Gabarito Lista 4

4 de dezembro de 2023

Ex.1

Dadas as equivalências $a \equiv x \pmod{n}$ e $b \equiv y \pmod{n}$, isso significa que:

$$n|(a-x) \quad \text{e} \quad n|(b-y)$$

Isso implica que existem inteiros k e l tais que:

$$a - x = kn \quad \text{e} \quad b - y = ln$$

Se somarmos essas duas equações, obtemos:

$$(a-x) + (b-y) = kn + ln$$

Simplificando, temos:

$$(a+b) - (x+y) = (k+l)n$$

Isso mostra que n divide a diferença $(a+b) - (x+y)$, o que por definição significa que:

$$a + b \equiv x + y \pmod{n}$$

Portanto, a classe de equivalência da soma, $[a+b]_n$, é a mesma que $[x+y]_n$. Isso prova que a operação de soma em $\mathbb{Z}_n$ é bem definida, independente dos representantes escolhidos para cada classe de equivalência.

Ex.2

Ex.2 (a)

Para provar que $7^n - 5^n$ é par para todo $n \in \mathbb{N}$, vamos usar indução matemática e propriedades das operações modulares. Um número é par se, e somente se, ele é divisível por 2. Isso significa que para provar que $7^n - 5^n$ é par, precisamos mostrar que $7^n - 5^n$ é divisível por 2, ou em termos de operações modulares, que $7^n - 5^n \equiv 0 \pmod{2}$.

Passo Base da Indução - Para $n = 1$:

$$7^1 - 5^1 = 7 - 5 = 2$$

$$2 \equiv 0 \pmod{2}$$

Portanto, a afirmação é verdadeira para $n = 1$.

Passo de Indução - Suponha que a afirmação é verdadeira para um certo $k \in \mathbb{N}$, ou seja, $7^k - 5^k$ é par. Precisamos mostrar que $7^{k+1} - 5^{k+1}$ também é par.

Prova do Passo de Indução:

$$7^{k+1} - 5^{k+1} = 7 \cdot 7^k - 5 \cdot 5^k$$
$$= (7 \cdot 7^k - 7 \cdot 5^k) + (7 \cdot 5^k - 5 \cdot 5^k)$$
$$= 7(7^k - 5^k) + 5^k(7 - 5)$$

Sabemos que $7^k - 5^k$ é par pela hipótese de indução, então podemos escrevê-lo como $2m$ para algum $m \in \mathbb{N}$. Além disso, $7 - 5 = 2$, que é claramente par. Portanto:

$$7(7^k - 5^k) + 5^k(7 - 5) = 7 \cdot 2m + 5^k \cdot 2$$
$$= 2(7m + 5^k)$$

Como $2(7m + 5^k)$ é claramente divisível por 2, $7^{k+1} - 5^{k+1}$ é par.

Assim, por indução matemática, provamos que $7^n - 5^n$ é par para todo $n \in \mathbb{N}$.

Ex.2 (b)

Para provar que 6 divide $n^3 - n$ para todo $n \in \mathbb{N}$, ou em termos de operações modulares, $n^3 - n \equiv 0 \pmod 6$, vamos utilizar o fato de que um número é divisível por 6 se e somente se é divisível por 2 e por 3 simultaneamente.

Divisibilidade por 2: Para provar que $n^3 - n$ é divisível por 2, observamos que:

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$$

Neste produto, $n(n-1)(n+1)$, temos três números consecutivos. Em qualquer trio de números consecutivos, pelo menos um deles é par. Portanto, $n^3 - n$ é divisível por 2.

Divisibilidade por 3: Para provar que $n^3 - n$ é divisível por 3, novamente olhamos para a expressão:

$$n^3 - n = n(n - 1)(n + 1)$$

Novamente, em qualquer trio de números consecutivos $(n - 1,\ n,\ n + 1)$, pelo menos um deles é divisível por 3. Isso se deve ao fato de que os números são representações de $3k$, $3k + 1$, e $3k + 2$ para algum inteiro k. Portanto, $n^3 - n$ é divisível por 3.

Como $n^3 - n$ é divisível tanto por 2 quanto por 3, segue que $n^3 - n$ é divisível por 6. Assim, para todo $n \in \mathbb{N}$, $6|(n^3 - n)$, ou em termos de operações modulares, $n^3 - n \equiv 0 \pmod 6$.

Ex.3

Para encontrar o inverso multiplicativo de 17 módulo 72, utilizamos o algoritmo de Euclides estendido, que nos permite calcular, além do máximo divisor comum de dois números, os coeficientes que satisfazem a identidade de Bézout: $au + bv = \text{mdc}(a, b) = d$.

No nosso caso, queremos encontrar x tal que $17x \equiv 1 \pmod{72}$. Aplicando o algoritmo, encontramos que o mdc entre 17 e 72 é 1, e o coeficiente x correspondente é 17. Portanto,

17×17 dá um produto de 289, que deixa um resto de 1 quando dividido por 72. Assim, 17 é o inverso multiplicativo de 17 módulo 72.

Inicializamos as variáveis com $a = 17$ e $b = 72$ e calculamos o MDC de a e b através da recursão até chegar na última linha, quando $a = 1$ e $b = 0$, onde temos o MDC de 17 e 72, que é 1. Então voltamos passo a passo atualizando os coeficientes u e v, de acordo com a saída do algoritmo: $return(d, v, u - qv)$.

Passo	a	b	q	r	d	u	v
1	72	17	4	4	1	-4	17
2	17	4	4	1	1	1	-4
3	4	1	4	0	1	0	1
4	1	0	$-$	$-$	1	1	0

Assim encontramos os coeficientes $u = -4$ e $v = 17$, que nos dão a relação de Bézout

$$-4 \cdot 72 + 17 \cdot 17 = 1.$$

Assim, $v = 17$ é o inverso multiplicativo de 17 módulo 72.

Ex.4

Para provar que a equação $14x^2 + 15y^2 = 7^{2000}$ não tem solução inteira (x, y), vamos usar propriedades de congruências modulares. Vamos considerar a equação módulo 7. Se a equação tem uma solução inteira, então a congruência

$$14x^2 + 15y^2 \equiv 7^{2000} \pmod 7$$

também deve ter uma solução.

Agora, aplicamos algumas propriedades:

- Sabemos que $7^{2000} \equiv 0 \pmod 7$, pois qualquer potência de 7 é divisível por 7.
- Substituindo na equação original, obtemos:

$$14x^2 + 15y^2 \equiv 0 \pmod 7$$

- Observe que $14x^2$ é claramente divisível por 7 para qualquer inteiro x, e portanto, $14x^2 \equiv 0 \pmod 7$.
- Agora, considere $15y^2 \pmod 7$. Sabemos que $15 \equiv 1 \pmod 7$, então $15y^2 \equiv y^2 \pmod 7$.

Assim, a equação se reduz a:

$$y^2 \equiv 0 \pmod 7$$

A única maneira de y^2 ser congruente a 0 módulo 7 é se y for divisível por 7. Portanto, y^2 deve ser uma potência de 7. No entanto, isso entra em contradição com a equação original $14x^2 + 15y^2 = 7^{2000}$, pois a soma de um múltiplo de 7 (que é $14x^2$) e uma potência de 7 (que é $15y^2$, ou mais precisamente y^2) não pode ser igual a uma potência par de 7 (ou seja, 7^{2000}).

Portanto, concluímos que não existe um par de inteiros (x, y) que satisfaça a equação $14x^2 + 15y^2 = 7^{2000}$.

1 Ex.5

Para provar que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer número natural n, vamos utilizar congruências. O número 133 pode ser fatorado como $133 = 7 \times 19$. Portanto, para mostrar que $11^{n+2} + 12^{2n+1}$ é divisível por 133, precisamos provar que é divisível por 7 e por 19, pois 7 e 19 são primos entre si.

Divisibilidade por 7

- Observe que $11 \equiv 4 \pmod 7$ e $12 \equiv 5 \pmod 7$.
- Então, $11^{n+2} \equiv 4^{n+2} \pmod 7$ e $12^{2n+1} \equiv 5^{2n+1} \pmod 7$.
- Sabemos que $4^2 \equiv 16 \equiv 2 \pmod 7$, então $4^{n+2} \equiv 2^{n+1} \pmod 7$.
- E $5^2 \equiv 25 \equiv 4 \pmod 7$, então $5^{2n+1} \equiv 4^n \cdot 5 \equiv 2^n \cdot (-2) \pmod 7$ porque $4 \equiv -3 \pmod 7$ e $5 \equiv -2 \pmod 7$.
- Portanto, $11^{n+2} + 12^{2n+1} \equiv 2^{n+1} - 2^{n+1} \equiv 0 \pmod 7$, mostrando que é divisível por 7.

Divisibilidade por 19

- Observe que $11 \equiv -8 \pmod{19}$ e $12 \equiv -7 \pmod{19}$.
- Então, $11^{n+2} \equiv (-8)^{n+2} \pmod{19}$ e $12^{2n+1} \equiv (-7)^{2n+1} \pmod{19}$.
- Como $(-8)^2 = 64 \equiv 7 \pmod{19}$, $11^{n+2} \equiv 7^{n+1} \pmod{19}$.
- E $(-7)^2 = 49 \equiv 11 \pmod{19}$, então $12^{2n+1} \equiv 11^n \cdot (-7) \pmod{19}$.
- Agora, $11^n \cdot (-7) \equiv (-1)^n \cdot 7^{n+1} \pmod{19}$ porque $11 \equiv -1 \pmod{19}$.
- Portanto, $11^{n+2} + 12^{2n+1} \equiv 7^{n+1} - 7^{n+1} \equiv 0 \pmod{19}$, mostrando que é divisível por 19.

Como $11^{n+2} + 12^{2n+1}$ é divisível tanto por 7 quanto por 19, e 7 e 19 são primos entre si, segue que $11^{n+2} + 12^{2n+1}$ é divisível por 133. Logo, a afirmação é verdadeira para qualquer número natural n.

2 Ex.6

Definição: A composição de g e f, denotada por $g \circ f$, é definida por $(g \circ f)(x) = g(f(x))$ para todo $x \in X$.

Definição: Uma função $h : A \to B$ é dita injetora se, para todos $a_1, a_2 \in A$, $h(a_1) = h(a_2)$ implica que $a_1 = a_2$.

Portanto, sejam $f : X \to Y$ e $g : Y \to Z$ duas funções injetoras. Para provar que $g \circ f$ é injetora, precisamos mostrar que se $g(f(x_1)) = g(f(x_2))$, então $x_1 = x_2$ para quaisquer $x_1, x_2 \in X$.

Dado que f e g são injetoras, temos que:

- Se $f(x_1) = f(x_2)$, então $x_1 = x_2$.
- Se $g(y_1) = g(y_2)$, então $y_1 = y_2$.

Suponha que $(g \circ f)(x_1) = (g \circ f)(x_2)$, ou seja, $g(f(x_1)) = g(f(x_2))$. Como g é injetora, de $g(f(x_1)) = g(f(x_2))$ segue que $f(x_1) = f(x_2)$. Como f é injetora e $f(x_1) = f(x_2)$, então $x_1 = x_2$.

Portanto, se $(g \circ f)(x_1) = (g \circ f)(x_2)$ implica que $x_1 = x_2$, então $g \circ f$ é uma função injetora.

3 Ex.7

3.1 Ex.7 (a)

Para determinar a imagem de $f(x) = \frac{x}{3+x}$ e verificar se f é sobrejetora, precisamos analisar os valores que $f(x)$ pode assumir quando x varia por todo o seu domínio, que é $\mathbb{R} \setminus \{-3\}$. Uma boa abordagem é fazer uma troca de variáveis. Vamos definir $y = f(x)$ e resolver para x em termos de y.

$$y = \frac{x}{3+x}$$

Multiplicamos ambos os lados por $3 + x$ para remover o denominador:

$$y(3+x) = x$$

Expandido, temos:

$$3y + xy = x$$

Isolando x, obtemos:

$$xy - x = -3y \implies x(y-1) = -3y \implies x = \frac{-3y}{y-1}$$

Agora, vamos analisar as restrições para y:

Restrição no denominador: Como $y - 1$ está no denominador, y não pode ser 1. Caso contrário, teríamos divisão por zero.

Limites de y quando x se aproxima de -3: Quando x se aproxima de -3, o valor de $f(x)$ se aproxima de um limite. Vamos calcular esses limites.

- Quando x se aproxima de -3 pela direita ($x \to -3^+$), $f(x) \to -\infty$.
- Quando x se aproxima de -3 pela esquerda ($x \to -3^-$), $f(x) \to +\infty$.

Valores de y para grandes valores de $|x|$: Quando $|x|$ é muito grande (tanto positivo quanto negativo), $f(x)$ se aproxima de 1 porque o 3 no denominador se torna insignificante em comparação com x.

Dado isso, podemos concluir que a imagem de f é $\mathbb{R} \setminus \{1\}$, pois $f(x)$ pode assumir qualquer valor real exceto 1.

Quanto à sobrejetividade, uma função é sobrejetora se cada elemento do codomínio é mapeado por algum elemento do domínio. Como $f(x)$ não pode assumir o valor 1, ela não é sobrejetora se considerarmos o codomínio como sendo todo o conjunto dos números reais.

3.2 Ex.7 (b)

Para determinar se a função $f(x) = \frac{x}{3+x}$, com domínio $\mathbb{R} \setminus \{-3\}$, é injetora, precisamos verificar se cada elemento do codomínio é mapeado por no máximo um elemento do domínio. Em outras palavras, se $f(a) = f(b)$, então deve ser verdade que $a = b$. Vamos provar isso usando a definição de injetividade:

Suponha que $f(a) = f(b)$ para dois números reais a e b, ambos diferentes de -3. Então:

$$\frac{a}{3+a} = \frac{b}{3+b}$$

Multiplicamos ambos os lados pelo denominador comum $(3+a)(3+b)$ para eliminar as frações:

$$a(3+b) = b(3+a)$$

Expandido, obtemos:

$$3a + ab = 3b + ab$$

Subtraindo ab de ambos os lados:

$$3a = 3b$$

Dividindo ambos os lados por 3, obtemos:

$$a = b$$

Portanto, se $f(a) = f(b)$, então $a = b$, o que prova que a função f é injetora.

4 Ex.8

4.1 Ex.8 (a)

Considere $x = 0.5$ e $y = 0.5$. Neste caso:

- $\lceil x \rceil = \lceil 0.5 \rceil = 1$
- $\lceil x \rceil + y = 1 + 0.5 = 1.5$
- $\lceil x + y \rceil = \lceil 0.5 + 0.5 \rceil = \lceil 1 \rceil = 1$

Vemos que $\lceil x + y \rceil \neq \lceil x \rceil + y$, então a primeira parte da afirmação é falsa.

- $\lfloor x \rfloor = \lfloor 0.5 \rfloor = 0$
- $\lfloor x \rfloor + y = 0 + 0.5 = 0.5$
- $\lfloor x + y \rfloor = \lfloor 0.5 + 0.5 \rfloor = \lfloor 1 \rfloor = 1$

Assim, $\lfloor x + y \rfloor \neq \lfloor x \rfloor + y$, o que prova que a segunda parte da afirmação também é falsa.

4.2 Ex.8 (b)

1. Prova de $\lceil x+y \rceil = \lceil x \rceil + y$

Hipótese: Seja $y \in \mathbb{Z}$ e $x \in \mathbb{R}$. Assuma que $\lceil x \rceil = n$, o que implica, pela propriedade fornecida, que $x \leq n < x+1$.

Objetivo: Mostrar que $\lceil x+y \rceil = n+y$.

De $x \leq n < x+1$, somamos y a cada parte da desigualdade, obtendo $x+y \leq n+y < x+y+1$. Isso implica que $n+y$ é o menor inteiro tal que $x+y \leq n+y$. Por definição, isso significa que $\lceil x+y \rceil = n+y$. Mas como $\lceil x \rceil = n$, então temos que $\lceil x+y \rceil = \lceil x \rceil + y$.

2. Prova de $\lfloor x+y \rfloor = \lfloor x \rfloor + y$

Hipótese: Seja $y \in \mathbb{Z}$ e $x \in \mathbb{R}$. Assuma que $\lfloor x \rfloor = m$, o que implica, pela propriedade fornecida, que $m \leq x < m+1$.

Objetivo: Mostrar que $\lfloor x+y \rfloor = m+y$.

De $m \leq x < m+1$, somamos y a cada parte da desigualdade, obtendo $m+y \leq x+y < m+y+1$. Isso implica que $m+y$ é o maior inteiro tal que $m+y \leq x+y$. Por definição, isso significa que $\lfloor x+y \rfloor = m+y$. Mas como $\lfloor x \rfloor = m$, então temos que $\lfloor x+y \rfloor = \lfloor x \rfloor + y$.

5 Ex.9

Para determinar se a relação $\mathcal{R}_\varepsilon$ é uma relação de equivalência, precisamos verificar se ela satisfaz as três propriedades que definem uma relação de equivalência:

- **Reflexividade** Para todo $x \in \mathbb{R}$, $(x,x) \in \mathcal{R}_\varepsilon$.
- **Simetria** Para todo $x, y \in \mathbb{R}$, se $(x,y) \in \mathcal{R}_\varepsilon$, então $(y,x) \in \mathcal{R}_\varepsilon$.
- **Transitividade** Para todo $x, y, z \in \mathbb{R}$, se $(x,y) \in \mathcal{R}_\varepsilon$ e $(y,z) \in \mathcal{R}_\varepsilon$, então $(x,z) \in \mathcal{R}_\varepsilon$.

Reflexividade: Para qualquer número real x, $\lfloor x/\varepsilon \rfloor$ é igual a si mesmo. Portanto, para todo $x \in \mathbb{R}$, temos que $\lfloor x/\varepsilon \rfloor = \lfloor x/\varepsilon \rfloor$, o que implica que $(x,x) \in \mathcal{R}_\varepsilon$. Isso mostra que a relação $\mathcal{R}_\varepsilon$ é reflexiva.

Simetria: Se $(x,y) \in \mathcal{R}_\varepsilon$, isso significa que $\lfloor x/\varepsilon \rfloor = \lfloor y/\varepsilon \rfloor$. Uma vez que a igualdade é simétrica, temos também $\lfloor y/\varepsilon \rfloor = \lfloor x/\varepsilon \rfloor$, e portanto, $(y,x) \in \mathcal{R}_\varepsilon$. Assim, a relação $\mathcal{R}_\varepsilon$ é simétrica.

Transitividade: Suponha que $(x,y) \in \mathcal{R}_\varepsilon$ e $(y,z) \in \mathcal{R}_\varepsilon$. Isso significa que $\lfloor x/\varepsilon \rfloor = \lfloor y/\varepsilon \rfloor$ e $\lfloor y/\varepsilon \rfloor = \lfloor z/\varepsilon \rfloor$. Como a igualdade é transitiva, podemos concluir que $\lfloor x/\varepsilon \rfloor = \lfloor z/\varepsilon \rfloor$, e portanto, $(x,z) \in \mathcal{R}_\varepsilon$. Isso mostra que a relação $\mathcal{R}_\varepsilon$ é transitiva.

Como a relação $\mathcal{R}_\varepsilon$ satisfaz reflexividade, simetria e transitividade, podemos concluir que é uma relação de equivalência.

As classes de equivalência para a relação $\mathcal{R}_\varepsilon$ são determinadas pelos elementos que compartilham o mesmo valor para $\lfloor x/\varepsilon \rfloor$. Cada classe de equivalência pode ser descrita como um

intervalo da forma:

$$[x]_\varepsilon = \{y \in \mathbb{R} \mid \lfloor y/\varepsilon \rfloor = \lfloor x/\varepsilon \rfloor\}$$

O que isso significa é que cada classe de equivalência consiste em todos os números reais que, quando divididos por ε e arredondados para baixo, dão o mesmo inteiro. De forma mais concreta, se $n = \lfloor x/\varepsilon \rfloor$, então a classe de equivalência de x é o intervalo de números reais de $n\varepsilon$ até $(n+1)\varepsilon$ (não incluindo $(n+1)\varepsilon$), já que esses são os números reais que, quando divididos por ε, são arredondados para baixo para n.
Portanto, as classes de equivalência são os intervalos semi-abertos:

$$[n\varepsilon, (n+1)\varepsilon[, \quad n \in \mathbb{Z}$$

Cada número real pertence exatamente a uma dessas classes, e cada classe é um intervalo que contém números que estão a uma distância menor que ε um do outro.