/ /

UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 30 de Março de 2017

- ARITMÉTICA MODULAR:

→ É a aritmética dos fenômenos cíclicos.

↳ órbitas dos planetas

↳ horas do dia

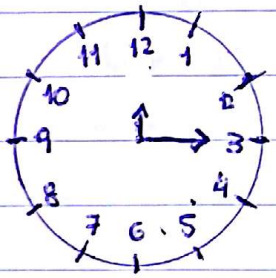
↳ etc.

PERGUNTA: Quando $22+12 = 10$?

↳ Nas horas do dia.

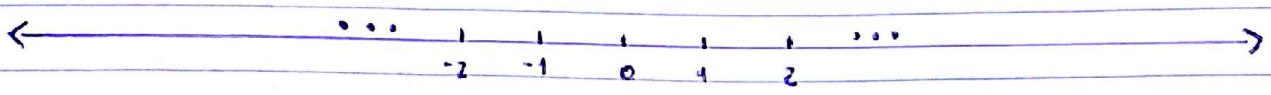
↳ Tenho um "ciclo" ou "período" ou "módulo" de 24 horas.

RELÓGIO:

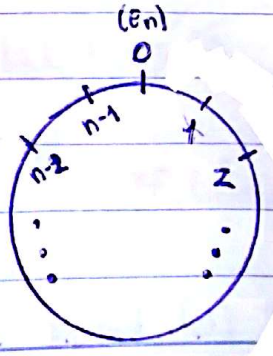


A aritmética modular usa uma ideia generalizada do relógio de horas.

Vamos considerar um ciclo ou período ou módulo de tamanho n.



(RETA DOS INTEIROS)

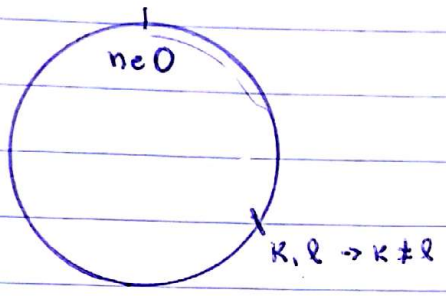


→ RELÓGIO COM N POSIÇÕES

"Enrolando" a reta dos inteiros nos dois sentidos, no relógio de n posições.

Ao fazer isso, diversos inteiros diferentes caem sobre a mesma posição do "relógio".

Inteiros diferentes que caem sobre uma mesma posição do "relógio" de n casas são chamados de congruentes módulo n.



NOTAÇÃO:

$k \equiv \ell \pmod{n}$

↳ k é congruente a ℓ módulo n.

Para que k e ℓ sejam congruentes, de k até ℓ é necessário que se percorra algum número t de voltas completas no "relógio"

↳ $\ell = k + t \cdot n$

$\Updownarrow$

$\ell - k = t \cdot n$

$\Updownarrow$

n divide $\ell - k$

ou

$\ell - k$ é multiplo de n.

DEFINIÇÃO:

$a \equiv b \pmod{n}$

$\Updownarrow$

$a-b$ é multiplo de n.

$\Updownarrow$

$a-b = n \cdot t$

$13 \equiv 7 \pmod{3}$

$(13-7 = 6$ é multiplo de $3)$

$14 \not\equiv 9 \pmod{3}$

$(14-9 = 5$ não é multiplo de $3)$

$13 \not\equiv 7 \pmod{4}$

$(13-7 = 6$ não é multiplo de $4)$

- RELAÇÕES DE EQUIVALÊNCIA:

→ Para estudar melhor as propriedades da congruência módulo n, precisamos estudar as relações de equivalência.

Seja x um conjunto. Uma relação $\sim$ entre um par de elementos de x é uma relação de equivalência se ela satizfaz as seguintes propriedades:

1) REFLEXIVIDADE: para $a \in x$, $a \sim a$.

2) SIMETRIA: para todo $a, b \in x$, se $a \sim b$, então $b \sim a$

3) Transitividade: para todo $a, b, c \in X$, se $a \sim b$ e $b \sim c$, então $a \sim c$

- Exemplos de Relação:

Conjunto $\mathbb{Z}$

- Relações: $=, \neq, <, >, \leq, \geq$

$2 \leq 3$, $3 \leq 3$, $7 \not\leq 3$

- Relação $(=)$

- Satisfaz reflexividade?

$a = a$? SIM!

- Satisfaz simetria?

Se $a = b$, então $b = a$? SIM!

- Satisfaz transitividade?

Se $a = b$ e $b = c$, então $a = c$? SIM!

$(=)$ é uma relação de equivalência

- Relação $(\neq)$

- Satisfaz reflexividade?

$a \neq a$? Não!

- Satisfaz simetria?

Se $a \neq b$, então $b \neq a$? SIM!

- Satisfaz transitividade?

Se $a \neq b$, e $b \neq c$, então $a \neq c$? NÃO

- Relação $<$

  - Reflexividade?

    $a < a$? Não!

  - Simetria?

    Se $a < b$, $b < a$? Não!

  - Transitividade?

    Se $a < b$ e $b < c$, então $a < c$? SIM!

- Relação $>$

  - Análogo à relação $<$

- Relação $\leq$

  - Reflexividade?

    $a \leq a$? SIM!

  - Simetria?

    Se $a \leq b$, então $b \leq a$? NÃO!

  - Transitividade?

    Se $a \leq b$ e $b \leq c$, então $a \leq c$? SIM!

Exemplo "bobo" de uma relação de equivalência:

Considerar, em uma piscina de bolas, como equivalentes as bolas de uma mesma cor.

Vamos mostrar que essa relação é de equivalência.

NOTAÇÃO: B → conjunto de bolas

$b, b', b'' \in B$

↳ bolas

$b \simeq b' \leftrightarrow$ b e b' tem a mesma cor.

- Reflexividade:

$b \simeq b'$?

b tem a mesma cor que b? SIM!

- Simetria:

Se $b \simeq b'$, então $b' \simeq b$? SIM!

- Transitividade:

Se $b \simeq b'$ e $b' \simeq b''$, então $b \simeq b''$? SIM!

Vamos mostrar que a relação de congruência módulo n, para um n pixado, é uma relação de equivalência

n FIXADO	1) REFLEXIVIDADE
$a, b \in \mathbb{Z}$	$a \equiv a \pmod n$? SIM!
$a \equiv b \pmod n$	$a \equiv a \pmod n \leftrightarrow a - a = n \cdot t$
⇕	⇕
$a - b$ é multiplo de n	$0 = n \cdot t$
⇕	⇕
$a - b = n \cdot t$	Verdade com $t = 0$.

2) SIMETRIA:

Se $a \equiv b \pmod n$, então $b \equiv a \pmod n$? SIM!

$a \equiv b \pmod n$

$\updownarrow$

$a - b = n \cdot t$

$\updownarrow$ ← MULTIPLICO POR (-1)

$b - a = -n \cdot t$

$\updownarrow$

$b - a = n \cdot (-t)$

$\updownarrow$

$b - a$ é multiplo de n

$\updownarrow$

$b \equiv a \pmod n$

3) TRANSITIVIDADE:

Se $a \equiv b \pmod n$ e $b \equiv c \pmod n$, então $a \equiv c \pmod n$?

$a \equiv b \pmod n \leftrightarrow a - b = n \cdot t$

$b \equiv c \pmod n \leftrightarrow \underline{b - c = n \cdot t'}$ SOMAR

$a - c = n \cdot t + n \cdot t'$

$\updownarrow$

$a - c \equiv n(t + t')$

$\updownarrow$

$a - c$ é multiplo de n

$\updownarrow$

$a \equiv c \pmod n$