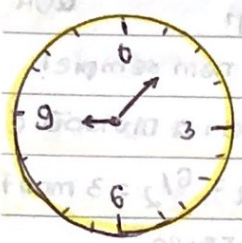
ARITMÉTICA MODULAR



a mod m

$\{0, \dots m-1\}$

↓

$x \bmod m = 0$

se $x = m$,,

↳ exemplo do relógio:

12 ≡ 0 no relógio, porque

12 mod 12 = 0, então o "universo" mod 12 vai de 0 até 11.

17 ≡ 5 (mod 12) → congruência

DEFINIÇÃO: Sejam a e m inteiros positivos. Nós denotamos a mod m como o resto quando a é dividido por m.

• 15 mod 12 = 3 mod 12 = 3

NOTAÇÃO DE CONGRUÊNCIA:

→ Dizemos que $a \equiv b \pmod m$ apenas se a mod m = b mod m. E é fácil ver que m divide a-b. Ou seja:

$$15 \equiv 3 \pmod{12}$$

ou: $7 \equiv 2 \pmod 5$

* Toda vez que $a < m$, a já é o resto.

↓

número menor que o módulo

TEOREMA: A congruência tem as seguintes propriedades:

i) se $a \equiv b \pmod m$, então $b \equiv a \pmod m$

ii) se $a \equiv b \pmod m$ e $b \equiv c \pmod m$, então $a \equiv c \pmod m$.

* $m \mid (a-b) \leftrightarrow a \equiv b \pmod m$

TEOREMA: Seja m um inteiro positivo. temos que:

i) $a+b \equiv (a \bmod m) + (b \bmod m) \pmod m$

ii) $a \cdot b \equiv (a \bmod m) \cdot (b \bmod m) \pmod m$

exemplo: calcule o resto de (2020 + 2021) por 7.

solução: $2020 + 2021 \equiv (2020 \bmod 7) + (2021 \bmod 7) \pmod 7$

→ $2020 \equiv 4 \pmod 7$ e sabemos que

$a \equiv b \pmod m \rightarrow a+k \equiv b+k \pmod m$. (1)

Então: $2020 \equiv 4 \pmod 7 \rightarrow 2021 \equiv 5 \pmod 7$

e $2020 + 2021 \equiv 4+5 \pmod 7$

$2020 + 2021 \equiv 9 \pmod 7$ e o resto = 2.

exemplo: calcule o resto (2020 + 2021 + 2023) por 7.

solução: sabemos (pelo ex. um) que:

$2020 + 2021 \equiv 9 \pmod 7$ → resto 2.

e pelo propriedade ① podemos fazer:

sendo $2020 \equiv 4 \pmod 7 \rightarrow$

$2023 \equiv 7 \pmod 7$

mas, $7 \bmod 7 = 0$, então ficaríamos com.

$$9 \pmod 7 + 7 \pmod 7 =$$
$$\downarrow \quad + \quad \downarrow = ②$$
$$2 \quad + \quad 0$$

exemplo: calcule o resto de 2020 · 2021 (mod 7):

$2020 \cdot 2021 \equiv 2020 \pmod 7 \cdot 2021 \pmod 7$

$2020 \cdot 2021 \equiv 4 \cdot 5 \pmod 7$

$2020 \cdot 2021 \equiv 20 \pmod 7 =$ C

/ /

Teorema: seja m um inteiro positivo.
se $a \equiv b \pmod m$ e $c \equiv d \pmod m$:

i) $a+c \equiv b+d \pmod m$

ii) $ac \equiv bd \pmod m$

algumas aplicações:

- funções hashing: $h(k) = k \pmod n$
- números pseudoramdômicos
- criptografia:
  cifra de deslocamento

exemplos e propriedades:

1) qual o resultado de quinta+sexta?

quinta: dia 4 > dia $4+5=9$

sexta: dia 5

$9 \bmod 7 = 2$ -> terça-feira

1.1) quinta · sexta?

$(4.5) \bmod 7$ -> $20 \bmod 7$ = sáb.

1.2) $(\text{sábado})^2$?

$(6)^2 \bmod 7$ -> $36 \bmod 7$ = seg

propriedades:

i) comutatividade

$(a+b) \bmod m = (b+a) \bmod m$

ii) associatividade

$((a+b)+c) \bmod m = (a+(b+c)) \bmod m$

iii) elemento neutro

- da soma: 0
- da ~~subtração~~ multiplicação: 1

Entretanto, como ficaria TER/QUA?

- $\frac{a}{c} \equiv \frac{b}{c} \pmod m$? ↳ nem sempre!

em alguns casos: a divisão é clara: $\text{sab}/\text{TER} = 6/2 = 3 \bmod 7$, que é quarta-feira.

mas $\text{TER}/\text{QUA} = 2/3$. e não trabalhamos com dias fracionados.

- como calcular?

por tentativa:

$\text{TER}/\text{QUA} = x \rightarrow x \cdot \text{QUA} = \text{TER}$

QUA = 3 e TER = 2.

$3 \cdot 3 = 9 \pmod 7 = 2$

x = quarta feira, pois:

$a \cdot x \equiv b \pmod 7$, $x \in z$.

- Generalizando a solução:

-> $a \cdot i \equiv 1 \pmod n$, i é um inverso de $a \pmod n$. $(\bar{a})$.

-> na aritmética usual:

$ax = b \rightarrow x = b \cdot 1/a$

-> na modular:

$3x \equiv 2 \pmod 7$

quem é $3 \cdot i \equiv (1) \pmod 7$? $= \bar{3}$

- o inverso de $3 \pmod 7$ é (5).

Podemos fazer:

$\bar{3} \cdot 3 x \equiv 2 \cdot \bar{3} \pmod 7$

$x \equiv 2 \cdot \bar{3} \pmod 7$

$x \equiv 10 \pmod 7$

Mas sabemos:

$10 \equiv 3 \pmod 7$

Então: $x = 3$

CONCLUSÕES:

i) NEM SEMPRE A CONGRUÊNCIA $ax \equiv b \pmod m$ TEM SOLUÇÃO!!!

ii) NEM SEMPRE PODEMOS DIVIDIR :O

iii) $\frac{x}{c} \equiv \frac{y}{c} \pmod m$, APENAS SE $mdc(c, m) = 1$, ISTO É: QUE SEJAM PRIMOS ENTRE SI!!

* LEMA: SE a, b E c SÃO INTEIROS POSITIVOS DE FORMA QUE a E $b \rightarrow$ SÃO PRIMOS ENTRE SI E $a \mid bc$ ENTÃO $a \mid c$.

↓

TEOREMA: SEJA m UM INTEIRO POSITIVO E SEJAM $a \in b$ E c INTEIROS: SE $ac \equiv bc \pmod m$ E c E m SÃO PRIMOS ENTRE SI, ENTÃO $a \equiv b \pmod m$.

OU SEJA:

$$\frac{a \cdot c}{c} \equiv \frac{b \cdot c}{c} \pmod m$$

$$a \equiv b \pmod m$$

APENAS SE c E m SÃO PRIMOS ENTRE SI ($mdc(c, m) = 1$).

* O MESMO NO EXEMPLO:

$$x \cdot a \equiv b \pmod m$$

$$\frac{x \cdot a}{a} \equiv \frac{b}{a} \pmod m$$

APENAS SE $mdc(a, m) = 1$

CALCULANDO CONGRUÊNCIAS:

① QUANDO ESTAMOS BUSCANDO O VALOR DE x EM $ax \equiv b \pmod m$, PRECISAMOS CALCULAR O INVERSO DE $a \pmod m$. COMO? POR QUE?

→ SEJA $\bar{a}$ UM INTEIRO DE MODO QUE

$$\bar{a} \cdot a \equiv 1 \pmod m$$

DIZEMOS QUE $\bar{a}$ É O INVERSO DE $a \pmod m$

COMO ENCONTRAR $\bar{a}$?

• COMO $mdc(a, m) = 1 \rightarrow$

$$\lambda \cdot a + T \cdot m = 1 \quad \text{(T. BEZOUT)}$$

ENTÃO: $\lambda \cdot a + T \cdot m \equiv 1 \pmod m$

$\lambda \cdot a \equiv 1 \pmod m$

↳ O COEFICIENTE DE a NA COMBINAÇÃO LINEAR É O INVERSO DE $a \pmod m$

* EXEMPLO: CALCULE O INVERSO DE:

$3 \bmod 7$

$a = 3$, $\bar{a} = ?$

$\bar{a} \cdot 3 \equiv 1 \bmod 7$

COMO SABEMOS QUE $mdc(3, 7) = 1$:

$$1 = \lambda \cdot 3 + 7 \cdot T$$

APLICANDO O ALGORITMO DE EUCLIDES, TEMOS:

$\lambda = -2$. DENTRO DO MOD 7 (0 A 6), TEMOS QUE $\bar{a} = 5$, OU $\bar{a} = -2 \pmod 7$

ENTÃO, PARA SOLUCIONARMOS $ax \equiv b \pmod m$:

→ ENCONTREMOS $\bar{a}$

→ COMO $\bar{a} \cdot a \equiv 1 \pmod m$:

→ $x \cdot \bar{a} \cdot a \equiv b \cdot \bar{a} \pmod m$

→ ENTÃO: $x \equiv b \cdot \bar{a} \pmod m$

CLASSES DE CONGRUÊNCIA

No universo mod m, todos os números podem ser reduzidos a

0 ... m-1

Por exemplo: MOD 4

quais os restos possíveis? 0, 1, 2, 3.

- isso significa que:

$i \equiv 0 \pmod 4$ ou

$i \equiv 1 \pmod 4$ ou

$i \equiv 2 \pmod 4$ ou

$i \equiv 3 \pmod 4$.

Temos 4 classes de congruência:

$\bar{0} = \{\ldots -8, -4, 0, 4, 8 \ldots\}$

↳ conjunto dos infinitos números que ao serem divididos por 4, dão resto 0. Analogamente:

$\bar{1} = \{\ldots -7, -3, 1, 5, 9 \ldots\}$

$\bar{2} = \{\ldots -6, -2, 2, 6, 10 \ldots\}$

$\bar{3} = \{\ldots -5, -1, 3, 7, 11 \ldots\}$

Os números que estão na mesma classe são congruentes dentro do mod 4.

Esses conjuntos são disjuntos e a união

$\bar{0} + \bar{1} + \bar{2} + \bar{3}$ = conjunto dos inteiros ($\mathbb{Z}$)

E podemos dizer que:

$\bar{0} = \bar{4} = \bar{8}$ etc. → $\mathbb{Z}_n = \mathbb{Z}_4$

E o conjunto das classes de c. do mod 4:

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ou $\{\bar{4}, \bar{5}, \bar{6}, \bar{7}\}$