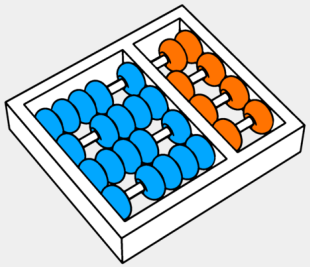
MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira



Instituto de computação

UNICAMP

30 de outubro de 2023

1. O conjunto dos inteiros módulos n via relações de equivalências

2. Funções

3. Perguntas, observações, comentários?

O conjunto dos inteiros módulos n via relações de equivalências

Operações modulares e relações de equivalências

Para qualquer inteiro $n \geq 2$, definimos a relação a seguir

$$\mathcal{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (a - b)\}$$

Como a relação depende de n, em vez de escrever apenas $a \equiv b$ quando a e b são equivalentes, escrevemos $a \equiv b \pmod{n}$. Também, $[a]_n$ em vez de $[a]_{\mathcal{R}}$.

Como mostrar que $\mathcal{R}$ é uma relação de equivalência? (reflexiva, simétrica e transitiva...)

Operações modulares e relações de equivalências

Para qualquer inteiro $n \geq 2$, definimos a relação a seguir

$$\mathcal{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (a - b)\}$$

Como a relação depende de n, em vez de escrever apenas $a \equiv b$ quando a e b são equivalentes, escrevemos $a \equiv b \pmod{n}$.
Também, $[a]_n$ em vez de $[a]_{\mathcal{R}}$.

Como mostrar que $\mathcal{R}$ é uma relação de equivalência? (reflexiva, simétrica e transitiva...)

Quais são as classes de equivalência?
Podemos provar o seguinte:

Teorema

Para todo natural $n \geq 2$ e inteiros a e b, temos que $a \equiv b \pmod{n}$ se, e somente se, o resto da divisão de a por n é igual ao resto da divisão de b por n.

As classes de equivalência módulo n

Vimos que dois inteiros são equivalentes se têm o mesmo resto da divisão por n.

Por exemplo, se $n = 3$,

- o resto pode ser $0, 1$ ou 2.
- todo inteiro é equivalente (módulo 3) ao 0, ao 1, ou ao 2.
- $[0]_3 = \{..., -6, -3, 0, 3, 6, ...\} = 3\mathbb{Z}$
- $[1]_3 = \{..., -5, -2, 1, 4, 7, ...\} = 3\mathbb{Z} + 1$
- $[2]_3 = \{..., -4, -1, 2, 5, 8, ...\} = 3\mathbb{Z} + 2$
- O quociente de $\mathbb{Z}$ por essa relação é denotado por $\mathbb{Z}_3$:

$$\mathbb{Z}_3 = \mathbb{Z}/\mathcal{R} = \{[0]_\mathcal{R}, [1]_\mathcal{R}, [2]_\mathcal{R}\}$$

As classes de equivalência módulo n

Vimos que dois inteiros são equivalentes se têm o mesmo resto da divisão por n.

Por exemplo, se $n = 3$,

- o resto pode ser $0, 1$ ou 2.
- todo inteiro é equivalente (módulo 3) ao 0, ao 1, ou ao 2.
- $[0]_3 = \{..., -6, -3, 0, 3, 6, ...\} = 3\mathbb{Z}$
- $[1]_3 = \{..., -5, -2, 1, 4, 7, ...\} = 3\mathbb{Z} + 1$
- $[2]_3 = \{..., -4, -1, 2, 5, 8, ...\} = 3\mathbb{Z} + 2$
- O quociente de $\mathbb{Z}$ por essa relação é denotado por $\mathbb{Z}_3$:

$$\mathbb{Z}_3 = \mathbb{Z}/\mathcal{R} = \{[0]_\mathcal{R}, [1]_\mathcal{R}, [2]_\mathcal{R}\}$$

Em geral,

$$\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$$

e esse conjunto é chamado de inteiros módulo n.

Operações para classes de equivalência módulo n

Assim como fizemos para as classes de equivalências representando frações, podemos definir operações para as classes de equivalências módulo n.

- Soma: $[a]_n + [b]_n = [a + b]_n$
- Produto: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Operações para classes de equivalência módulo n

Assim como fizemos para as classes de equivalências representando frações, podemos definir operações para as classes de equivalências módulo n.

- Soma: $[a]_n + [b]_n = [a + b]_n$
- Produto: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Mas precisamos verificar que estão bem definidas...

- Como $a + b$ e $a \cdot b$ são inteiros e há uma classe de equivalência para cada inteiro, então tanto a soma quanto o produto geram classes de equivalências válidas.
- Se $[a]_n = [x]_n$ e $[b]_n = [y]_n$, então
  - $[a]_n + [b]_n = [x]_n + [y]_n$?
  - $[a]_n \cdot [b]_n = [x]_n \cdot [y]_n$?

Exemplo de operações com classes de equivalência módulo n

Considere $n = 5$. Assim $\mathbb{Z}_5 = \{[0]_n, [1]_n, [2]_n, [3]_n, [4]_n\}$.
Então,

- $[2]_5 + [3]_5 = [5]_5 = [0]_5$
- $[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$
- $[4]_5 \cdot [2]_5 + [1]_5 = [8]_5 + [1]_5 = [9]_5 = [4]_5$

Para facilitar a notação, escrevemos apenas

- $2 + 3 \equiv 5 \equiv 0 \pmod 5$
- $2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$
- $4 \cdot 2 + 1 \equiv 8 + 1 \equiv 9 \equiv 4 \pmod 5$

Exemplo: equações módulares

1. Sabendo que $x \in \mathbb{Z}$ e que

$$2x + 15 = 31$$

   qual é o valor de $x \pmod 5$?

2. Encontre $x, y \in \mathbb{Z}_5$ tais que

$$\begin{cases} x + 2y \equiv 15^{30} \pmod 5 \\ 3x - 16^{999}y \equiv 97 \pmod 5 \end{cases}$$

Inverso multiplicativo módulo n

Multiplicação, soma e subtração são fáceis de definir para qualquer elemento de $\mathbb{Z}_n$.
Mas como podemos definir divisão?

Inverso multiplicativo módulo n

Multiplicação, soma e subtração são fáceis de definir para qualquer elemento de $\mathbb{Z}_n$.
Mas como podemos definir divisão?
Para $a \in \mathbb{Z}_n$, queremos $b \in \mathbb{Z}_n$ tal que

$$a \cdot b \equiv 1 \pmod{n}$$

Escrevemos então b como a^{-1} e o chamamos inverso multiplicativo.

Inverso multiplicativo módulo n

Multiplicação, soma e subtração são fáceis de definir para qualquer elemento de $\mathbb{Z}_n$.
Mas como podemos definir divisão?
Para $a \in \mathbb{Z}_n$, queremos $b \in \mathbb{Z}_n$ tal que

$$a \cdot b \equiv 1 \pmod{n}$$

Escrevemos então b como a^{-1} e o chamamos inverso multiplicativo.

Teorema

Seja n um inteiro maior que ou igual a 2. Para todo $x \in \mathbb{Z}$,

$$\exists\, x^{-1} \in \mathbb{Z} : x \cdot x^{-1} \equiv 1 \pmod{n} \Leftrightarrow \texttt{mdc}(x, n) = 1$$

Funções

Totalidade e funcionalidade

Dizemos que uma relação $\mathcal{R} \subseteq X \times Y$ é

- total, se $\forall x \in X \ (\exists y \in Y \ (x, y) \in \mathcal{R})$;
- funcional, se $\forall x \in X \ ((x, y) \in \mathcal{R} \wedge (x, y') \in \mathcal{R}) \Rightarrow y = y'$.

Note que ser total significa $\mathrm{dom}(\mathcal{R}) = X$.

Totalidade e funcionalidade

Dizemos que uma relação $\mathcal{R} \subseteq X \times Y$ é

- total, se $\forall x \in X\ (\exists y \in Y\ (x, y) \in \mathcal{R})$;
- funcional, se $\forall x \in X\ ((x, y) \in \mathcal{R} \wedge (x, y') \in \mathcal{R}) \Rightarrow y = y'$.

Note que ser total significa $\mathrm{dom}(\mathcal{R}) = X$.

Uma função de X para Y é uma relação total e funcional.

Note que colocando essas duas propriedades juntas, temos

$$\forall x \in X(\exists! y \in Y\ ((x, y) \in f))$$

Totalidade e funcionalidade

Dizemos que uma relação $\mathcal{R} \subseteq X \times Y$ é

- total, se $\forall x \in X\ (\exists y \in Y\ (x, y) \in \mathcal{R})$;
- funcional, se $\forall x \in X\ ((x, y) \in \mathcal{R} \wedge (x, y') \in \mathcal{R}) \Rightarrow y = y'$.

Note que ser total significa $\mathrm{dom}(\mathcal{R}) = X$.

Uma função de X para Y é uma relação total e funcional.

Note que colocando essas duas propriedades juntas, temos

$$\forall x \in X(\exists! y \in Y\ ((x, y) \in f))$$

Tradicionalmente, em vez de $(x, y) \in f$, escrevemos $f(x) = y$, já que há apenas um y para cada x.

Exemplos

Considere $X = \{0, 1, 2, 3\}$ e $Y = \{0, \pi, 1/\pi\}$.
Então $f = \{(0, \pi), (1, \pi), (2, \pi), (3, \pi)\} \subset X \times Y$ é a função constante $f(x) = \pi$.

Exemplos

Considere $X = \{0, 1, 2, 3\}$ e $Y = \{0, \pi, 1/\pi\}$.
Então $f = \{(0, \pi), (1, \pi), (2, \pi), (3, \pi)\} \subset X \times Y$ é a função constante $f(x) = \pi$.

E $f = \{(0, 0), (1, \pi), (3, 1/\pi)\} \subset X \times Y$, é uma função?

Exemplos

Considere $X = \{0, 1, 2, 3\}$ e $Y = \{0, \pi, 1/\pi\}$.
Então $f = \{(0, \pi), (1, \pi), (2, \pi), (3, \pi)\} \subset X \times Y$ é a função constante $f(x) = \pi$.

E $f = \{(0, 0), (1, \pi), (3, 1/\pi)\} \subset X \times Y$, é uma função?

E $f = \{(0, 0), (1, \pi), (2, \pi), (3, 1/\pi), (0, \pi)\} \subset X \times Y$, é uma função?

Composição de funções

Sabemos que nem sempre a composição de relações preserva as propriedades das relações.
Por exemplo, a composição de duas relações de ordem pode não ser uma relação de ordem.
E quanto às funções?

Teorema

Considere duas funções $f \subseteq X \times Y$ e $g \subseteq Y \times Z$. A composição $g \circ f$ é uma função de X para Z.

Inversa de uma função

Lembre-se que uma função é uma relação, então, a inversa de uma função é simplesmente a relação inversa, conforme definição vista anteriormente:

$$f \subseteq X \times Y \Rightarrow f^{-1} = \{(y, x) \in Y \times X : (x, y) \in f\}$$

Inversa de uma função

Lembre-se que uma função é uma relação, então, a inversa de uma função é simplesmente a relação inversa, conforme definição vista anteriormente:

$$f \subseteq X \times Y \Rightarrow f^{-1} = \{(y, x) \in Y \times X : (x, y) \in f\}$$

Atenção: a inversa de uma função não necessariamente é uma função! Por exemplo:

$$f = \{(x, x^2) : x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$$

é uma função (por que?). Mas a inversa é

$$f^{-1} = \{(x^2, x) : x \in \mathbb{Z}\}$$

Então, $(1, 1), (1, -1) \in f$, ou seja, f^{-1} não é funcional.
Além disso, ela não é total (por exemplo, $f^{-1}(2)$ não está definido).

Função injetora e sobrejetora

Vimos que a inversa de f não é uma função. Mas por qual razão? Primeiramente, f^{-1} não é funcional. Por que isso ocorre?

- f leva dois pontos diferentes na mesma imagem.
- Por exemplo, $f(2) = f(-2) = 4$.
- Se $(x, y), (x', y) \in f$, então, temos (y, x) e (y, x') em f^{-1}.
- Isso nos leva a seguinte definição:

Função injetora e sobrejetora

Vimos que a inversa de f não é uma função. Mas por qual razão? Primeiramente, f^{-1} não é funcional. Por que isso ocorre?

- f leva dois pontos diferentes na mesma imagem.
- Por exemplo, $f(2) = f(-2) = 4$.
- Se $(x, y), (x', y) \in f$, então, temos (y, x) e (y, x') em f^{-1}.
- Isso nos leva a seguinte definição:

Definição

Uma função $f \subseteq X \times Y$ é *injetora* se

$$f(x) = f(x') \Rightarrow x = x'$$

Função sobrejetora

Além disso, no nosso exemplo, f^{-1} não era total. Por que isso ocorre?

- Existem elementos de Y que não pertencem à imagem de f.
- Por exemplo, não há nenhum $x \in \mathbb{Z}$ para o qual $f(x) = 2$.
- Se $(x, y) \notin f$, então, $(y, x) \notin f^{-1}$.
- Isso nos leva a seguinte definição:

Definição

Uma função $f \subseteq X \times Y$ é *sobrejetora* se

$$\forall y \in Y \; \exists x \in X \; f(x) = y$$

(Ou seja, $\text{img}(f) = Y$).

Bijeção

Definição

Uma função $f \subseteq X \times Y$ é *bijetora* se for injetora e sobrejetora.

Bijeções e funções invertíveis na verdade são as mesmas funções.

Teorema

Uma função $f \subseteq X \times Y$ é bijetora se, e somente se, f^{-1} é uma função.

Exemplos de funções tipicamente usadas em ciência da computação

- Função piso: $f : \mathbb{R} \to \mathbb{Z}$ definida como $f(x) = \max\{z \in \mathbb{Z} : z \leq x\}$.
  - Notação: $\lfloor x \rfloor$
  - $x - 1 < \lfloor x \rfloor \leq x$
  - $\forall x \in \mathbb{R}\ \exists \epsilon \in [0, 1[\ (x = \lfloor x \rfloor + \epsilon)$
- Função teto: $f : \mathbb{R} \to \mathbb{Z}$ definida como $f(x) = \min\{z \in \mathbb{Z} : x \leq z\}$.
  - Notação: $\lceil x \rceil$
  - $x \leq \lceil x \rceil < x + 1$
  - $\forall x \in \mathbb{R}\ \exists \epsilon \in [0, 1[\ (x = \lceil x \rceil - \epsilon)$

Podemos provar que

$$\lfloor -x \rfloor = -\lceil x \rceil$$

Perguntas, observações, comentários?