Aritmetika Modular

Haikal Isa

Daftar Isi

1 Modulo

Modulo adalah operasi biner untuk menentukan sisa pembagian dari dua bilangan. Contohnya

- $9 \bmod 7 = 2$ karena 9 dibagi 7 bersisa 2
- $81 \bmod 5 = 1$. 80 habis dibagi 5, namun 81 bersisa 1 saat dibagi 5.

Selain itu, modulo dapat dinyatakan dengan fungsi $\mathrm{mod}(x, y)$ yang artinya sisa pembagian saat x dibagi y, ataupun dinyatakan dengan hubungan kongruensi

$$a \equiv c \pmod b$$

Yang artinya adalah **c adalah sisa pembagian** saat **a dibagi dengan b**. Kita akan memakai modulo sebagai operasi biner ataupun hubungan kongruensi.

1.1 Sifat Aritmetika Modular

Berikut disajikan sifat dari aritmetika modular:

- $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $(a \times b) \bmod m = ((a \bmod m) \times (b \bmod m)) \bmod m$
- $a^n \bmod m = (a \bmod m)^n \bmod m$

2 Fungsi Euler

Fungsi euler $\phi(x)$ menyatakan jumlah bilangan yang koprima dengan x antara 1 sampai x. Misalkan x $difaktorisasiprimakan$. Begitulah, sehingga

$$x = \prod p_i^{k_i}$$

yang mana p_i adalah bilangan prima.

$$\phi(x) = \prod p_i^{k_i - 1}(p_i - 1)$$

2.1 Modulo invers

Untuk

$$a \bmod m = k$$

a^{-1} adalah modulo invers sehingga

$$aa^{-1} \bmod m = 1$$

Modulo invers dapat dihitung dengan

$$a^{-1} = a^{\phi(m)-1} \bmod m$$

Itupun kalau ada.
Ataupun dihitung 'manual' dengan menentukan nilai a^{-1} sehingga

$$aa^{-1} - 1 = km$$

dengan $k \in \mathbb{Z}$.

3 Teorema Sisa Cina (penting)

Diketahui suatu sistem kongruensi

$$\begin{gathered} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_n \bmod m_n \end{gathered}$$

Jika,

- $m_1, m_2, \ldots, m_n$ saling prima.
- $N = m_1 m_2 m_3 \ldots m_n$
- $X_i = N/m_i$
- $XX_i^{-1} \bmod m_i = 1$

maka,

$$x = \sum_{i=1}^{n} a_i X_i X_i^{-1}$$

Catatan. Sebagai tambahan, Jika terdapat 2 solusi v dan w, maka v dan w kongruen modulo dengan N, atau $v \equiv w \bmod N$

4 Teorema Lainnya

4.1 Teorema Wilson

Teorema Wilson menyatakan bahwa

$$(p-1)! \equiv -1 \pmod{p}$$

Untuk bilangan prima p.

4.2 Teorema Kecil Fermat dan Teorema Euler

Teorema Fermat menyatakan bahwa untuk bilangan prima p dan bilangan bulat a

$$a^p \equiv a \pmod{p}$$

Sementara itu, terdapat pula Teorema Euler. Teorema Euler merupakan generalisasi dari teorema kecil fermat yang menyatakan bahwa

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

dengan $\text{FPB}(a, n) = 1$

5 Contoh Soal

1. Tentukan hasil dari $(82 \cdot 88)$ mod 9

Solusi. Kita cukup menentukan

$$((82 \text{ mod } 9) \cdot (88 \text{ mod } 9)) \text{ mod } 9$$

Hasilnya menjadi $(1 \cdot 7) \bmod 9$.
Hasilnya adalah $\boxed{7}$

2. Tentukan digit terakhir dari 2023^{2022}

Solusi. Kelihatan mengerikan? Tidak juga.
Menentukan digit terakhir dari suatu bilangan artinya menentukan sisa bagi suatu bilangan dengan 10. Artinya kita akan menentukan hasil dari

$$2023^{2022} \bmod 10$$

Kita cukup menentukan

$$(2023 \bmod 10)^{2022} \bmod 10$$

Ini menjadi

$$3^{2022} \bmod 10$$

Kita akan ubah bentuknya. Karena $3^4 = 81$, dengan begitu

$$3^{4 \cdot 505 + 2} \bmod 10$$
$$\downarrow$$
$$81^{505} \cdot 3^3 \bmod 10$$
$$\downarrow$$
$$((81 \bmod 10)^{505} \cdot (9 \bmod 10)) \bmod 10$$
$$\downarrow$$
$$(1^{505} \cdot 9) \bmod 10$$

Hasilnya adalah $\boxed{9}$

(Hard) Tentukan hasil dari $12! \bmod 91$

Solusi. Anda dipersilahkan untuk menghitung

$$\left(\prod_{k=1}^{12} k \bmod 91\right) \bmod 91$$

Namun bukan ini yang diinginkan. Mari kita gunakan teorema wilson dan teorema sisa cina.

(a) Jelaslah bahwa $91 = 13 \cdot 7$, dan kita tahu bahwa

$$12! \bmod 7 = 0$$

$$12! \bmod 13 = -1$$

(b) Kita anggap solusi lainnya adalah x yang mana x memenuhi

$$x \equiv -1 \pmod{13}$$

$$x \equiv 0 \pmod{7}$$

(c) Diketahui

- $N = 91$
- $a_1 = -1$
- $X_1 = 7$
- $X_1^{-1} = 2$

(d) karena $a_2 = 0$, kita tak perlu cari X_2 dan X_2^{-1}

Akhirnya, solusinya adalah $(-1)(7)(2) \bmod 91 = -14$. Ini bisa juga ditulis sebagai $91 - 14 = \boxed{77}$

Catatan. Solusi untuk X_1^{-1} adalah 2 karena $(7 \cdot 2) \bmod 7 = 1$

Kerjakan soal berikut

1. Tentukan digit terakhir dari $1 + 2 + 3 + 4 + ... + 98 + 99$
2. Tentukan hasil dari $75^{6!} \bmod 4$
3. Diketahui $f(n) = n^2 - 3n + 5$, tentukan $f(10) \bmod f(9)$
4. Asep mempunyai banyak stroberi. Stroberi tersebut dibagikan kepada anak-anak (merata). Diketahui stroberi itu bersisa 3 saat dibagikan kepada 5 anak, bersisa 2 saat dibagikan kepada 3 anak, dan bersisa 6 saat dibagikan kepada 7 anak.

   Tentukan jumlah stroberi terkecil yang mungkin pada situasi tersebut.
5. Jika sekarang pukul 15:00, pukul berapa setelah 12345 jam?

Kunci Jawaban

1. 0
2. 1
3. 16
4. 83
5. 00:00

Pustaka

[1] Chinese remainder theorem. https://brilliant.org/wiki/chinese-remainder-theorem/. Diakses pada 15 Nov 2023.

[2] Euler's theorem. https://brilliant.org/wiki/eulers-theorem/. Diakses pada 15 Nov 2023.

[3] Fermat's little theorem. https://brilliant.org/wiki/fermats-little-theorem/. Diakses pada 15 Nov 2023.