q}$ memiliki w penyelesaian. Olehnya itu, cukuplah dengan menunjukkan bahwasanya $h(x) \equiv 0 \pmod{q}$ tidak memiliki penyelesaian atau hanya memiliki satu penyelesaian. Apabila $h(x) \equiv 0 \pmod{q}$ tidak memiliki penyelesaian, maka teorema terbukti. Dan apabila $h(x) \equiv 0 \pmod{q}$ memiliki paling tidak satu penyelesaian, misalnya b, $h(b) \equiv 0 \pmod{q}$ dan b adalah suatu sisa bagi terkecil modulo q.

Jika $h(x)$ dibagi dengan $(x-b)$, didapati $h(x) = (x-b)\,u(x) + v$.

Polinomial $u(x)$ berderajat $s-1$ dengan koefisien bulat dan v juga merupakan bilangan bulat. Substitusi $x = b$ pada $h(x) \equiv 0 \pmod{q}$ dan pada $h(x) = (x-b)\,u(x) + v$ sehingga diperoleh:

$$0 \equiv h(b) = (b-b)u(b) + v \pmod{q}$$

$$v \equiv 0 \pmod{q}$$

sehingga $h(x) \equiv (x-b)\,u(x) \pmod{q}$

andaikan a adalah penyelesaian lainnya dari $h(x) \equiv 0 \pmod{q}$ dengan $a \not\equiv b \pmod{q}$ maka $0 \equiv h(a)(a-b)\,u(a) \pmod{q}$. Karena q prima dan $a - b \not\equiv 0 (mod\ q)$ maka $u(a) \equiv 0 \pmod{q}$. Olehnya itu, penyelesaian dari $h(x) \equiv 0 \pmod{q}$ yang berlainan dengan b merupakan penyelesaian dari $u(x) \equiv 0 \pmod{q}$. Deret

pangkat $u(x)$ memiliki paling banyak $(s-1)$ penyelesaian, sehingga $h(x) \equiv 0 \pmod{q}$ tidak akan memiliki lebih dari s penyelesaian.

Perlu penegasan bahwa teorema 6. bernilai benar hanya jika modulonya merupakan bilangan prima. Apabila bukan prima, teorema tidak benar.

Teorema 7.

Jika q adalah bilangan prima dan $c \mid q - 1$, kekongruenan $x^c - 1 \equiv 0 \pmod{q}$ tepat memiliki c penyelesaian.

Selanjutnya amati bilangan prima 11 dan $\phi(11) = 10$. $\psi(c) =$ semua bilangan bulat positif s yang kurang dari 11 dan bertingkat c dengan $c \mid 10$.

Pada modulo 11 ini, 1 bertingkat 1 berarti $\psi(1) = 1$

3, 4, 5, dan 9 masing-masing bertingkat 5 berarti $\psi(5) = 4$

2, 6, 7 dan 8 masing-masing bertingkat 10 berarti $\psi(10) = 4$

10 bertingkat 2 berarti $\psi(2) = 1$

Sehingga

$$\sum_{c/10} \psi(c) = \psi(1) + \psi(2) + \psi(5) + \psi(10)$$

$$= 1 + 1 + 4 + 4$$

Perhatikan juga bahwa

$\psi(1) = 1 = \phi(1)$ $\psi(5) = 4 = \phi(5)$

$\psi(2) = 1 = \phi(2)$ $\psi(10) = 4 = \phi(5)$

Contoh di atas memberikan gambaran untuk teorema berikut

Teorema 8.

Jika q suatu bilangan prima dan $c|q-1$, terdapat $\phi(c)$ bilangan bulat positif kurang dari q bertingkat c modulo q.

Bukti

Andaikan $c \mid q-1$ dan $\psi(c)$ merupakan banyaknya bilangan bulat positif s dimana $1 \leq s \leq q-1$ yang memiliki tingkat c modulo q. Karena setiap bilangan bulat antara 1 dan $q-1$ selalu bertingkat c dengan $c \mid q-1$ maka

$$q-1=\sum_{c|q-1}\psi(c)$$

Sementara, telah diketahui bahwa $q-1=\sum_{c|q-1}\phi(c)$, sehingga harus dibuktikan bahwa $\psi(c)=\phi(c)$.

Ambil sembarang c, yakni pembagi $q-1$ sedemikian hingga $\psi(c)>0$ maka terdapat bilangan bulat positif b bertingkat c maka

$$b, b^2, b^3, \ldots, b^c$$

Tidak terdapat dua suku yang kongruen modulo q dan setiap suku memenuhi kekongruenan $x^c \equiv 1 \pmod q$ karena $(b^s)^c \equiv (b^c)^s \equiv 1 \pmod q$ dengan $1 \leq s \leq c$

Berdasarkan teorema 8., kekongruenan tersebut memiliki c penyelesaian. Suatu bilangan bulat positif bertingkat c modulo q haruslah kongruen modulo q dengan satu bilangan pada $b, b^2, b^3, \ldots, b^c$. Terdapat $\phi(c)$ dari kepangkatan b yang bertingkat c, yakni b^s dimana $(s,c)=1$. Oleh karena itu, akan ada bilangan bulat positif kurang dari q dan memiliki tingkat c modulo q sebanyak $\phi(c)$ sehingga $\psi(c)=\phi(c)$.

Ambil $c=q-1$ pada teorema 8. diperoleh akibat berikut

Akibat

Setiap bilangan prima q, akan memiliki $\phi(q-1)$ akar primitif

Contoh 4.

Carilah akar-akar primitif dari 31 dan cari juga semua bilangan bulat positif kecil dari 31 yang memiliki $\text{ord}_{31}6$!

Jawab:

Akar primitif dari 31 adalah sebanyak $\phi(\phi(31) = \phi(30) = 8$. Sebab $2^5 \equiv 1 \pmod{31}$ maka 2 bukanlah akar primitif dari 31.

Akan kita coba kepangkatan 3 dengan perpangkatan bulat yang kurang dari 15 sebab tingkat 3 pastimembagi $\phi(31) = 30$.

$$3^{15} \equiv 27^5 \equiv -4^5 \equiv (16)(-64) \equiv (16)(-2) \equiv -1 \not\equiv 1 \pmod{31}$$

Sebab $3^{15} \not\equiv 1 \pmod{31}$ dan $3^s \not\equiv 1 \pmod{31}$ untuk $1 \leq s \leq 15$ sehingga tingkat dari 3 haruslah lebih besar dari 15. Karena tingkat 3 pasti membagi $\phi(31) = 30$, dapat disimpulkan bahwa 30 merupakan ordeer dari 3 (mod 31). Oleh karena itu, 3 adalah akar primitif dari 31. Adapun akar primitif yang lainnya adalah 3^s dimana $(s, 30) = 1$.

Sebab 3 merupakan akar primitif dari 31, maka semua bilangan bulat positif kurang dari 31 dapat dituliskan dalam bentuk 3^sdengan $1 \leq s \leq 30$. Berdasarkan teorema 8., diperoleh $\text{ord}_{31}3^s = \frac{30}{(s,30)}$ sehingga 3^s yang bertingkat 6 jika $(s, 30) = 5$. Nilai s yang sesuai adalah $s = 5$ dan $s = 25$. Akibatnya, 3^5 dan 3^{25}. Selanjutnya akan ditentukan sisa bagi terkecilnya.

$$3^5 \equiv (9)(27) \equiv (9)(4) \equiv (-36) \equiv 26 \pmod{31}$$

$$3^{25} \equiv (3^5)^5 \equiv (26)^5 \equiv (-5)^5 \equiv (25)(-125) = 6 \pmod{31}$$

sehingga 6 dan 26 adalah bilangan-bilangan yang bertingkat 6 modulo 31.

Tabel 9.3. Bilangan Prima Kurang dari 105 beserta Akar Primitif Terkecilnya

Prima	Akar Primitif Terkecil	Prima	Akar Primitif Terkecil	Prima	Akar Primitif Terkecil
2	1	29	2	67	2
3	2	31	3	71	7
5	2	37	2	73	5
7	3	41	6	79	3
11	2	43	3	83	2
13	2	47	5	89	3
17	3	53	2	97	5
19	2	59	2	101	2
23	5	61	2	103	5

9.3 Indeks

Bahasan mengenai akar primitif bisa dibatasi cukup pada bilangan prima saja. Reorema Lagrange dan Polinomial merupakan 2 buah teorema yang dikembangkan sebagai acuan untuk menunjukkan bahwa setiap bilangan prima pasti akan memiliki suatu akar primitif. Untuk selanjutnya, dapat juga ditunjukkan bahwa semua bilangan bulat positif memiliki akar-akar primitf.

Aritmatika modulo juga dapat diselesaikan menggunakan akar primitif. Aritmatika mengenai modulo dikenal dengan istilah aritmatika indeks, yakni suatu konsep tertentu yang bisa dijadikan solusi untuk penyelesaian kongruensi yang mencakup kepangkatan (Hefferon, 2003).

Konsep mengenai Indeks dikenalkan oleh Gauss dalam *Disquisitions Arithmeticae.*

Misalkan n bilangan bulat yang memiliki akar primitif b, seperti yang telah kita ketahui pangkat $\phi(n)$ adalah

$b, b^2, b^3, \ldots, b^{\phi(n)}$ kongruen modulo n, dalam urutan tertentu dengan bilangan bulat kurang dari n dan relatif utama untuk modulo n. Oleh karena itu, jika a adalah relatif prima terhadap n, maka a dapat dituliskan dalam bentuk $a \equiv b^r \pmod{n}$, dimana $1 \leq r \leq \phi(n)$. Hal ini mengarahkan kita pada sebuah definisi:

Definisi 3.

diberikan n bilangan bulat positif dengan akar primitif b. Jika a bilangan bulat dan $(a, n) = 1$, maka terdapat r bilangan bulat yang tunggal dengan $1 \leq r \leq \phi(n)$ dan $a \equiv b^r \pmod{n}$, r disebut indeks a pada basis b modulo n. Ditulis $r = \text{ind}_b a$ dan dinyatakan dalam bentuk $b^{\text{ind}_b a} \equiv a \pmod{n}$ atau bentuk $a \equiv b^{\text{ind}_b a} \pmod{n}$.

Dari definisi 3. kita mengetahui bahwa jika a dan t bilangan bulat yang relatif prima terhadap modulo n dan $t \equiv a \pmod{n}$ maka $\text{ind}_b a = \text{ind}_b t$.

Contoh 1

2 adalah akar primitif dari modulo 9 karena $2^6 \equiv 1 (\text{mod } 9)$. Perhatikan $2^1 \equiv 2 (\text{mod } 9), 2^2 \equiv 4 (\text{mod } 9), 2^3 \equiv 8 (\text{mod } 9), 2^4 \equiv 7 (\text{mod } 9), 2^5 \equiv 5 (\text{mod } 9), 2^6 \equiv 1 (\text{mod } 9)$. Dapat dituliskan bahwa:

$\text{ind}_2 2 = 1, \text{ind}_2 4 = 2, \text{ind}_2 8 = 3, \text{ind}_2 7 = 4, \text{ind}_2 5 = 5$, dan $\text{ind}_2 1 = 6$.

Teorema 9.

Jika b adalah suatu akar primitif modulo n, a dan t masing-masing bilangan bulat positif, $(a, n) = (t, n) = 1$, maka:

i. $\text{ind}_b(at) \equiv \text{ind}_b a + \text{ind}_b t = (\text{mod } \phi(n))$
ii. $\text{ind}_b a^r \equiv r.\text{ind}_b a (\text{mod } \phi(n))$ untuk $r > 0$
iii. $\text{ind}_b 1 \equiv 0 \pmod{\phi(n)}$

Bukti:

i. Berdasarkan definisi indeks: $b^{\text{ind}_b a} \equiv a \pmod{n}$, berarti $b^{\text{ind}_b (at)} \equiv at \pmod{n}$, yaitu:

$$b^{\text{ind}_b (at)} \equiv b^{\text{ind}_b a} a \pmod{n}. b^{\text{ind}_b t} \pmod{n}$$
$$\equiv b^{\text{ind}_b a}. b^{\text{ind}_b t} \pmod{n}$$
$$\equiv b^{\text{ind}_b a + \text{ind}_b t} \pmod{n}$$

ii. Berdasarkan definisi indeks, $b^{\text{ind}_b a} \equiv a \pmod{n}$, maka $b^{\text{ind}_b a^r} \equiv a^r \pmod{n}$ dan $b^{\text{r.ind}_b a} \equiv (b^{\text{ind}_b a})^r \equiv a^r \pmod{n}$. Sehingga diperoleh: $b^{\text{ind}_b a^r} \equiv b^{r.\text{ind}_b a}$ dan sesuai definisi indeks: $\text{ind}_b a^r \equiv r.\text{ind}_b a \pmod{\phi(n)}$

iii. Berdasarkan teorema Euler, $b^{\phi(n)} \equiv 1 \pmod{n}$ dan karena b adalah suatu akar primitif modulo n, tidak terdapat pangkat bilangan positif dari b yang kongruen terhadap 1 modulo n. Jadi, $\text{ind}_b 1 = \phi(n) \equiv 0 \pmod{\phi(n)}$.

Contoh 2.

Dari contoh 11.3.2 diketahui bahwa $\text{ind}_2 2 = 1$ dan $\text{ind}_2 4 = 2$ dan $\phi(9) = 8$, maka $\text{ind}_2 8 = \text{ind}_2 2.4 = \text{ind}_2 2 + \text{ind}_2 4 = 1 + 2 = 3 \equiv 3 \pmod{8}$. Selanjutnya, dari $\text{ind}_2 4 = 2$ dapat ditentukan bahwa $\text{ind}_2 4^3 \equiv 3.\text{ind}_2 4 \pmod{8} \equiv 3.2 \pmod{8} \equiv 6 \pmod{8}$

Contoh 3.

Hitunglah $4x^9 \equiv 7 \pmod{13}$

Jawab:

2 merupakan salah satu akar primitif dari 13 karena $2^{12} = 2^{\phi(13)} \equiv 1 \pmod{13}$. Dengan akar primitif tersebut, kita dapat menghitung pangkat-pangkat dari $2, 2^2, 2^3, \ldots, 2^{12} \pmod{13}$, diperoleh:

$$2^1 \equiv 2 \pmod{13}, 2^2 \equiv 4 \pmod{13}, 2^3 \equiv 8 \pmod{13},$$

$$2^4 \equiv 3 \pmod{13}, 2^5 \equiv 6 \pmod{13}, 2^6 \equiv 12 \pmod{13},$$

$$2^7 \equiv 11 \pmod{13}, 2^8 \equiv 9 \pmod{13}, 2^9 \equiv 5 \pmod{13},$$

$$2^{10} \equiv 10 \pmod{13}, 2^{11} \equiv 7 \pmod{13}, 2^{12} \equiv 1 \pmod{13}$$

Adapun tabel indeks nya:

b	1	2	3	4	5	6	7	8	9	0	11	12
$\text{ind}_2 b$	12	1	4	2	9	5	11	3	8	10	7	6

$4x^9 \equiv 7 \pmod{13}$, maka $\text{ind}_2(4x^9) \equiv \text{ind}_2 7 \equiv 11 \pmod{12}$.
Gunakan teorema 9. bagian i dan ii sehingga diperoleh:

$$\text{ind}_2(4x^9) \equiv \text{ind}_2 4 + \text{ind}_2(x^9) \equiv 2 + 9.\text{ind}_2 x \pmod{12}$$

Dari $\text{ind}_2(4x^9) \equiv \text{ind}_2 7 \equiv 11 \pmod{12}$ dan $\text{ind}_2(4x^9) \equiv 2 + 9.\text{ind}_2 x \pmod{12}$ diperoleh:

$$2 + 9.\text{ind}_2 x \pmod{12} = 11 \pmod{12}.$$

$$9.\text{ind}_2 x \equiv 9 \pmod{12}$$

$$\text{ind}_2 x \equiv 1 \pmod{4}$$

Dengan demikian diperoleh:

$$\text{ind}_2 x \equiv 1, 5, 9 \pmod{4}$$

Berarti:

$x \equiv 2^1, 2^5, 2^9 \pmod{13}$

$x \equiv 2, 6, 5 \pmod{13}$

DAFTAR PUSTAKA

Burton, D.M. (2010) *Elementary Number Theory Seventh Edition*. Seventh. New York: McGraw-Hill Higher Education.

Hefferon, J. (2003) *Elementary Number Theory*. Florida: St Michael's College.

Rosen, K.H. (2005) *Elementary Number Theory and Its Applications Fifth Edition*. Boston: Pearson/Addison Wesley.

BAB 10
FUNGSI TANGGA

Oleh Prida N. L. Taneo

10.1 Fungsi Tangga

Staircase function ia a function composed of a set of equally spaced jumps of equal length, such as the ceiling function $f(q) = \lceil q \rceil$*, floor function* $f(q) = \lfloor q \rfloor$ *or nearest integer function* $f(q) = [q]$.

Fungsi tangga (*staircase function*) adalah fungsi yang terdiri dari sebuah himpunan fungsi $f(q)$ yang berbentuk interval sejajar seperti fungsi *ceiling* (pembulatan ke atas), fungsi *floor* (pembulatan ke bawah) atau fungsi bulat (pembulatan ke bilangan bulat terdekat). Misalkan terdapat sebuah bilangan real q, tentunya q terletak diantara dua bilangan bulat (integer). Fungsi ceiling dan floor memetakan bilangan real q tersebut terhadap bilangan bulat terdekat.

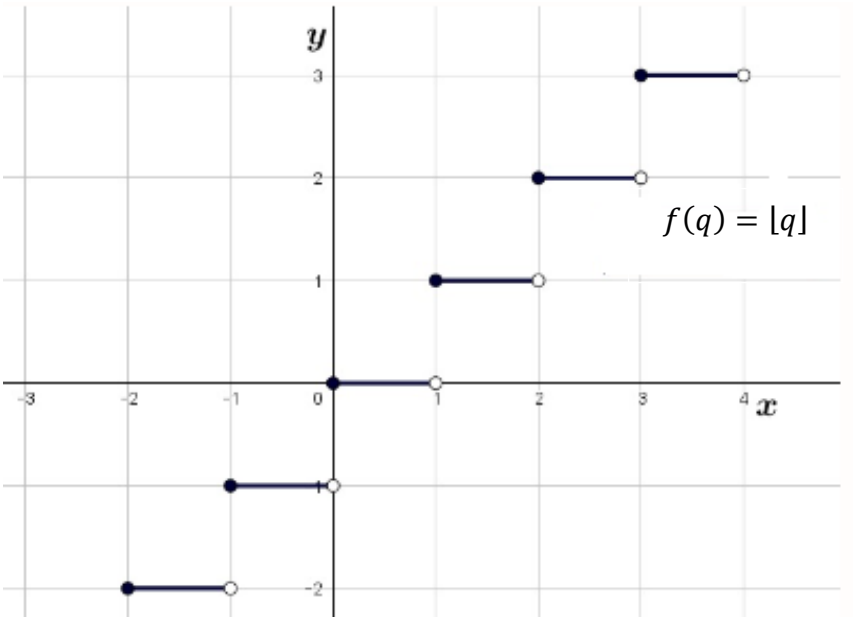
10.2 Fungsi Floor

Arti *floor* dalam bahasa indonesia adalah lantai atau dasar, sehingga secara sederhana fungsi floor dapat dinyatakan sebagai fungsi pembulatan ke bawah dimana nilai yang dipilih adalah bilangan bulat. Simbol untuk fungsi floor q adalah $f(q) = \lfloor q \rfloor$ yang didefinisikan sebagai bilangan bulat terbesar yang lebih kecil atau sama dengan q.

Notasi matematika fungsi floor adalah:

$$f(q) = maks\,\{n \in Z, n \leq q\}$$

Grafik fungsi floor pada bidang kartesius menyerupai tangga sehingga fungsi ini sering dinyatakan sebagai fungsi tangga.



Gambar 10.1. Fungsi Floor

Dari definisi dan gambar grafik di atas maka:

$$\lfloor 18 \rfloor = 18$$

$$\lfloor -5 \rfloor = -5$$

$$\lfloor 0{,}7 \rfloor = 0$$

$$\lfloor -0{,}7 \rfloor = -1$$

$$\lfloor -4{,}6 \rfloor = -5$$

$$\lfloor 4{,}6 \rfloor = 4$$

Adapun beberapa sifat yang berlaku pada fungsi floor adalah sebagai berikut:

1) $\lfloor q \rfloor = q$, untuk q bilangan bulat

2) $q - 1 < \lfloor q \rfloor \leq q$, untuk q bilangan real
   $\lfloor q \rfloor = a \leftrightarrow q - 1 < a \leq q$, untuk a bilangan bulat dan q bilangan real.
3) $\lfloor q \rfloor = a \leftrightarrow a \leq q < a + 1$, untuk a bilangan bulat dan q bilangan real.
4) $\lfloor q \rfloor < a \leftrightarrow q < a$, untuk a bilangan bulat dan q bilangan real.
5) $a \leq \lfloor q \rfloor \leftrightarrow a \leq q$, untuk a bilangan bulat dan q bilangan real
6) $\lfloor q + a \rfloor = \lfloor q \rfloor + a$, untuk a bilangan bulat dan q bilangan real
7) $\lfloor q \rfloor + \lfloor r \rfloor \leq \lfloor q + r \rfloor$, untuk q dan r bilangan real
8) $\lfloor q.r \rfloor \leq \lfloor q \rfloor . \lfloor r \rfloor$, untuk q dan r bilangan real

Contoh Soal:

1. Pada persamaan fungsi floor berikut berlaku:

$$\left\lfloor \sqrt{\left\lfloor \sqrt{2023} \right\rfloor} \right\rfloor = \left\lfloor \sqrt{\sqrt{2023}} \right\rfloor + \left\lfloor \frac{a}{2023} \right\rfloor$$

   Jika $\lfloor q \rfloor$ menyatakan bilangan bulat terbesar yang lebih kecil atau sama dengan q maka tentukan nilai a yang memenuhi persamaan diatas.
   Penyelesaian:

$$\left\lfloor \sqrt{\left\lfloor \sqrt{2023} \right\rfloor} \right\rfloor = \left\lfloor \sqrt{\sqrt{2023}} \right\rfloor + \left\lfloor \frac{a}{2023} \right\rfloor$$

$$\left\lfloor \sqrt{\lfloor 44{,}977 \rfloor} \right\rfloor = \lfloor \sqrt{44{,}997} \rfloor + \left\lfloor \frac{a}{2023} \right\rfloor$$

$$\lfloor \sqrt{44} \rfloor = \lfloor 6{,}706 \rfloor + \left\lfloor \frac{a}{2023} \right\rfloor$$

$$\lfloor 6{,}633 \rfloor = 6 + \left\lfloor \frac{a}{2023} \right\rfloor$$

$$6 = 6 + \left\lfloor \frac{a}{2023} \right\rfloor$$

$$0 = \left\lfloor \frac{a}{2023} \right\rfloor$$

$$0 \leq a < 2023$$

$$a = 0,1,2,3,4, \ldots, 2022$$

Jadi nilai a yang memenuhi persamaan diatas adalah a=0,1,2,…, 2022.

2. $\lfloor x \rfloor$ menyatakan bilangan bulat terbesar yang lebih kecil atau sama dengan q. Bilangan real x merupakan solusi dari pertidaksamaan
$0 < 3\lfloor 3x + 3 \rfloor < 7$. Jika $A = q$ dan $B = -1$ maka tentukan hubungan antara kuantitas A dan B.
Penyelesaian:
Dari pertidaksamaan $0 < 3\lfloor 3x + 3 \rfloor < 7$ diketahui bahwa $\lfloor 3x + 3 \rfloor$ merupakan bilangan bulat sehingga ketidaksamaan diatas bernilai benar jika $\lfloor 3x + 3 \rfloor$ bernilai 1 atau 2.
Jika $\lfloor 3x + 3 \rfloor = 1$ maka:

$$\begin{gathered} \lfloor 3x \rfloor + 3 = 1 \\ \lfloor 3x \rfloor = 1 - 3 \\ \lfloor 3x \rfloor = -2 \\ -2 \leq x < -2 + 1 \\ -2 \leq x < -1 \\ -\frac{2}{3} \leq x < -\frac{1}{3} \end{gathered}$$

Jika $\lfloor 3x + 3 \rfloor = 2$ maka:

$$\begin{gathered} \lfloor 3x \rfloor + 3 = 2 \\ \lfloor 3x \rfloor = 2 - 3 \\ \lfloor 3x \rfloor = -1 \\ -1 \leq x < -1 + 1 \\ -1 \leq x < 0 \\ -\frac{1}{3} \leq x < 0 \end{gathered}$$

Untuk nilai $-\frac{2}{3} \leq x < -\frac{1}{3}$ atau $-\frac{1}{3} \leq x < 0$, nilai x yang memenuhi adalah $-\frac{2}{3} \leq x < 0$. Diketahui $A = q$ dimana q adalah salah satu yang memenuhi $-\frac{2}{3} \leq x < 0$ dan $B = -1$ maka dapat disimpulkan hubungan kuantitas A dan B adalah Kuantitas A lebih besar daripada B.

3. $\lfloor k \rfloor$ menyatakan bilangan bulat terbesar yang lebih kecil atau sama dengan k. Bilangan real k merupakan solusi dari pertidaksamaan
$0 < 3\lfloor 5 - 3k \rfloor < 11$. Jika $X = k$ dan $Y = 0$ maka tentukan hubungan antara kuantitas X dan Y.
Penyelesaian:
Dari pertidaksamaan $0 < 3\lfloor 5 - 3k \rfloor < 11$diketahui bahwa $\lfloor 5 - 3k \rfloor$ merupakan bilangan bulat sehingga ketidaksamaan diatas bernilai benar jika $\lfloor 5 - 3k \rfloor$ bernilai 1, 2 atau 3

Jika $\lfloor 5 - 3k \rfloor = 1$ maka:

$$\begin{gathered} \lfloor 5 - 3k \rfloor = 1 \\ \lfloor -3k \rfloor + 5 = 1 \\ \lfloor -3k \rfloor = 1 - 5 \\ \lfloor -3k \rfloor = -4 \\ -4 \leq -3k < -4 + 1 \\ -4 \leq -3k < -3 \\ 1 < k \leq \frac{4}{3} \end{gathered}$$

Jika $\lfloor 5 - 3k \rfloor = 2$ maka:

$$\begin{gathered} \lfloor 5 - 3k \rfloor = 2 \\ \lfloor -3k \rfloor + 5 = 2 \\ \lfloor -3k \rfloor = 2 - 5 \\ \lfloor -3k \rfloor = -3 \\ -3 \leq -3k < -3 + 1 \\ -3 \leq -3k < -2 \\ \frac{2}{3} < k \leq 1 \end{gathered}$$

Jika $\lfloor 5 - 3k \rfloor = 3$ maka:

$$\begin{gathered} \lfloor 5 - 3k \rfloor = 3 \\ \lfloor -3k \rfloor + 5 = 3 \\ \lfloor -3k \rfloor = 3 - 5 \\ \lfloor -3k \rfloor = -2 \end{gathered}$$

$$-2 \leq -3k < -2 + 1$$
$$-2 \leq -3k < -1$$
$$\frac{1}{3} < k \leq \frac{2}{3}$$

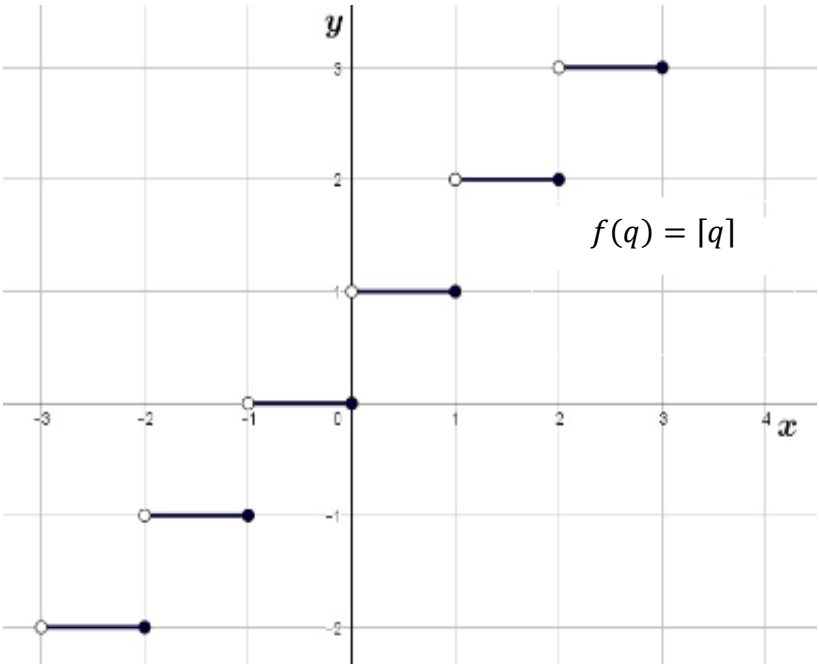
Untuk nilai $\frac{1}{3} < k \leq \frac{2}{3}$ atau $\frac{2}{3} < k \leq 1$ atau $1 < k \leq \frac{4}{3}$, nilai k yang memenuhi adalah $\frac{1}{3} < k \leq \frac{4}{3}$. Diketahui $X = k$ dimana k adalah salah satu yang memenuhi $\frac{1}{3} < k \leq \frac{4}{3}$ dan $Y = 0$ maka dapat disimpulkan hubungan kuantitas X dan Y adalah Kuantitas X lebih besar daripada Q.

10.3 Fungsi Ceiling

Ceiling mempunyai arti langit-langit dalam bahasa indonesia, sehingga secara sederhana fungsi ceiling dikatakan sebagai fungsi pembulatan ke atas dimana nilai yang dipilih adalah bilangan bulat. Fungsi ceiling q dinotasikan dengan $f(q) = \lceil q \rceil$ merupakan bilangan bulat terkecil yang lebih besar atau sama dengan q. Definisi ini dinotasikan sebagai:

$$f(q) = min\,\{n \,\epsilon\, Z, n \leq q\}$$

Seperti fungsi floor, grafik fungsi ceilingpun menyerupai tangga.



Gambar 10.2. Grafik Fungsi Ceiling

Dari definisi dan gambar grafik di atas

⌊18⌋=8
⌊-5⌋=-5
⌊0,7⌋=1
⌊-0,7⌋=0
⌊-4,6⌋=-4
⌊4,6⌋=5

Beberapa sifat yang berlaku pada fungsi ceiling adalah sebagai berikut:

1) $\lceil q \rceil = q$, untuk q bilangan bulat
2) $q < \lceil q \rceil \leq q + 1$, untuk q bilangan real
   $\lceil q \rceil = a \leftrightarrow q \leq a < q + 1$, untuk a bilangan bulat dan q bilangan real.
3) $\lceil q \rceil = a \leftrightarrow a - 1 < q \leq a$, untuk a bilangan bulat dan q bilangan real.
4) $a < \lceil q \rceil \leftrightarrow a < q$, untuk a bilangan bulat dan q bilangan real.

5) $\lceil q \rceil \leq a \leftrightarrow q \leq a$, untuk a bilangan bulat dan q bilangan real
6) $\lceil q + a \rceil = \lceil q \rceil + a$, untuk a bilangan bulat dan q bilangan real
7) $\lceil q + r \rceil \geq \lceil q \rceil + \lceil r \rceil$, untuk q dan r bilangan real
8) $\lceil q . r \rceil \geq \lfloor q \rfloor . \lfloor r \rfloor$, untuk q dan r bilangan real.

Contoh Soal:

1. $\lceil q \rceil$ menyatakan bilangan bulat terkecil yang lebih besar atau sama dengan q. Bilangan real k adalah solusi dari $1 < \left\lceil \frac{1}{2}q - 1 \right\rceil < 3$. Jika $X = q$ dan $Y = 7$, tentukan hubungan antara kuantitas X dan Y.
   Penyelesaian:

$$1 < \left\lceil \frac{1}{2}q - 1 \right\rceil < 3$$
$$1 < \left\lceil \frac{1}{2}q \right\rceil - 1 < 3$$
$$1 + 1 < \left\lceil \frac{1}{2}q \right\rceil < 3 + 1$$
$$2 < \left\lceil \frac{1}{2}q \right\rceil < 4$$

$\left\lceil \frac{1}{2}q \right\rceil$ merupakan bilangan bulat sehingga agar ketidaksamaan di atas bernilai benar maka nilai $\left\lceil \frac{1}{2}q \right\rceil$ yang mungkin adalah 3

$$\left\lceil \frac{1}{2}q \right\rceil = 3$$
$$3 - 1 < \frac{1}{2}q \leq 3$$
$$2 < \frac{1}{2}q \leq 3$$
$$2.2 < 2.\frac{1}{2}q \leq 2.3$$
$$4 < q \leq 6$$

Diketahui $X = q$ dimana q memenuhi $4 < q \leq 6$ dan $Y = 7$ maka dapat disimpulkan hubungan kuantitas X dan Y adalah Kuantitas X lebih kecil daripada Q.

2. $\lceil r \rceil$ menyatakan bilangan bulat terkecil yang lebih besar atau sama dengan r. Jika

$$r = \frac{3}{\frac{1}{2021} + \frac{2}{2022} + \frac{3}{2023} + \cdots + \frac{10}{2030}}$$

Maka tentukan $\lceil r \rceil$.

Penyelesaian:

Nilai Minimum untuk r adalah:

$$r = \frac{3}{\frac{1}{2021} + \frac{2}{2021} + \frac{3}{2021} + \cdots + \frac{10}{2021}}$$

$$r = \frac{3}{\frac{1 + 2 + \cdots + 10}{2021}}$$

$$r = \frac{3}{\frac{55}{2021}}$$

$$r = \frac{6063}{55}$$

$$r = 110{,}2364$$

Nilai Maksimum untuk r adalah:

$$r = \frac{3}{\frac{1}{2023} + \frac{2}{2023} + \frac{3}{2023} + \cdots + \frac{10}{2023}}$$

$$r = \frac{3}{\frac{1 + 2 + \cdots + 10}{2023}}$$

$$r = \frac{3}{\frac{55}{2023}}$$

$$r = \frac{6069}{55}$$

$$r = 110{,}3455$$

Maka diperoleh $110{,}2364 \leq r \leq 110{,}3455$ sehingga $\lceil r \rceil = 111$.

3. $\lceil s \rceil$ menyatakan bilangan bulat terkecil yang lebih besar atau sama dengan s. Bilangan real t adalah solusi dari $0 < \lceil s - 1 \rceil < 2$ dan
$1 < \lceil s + 1 \rceil < 4$. Jika $X = s$ dan $Y = 4$, tentukan hubungan antara kuantitas X dan Y.
Penyelesaian:
Dari ketidaksamaan $0 < \lceil s - 1 \rceil < 2$ diketahui bahwa $\lceil s - 1 \rceil$ adalah bilangan bulat sehingga agar ketidaksamaan bernilai benar maka nilai $\lceil s - 1 \rceil$ yang memenuhi adalah 1.

$$\lceil s - 1 \rceil = 1$$
$$1 - 1 < s - 1 \leq 1$$
$$0 < s - 1 \leq 1$$
$$0 + 1 < s \leq 1 + 1$$
$$1 < s \leq 2$$

Dari ketidaksamaan $0 < \lceil s + 1 \rceil < 4$ diketahui bahwa $\lceil s + 1 \rceil$ adalah bilangan bulat sehingga agar ketidaksamaan bernilai benar maka nilai $\lceil s - 1 \rceil$ yang memenuhi adalah 2, atau 3

Jika $\lceil s + 1 \rceil = 2$
$$2 - 1 < s + 1 \leq 2$$
$$1 < s + 1 \leq 2$$
$$1 - 1 < s \leq 2 - 1$$
$$0 < s \leq 1$$

Jika $\lceil s + 1 \rceil = 3$
$$3 - 1 < s + 1 \leq 3$$
$$2 < s + 1 \leq 3$$
$$2 - 1 < s \leq 3 - 1$$
$$1 < s \leq 2$$

Himpunan bilangan real s yang memenuhi $1 < s \leq 2$, $0 < s \leq 1$ dan $1 < s \leq 2$ adalah $0 < s \leq 2$. Jika $X = s$ dan $Y = 4$, maka hubungan antara kuantitas X dan Y adalah kuantitas JX lebih kecil dari Y.

10.4 Hubungan Fungsi Floor dan Ceiling

Berdasarkan sifat-sifat pada fungsi floor dan fungsi ceiling maka terdapat beberapa hubungan antara kedua fungsi tersebut yaitu:

a) $q - 1 < \lfloor q \rfloor \leq \lceil q \rceil \leq q + 1$, untuk q bilangan real.
b) $-\lfloor q \rfloor = \lceil -q \rceil$, untuk q bilangan real.
c) $\lfloor -q \rfloor = -\lceil q \rceil$, untuk q bilangan real.
d) $\lceil q \rceil - \lfloor q \rfloor = 0$, untuk q bilangan bulat.
e) $\lceil q \rceil - \lfloor q \rfloor = 1$, untuk q bukan bilangan bulat.

DAFTAR PUSTAKA

Graham, R. L., Knuth, D. E. &. Patashnik, O. 1994. *Concrete Mathematics: A Foundation for Computer Science Second edition*. Reading, MA. Addison-Wesley Professional.

Grimaldi, R.P. 1989. *Discrete and Combinatorial Mathematics, An Applied Introduction*. New York: Addison-Wesley Professional.

Grinberg, D. 2016. *18.781 (Spring 2016): Floor and Arithmetic Functions*.

Mott, J.L., Kandel, A. & Baker, T.P. 1983. *Discrete Mathematics for Computer Scientists*. Reston. Prentice-Hall.

Rosen, K.H. 1988. *Discrete Mathematics and Its Applications*. New York: Random House.

BIODATA PENULIS

Samuel Urath, S. Si., M. Pd.
Dosen Program Studi Pendidikan Matematika
Fakultas Ilmu Sosial dan Humaniora (FISH)
Universitas Lelemuku Saumlaki (UNLESA)

Penulis lahir di Lelingluan, Kecamatan Tanimbar Utara, Kabupaten Kepulauan Tanimbar, Provinsi Maluku pada Tanggal 28 Bulan November Tahun 1986. Penulis adalah anak pertama dari 4 (empat) bersaudara yang lahir dari pasangan suami istri, ayah Dolfinus Urath dan Ibu Fransina Itrandulan.

Penulis menamatkan studi pada jenjang sebagai berikut, TK Oikumene Desa Lelingluan pada Tahun 1993, SD Kristen Lelingluan pada Tahun 1998, SMP Negeri 3 Tanimbar Utara pada Tahun 2001, SMA Negeri 1 Tanimbar Utara pada Tahun 2004, Starata Satu (S1) Jurusan Matematika FMIPA Universitas Pattimura pada tahun 2009, dan Strata Dua (S2) pada Program Pasca Sarjana Universitas Pattimura Ambon Tahun 2019. Saat ini penulis aktif mengajar sebagai Dosen Tetap pada Program Studi Pendidikan Matematika Fakultas Ilmu Sosial dan Humaniora (FISH) Universitas Lelemuku Saumlaki (UNLESA). Penulis juga aktif menulis Buku di Bidang Matematika dan saat ini telah menyelesaikan 3 (tiga) Buku dengan Judul *Matematika Ekonomi untuk Perguruan Tinggi* dan *Geometri untuk Perguruan Tinggi* serta *Logika dan Himpunan*.

BIODATA PENULIS

Yunita Oktavia Wulandari, S.Si., M.Pd.
Dosen Program Studi Pendidikan Matematika
Fakultas Keguruan dan Ilmu Pendidikan Universitas Wisnuwardhana

Penulis lahir di Malang tanggal 31 Oktober 1988. Penulis adalah dosen tetap pada Program Studi Pendidikan Matematika Fakultas Keguruan dan Ilmu Pendidikan, Universitas Wisnuwardhana. Menyelesaikan pendidikan S1 pada Jurusan Matematika, Universitas Negeri Malang dan melanjutkan S2 pada Jurusan Pendidikan Matematika di Universitas Negeri Malang.

BIODATA PENULIS

Rifka Agustianti, M. Pd
Dosen Matematika Program Studi Motor Pesawat
Fakultas Teknik Universitas Nurtanio Bandung

Penulis lahir di Kota Palopo (Sulawesi Selatan) pada tanggal 27 Agustus 1988. Penulis adalah dosen tetap mata kuliah matematika pada Program Studi Motor Pesawat Fakultas Teknik, Universitas Nurtanio Bandung. Menyelesaikan pendidikan S1 pada tahun 2013 dan langsung melanjutkan pendidikan S2 pada Jurusan Pendidikan Matematika pada tahun 2015 di STKIP Siliwangi Bandung (sekarang IKIP Siliwangi Bandung).

Tak hanya mengajar di perguruan tinggi, penulis juga aktif menjadi tutor matematika pada beberapa bimbingan belajar dan privat di Bandung. Penulis juga merupakan Ketua Biro Pertemuan Ilmiah DPD Bandung Barat pada Perkumpulan Dosen Peneliti Indonesia (PDPI) dan Wakil Sekretaris Umum pada Forum Komunikasi Dosen (FKD) periode 2022-2027. Penulis juga telah menulis beberapa judul *book chapter* baik sebagai *author* maupun editor, diantaranya Media Pembelajaran, Filsafat Pendidikan Matematika, Konsep Dasar Matematika, Teknologi Pendidikan, Inovasi Teknologi Pembelajaran, Logika dan Struktur Diskrit, Metode Penelitian Kualitatif dan Kuantitatif, Strategi Pembelajaran, dan Model-Model Pembelajaran.

Selain menulis *book chapter*, penulis juga aktif menulis beberapa artikel ilmiah pada jurnal nasional baik dalam ranah penelitian maupun ranah pengabdian kepada masyarakat yang terakreditasi Kemendikbud yang bertemakan matematika dan pendidikan matematika.

BIODATA PENULIS

Hetty Elfina, S.Pd., M.Pd.
Dosen Program Studi Teknik Mesin
Fakultas Teknik dan Ilmu Komputer
Universitas Pembinaan Masyarakat Indonesia
Medan

Penulis lahir di kota Sibolga pada tanggal 07 Januari 1990. Penulis merupakan dosen tetap pada Program Studi Teknik Mesin, Fakultas Teknik dan Ilmu Komputer, Universitas Pembinaan Masyarakat Indonesia. Penulis menyelesaikan pendidikan S1 pada Jurusan Pendidikan Matematika di Universitas Negeri Medan tahun 2013 dan melanjutkan S2 pada tahun yang sama di Jurusan Pendidikan Matematika di Universitas Negeri Medan dan lulus tahun 2015.

BIODATA PENULIS

Titik Pitriani Muslimin, S.Pd., M.Pd.
Dosen Program Studi Pendidikan Matematika
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sawerigading Makassar

Penulis lahir di Desa Baroko Kabupaten Enrekang tanggal 11 Agustus 1989. Penulis adalah dosen tetap pada Program Studi Pendidikan Matematika Fakultas Keguruan dan Ilmu Pendidikan Universitas Sawerigading makassar. Menyelesaikan pendidikan S1 pada Jurusan Pendidikan Matematika FMIPA Universitas Negeri Makassar dan melanjutkan S2 pada Program Studi Pendidikan Matematika Pascasarjana Universitas Negeri Makassar. Memulai karir sebagai dosen pada tahun 2014 di Universitas Cokroaminoto Palopo, kemudian setelah menikah memutuskan untuk pindah mengikuti tempat kerja suami, sehingga pada tahun 2018 hingga sekarang menjadi dosen tetap di Universitas Sawerigading Makassar. Selain mengajar, penulis juga menekuni kegiatan menulis. Baik dalam menulis buku-buku refrensi terkait pendidikan matematika dan pendidikan secara umum, penulis juga aktif menulis artikel dari penelitian-penelitian yang telah dilakukan. Beberapa buku telah berhasil diterbitkan penulis.

BIODATA PENULIS

Haerudin, S.Pd., M.Pd.
Dosen Program Studi Pendidikan Matematika
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Singaperbangsa Karawang

Penulis lahir di Karawang tanggal 29 April 1972. Penulis adalah dosen tetap pada Program Studi Pendidikan Matematika Fakultas Keguruan dan Ilmu Pendidikan (FKIP) Universitas Singaperbangsa Karawang. Menyelesaikan pendidikan S1 pada Jurusan Pendidikan Matematika dan menyelesaikan S2 pada Jurusan Pendidikan Matematika. Penulis mulai menekuni bidang menulis sejak 2020. Buku yang sudah terbit adalah Buku Monograf berjudul Pentingnya Memahami Bimbingan dan Konseling bagi Guru Mata Pelajaran yang diterbitkan oleh Deepublish Publisher pada Juli 2022 ber-ISBN 978-623-02-4962-4; Buku referensi berjudul Penerapan Aplikasi Pembelajaran Matematika Berbasis Daring oleh Penerbit PT Mitra Ilmu yang diterbitkan pada Oktober 2022 ber-ISBN 978-623-8022-24-3; dan buku chapter LOGIKA INFORMATIKA ber-ISBN_978-623-198-177-6 oleh PT Get Press Indonesia pada Maret 2023.

BIODATA PENULIS

Ahmad Choirul Anam, M.Pd
Dosen Tadris Matematika Fakultas Tarbiyah
Universitas Ibrahimy, Situbondo

Penulis lahir di Banyuwangi pada 02 Juli 1994. Penulis adalah anak pertama dari dua bersaudara yang merupakan dosen Tadris Matematika Fakultas Tarbiyah Universitas Ibrahimy Situbondo. Menyelesaikan Pendidikan S1 pada program studi Pendidikan Matematika di UIN Sunan Ampel Surabaya, kemudian melanjutkan Pendidikan S2 pada program studi Pendidikan Matematika di Universitas Negeri Surabaya. Penulis menekuni bidang Pendidikan Matematika, utamanya pada pengajaran, pembelajaran, Statistika dan Teori Bilangan. Karya buku yang telah ditulis dan diterbitkan adalah Buku Matematika kelas XII dan Pedoman untuk Guru Matematika kelas XII yang diterbitkan tahun 2021, serta menulis Buku Matematika Kelas VIII dan Pedoman untuk Guru Matematika Kelas VIII yang diterbitkan pada tahun 2022 oleh Pusat Perbukuan Kementerian Pendidikan dan Kebudayaan. Selain itu, juga menulis buku secara kolaboratif berjudul Manajemen Pendidikan, Pengantar Statistika dan Teori Peluang.

BIODATA PENULIS

Dr. H. Nanang, M.Pd.
Staf Dosen Jurusan Teknik Sipil
Institut Teknologi Garut

Penulis lahir di Bandung tanggal 1 Juli 1964. Penulis adalah dosen dpk Kopertis Wilayah VII Surabaya pada Program Studi Pendidikan FKIP Universitas Muhammadiyah Jember dari tahun 1990 s.d. 2000 dan dosen LLDIKTI Wilayah IV Jawa Barat dan Banten pada Jurusan Teknik Sipil Fakultas Teknik Sipil dan Arsitektur Institut Teknologi Garut (ITG) dari Tahun 2000 s.d. sekarang. Dari tahun 1986 s.d 1990, penulis bekerja sebagai guru di SMAN 1 Bandung, SMA 55 Asia Afrika Bandung, SMA Karya Agung Bandung, SMA Swadaya Bandung.

Penulis menyelesaikan: S1 Pendidikan Matematika di IKIP Bandung (UPI) Tahun 1989, S2 Pendidikan Matematika di IKIP Surabaya (UNESA) Tahun 1999, dan S3 Pendidikan Matematika di UPI Bandung Tahun 2009. Penulis menekuni bidang Pembelajaran. Penulis juga sebagai Tim Penilai DUPAK Kepangkatan Guru-guru di Kabupaten Garut dari tahun 2015 s.d. sekarang. Telah beberapa kali memperoleh hibah penelitian dan pengabdian pada masyarakat dari Universitas Muhammadiyah Jember, Institut Teknologi Garut, dan Ristek Dikti Kemendikbud.

BIODATA PENULIS

Azmidar, M.Pd.
Dosen Program Studi Tadris Matematika
Fakultas Tarbiyah Institut Agama Islam Negeri Parepare

Penulis lahir di Mundan (Enrekang) tanggal 21 Desember 1991. Penulis adalah dosen tetap pada Program Studi Tadris Matematika Fakultas Tarbiyah, Institut Agama Islam Negeri Parepare. Menyelesaikan pendidikan S1 pada Jurusan Pendidikan Matematika Universitas Islam Negeri Alauddin Makassar dan melanjutkan S2 pada Jurusan Pendidikan Matematika Universitas Pendidikan Indonesia. Penulis menekuni bidang Pendidikan Matematika.

BIODATA PENULIS

Prida N. L. Taneo, S.Pd., M.Pd
Dosen Pendidikan Matematika
Institut Pendidikan Soe

Penulis lahir di Besnam tanggal 19 Oktober 1979. Penulis adalah dosen pada Program Studi Pendidikan Matematika Institut Pendidikan Soe. Menyelesaikan pendidikan S1 pada program studi pendidikan Matematika Universitas Kristen Satya Wacana Salatiga tahun 2010 dan menyelesaikan pendidikan S2 pada program studi pendidikan matematika Universitas Negeri Semarang tahun 2015. Penulis sementara melanjutkan studi S3 di program studi pendidikan matematika Universitas Pendidikan Indonesia. Penulis menekuni bidang aljabar, matematika diskrit, kajian matematika sekolah, geometri dan etnomatematika dalam pelaksanaan tridharma perguruan tinggi. Buku Ajar yang pernah ditulis antara lain Kalkulus Integral Berbasis Maple (2018) dan Teori Graf (2019).