Matematika Diskrit

TEORI BILANGAN

May 16, 2026

Teori bilangan mempelajari tentang bilangan bulat (integer) dan sifat-sifatnya. Di dalam bagian ini akan dibahas konsep-konsep penting di dalam teori bilangan yang digunakan di dalam ilmu komputer. Himpunan semua bilangan **bulat** (*integer*) dituliskan $\mathbb{Z}$, yaitu

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

Keterbagian

Diberikan bilangan bulat a dan b dengan $a \neq 0$. Jika bilangan b dibagi dengan a maka hasilnya bisa bilangan bulat atau bukan bilangan bulat. Misalnya

$$\frac{12}{6} = 2$$
$$\frac{13}{4} = 3,25.$$

Definisi 1. *Diberikan bilangan $a, b \in \mathbb{Z}$ dengan $a \neq 0$. Bilangan a dikatakan* **membagi** *b jika ada bilangan $m \in \mathbb{Z}$ sehingga*

$$b = ma.$$

Dalam hal ini dituliskan $a|b$ dan a dinamakan pembagi b; sedangkan notasi $a \nmid b$ menyatakan a tidak membagi b.

Definisi 1 juga dapat dinyatakan dengan cara sebagai berikut: Bilangan a dikatakan **membagi** b jika

$$\frac{b}{a} \quad \text{bilangan bulat (integer).}$$

Contoh 1. (a) $2|6$, karena $6 = 2 \cdot 3$ (atau karena $6/2$ integer)

(b) $3|(-12)$, karena $-12 = (-4) \cdot 3$ (atau karena $-12/3$ integer).

(c) $3 \nmid 5$, karena tidak ada bilangan bulat m sehingga $5 = m \cdot 3$ (atau karena $5/3$ bukan integer).

Teorema 1. *Diberikan integer $a, b,$ dan c dengan $a \neq 0$.*

(i) Jika $a|b$ dan $a|c$, maka $a|(b + c)$

(ii) Jika $a|b$ maka $a|bc$ untuk semua integer c

(iii) Jika $a|b$ dan $b|c$ maka $a|c$.

Bukti. Perlu diingatkan bahwa jumlah dua integer adalah integer dan hasil kali dua integer adalah integer.

(i) Diketahui $a|b$ dan $a|c$, yakni ada integer m sehingga $b = ma$ dan ada integer n sehingga $c = na$. Akibatnya

$$b + c = ma + na = (m + n)a,$$

yang berarti $a|(b + c)$.

(ii) Diketahui $a|b$ dan integer c. Jadi terdapat integer m sehingga $b = ma$. Oleh karena itu

$$cb = cma$$

yang berarti $a|bc$.

(iii) Diketahui $a|b$ dan $b|c$, yakni ada integer m dan n sehingga $b = ma$ dan $c = nb$. Akibatnya

$$c = nb = nma,$$

yang berarti $a|c$.

□

Contoh 2. Buktikan bahwa jika $a|1$ maka $a = \pm 1$.

Penyelesaian. Bilangan bulat yang membagi 1 hanya 1 dan -1. Oleh karena itu jika $a|1$ maka $a = 1$ atau $a = -1$.

Contoh 3. Jika $a|b$ dan $b|a$ maka $a = \pm b$.

Penyelesaian. Jika $a|b$ maka ada $m \in \mathbb{Z}$ sehingga $b = ma$. Demikian pula jika $b|a$ berarti ada $n \in \mathbb{Z}$ sehingga $a = nb$. Oleh karena itu

$$b = ma = mnb,$$

yang hanya benar jika $mn = 1$. Akibatnya $m = n = 1$ atau $m = n = -1$. Dengan demikian

$$b = ma = 1 \cdot a = a \quad \text{atau} \quad b = ma = (-1) \cdot a = -a.$$

Teorema 2. *Jika $a|b$ dan $a|c$, maka untuk sebarang integer m dan n,*

$$a|mb + nc.$$

Bukti. Karena $a|b$ maka ada $p \in \mathbb{Z}$ sehingga $b = pa$; demikian pula karena $a|c$ maka ada $q \in \mathbb{Z}$ sehingga $c = qa$. Akibatnya

$$mb + nc = mpa + nqa = (mp + nq)a.$$

Karena $mp + nq$ bilangan bulat ini berarti a membagi $mb + nc$. □

Jika bilangan bulat a dibagi bilangan bulat b, maka akan diperoleh hasil bagi dan sisa. Misalnya, jika 14 dibagi 3 maka hasil baginya 4 dan sisanya 2, yaitu

$$14 = 4 \cdot 3 + 2.$$

Perhatikan bahwa sisanya lebih kecil dari pembaginya.

Teorema 3 (Algoritma pembagian)**.** *Jika $a, b \in \mathbb{Z}$, $a \neq 0$ maka ada $q, r \in \mathbb{Z}$ sehingga*

$$b = qa + r \quad \textit{dan} \quad 0 \leq r < |a|.$$

Bilangan q dinamakan **hasil bagi** *dan r dinamakan* **sisa**.

Definisi 2. *Jika b dibagi a memberikan hasil bagi q dan sisa r, maka dituliskan*

$$q = b \ div \ a \qquad dan \qquad r = b \mod a.$$

Contoh 4. Carilah hasil bagi dan sisanya jika 17 dibagi 5.

Penyelesaian. Dapat Anda periksa

$$17 = 3 \cdot 5 + 2.$$

Oleh karena itu hasil baginya adalah 3 dan sisanya adalah 2, yang dapat dituliskan

$$3 = 17 \text{ div } 5 \qquad \text{dan} \qquad 2 = 17 \mod 5.$$

Contoh 5. Carilah hasil bagi dan sisa jika -21 dibagi 6.

Penyelesaian. Dapat Anda periksan bahwa

$$-21 = (-4) \cdot 6 + 3.$$

Dengan demikian

$$-4 = -21 \text{ div } 6 \qquad \text{dan} \qquad 3 = -21 \mod 6.$$

Bilangan prima

Definisi 3. *Bilangan integer positif c dinamakan pembagi sekutu terbesar (greatest common divisor) a dan b, jika*

(1) c merupakan pembagi a dan b

(2) Setiap bilagan pembagi a dan b adalah pembagi c.

Selanjutnya pembagi sekutu terbesar a dan b dituliskan $gcd(a, b)$.

Contoh 6. Integer 4 merupakan pembagi sekutu terbesar 12 dan 16, yakni $gcd(12, 16) = 4$. Bilangan 2 juga pembagi 12 dan 16, namun bukan pembagi sekutu terbesar.

Teorema 4. *Jika a dan b integer dan tidak keduanya 0, maka pembagi sekutu terbesar $gcd(a, b)$ ada; lebih lanjut ada integer n dan m sehingga $gcd(a, b) = ma + nb$.*

Definisi 4. *Integer a dan b dikatakan* **relatif prima** *jika $gcd(a, b) = 1$.*

Contoh 7. (1) Bilangan 3 dan 4 relatif prima, sebab $gcd(3, 4) = 1$.

(2) bilangan 5 dan 12 relatif prima, sebab $gcd(5, 12) = 1$.

(3) Bilangan 7 dan 21 tidak relatif prima, sebab $gcd(7, 21) = 7$, yakni pembagi sekutu terbesar kedua bilangan bukan 1.

Definisi 5. *Bilangan $p > 1$ dinamakan bilangan prima jika pembaginya hanya bilangan ± 1 dan $\pm p$.*

Dengan kata lain $p > 1$ bilangan prima jika untuk sebarang bilangan a, berlaku $gcd(p, a) = 1$ atau $p|a$.

Contoh 8. (1) Bilangan 5 adalah prima, sebab pembagi 5 hanya ± 1 dan ± 5.

(2) Bilangan-bilangan $2, 3, 5, 7, 11, 13, 17, 19, \cdots$ merupakan bilangan prima.

Teorema 5. *Jika a dan b relatif prima dan $a|bc$, maka $a|c$.*

Dari teorema tersebut dapat diambil akibat berikut.

Teorema 6. *Jika suatu bilangan prima p membagi hasil kali bilangan-bilangan integer, maka p membagi paling sedikit satu dari integer-integer tersebut.*

Bilangan prima merupakan blok pembangun bilangan integer, seperti dinyatakan dalam teorema berikut.

Teorema 7. *Setiap interger $a > 1$ dapat difaktorkan secara tunggal dengan cara*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

dimana $p_1 > p_2 > \cdots > p_r$ bilangan-bilangan prima dan $\alpha_i > 0$.

Contoh 9. Bilangan prima 126 dapat difaktorkan

$$126 = 7 \cdot 3^2 \cdot 2.$$

Integer modulo

Dalam banyak hal sering dijumpai didalam pembagian yang diperlukan hanya sisanya saja. Misalnya didalam sistem jam yang menggunakan angka 1 sampai 12, jika sekarang jam 09.00, jam berapakah 6 jam kemudian? Tentu Anda akan menjawab jam 03.00, yaitu sisa dari $9 + 6 = 15$ dibagi 12. Jadi di dalam contoh ini jam 03.00 sama dengan jam 15.00. Perhatikan bahwa $12|(15 - 3)$. Didalam matematika hal demikian dikatakan bahwa 15 kongruen 3 modulo 12.

Definisi 6. *Jika a, b, $n > 0$ integer dan n membagi $b-a$, maka dikatakan a kongruen b modulo n dan dituliskan $a \equiv b \mod n$. Jadi*

$$a \equiv b \mod n \quad \textit{jika} \quad n|(b - a).$$

Contoh 10. (a) $15 \equiv 3 \mod 4$, sebab $4|(15 - 3)$.

(b) $73 \equiv 4 \mod 23$, sebab $23|(73 - 4)$.

(c) $21 \equiv -9 \mod 10$, sebab $10|(21 - (-9))$.

Teorema 8. *Jika a, b, $n > 0$ integer dan $a \equiv b \mod n$, maka $b \equiv a \mod n$.*

Bukti. Jika $a \equiv b \mod n$, yakni $n|(b-a)$ maka n membagi $-(b-a) = a-b$, yakni $n|(a - b)$. Ini berarti $b \equiv a \mod n$. □

Contoh 11. Perhatikan bahwa $15 \equiv 3 \mod 12$, sebab $12|(15 - 3)$. Oleh karena itu $3 \equiv 15 \mod 12$. Hal ini juga bisa diperiksa bahwa $\frac{3-15}{12} = -1$.

Teorema 9. *Diberikan integer positif n. $a \equiv b \mod n$ jika dan hanya jika ada integer k sehingga $a = b + kn$.*

Bukti. Diketahui n integer positif. Berdasarkan definisi,

$$\begin{aligned} a \equiv b \mod n &\iff n|(b - a) \\ &\iff a - b = kn, \quad \text{untuk suatu integer } k \\ &\iff a = b + kn. \end{aligned}$$

□

Contoh 12. Carilah bilangan-bilangan yang kongruen dengan 3 modulo 12.

Penyelesaian. Misalkan a kongruen 3 modulo 12. Berdasarkan teorema di atas

$$a = 3 + k \cdot 12, \quad k \in \mathbb{Z},$$

sehingga bilangan yang kongruen dengan 3 modulo 12 adalah

$$\cdots, -33, -21, -9, 3, 15, 27, 39, \cdots.$$

Dapat Anda periksa bahwa jika bilangan-bilangan tersebut dikurangi 3 kemudian dibagi 12, maka hasilnya bilangan bulat.

Teorema 10. *Diberikan integer positif n. Jika $a \equiv b \mod n$ dan $c \equiv d \mod n$, maka*

$$a + c \equiv b + d \mod n \qquad dan \qquad ac \equiv bd \mod n.$$

Bukti. Diketahui $a \equiv b \mod n$ dan $c \equiv d \mod n$, yang berarti ada integer p dan q sehingga

$$b - a = pn \qquad \text{dan} \qquad d - c = qn,$$

atau dituliskan kembali menjadi

$$b = a + pn \qquad \text{dan} \qquad d = c + qn.$$

Akibatnya

$$b + d = a + c + (p + q)n,$$

dan karena $p + q$ integer, ini berarti $a + c \equiv b + d \mod n$.
Selanjutnya,

$$bd = (a + pn)(c + qn) = ac + (aq + cp + pqn)n,$$

dan karena $aq + cp + pqn$ interger, ini bearti $ac \equiv bd \mod n$. □

Contoh 13. Dapat Anda periksa bahwa $7 \equiv 2 \mod 5$ dan $11 \equiv 1 \mod 5$, sehingga berdasarkan teorema di atas,

$$7 + 11 = 18, \quad 2 + 1 = 3, \quad \text{dan } 5|(18 - 3),$$

yakni $7 + 11 \equiv 2 + 1 \mod 5$. Demikian pula

$$7 \cdot 11 \equiv 2 \cdot 1 \mod 5.$$

Aljabar modulo n

Diperkenalkan himpunan

$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\},$$

yakni $\mathbb{Z}_n$ adalah himpunan semua integer tak negatif yang kurang dari n. Perhatikan bahwa $\mathbb{Z}_n$ memilki n anggota. Pada himpunan $\mathbb{Z}_n$ dapat didefinisikan dua operasi sebagai berikut. Sebagai contoh,

$$\begin{aligned}\mathbb{Z}_6 &= \{0, 1, 2, 3, 4, 5\}\\ \mathbb{Z}_{12} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.\end{aligned}$$

Definisi 7. *Operasi $+_n$ dan $\cdot_n$ adalah operasi pada $\mathbb{Z}_n$ dengan dengan aturan sebagai berikut*

$$a +_n b = (a + b) \mod n$$

$$a \cdot_n b = (a \cdot b) \mod n.$$

Contoh 14. Hasil operasi pada $\mathbb{Z}_n$ misalnya adalah

$$\begin{aligned}1 +_6 2 &= (1 + 2) \mod 6 = 3\\ 3 +_8 5 &= (3 + 5) \mod 8 = 0\\ 2 +_{10} 4 &= (2 + 4) \mod 10 = 6\end{aligned}$$

$$\begin{aligned}2 \cdot_6 4 &= (2 \cdot 4) \mod 6 = 2\\ 4 \cdot_9 3 &= (4 \cdot 3) \mod 9 = 3\\ 5 \cdot_{12} 5 &= (5 \cdot 5) \mod 12 = 1\end{aligned}$$

Tes Formatif

1. Apakah 13 membagi bilangan 60, 52, 130, -26?
2. Tuliskan dalam bentuk $b = qa + r$ dengan q hasil bagi dan dan r sisa apabila
   (a) 87 dibagi 5
   (b) 123 dibagi 6
   (c) -124 dibagi 2
   (d) -14 dibagi 3
3. Pada sistem 12 jam, pukul berapakah
   (a) 20 jam kemudian jika sekarang pukul 07.00
   (b) 15 jam kemudian jika sekarang pukul 11.00.
4. Jelaskan apakah yang berikut benar?
   (a) $7 \equiv 19 \mod 4$
   (b) $-1 \equiv 109 \mod 10$
   (c) $134 \equiv 4 \mod 13$
   (d) $6 \equiv 9 \mod 2$.
5. Carilah 5 bilangan x sehingga $x \equiv 6 \mod 7$.
6. Carilah hasil operasi berikut.
   (a) $3 +_4 5$
   (b) $5 +_{12} 10$
   (c) $2 +_3 2$
   (d) $7 +_8 6$.

Kunci jawaban tes formatif

1. $13 \nmid 60$, $13|52$, $13|130$, $13|-26$.
2. (a) $q = 17$, $r = 2$
   (b) $q = 20$, $r = 3$
   (c) $q = -62$, $r = 0$
   (d) $q = -5$, $r = 1$
3. (a) pukul 01.00
   (b) pukul 02.00.
4. (a) benar
   (b) benar
   (c) benar
   (d) salah
5. misalnya: $-8, -1, 6, 13, 20$.
6. (a) 3
   (b) 3
   (c) 1
   (d) 5.

Tugas

Dikirim paling lambat satu hari sebelum perkuliahan berikutnya

1. Didalam sistem 24 jam, jika sekarang pukul 15.00, pukul berapakah
   (a) 12 jam kemudian
   (b) 20 jam yang lalu
2. Tuliskan hasil bagi dan sisa, apabila
   (a) 127 dibagi 9
   (b) -20 dibagi 3
   (c) 1234 dibagi 125
3. Carilah lima bilangan x sehingga $x \equiv 3 \mod 6$.
4. Jelaskan mengapa pernyataan berikut benar atau salah!
   (a) $4 \equiv 7 \mod 3$
   (b) $17 \equiv 7 \mod 5$
   (c) $14 \equiv 7 \mod 6$
   (d) $1234 \equiv 34 \mod 100$
5. Carilah hasil operasi berikut
   (a) $3 +_7 6$
   (b) $4 +_9 7$
   (c) $6 +_{10} 8$
   (d) $5 +_8 7$.

Kriptografi

Teori bilangan memegang peran kunci dalam kriptografi. Teori bilangan ini telah digunakan sebagai dasar sandi sejak berabad-abad yang lalu dan hingga saat ini. Sandi demikian mengenkripsi pesan dengan mengubah setiap huruf menjadi huruf yang berbeda, atau setiap blok huruf ke blok huruf yang berbeda.

Salah satu penggunaan kriptografi paling awal adalah oleh Julius Caesar. Dia merahasiakan pesan dengan menggeser setiap huruf tiga huruf ke depan dalam alfabet (mengirim tiga huruf terakhir dari alfabet ke tiga yang pertama). Misalnya, dengan menggunakan skema ini huruf B dikirim ke E dan huruf X dikirim ke A. Contoh demikian dinamakan **enkripsi**, yaitu proses membuat pesan menjadi rahasia.

Proses enkripsi Caesar dapat dijelaskan sebagai berikut. Pertama setiap abjad diganti dengan dengan satu eleman dalam $\mathbb{Z}_{26}$, yaitu integer 0 sampai dengan 25. Misalnya A diganti dengan 0, B dengan 1, C dengan 2 dan seterusnya hingga Z diganti dengan 25.

Metode enkripsi Caesar dapat dinyatakan dengan fungsi f yang memetakan integer p dengan $p \leq 25$, ke integer $f(p)$ dengan

$$f(p) = (p+3) \mod 26.$$

Contoh 15. Tuliskan pesan rahasia dari pesan

"KITA BERTEMU DI TAMAN ZEBRA"

dalam enkripsi Caesar?

Penyelesaian. Terlebih dahulu pesan asli tersebut diubah menjadi bilangan integer, misalnya K menjadi 10, I menjadi 8 dan seterusnya sehingga diperoleh pesan dalam bentuk bilangan:

10 8 19 0 1 4 17 19 4 12 20 3 8 19 0 12 0 13 25 4 1 17 0

Kemudian setiap bilangan p diubah menjadi $f(p) = (p+3) \mod 26$. Misalnya

$$f(10) = (10+3) \mod 26 = 13$$
$$f(25+3) \mod 26 = 2$$

Ini menghasilkan

13 11 22 3 4 7 20 22 7 15 23 6 11 22 3 15 3 16 2 7 4 20 3

Selanjutnya pesan dalam kode angka ini diubah kembali menjadi pesan abjad, menghasilkan pesan rahasia:

"MLVD EGUWHPX FL VDODQ CGEUD".

Untuk mengubah pesan rahasia (enkripsi) ke pesan asli dengan metode Caesar, digunakan fungsi f^{-1}, yaitu invers f. Proses merubah pesan yang dienkripsi menjadi pesan asli dinamakan **dekripsi**. Metode Caesar dapat diperumum dengan menggeser ke depan setiap abjad sejauh k, yaitu

$$f(p) = (p+k) \mod 26.$$

Dekripsi dapat dilakukan dengan menggeser setiap huruf ke belakang sejauh k, yaitu

$$f^{-1}(p) = (p-k) \mod 26.$$

Bilangan k tersebut dinamakan **kunci**.

Pada contoh 15 proses dekripsi dari pesan rahasia dilakukan dengan fungsi

$$f^{-1}(p) = (p-3) \mod 26.$$