Aritmatika Modular

$3 \bmod 2 =$

3: terbagi / Numerus

2: Pembagi

$$\begin{array}{r} 1 \\ 2\overline{)\,3} \\ \underline{2} \\ 1 \end{array}$$

Sisa $<$ Pembagi

- $a \bmod n \equiv k$

$k \in \mathbb{Z}^+ < N$

$a \bmod 5 \equiv k$

$k < 5 \rightarrow k = \{0, 1, 2, 3, 4\}$

$a \bmod n \equiv k$

$xn + k$ → Memenuhi a

$x = \{0, 1, 2, 3, 4, \ldots\}$

$$x \bmod 5 = 3$$

sisa bagi

$$x \equiv \underbrace{5k}_{\text{Bil kelipatan 5}} + \overset{\text{sisa bagi}}{3} \quad (k = \{0, 1, 2, 3, 4, 5, \ldots\})$$

Suatu bilangan bulat positif a dan a kelipatan n

$$(a + c) \bmod n \equiv c$$

$$a \mid n$$

$$x \bmod 5 \equiv 3$$

$$x = \underline{5k} + 3 \quad (k = \underline{0}, \underline{1}, 2, 3, 4, \ldots)$$

$$5 \cdot 0 + 3 \bmod 5 = 3$$

$$5 \cdot 1 + 3 \bmod 5 = 3$$

$$\vdots$$

$$1 \le x \le 2024$$

$$5k + 3 \le 2024$$

$$5k \le 2021$$

$$k \le \left\lfloor \frac{2021}{5} \right\rfloor$$

$$k = 404$$

ada $404 + 1$ x yang memenuhi

```
int n;
int ret = 0;
int k = 1;
while (k <= 100)
{
1)  if ((n + 2 * k) % 5 == 0){
        ret++;
        k++;
2)  }else if ((n + 5 * k) % 3 == 0){
3)      if ((n * k) % 4 != 0){
            ret++;
            k++;
        }else{
            k++;
        }
    }else{
        k++;
    }
}
n = 29, ret berapa?
```

40

if a {
  if b { }
}
if (a and b)

$k =$

$\to 29 + 2k \bmod 5 \equiv 0$ C1

$k\ 12$

$\to 29 + 5k \bmod 3 \equiv 0$ C2

$\to 29k \bmod 4 \; != 0$ C3

k

(if 1) true) and xor (if 2) and if 3) true)

inclusion exclusion

Berapa banyak k yg memenuhi

$C_1 \cup (C_2 \cap C_3)$

$$|A \cup B| = |A| + |B| - |A \cap B|$$

C_1 : $2g + 2k \bmod 5 \equiv 0 \rightarrow 2g + 2k \mid 5$

$$(a \overset{\times}{\pm} b \bmod n) \equiv (a \bmod n \overset{*}{\pm} b \bmod n) \bmod n$$

kelipatan 5 → digit terakhir 5 / 0

$2g + 2k \bmod 5 \equiv 0$

k_0

$\cancel{1}, \cancel{2}, \cancel{2}, 3 ✓, \cancel{4}, \cancel{5}, 6, \cancel{7},$

$k = \{3, 8, 13, 18, \ldots,$

$+5$

Kat pembagi

$35 \bmod 5 \equiv 0$

35

$2.3.1$

3.2

9

$U_n = a + (n-1)b$

$U_n = 3 + (n-1)5$

$= 3 + 5n - 5$

$= 5n - 2$

$K = \{3, 8, 13, 18, \ldots,$

$K \leq 100 \ldots ?$

$K = \{5n - 2\}$

$5n - 2 \leq 100 \Leftrightarrow 5n \leq 102$

$n = \left\lfloor \frac{102}{5} \right\rfloor$

$n = 20$

ada 20 K yang memenuhi $2a + 2K \mid 5$

$(0 \leq K \leq 100)$

$$x \bmod n \equiv 0$$

$$x = \{kn\} \quad k = (0, 1, 2, 3, \dots)$$

$$x = \{(k+\ell)n\}$$

C_2 : $2q + 5k \bmod 3 \equiv 0$ $+3$

$k_0 = 2$, $k = \{\overset{\frown}{2, 5}, 8, 11, \dots\}$

$$U_n = 2 + (n-1)3$$
$$= 3n - 3 + 2$$
$$= 3n - 1 \qquad (k \leq 100)$$

ada $\underline{33}$ k yg memenuhi C_2

$$3n - 1 \leq 100 \rightarrow 3n \leq 101 \rightarrow n = \left\lfloor \frac{101}{3} \right\rfloor$$

$$n = 33$$

$C_3 \subseteq C_2 \rightarrow K$

$C_2 \,\&\, C_3 \rightarrow \quad 29 + 5K \mid 3 \quad$ (K bukan kelipatan 4)

$^K C_2 = \{2, 5, \underline{8}, 11, 14, 17, \underline{20}, 23, \ldots\}$

$K \neg C_3 = \{8, \underbrace{20, 32}_{12}, 44, 56, 68, 80, 92\}$
$= C_2$

$^K C_3 \subseteq {}^K C_2$

$|C_2 \cap C_3| = {}^K C_2 - K \neg C_3$

$= 33 - 8$

$= 25$

$$|C_1 \cup C_2 \& C_3| = |C_1| + |C_2 \& C_3| - |C_1 \cap \underline{C_2} \& \underline{C_3}|$$

$\#C_1 = \{3, 8, 13, 18, \underline{23}, 28, 33, \underline{38}$

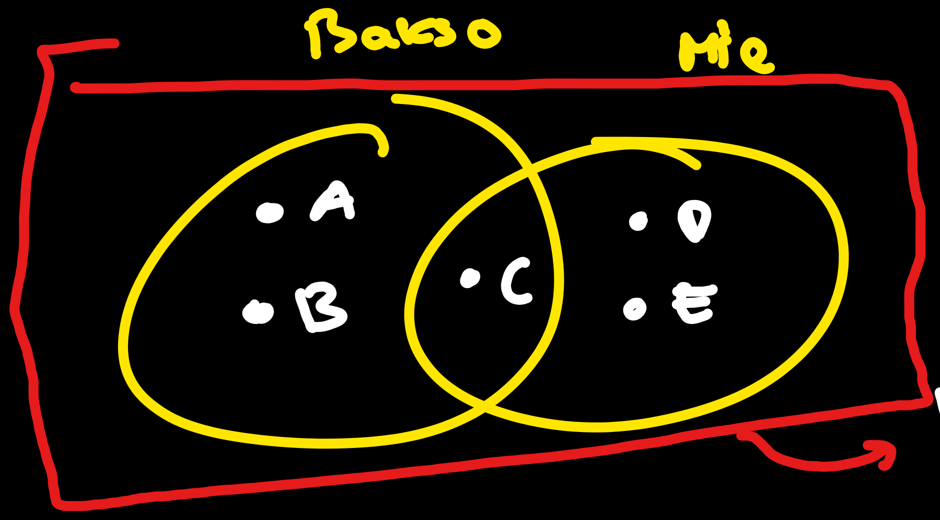
$\#C_2 \& C_3 = \{2, 5, 11, 14, 17, \underline{23}, \ldots, \underline{38}$

14 sbolen

$\#C_1 \& C_2 \& C_3 = \{23, \overset{+15}{38}, \overset{+15}{53}, \cancel{68}, 83, 98\}$

$= 5$

$$\text{ans} = 20 + 25 - 5 = \underline{\underline{40}}$$



Bakso = { A, B, C }

Mie = { C, D, E }

Bakso $\cup$ Mie = { A, B, C, D, E }

remove

Bakso + Mie = { A, B, C, $\cancel{C}$, D, E }

duplicate → intersect

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$a^b \bmod n \equiv (a \bmod n)^b \bmod n$$

$$a^b \bmod n \equiv a^{b \bmod \phi(n)} \bmod n$$

Digit satuan 2024^{2025}

$$2024^{2025} \bmod 10 \equiv 4^{2025} \bmod 10$$

$$\left(4^{\underline{2025}}\right) \bmod 10 \equiv$$

$$\left(4^{\underline{2022}} \cdot 4^{\underline{3}}\right) \bmod 10$$

$$\left(4^{2}\right)^{1011} \cdot 64 \bmod 10$$

$$(16)^{1011} \cdot 64 \bmod 10$$

$$\left(\left(6^{1011}\right) \cdot 4 \bmod 10\right)$$

$$(6 \cdot 4 \mod 10)$$

$$24 \mod 10 = \underline{\underline{4}}$$

$$4^{2025} \mod 10 =$$

$4^{1} \bmod 10 = 4$

$4^{2} \bmod 10 = 6$

$4^{3} \bmod 10 = 4$

$4^{4} \bmod 10 = 6$

$\vdots$

$4^{x} \bmod 10 = 6$ $\quad x12$

$4^{2025 \bmod 2} \bmod 10 \equiv$

$4^{1} \bmod 10 = 4$

$3^{2025} \bmod 10$

$3^{2025 \bmod 4} \bmod 10 =$

$\phi(10) = 4$

$\phi(n) = \text{Phi}(n) =$ banyaknya bil relatif prima dgn n

$Kp(10) = \{1, 3, 7, 9\}$ ada 4

$\phi(10) = 4$

$3^1 \bmod 10 = 3$

$3^2 \bmod 10 = 9$

$3^3 \bmod 10 = 7$

$3^4 \bmod 10 = 1$

$3^5 \bmod 10 = 3$

$3^6 \bmod 10 = 9$

$3^7 \bmod 10 = 7$

$3^8 \bmod 10 = 1$

$$\phi(100)$$

$$\phi(n) = n * \left(1 - \frac{1}{p_1}\right) * \left(1 - \frac{1}{p_2}\right) * (\ldots)$$

$$100 = (2 \cdot 5)^2 = \overset{p_1}{2} \cdot \overset{p_2}{5}$$

$$\phi(100) = 100 * \left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{5}\right)$$

$$= 100 * \frac{1}{2} * \frac{4}{5}$$

$$= \frac{40\cancel{0}}{1\cancel{0}} = 40$$

$$3^{2025} \bmod 100 = 3^{2025 \bmod \phi(100)} \bmod 100$$

$$= 3^{2025 \bmod 40} \bmod 100$$

$$3^{50} \bmod 100 = (3^5)^{10} \bmod 100$$

$$= 243^{10} \bmod 100$$

$$= 43^{10} \bmod 100$$

$$= (43^2)^5 \bmod 100$$

$$= (49^5 \bmod 100)$$

$$\ldots$$

$$\begin{array}{r} 43 \\ \times\ 43 \\ \hline 1\,2\,9 \\ 2 \end{array}$$

* Euler totient Function

$$a^b \bmod n \equiv a^{b \bmod \phi(n)} \bmod n$$

$FPB(a, n) = 1$

* Fermat Little theorm

$$a^b \bmod p \equiv a \qquad p \text{ is } \underline{\underline{\text{Prime}}}$$

$$a^p \bmod (p - 1) \equiv 1$$

$$\underset{a}{\underline{9999}}^{399999999} \bmod \underset{p}{\underline{3}} \equiv 9999$$

$$2024^{\underset{p}{\underline{17}}} \bmod \underset{p-1}{\underline{16}} \equiv 1$$

$$\gcd(4,6) = \gcd(4 \bmod 4,\ 6 \bmod 4)$$

$$= \gcd($$

$$6 \bmod 4 = \underbrace{2}_{\text{faktor}}$$

$$4 \bmod 2 = 0$$

$$6/2 = 6 - 2 - 2 - 2$$

$$5 \bmod 2 = 5 - 2 - 2 = 1$$

$$x/\mathrm{fpb}(x,y) \cdot y/\mathrm{fpb}(x,y)$$

$$\frac{6 : \text{FPB}(6,3)}{3 : \text{FPB}(6,3)} = \frac{2}{1}$$

6