Teori Bilangan

Departemen Matematika, FSAD-ITS

13 Juli 2024

Daftar Isi

Bab 1

Himpunan Bilangan Bulat

Bilangan bulat adalah bilangan nol (0), bilangan asli positif ($1, 2, 3$, dst.) atau bilangan bulat negatif bertanda minus ($-1, -2, -3$, dst.). Bilangan **negatif** adalah **kebalikan penjumlahan dari bilangan positif** yang bersesuaian. Dalam bahasa matematika, himpunan bilangan bulat sering dilambangkan dengan huruf $\mathbb{Z}$, jadi himpunan bilangan bulat adalah:

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

Himpunan bilangan asli $\mathbb{N}$ adalah himpunan bagian dari $\mathbb{Z}$

$$\mathbb{N} = \{1, 2, 3, \ldots\} \subset \mathbb{Z}$$

yang merupakan himpunan bagian dari semua bilangan rasional $\mathbb{Q}$,

$$\mathbb{Z} \subset \mathbb{Q} = \{\frac{m}{n} \mid m.n \in \mathbb{Z}, n \neq 0\}$$

yang merupakan himpunan bagian dari bilangan real $\mathbb{R}$

$$\mathbb{Q} \subset \mathbb{R}.$$

Himpunan $\mathbb{R}$ terdiri dari bilangan rasional dan bilangan irrasional, yaitu bilangan real yang tidak bisa dinyatakan sebagai bentuk pecahan $\frac{m}{n} \in \mathbb{Q}, m, n \in \mathbb{Z}, n \neq 0$. Contohnya: $\sqrt{2}, \pi$. Seperti bilangan asli, $\mathbb{Z}$ juga tak terhingga. Bilangan bulat dapat dianggap sebagai bilangan real yang dapat ditulis tanpa komponen pecahan. Misalnya, $23, 6, 0$, dan -2023 adalah bilangan bulat, sedangkan $9, 65, 5\frac{1}{2}$, dan $\sqrt{3}$ bukan bilangan bulat.

1.1 Sejarah

Kata bilangan bulat berasal dari bahasa Latin integer yang berarti "utuh" atau (secara harfiah) "tak tersentuh", dari dalam ("tidak") ***plus tangere*** ("menyentuh"). "Keseluruhan" berasal dari asal yang sama melalui kata Perancis ***entier***, yang berarti keseluruhan dan bilangan bulat. Secara historis, istilah ini digunakan untuk bilangan yang merupakan kelipatan 1, atau seluruh bagian dari bilangan campuran. Hanya bilangan bulat positif yang dipertimbangkan, menjadikan istilah ini sinonim dengan bilangan asli. Definisi bilangan bulat diperluas dari waktu ke waktu untuk memasukkan bilangan negatif seiring dengan diakuinya kegunaannya. Misalnya Leonhard Euler pada tahun 1765 **Elemen Aljabar** mendefinisikan bilangan bulat mencakup bilangan positif dan negatif. Namun, sebagian besar matematikawan Eropa menolak konsep bilangan negatif hingga pertengahan abad ke-19.

Penggunaan huruf $\mathbb{Z}$ untuk menunjukkan himpunan bilangan bulat berasal dari kata Jerman ***Zahlen*** ("bilangan") dan dikaitkan dengan David Hilbert. Penggunaan notasi paling awal yang diketahui dalam buku teks terjadi dalam Aljabar yang ditulis oleh **Nicolas Bourbaki**, sejak tahun 1947. Notasi tersebut tidak segera diadopsi, misalnya, buku teks lain menggunakan huruf $\mathbb{J}$, dan makalah tahun 1960 menggunakan $\mathbb{Z}$ untuk menunjukkan bilangan bulat non-negatif. Namun pada tahun 1961, $\mathbb{Z}$ secara umum digunakan oleh teks aljabar modern untuk menunjukkan bilangan bulat positif dan negatif.

Simbol $\mathbb{Z}$ sering dianotasi untuk menunjukkan berbagai himpunan, dengan penggunaan yang berbeda-beda di antara penulis yang berbeda: $\mathbb{Z}^+, \mathbb{Z}_+$ atau $\mathbb{Z}^>$ untuk bilangan bulat positif, $\mathbb{Z}^{0+}$ atau $\mathbb{Z}^\geq$ untuk bilangan bulat non-negatif, dan $\mathbb{Z}^{\neq}$ untuk bilangan bulat bukan -nol bilangan bulat. Beberapa penulis menggunakan $\mathbb{Z}^*$ untuk bilangan bulat bukan nol, sementara yang lain menggunakannya untuk bilangan bulat bukan negatif, atau untuk $\{-1, 1\}$ (grup satuan $\mathbb{Z}$) . Selain itu, $\mathbb{Z}_p$ digunakan untuk menunjukkan himpunan bilangan bulat modulo p (yaitu, himpunan kelas kongruensi bilangan bulat), atau himpunan bilangan bulat p-adic.

Bilangan bulat identik dengan bilangan bulat hingga awal tahun 1950an. Pada akhir tahun 1950-an, sebagai bagian dari gerakan Matematika Baru, para guru sekolah dasar di Amerika mulai mengajarkan bahwa “bilangan bulat” mengacu pada bilangan asli, tidak termasuk bilangan negatif, sedangkan “bilangan bulat” mengacu pada bilangan negatif. “Bilangan bulat” masih bersifat ambigu hingga saat ini.

1.2 Terurut Secara Baik

Pada bagian ini dibahas beberapa sifat dasar bilangan bulat, banyak yang akan menjadi penting kemudian dalam mengidentifikasi contoh berbagai jenis struktur aljabar, dimana $\mathbb{Z}$ akan memainkan peran penting bagi suatu model dasar. Bahasan dimulai dengan sifat relasi urutan biasa pada $\mathbb{Z}$ kemudian beralih ke sifat-sifat yang melibatkan operasi yang sudah dikenal penjumlahan, pengurangan, perkalian, dan pembagian. Akhirnya, diperkenalkan struktur aljabar baru terkait erat dengan bilangan bulat, yang disebut bilangan bulat mod n untuk setiap bilangan bulat $n > 1$.

Elemen-elemen himpunan bilangan bulat positip $\mathbb{N}$ dapat ditulis dalam urutan menaik dengan tanda pertaksamaan berulang, yaitu

$$1 < 2 < 3 < 4 < 5 < \cdots$$

Misalkan $S \subset \mathbb{N}$ dengan $S \neq \varnothing$ dan $n \in \mathbb{N}$. Dari bilangan bulat berikut $1, 2, 3, \ldots, n$ dapat dipilih satu yang merupakan elemen terkecil yang berada di S. Secara intuisi didapat aksiomatik berikut.

Aksioma (Prinsip Keterurutan Secara Baik dalam $\mathbb{N}$

Setiap himpunan bagian $S \subset \mathbb{N}$ dengan $S \neq \varnothing$ mempunyai suatu **elemen terkecil** di S, yaitu elemen pertama di S setelah elemen-elemennya diurutkan secara menaik. ■

Sering dalam membuktikan beberapa teorema atau membangun beberapa struktur diinginkan memilih elemen positip terkecil dari himpunan tak-kosong yang diberikan. Prinsip keterurutan secara baik menyatakan bahwa elemen tersebut dijamin ada. Berikut ini diberikan suatu penggunaan aksioma keterurutan secara baik.

Tidak ada bilangan bulat $n \in \mathbb{Z}$ yang memenuhi $0 < n < 1$. Hal ini ditunjukkan sebagai berikut. Misalkan $S = \{m \in \mathbb{Z} \mid 0 < m < 1\}$. Bila $S \neq \varnothing$, maka berdasarkan aksioma keterurutan secara baik ada $a \in S$ merupakan elemen terkecil sehingga $0 < a < 1$ Akibatnya $0 < a^2 < a < 1$. Jadi a^2 di S, hal ini kontradiksi dengan kenyataan bahwa a adalah elemen terkecil di S. Jadi haruslah $S = \varnothing$. Pada pembahasan ini, diskusikan mengapa $a^2 < a$! Dari apa yang telah dibahas ini, secara umum tidak ada bilangan bulat m yang memenuhi $n < m < n + 1$, $\forall n \in \mathbb{Z}$. Buktikan hal ini.

1.3 Algorithma Pembagian

Kita semua sudah akrab sejak **Sekolah Dasar** dengan **proses pembagian**, yaitu diberikan bilangan bulat a selalu dapat disajikan sebagai jumlah dari suatu kelipatan bilangan bulat lain yang diberikan yaitu $b \geq 1$ ditambah suatu sisa yang lebih kecil dari b. Hal ini akan terlihat pada teorema berikut yang dijamin oleh **prinsip keterutan secara baik** dari himpunan bilangan bulat.

Contoh 1.3.1

Berikut ini penyajian hasil dari proses pembagian dari beberapa pasang bilangan bulat a dan b.
Untuk $a = 84$ dan $b = 60$ kita mempunyai $84 = 1 \times 60 + 24$.
Untuk $a = 924$ dan $b = 105$ kita mempunyai $924 = 8 \times 105 + 84$.
Untuk $a = -10$ dan $b = 3$ kita mempunyai $-10 = -4 \times 3 + 2$.

Masing-masing kasus bilangan yang pertama merupakan kelipatan dari bilangan yang kedua tambah suatu bilangan bulat yang lebih kecil dari bilangan yang kedua.

Teorema 1.3.1 (Algorithma Pembagian)

Misalkan a adalah sebarang bilangan bulat dan b juga sebarang bilangan bulat tetapi $b \geq 1$. Maka ada dengan tunggal bilangan bulat q dan r yang memenuhi

1. $a = qb + r$,
2. $0 \leq r < b$.

Bukti
Misalkan $P = \{a - kb \mid k \in \mathbb{Z} \text{ dan } a - kb \geq 0\}$. Bila $a \geq 0$, maka $a \in P$ (sebab $a = a - 0b$). Bila $a < 0$, maka $a - 2ab > 0$. Jadi $a - 2ab \in P$, dengan demikian $P \neq \varnothing$. Gunakan aksiomatik keterurutan secara baik dari bilangan bulat positip didapat: Ada $r \in P$ dengan r adalah elemen terkecil. Karena $r \in P$, maka $r = a - qb$ untuk beberapa $q \in \mathbb{Z}$ atau $a = qb + r$ (memenuhi (**1**)) dan $r \geq 0$. Tinggal menunjukkan bahwa $r < b$. Andaikan $r \not< b$ ini berarti $r \geq b$, sehingga kita mempunyai

$$0 \leq r - b = (a - qb) - b = a - \underbrace{(q + 1)}_{k \in \mathbb{Z}} b \in P,$$

tetapi $r - b < r$ ini menunjukkan bahwa ada bilangan bulat positip yang lebih kecil dari r berada di P. Hal ini bertentangan dengan kenyataan bahwa r adalah elemen terkecil di P. Jadi haruslah $r < b$. Dengan demikian (**2**) dipenuhi, yaitu r memenuhi $0 \leq r < b$. Tinggal menunjukkan bahwa q dan r tunggal. Misalkan q_1 dan r_1 adalah bilangan bulat yang memenuhi $a = q_1 b + r_1$. Kita mempunyai

$$a = qb + r = aq_1 + r_1,$$

dimana $0 \leq r < b$ dan $0 \leq r_1 < b$. Maka $r_1 - r = qb - q_1 b = (q - q_1)b$. Sebagai akibat, kita mempunyai

$$|r_1 - r| = |(q - q_1)b| = |q - q_1|\,|b| = |q - q_1|\,b. \tag{1.1}$$

Tambahkan dua pertidaksamaan $-b < -r \leq 0$ dan $0 \leq r_1 < b$. Sehinggga kita mempunyai

$$-b < r_1 - r < b \quad \text{atau} \quad |r_1 - r| < b.$$

Berdasarkan Persamaan (1.1), maka $|q - q_1|b < b$. Sehingga didapat

$$0 \leq |q - q_1| < 1.$$

Karena $|q - q_1|$ adalah bilangan bulat taknegatip dan memenuhi $0 \leq |q - q_1| < 1$, maka haruslah $q - q_1 = 0$ atau $q = q_1$. Dengan demikian didapat $q_1 b + r_1 = qb + r$, yaitu $r_1 = r$. Jadi terbukti bahwa q dan r tunggal. ■

Bilangan q dalam Teorema 1.3.1 (**Algoritma Pembagian**) dinamakan **hasil bagi** sedangkan r dinamakan **sisa pembagian** dari a dibagi oleh b.

Kesimpulan 1.3.1

Bila $a, b \in \mathbb{Z}$ dengan $b \neq 0$, maka ada tunggal bilangan bulat q dan r yang memenuhi

$$a = qb + r,\ 0 \leq r < |b|.$$

Bukti

Mengikuti bukti Teorema 1.3.1 (**Algoritma Pembagian**), cukup dibuktikan untuk kasus b adalah negatif. Maka $|b| > 0$ atau $|b| \geq 1$. Dengan demikian menurut Teorema 1.3.1 (**Algoritma Pembagian**) ada dengan tunggal bilangan bulat q_1 dan r yang memenuhi $a = q_1|b| + r,\ 0 \leq r < |b|$. Karena $|b| = -b$, maka bisa diplih $q = -q_1$, sehingga didapat

$$a = q_1|b| + r = (-q)(-b) + r = qb + r,\ 0 \leq r < |b|. \quad ■$$

1.4 Pembagian Bilangan bulat dan hal-hal terkait

Definisi 1.4.1 Pembagian di $\mathbb{Z}$

Diberikan dua bilangan bulat a dan b, dengan $a \neq 0$ dikatakan bahwa a adalah pembagi dari b ditulis $a \mid b$, bila $b = ac$ untuk beberapa bilangan bulat c. Bila a tidak membagi b, maka ditulis $a \nmid b$.
Catatan bahwa dibolehkan $a \leq 0$ dalam definisi ini. ■

Beberapa akibat langsung dari Definisi 1.4.1 tentang pembagian di $\mathbb{Z}$ diberikan dalam teorema berikut.

Teorema 1.4.1 (Pembagian)

Diberikan $a, b, c \in \mathbb{Z}$. Maka

1. $a \mid 0, 1 \mid a$ dan $a \mid a$.
2. $a \mid \pm 1$ bila dan hanya bila $a = \pm 1$.
3. Bila $a \mid b$, maka $ac \mid bc$.
4. Bila $a \mid b$ dan $b \mid c$, maka $a \mid c$.
5. $a \mid b$ dan $b \mid a$ bila dan hanya bila $a = \pm b$.
6. Bila $c \mid a$ dan $c \mid b$, maka $c \mid (ax \pm by)$ untuk setiap $x, y \in \mathbb{Z}$.
7. Bila $a \mid b$ dan $a \mid c$, maka $a \mid (b \pm c)$.

Bukti: Sebagai latihan! ■

Definisi 1.4.2 Pembagi Persekutuan

Diberikan dua bilangan bulat a dan b, suatu bilangan bulat d yang memenuhi kondisi $d \mid a$ dan $d \mid b$ dinamakan suatu **pembagi persekutuan dari** a dan b.

Contoh 1.4.1

Bilangan bulat 252 dan 180 mempunyai pembagi persekutuan positip: $1, 2, 3, 6, 9, 12$ dan 36. Tidak ada bilangan bulat positip yang lebih besar dari 36 yang merupakan pembagi persekutuan dari 252 dan 180.

Pada pembahasan berikutnya akan sering tertarik untuk mencari pembagi persekutuan terbesar dari dua bilangan bulat.

Definisi 1.4.3 Pembagi Pesekutan Terbesar (FPB)

Diberikan dua bilangan bulat a dan b keduanya taknol, **pembagi persekutuan terbesar** dari a dan b adalah suatu bilangan bulat $d \geq 1$ yang memenuhi

1. $d \mid a$ dan $d \mid b$.
2. Untuk sebarang bilangan bulat c, bila $c \mid a$ dan $c \mid b$, maka $c \mid d$.

Dalam hal ini ditulis $d = \text{fpb}(a, b)$.

Secara ringkas, $\text{fpb}(a, b)$ adalah bilangan bulat terbesar di dalam himpunan dari semua pembagi persekutuan terbesar dari a dan b. Suatu pertanyaan yang wajar adalah apakah bilangan bulat a dan b bisa mempunyai pembagi-pembagi persekutuan terbesar yang berbeda. Untuk menjawab pertanyaan ini, misalkan ada dua bilangan bulat positip d dan d_1 yang merupakan $\text{fpb}(a, b)$. Maka berdasarkan Definisi 1.4.3 bagian (**2**) didapat $d \mid d_1$ juga $d_1 \mid d$. Dengan demikian, berdasarkan Teorema 1.4.1 bagian (5), maka $d = \pm d_1$. Karena d dan d_1 keduanya adalah bilangan bulat positip, maka haruslah $d = d_1$. Jadi bila $\text{fpb}(a, b)$ **ada**, maka keberadaannya adalah **tunggal**.

Algorithma pembagian beserta aplikasi yang lain dari prinsip keterurutan secara baik, menjamin keberadaan dari $\text{fpb}(a, b)$, sebagaimana diberikan oleh teorema berikut.

Teorema 1.4.2 (Eksistensi FPB)

Misalkan a dan b adalah bilangan bulat keduanya taknol. Maka

1. $d = \text{fpb}(a, b)$ ada (eksis).
2. Ada bilangan bulat u dan v yang memenuhi $d = ua + vb$.

Bukti
Misalkan $S = \{xa + yb \mid x, y \in \mathbb{Z} \text{ dan } xa + yb \geq 1\}$. Karena $S \neq \varnothing$ sebab $aa + bb \in S$. Maka dengan menggunakan prinsip keterurutan secara baik S mempunyai elemen terkecil d. Karena $d \in S$ didapat $d = sa + tb$ untuk beberapa $s, t \in \mathbb{Z}$ dan $d \geq 1$. Bila k adalah suatu pembagi persekutuan dari a dan b, maka $a = uk$ dan $b = vk$ untuk beberapa $u, v \in \mathbb{Z}$. Didapat $d = sa + tb = (su + tv)k$, yaitu k membagi d. Selanjutnya ditunjukkan bahwa $d = \text{fpb}(a, b)$, hanya diperlukan d pembagi persekutuan dari a dan b. Gunakan Algoritma Pembagian didapat $a = qd + r$ dengan $0 \leq r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b < d$. Karena d elemen terkecil di S, maka tidak akan $r \geq 1$. Jadi haruslah $r = 0$, dengan demikian $a = qd$ atau d adalah pembagi dari a. Dengan cara yang sama dapat ditunjukkan bahwa d juga pembagi dari b. Dengan demikian sudah terbukti bahwa $d = \text{fpb}(a, b)$. ■

Teorema 1.4.2 (**Eksistensi FPB**) bagian (**1**) menjamin eksistensi dari $\text{fpb}(a, b)$, sedangkan pada bagian (**2**) menyatakan bahwa $\text{fpb}(a, b)$ dapat diungkapkan sebagai suatu **kombinasi linier** dari a dan b yaitu $ua + vb$. Mungkin pada awal yang terlihat saat ini kurang menarik, namun nanti pada kenyataannya ternyata **sangat berguna**.

Apa yang diberikan dalam contoh ini menggambarkan bagaimana menghitung faktor persekutuan terbesar untuk kasus sederhana. Faktor persekutan terbesar dari 84 dan 60 didapat dengan berulang kali menerapkan Algoritma Pembagian, sebagai berikut:

$$\begin{aligned} 84 &= 1 \times 60 + 24 \\ 60 &= 2 \times 24 + 12 \\ 24 &= 2 \times 12 + 0. \end{aligned}$$

Dari persamaan ke-3 terlihat bahwa $12 \mid 12$ dan $12 \mid 24$. Sehingga berakibat pada persamaan ke-2 yaitu $12 \mid 60$. Karena $12 \mid 24$ dan $12 \mid 60$, maka persamaan ke-1 berakibat $12 \mid 84$. Jadi 12 adalah pembagi persekutuan dari 84 dan 60. Bila selain 12, d' juga pembagi persekutuan dari 84 dan 60, maka dari persamaan pertama $d' \mid 60$ dan $d' \mid 24$. Sehingga dari persamaan kedua berakibat $d' \mid 24$ dan $d' \mid 12$. Jadi $12 = \text{fpb}(84, 60)$.

Teorema 1.4.3 (Algoritma Euclide)

Untuk sebarang pasangan bilangan bulat a dan $b \geq 1$ dapat dilakukan penghitungan $\text{fpb}(a, b)$ dengan melakukan algoritma pembagian secara berulang sebagai berikut:

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{dimana } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \quad \text{dimana } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \quad \text{dimana } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

berhenti ketika diperoleh sisa pembagian sama dengan nol:

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \quad \text{dimana } 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad \text{dimana } 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Sisa pembagian terakhir taknol $r_n = \text{fpb}(a, b)$. Metoda perhitungan $\text{fpb}(a, b)$ ini dinamakan **Algorithma Euclide**.

Bukti

Hasil akhir sisa pembagian adalah nol, dengan menggunakan prinsip keterutan secara baik berakibat bahwa himpunan semua sisa yang positip harus mempunyai suatu elemen terkecil. Karena barisan sisa pembagian positip $r_1 > r_2 > r_3 > \cdots$ adalah barisan turun, maka sisa pembagian positip terkecil adalah sisa pembagian terakhir, yang mana sisa pembagian berikutnya adalah nol. Dalam hal ini r_n adalah sisa pembagian positip yang terakhir, maka

$$\begin{aligned}
\mathrm{fpb}(a,b) &= \mathrm{fpb}(b,r_1)\\
&= \mathrm{fpb}(r_1,r_2)\\
&= \mathrm{fpb}(r_2,r_3)\\
&\vdots\\
&= \mathrm{fpb}(r_{i-1},r_i)\\
&\vdots\\
&= \mathrm{fpb}(r_{n-2},r_{n-1})\\
&= \mathrm{fpb}(r_{n-1},r_n)\\
&= r_n. \qquad \blacksquare
\end{aligned}$$

Contoh 1 Pembagi Persekutuan Terbesar

Hitung $\mathrm{fpb}(924, 105)$. Perhitungan dilakukan sebagai berikut:

$$\begin{aligned}
924 &= 8 \cdot 105 + 84\\
105 &= 1 \cdot 84 + 21\\
84 &= 4 \cdot 21 + 0.
\end{aligned}$$

Jadi $\mathrm{fpb}(924, 105) = 21$. Dari persamaan kedua didapat $21 = 105-84$. Dari persamaan yang pertama didapat $84 = 924 - 8 \cdot 105$. Gabungkan hasil pertama dengan kedua didapat

$$21 = 105 - (924 - 8 \cdot 105) = \boxed{\text{-1}} \cdot 924 + \boxed{9} \cdot 105.$$

Terihat bahwa fpb adalah sebagai suatu kombinasi linier $\boxed{\text{u}} \cdot 924 + \boxed{\text{v}} \cdot 105$ dimana $u = -1$ dan $v = 9$.
Catatan, bilangan bulat u dan v yang memenuhi $\mathrm{fpb}(a, b) = ua + vb$ adalah tidak tunggal. Misalnya, bila $a = 90$ dan $b = 252$, maka

$$\mathrm{fpb}(90, 252) = 18 = (3)90 + (-1)252.$$

dan

$$\mathrm{fpb}(90, 252) = 18 = (3+252)90+(-1-90)252 = (255)90+(-91)252.$$

$\square$

Teorema Dasar Aritmatika

Konsekuensi lain yang penting dari algoritma pembagian dan prinsip keterutan secara baik adalah setiap bilangan bulat $n > 1$ dapat ditulis sebagai produk dari bilangan prima, yaitu bilangan bulat yang tidak dapat ditulis sebagai produk dengan cara taktrivial.

Contoh 2 Prima Relatif

Misalkan dihitung $\text{fpb}(385, 48)$ sebagai berikut:

$$\begin{aligned} 385 &= 8 \cdot 48 + 1 \\ 48 &= 48 \cdot 1 + 0. \end{aligned}$$

Terlihat bahwa $\text{fpb}(385, 48) = 1$, dengan kata lain bilangan bulat positip yang terbesar dan hanya satu bilangan ini yaitu 1 yang bisa membagi 385 dan 48.

□

Definisi 1.4.4 Prima Relatif dan Prima

Dua bilangan bulat a dan b dikatakan **prima relatif** bila $\text{fpb}(a, b) = 1$ dengan kata lain pembagi persekutuan positip dari a dan b hanya bilangan bulat 1. Suatu bilangan bulat $p > 1$ dinamakan **prima** bila banyaknya pembagi positipnya adalah **dua yang berbeda** yaitu 1 dan dirinya sendiri.

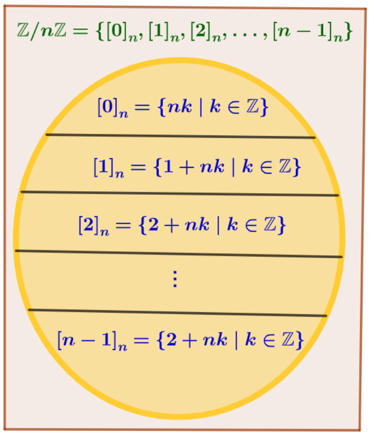
□

Contoh 3 Prima

Bilangan 1 bukan bilangan prima sebab hanya memiliki satu pembagi yaitu dirinya sendiri, sedangkan 2 bilangan prima sebab mempunyai dua pembagi yang berbeda yaitu 1 dan dirinya sendiri yaitu 2.

□

Berkaitan dengan algoritma pembagian bilangan bulat bila dibagi oleh $n > 0$, maka kemungkinan sisanya ada sebanyak n keadaan: $0, 1, 2, \ldots, n-1$. Keadaan ini disajikan oleh Gambar 1.1. Notasi $\mathbb{Z}/n\mathbb{Z}$ dalam pembahasan ini kita tulis sebagai $\mathbb{Z}_n$ yang menyatakan himpunan bilangan bulat modulo n.



Gambar $\mathbb{Z}$ dipartisi menjadi n himpunan bagian yang saling asing

Gambar 1.1:

Dalam himpunan bilangan bulat Modulo n, untuk $n = 10$ kita mempunyai

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, [2]_{10}, [3]_{10}, [4]_{10}, [5]_{10}, [6]_{10}, [7]_{10}, [8]_{10}, [9]_{10}\}.$$

Himpunan

$$\mathbb{U}(10) = \{a \in \mathbb{Z}_{10} \mid \text{fpb}(a, 10) = 1\} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}.$$

Banyaknya elemen $|\mathbb{U}(10)| = 4$ dinotasikan sebagai $\varphi(10) = 4$ dan dibaca **phi Euler** dari 10 adalah 4. Bilangan phi Euler sangat penting dalam teori bilangan. Bagaimana mencari bilangan $\varphi(n)$ bila n adalah bilangan bulat yang cukup besar? Untuk menjawab pertanyaan diberikan beberapa kasus:

1. Bila $n = p$ dengan p bilangan prima maka $\boxed{\varphi(p) = p - 1}$.
2. Bila $n = p_1 p_2 \cdots p_k$ dengan $p_i, i = 1, 2, \ldots, k$ bilangan prima semuanya berbeda maka $\boxed{\varphi(n) = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1)}$.
3. Bila $n = p^m$ dengan p bilangan prima maka $\boxed{\varphi(n) = p^{m-1}(p - 1)}$.

Dari **2.** dan **3.** kita mempunyai bila $\text{fpb}(p, q) = 1$, maka $\boxed{\varphi(pq) = \varphi(p)\varphi(q)}$.

Contoh 4 Phi Euler

$\varphi(2) = 2 - 1 = 1, \varphi(256) = \varphi(2^8) = 2^{8-1}(2-1) = 2^7 = 128$, $\varphi(2304) = \varphi(2^8\, 3^2) = 2^{8-1}(2-1)\, 3^{2-1}(3-1) = 2^7\, 3(2) = 128 \times 6 = 768$, $\varphi(231) = \varphi(3 \times 7 \times 11) = \varphi(3)\varphi(7)\varphi(11) = 2 \times 6 \times 10 = 120$. □

Berikut ini kita berikan **Teorema Euler**:
Bila fpb$(a, n) = 1$, maka $\boxed{a^{\varphi(n)} = 1 \pmod{n}}$. □

Dari **Teorema Euler** bila kedua ruas $a^{\varphi(n)} = 1 \pmod{n}$ dikalikan dengan a kita mempunyai $a^{\varphi(n)+1} = a \pmod{n}$. Selanjutnya bila $n = p$ dengan p adalah bilangan prima, maka kita mempunyai $a^{\varphi(p)+1} = a \pmod{p} \Rightarrow$ $\boxed{a^p = a \pmod{p}}$ berlaku untuk sebarang bialangan bulat positip a. Hasil akhir ini dinamakan **Teorema Fermat Kecil**.

Teorema berikut sebagai akibat dari Teorema Eksistensi FPB bagian (2).

Teorema 1.4.4 Prima Relatif

Misalkan a dan b adalah prima relatif dan c adalah suatu bilangan bulat. Maka

1. Sebarang pembagi persekutuan dari a dan bc adalah suatu pembagi persekutuan dari a dan c.
2. Bila a membagi bc, maka a membagi c.
3. Bila a dan c adalah prima relatif, maka a dan bc prima relatif.

Bukti
Misalkan fpb$(a, b) = 1$ dan misalkan $d \,|\, a$ dan $d \,|\, bc$. Maka, dengan menggunakan Teorema Eksistensi FPB didapat $1 = sa + tb$ untuk beberapa bilangan bulat s dan t, juga $a = dx$ dan $b = dy$ untuk beberapa bilangan bulat x dan y. Dengan demikian didapat

$$c = c \cdot 1 = c(sa + tb) = acs + bct = dxcs + dyct = d(xcs + yct),$$

terlihat bahwa $d \,|\, c$ sebagaimana dibutuhkan untuk membuktikan (1). Misalkan bahwa $a \,|\, bc$, maka $bc = ad'$ untuk beberapa bilangan bulat d' dan

$$c = c \cdot 1 = c(sa + tb) = acs + bct = acs + ad't = a(cs + d't),$$

terlihat bahwa $a \,|\, c$ sebagaimana diharapkan bukti bagian (2). Dari (1), d adalah pembagi persekutuan dari a dan bc dan juga pembagi persekutuan dari a dan c. Bila a dan b adalah prima relatif, maka $\text{fpb}(a, c) = 1 = d$. Hal ini berakibat juga $\text{fpb}(a, bc) = 1$. Jadi a dan bc adalah prima relatif. $\square$

Sebagai akibat langsung adalah kesimpulan penting berikut.

Lemma 1.4.1 Euclide

Misalkan b dan c adalah bilangan bulat. Bila p adalah prima dan $p \,|\, bc$, maka $p \,|\, b$ atau $p \,|\, c$.

Bukti
Jika $p \,|\, b$, maka tidak ada yang perlu dibuktikan. Jika tidak $p \,|\, b$, maka $\text{fpb}(p, b) = 1$. Hal ini berakibat bahwa $1 = xp + yb$ untuk beberapa bilangan bulat x dan y. Dari $1 = xp + yb$ didapat $c = xpc + ybc$. Jelas bahwa $p \,|\, xpc$ dan $p \,|\, ybc$ (hipotisis bahwa $p \,|\, bc$). Jadi $p \,|\, c$. $\square$

Contoh 5 Lemma Eulcide

Adalah sangat penting dalam Lemma Euclid bahwa p adalah prima. Misalkan sebagai mana diketahui bahwa 6 membagi $3 \cdot 4 = 12$ tetapi $6 \nmid 3$ dan $6 \nmid 4$. $\square$

Untuk membuktikan Teorema **Fundamental Aritmatika** dibutuhkan **Lemma Euclide** dalam suatu bentuk yang lebih umum, sebagaimana kesimpulan berikut.

Kesimpulan
Misalkan $b_1, b_2, \ldots, b_r$ adalah bilangan bulat. Bila p adalah prima dan $p \,|\, b_1, b_2, \ldots, b_r$, maka $p \,|\, b_i$ untuk beberapa i, dengan $1 \leq i \leq r$.

Bukti
Digunakan induksi matematika pada r. Untuk $r = 1$, jelas dipenuhi. Kasus $r = 2$ adalah Lemma Euclide. Selanjutnya misalkan pernyataan benar untuk $r = k$ dan $p \,|\, (b_1, b_2, \ldots, b_k)b_{k+1}$. Gunakan Kesimpulan (**Lemma Euclide**), didapat salah satu dari $p \,|\, b_{k+1}$ hal ini sebagaimana diinginkan atau $p \,|\, b_1 b_2 \ldots b_k$, dengan menggunakan hipotesis induksi $p \,|\, b_i$ untuk beberapa i, dengan $1 \leq i \leq k$. $\square$

Teorema (**Fundamental Aritmatika**)
Misalkan n adalah suatu bilangan bulat dengan $n > 1$. Maka

1. n adalah salah satu dari prima atau suatu produk dari prima.

2. Faktorisasi dari n dalam suatu produk dari prima adalah tunggal, kecuali untuk urutan primanya. Yaitu, bila

$$n = p_1 p_2 \cdots p_r \text{ dan } n = q_1 q_2 \cdots q_s,$$

   yang mana p_i dan q_j adalah prima, maka $r = s$ dan, bila perlu dengan melakukan pengurutan kembali didapat $p_i = q_i$ untuk semua $i = 1, 2, \ldots, r$.

Bukti
Untuk membuktikan (1) dan (2) digunakan induksi matematika pernyataan benar untuk $n \geq 2$.

1. Untuk $n = 2$, pernyataan (1) dipenuhi, sebab 2 adalah prima. Untuk membuktikan (1) dipenuhi untuk n, asumsikan bahwa (1) benar untuk sebarang bilangan bulat k dengan $2 \leq k < n$. Bila n adalah prima adalah sebagaimana diinginkan. Bila n bukan prima, pilih bilangan bulat u dan v dengan $1 < u, v < n$ yang memenuhi $uv = n$. Dengan hipotesis induksi masing-masing u dan v salah satu dari prima atau bisa dituliskan sebagai produk dari prima. Didapat, $n = uv$ dapat dituliskan sebagai produk dari prima.

2. Untuk $n = 2$, pernyataan (2) jelas dipenuhi, sebab 2 adalah prima yang tidak bisa dituliskan sebagai produk prima yang lainnya yang lebih besar dari 2. Jadi untuk membuktikan n memenuhi pernyataan (2) diasumsikan (2) dipenuhi untuk sebarang k dimana $2 \leq k < n$. Misalkan

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

   Terlihat bahwa $p_1 \mid n$, maka $p_1 \mid q_1 q_2 \cdots q_s$. Dengan menggunakan Kesimpulan yang telah dibahas didapat $p_1 \mid q_i$ untuk beberapa i dengan $1 \leq i \leq s$. Bila diperlukan, dilakukan pengurutan kembali pada q_i sehingga q_j ini menjadi q_1. Dengan demikian didapat $p_1 \mid q_1$. Karena q_1 prima haruslah $p_1 = q_1$. Selanjutnya misalkan $k = n/p_1 = n/q_1 < n$, didapat

$$k = p_2 \cdots p_r = q_2 \cdots q_s.$$

   Lakukan lagi proses hipotesis induksi secara berulang. Dengan demikian didapat banyaknya bilangan prima pada masing-masing faktor harus sama, yaitu $r - 1 = s - 1$, akibatnya $r = s$. Jadi $p_i, 2 \leq i \leq r$ dan $q_j, 2 \leq j \leq r$ harus sama kecuali hanya pada urutannya.

□

Terema Fundamental Aritmatika yang baru saja dibuktikan berakibat bahwa diberikan sebarang bilangan bulat $n > 1$, maka n dapat ditulis sebagai produk

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

dimana p_i adalah bilangan prima berbeda untuk masing-masing i dan, p_i ini dan pangkat-pangkatnya a_i adalah tunggal. Bila bilangan-bilangan bulat dituliskan dalam cara tersebut, maka mudah untuk memperoleh pembagi persekutuan terbesaranya, sebagaimana diberikan oleh contoh berikut.

Contoh
Sebagaimana telah dibahas dalam Contoh sebelumnya, $\mathrm{fpb}(924, 105) = 21$. Tetapi $924, 105$ dan 21 dapat difaktorkan kedalam bentuk pangkat dari bilangan prima sebagai berikut:

$$924 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 11^1 \qquad 105 = 3^1 \cdot 5^1 \cdot 7^1 \qquad 21 = 3^1 \cdot 7^1.$$

Sekedar untuk membandingkan, ditulis lagi

$$924 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \qquad 105 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0$$
$$21 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0.$$

Terlihat bahwa yang mana saja pangkat pada bilangan prima dalam faktorisasi 21 lebih kecil dari pangkat pada bilangan prima yang sama dalam faktorisasi dari 924 dan 105. Sebaliknya, bila diambil pangkat-pangkat yang lebih besar, maka didapat bilangan

$$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 4620.$$

Sebagaiman telah diketahui bahwa 21 adalah pembagi persekutuan terbesar dari 924 dan 105, sebaliknya 4620 adalah kelipatan persekutuan terkecil dari 924 dan 105.

□

Definisi Kelipatan Persekutuan Terkecil
Diberikan dua bilangan bulat n dan m keduanya taknol, **kelipatan persekutuan terkecil** dari n dan m adalah bilangan bulat $l \geq 1$ yang memenuhi

1. $n\,|\,l$ dan $m\,|\,l$.
2. Untuk sebarang bilangan bulat k, bila $n\,|\,k$ dan $m\,|\,k$, maka $l\,|\,k$.

Dalam hal ini ditulis $l = \mathrm{kpk}(n, m)$.

□

Teorema
Diberikan

$$n = p_1^{a_1} p_2^{a_2} \cdot p_k^{a_k} \text{ dan } m = p_1^{b_1} p_2^{b^2} \cdots p_k^{b^k},$$

dimana p_i bilangan prima berbeda dan $a_i, b_i \geq 0$, maka

1. $\text{fpb}(n, m) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, dimana $c_i = \min\{a_i, b_i\}$,

2. $\text{kpk}(n, m) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, dimana $d_i = \max\{a_i, b_i\}$,

3. $\text{kpk}(n, m) \cdot \text{fpb}(n, m) = nm$.

Bukti Sebagai latihan! □

1.5 Bilangan Bulat modulo n

Untuk mengakhiri bagian ini dibahas kembali topik relasi ekivalen. Yaitu relasi ekivalen yang khusus pada $\mathbb{Z}$ yang mana sifat-sifat $\mathbb{Z}$ ini telah dibahas sebelumnya.

Definisi 1.5.1 Kongruen mod n

Misalkan $n > 0$ adalah sebarang bilangan bulat tetapi tetap. Untuk sebarang dua bilangan bulat a dan b adalah **kongruen mod** n ditulis $a \equiv b \mod n$ bila $n \,|\, (ab)$ □

Dari Definisi 1.5.1 kita dapatkan teorema berikut.

Teorema 1.5.1 Pembagian

1. 1. Relasi kongruen mod n adalah suatu relasi ekivalen pada $\mathbb{Z}$.
2. Relasi ekivalen tersebut mempunyai tepat sebanyak n klas ekivalen yaitu
$$n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}.$$
3. Bila $a \equiv b \mod n$ dan $c \equiv d \mod n$, maka
$$a+c \equiv b+d \mod n \qquad ac \equiv bd \mod n.$$
4. Bila a dan n prima relatif, maka
$$ab \equiv ac \mod n \quad \text{berakibat} \quad b \equiv c \mod n.$$

Bukti

1. Untuk semua $a, b, c \in \mathbb{Z}$ didapat $a \equiv a \mod n$ sebab $n \,|\, 0 = (a-a)$. Selanjutnya, bila $a \equiv b \mod n$, maka $n \,|\, b(a-b) = -(b-a)$. Jadi $b \equiv a \mod n$. Berikutnya, bila $a \equiv b \mod n$ dan $b \equiv c \mod n$, maka $n \,|\, (a-b)$ dan $n \,|\, (b-c)$. Jadi $n \,|\, ((a-b)+(b-c)) = (a-c)$. Terlihat bahwa $n \,|\, (a-c)$ atau $a \equiv c \mod n$.

2. Untuk sebarang $a \in \mathbb{Z}$, misalkan $[a]_n$ adalah klas ekivalen dari $a \in \mathbb{Z}$. Dengan menggunakan algoritma pembagian didapat $a = qn + r$ untuk beberapa $q, r \in \mathbb{Z}$ dengan $0 \leq r < n$. Terlihat bahwa $a \equiv r \mod n$. Jadi $[a]_n = [r]_n$. Jadi hanya ada n klas ekivalen yaitu:
$$0+n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}.$$
Semuanya berbeda, sebab untuk r dan s dengan $0 \leq r, s < n$ didapat $n \,|\, (r-s)$ bila dan hanya bila $r = s$.

3. Bila $a \equiv b \mod n$ dan $c \equiv d \mod n$, maka $n \,|\, (a-b)$ dan $n \,|\, (c-d)$. Didapat
$$n \,|\, ((a-b)+(c-d)) = (a+c)-(b+d).$$
Terlihat bahwa $a+b \equiv b+d \mod n$. Juga
$$n \,|\, (c-b) \Rightarrow n \,|\, (ac-bd).$$
Terlihat bahwa $ac \equiv bd \mod n$.

4. Bila a dan n prima relatif dan $ab \equiv ac \mod n$, maka

$$n \mid (ab - ac) = a(b - c),$$

berdasarkan Teorema Prima relatif bagian (2), maka $n \mid (b - c)$. Jadi $b \equiv c \mod n$.

$\square$

Bab 2

Latihan Soal-soal

Untuk mengakhiri bagian ini diberikan pembahasan soal-soal dan beberapa sisanya digunakan sebagai latihan.

1. Tunjukkan bahwa: $1^{1997} + 2^{1997} + \cdots + 1996^{1997}$ dapat dibagi oleh 1997.

   Jawab
   Kita susun ulang secara kelompok sebagai berikut:

   $$(1^{1997} + 1996^{1997}) + (2^{1997} + 1995^{1997}) + \cdots + (998^{1997} + 999^{1997}). \quad (2.1)$$

   Di sini setiap tanda kurung berbentuk $(a_i^{2n+1} + b_i^{2n+1})$. Selanjutnya kita menggunakan persamaan

   $$\boxed{a^{2n+1} + b^{2n+1} = (a+b)(a^{2n} - a^{2n-1}b + a^{2n-2}b^2 - \cdots + b^{2n})}$$

   maka, $(a_i^{2n+1} + b_i^{2n+1})$ habis dibagi $(a_i + b_i)$. Tetapi $(a_i + b_i) = 1997$ untuk semua i. Jadi (2.1) dapat dibagi oleh 1997.

2. Tunjukkan bahwa untuk setiap bilangan alam n, maka $B = 2903^n - 803^n - 464^n + 261^n$ dapat dibagi oleh 1897.

   Jawab
   Kita mempunyai $1897 = 7 \times 271$. Selanjutnya B dapat disusun ulang sebagai $(2903^n - 803^n) - (464^n - 261^n)$. Kita gunakan persamaan:

   $$\boxed{x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}).}$$

   Maka, didapat: $(2903^n - 803^n)$ dapat dibagi oleh $(2903 - 803) = 2100$ dan $(464^n - 261^n)$ dapat dibagi oleh $(464 - 261) = 203$ atau $2100 =$

$7 \times 300 \mid (2903^n - 803^n)$ dan $203 = 7 \times 29 \mid (464^n - 261^n)$. Jadi $7 \mid (2903^n - 803^n)$ dan $7 \mid (464^n - 261^n)$. Dengan demikian $7 \mid B$. Sekali lagi B kita susun ulang sebagai:

$$2903^n - 803^n - 464^n + 261^n = (2903^n - 464^n) - (803^n - 261^n).$$

Dengan alur pemikiran sebagaimana sebelumnya kita dapatkan $2903 - 464 = 2439 = 271 \times 9 \mid (2903^n - 464^n)$ dan $(803 - 261) = 542 = 271 \times 2 \mid (803^n - 261^n)$. Jadi $271 \mid (2903^n - 464^n)$ dan $271 \mid (803^n - 261^n)$. Dengan demikian $271 \mid B$. Akibatnya $1897 = 7 \times 271 \mid B$.

3. Tunjukkan bahwa: $3x + 11y$ dan $29x + 23y$ habis dibagi 125 untuk himpunan nilai-nilai bilangan bulat positif yang sama dari x, y. Dapatkan setidaknya dua pasangan (x, y) yang memenuhi $3x + 11y$ dan $29x + 23y$ dapat dibagi 125.

   Jawab
   Karena $3(3x + 11y) + 4(29x + 23y) = 125(x + y)$, dan $\text{fpb}(3, 125) = 1, \text{fpb}(4, 125) = 1$, maka $125 \mid (3x + 11y)$ juga $125 \mid (29x + 29y)$. Di sini kita telah menggunakan sifat yang berikut dengan benar: Untuk $a \mid b$ dan $a \mid c$ maka $a \mid (ka + lb)$ sebaliknya $a \mid (ka + lb)$ dan $a \mid ka$, maka $a \mid lb$ dan jika $\text{fpb}(a, l) = 1$, maka $a \mid b$. Untuk mencari nilai x dan y yang kedua persamaannya habis dibagi 125, kita selesaikan sistem persamaan (2.2) dan (2.3) berikut:

$$3x + 11y = 125n_1 \tag{2.2}$$
$$29x + 23y = 125n_2 \tag{2.3}$$

   Didapat $x = \frac{11n_2 - 23n_1}{2}, y = \frac{29n_1 - 3n_2}{2}$ untuk $n_1, n_2 \in \mathbb{Z}$ dengan n_1 dan n_2 mempunyai paritas yang sama yaitu kedua genap atau keduanya ganjil. Dua nilai pasangan (x, y) bisa kita tentukan untuk $n_1 = n_2 = 1$ didapat $(x, y) = (-6, 13)$ dan untuk $n_1 = 2, n_2 = 4$ didapat $(-1, 23)$.

4. Tunjukkan bahwa 9765624 habis dibagi oleh 11.

   Jawab
   Kita gunakan Teorema Euler sebagai berikut:
   $9765624 = 9765625 - 1 = 5^{10} - 1 \Rightarrow 5^{10} - 1 = 0 \pmod{11}$. Jadi 9765624 habis dibagi oleh 11.

5. Tentukan sisa pembagian dari 3001^{2023} dibagi 7.

Jawab
Karena 7 adalah bilangan prima dan $3001 = 5 \pmod 7$, selanjutnya kita gunakan Teorema Euler didapat

$$3001^{2023} \pmod 7 = 3001^{2023 \pmod 6} \pmod 7 = 5^1 \pmod 7 = 5 \pmod 7.$$

Jadi sisa pembagian dari 3001^{2023} dibagi 7 adalah 5.

6. Tentukan nilai dari x yang memenuhi $3x = 4 \pmod 5$.

   Jawa
   Karena 5 bilangan prima dan kita gunakan Teorema Euler, kita mempunyai

$$\begin{aligned} 3x &= 4 \pmod 5 \\ 3^3 \times 3x &= 3^3 \times 4 \pmod 5 \\ (3^3 \times 3)x &= 3^3(3+1) \pmod 5 \\ 3^4 \cdot x &= 3^4 + 27 \pmod 5 \\ 1 \cdot x &= 1 + 2 \pmod 5 \\ x &= 3 \pmod 5. \end{aligned}$$

7. Diberikan $x \in \mathbb{R}$ dan

$$m = \frac{-1+3x}{1+x} - \frac{\sqrt{|x|-2} + \sqrt{2-|x|}}{|2-x|}.$$

   Tunjukkan bahwa m adalah suatu bilangan bulat dan tentukan digit satuan dari nilai m^{2023}.

   Jawab
   Karena $|x| - 2 \geq 0$ dan $2 - |x| \geq 0$ atau $|x| \geq 2$ dan $|x| \leq 2$. Hal ini berakibat $|x| = 2$. Sehingga kita memperoleh $x = \pm 2$. Karena penyebut dari suatu pecahan tidak boleh sama dengan nol, maka $|2 - x| \neq 0$. Dengan demikian nilai x yang memenuhi adalah $\boldsymbol{x = -2}$. Sehingga kita memperoleh $m = 7$ adalah bilangan bulat. Selanjutnya untuk menentukan digit satuan dari $m^{2022} = 7^{2022}$. Kita menggunakan mod 10, dalam hal ini $7^4 = 1 \pmod{10}$ (sebab $\varphi(10) = 4$). Sehingga kita mempunyai

$$7^{2023} = 7^{(4\times 505+3)} = (7^4)^{505} 7^3 = 3 \pmod{10}.$$

   Jadi, digit satuan dari $\mathbf{7^{2023}}$ adalah **3**

8. Tentukan angka satuan dari bilangan 1997^{2013}.

9. Tunjukkan bahwa $(an + b)^m \equiv b^m \pmod{n}$.

10. Dengan menggunakan konsep kekongruenan bilangan, tentukan angka satuan dari bilangan 1997^{1991}.

11. Tentukan angka satuan dari bilangan 7^{7^7}.

12. Tentukan dua angka terakhir dari bilangan 3^{2002}!

13. Tentukan sisa pembagian 33×263 oleh 31!

14. Tentukan sisa pembagian $3(53) + 27^2$ oleh 7!

15. Tentukan sisa pembagian 6^{1987} oleh 37.

16. Tunjukkan bahwa $32^{n+1} + 2^{n+2}$ habis dibagi 7 untuk semua bilangan asli n.

17. Tentukan semua bilangan bulat positif n sehingga $2n - 1$ habis dibagi oleh 7.

18. Tentukan semua nilai bilangan kuadrat sempurna modulo 13.

19. Selidiki apakah ada pasangan bulat (x, y) yang memenuhi $x^2 - 5y^2 = 2$.

20. Tentukan sisa pembagian 14^{30} oleh 11.

21. Berapakah sisa pembagian $6^{273} + 8^{273}$ oleh 49?

22. Misalkan $A = 3^{105} + 4^{105}$. Tunjukkan bahwa 7 membagi A.

23. Tunjukkan bahwa $5555^{2222} + 2222^{5555}$ habis dibagi 7.

24. Berapakah sisa pembagian $43^{43^{43}}$ oleh 100?

Bibliografi

[1] Subiono. ***Aljabar suatu Pondasi Matematika***, **ITS Press** (2022).