Nome: Marcos Reveles Redroso RA: 202693

MC358 - 2S 2023 - 4ª Lista de Exercícios

① Seja n um inteiro maior ou igual a 2. Considere a operação de soma sobre $\mathbb{Z}_n$ definida como: $[a]_n + [b]_n = [a+b]_n$. Prove que essa operação é bem definida (ou seja, prove que se $a \equiv x \pmod n$ e $b \equiv y \pmod n$, então $a+b \equiv x+y \pmod n$).

Para provar que a operação de soma sobre o conjunto dos inteiros módulo n ($\mathbb{Z}_n$) é bem definida, precisamos mostrar que se $a \equiv x \pmod n$ e $b \equiv y \pmod n$, então $a+b \equiv x+y \pmod n$

Começamos com as hipóteses: i) $a \equiv x \pmod n$ ii) $b \equiv y \pmod n$

Isso significa que $a-x$ é um múltiplo de n e $b-y$ é um múltiplo de n. Ou seja, existem inteiros k e m tais que:

i) $a - x = kn$ ii) $b - y = mn$

Agora, queremos mostrar que $a+b \equiv x+y \pmod n$. Para fazer isso, somamos as duas equações acima: $(a-x)+(b-y) = kn+mn$.

Por fim, combinamos os termos: $(a+b)-(x+y) = (k+m)n$

Aqui, temos a diferença entre a soma $(a+b)$ e $(x+y)$ igual a um múltiplo de n. Isso implica que $(a+b)$ e $(x+y)$ são congruentes módulo n. Portanto, a operação de soma em $\mathbb{Z}_n$ é bem definida, pois se $a \equiv x \pmod n$ e $b \equiv y \pmod n$, então temos que $a+b \equiv x+y \pmod n$.

② Usando operações modulares, prove as seguintes afirmações:

a) Para todo $n \in \mathbb{N}$, $7^n - 5^n$ é par.

* Podemos usar o princípio da indução matemática para provar.

i) Base da indução ($n=1$): $7^1 - 5^1 = 7 - 5 = 2$

O resultado é um número par, então o caso-base é válido.

ii) Hipótese da indução: Suponha que a afirmação seja verdadeira para algum valor k, ou seja, $7^k - 5^k$ é um número par.

$(k+1)(k+1)(k+1) = (k^2+2k+1)(k+1) = k^3+3k^2+3k+1$

DOM SEG TER QUA QUI SEX SÁB

08 11 23

iii) Passo da indução: Agora, precisamos provar que a afirmação é verdadeira para $k+1$.

Para demonstrar isso: $7^{(k+1)} - 5^{(k+1)} = 7^k \cdot 7^1 - 5^k \cdot 5^1 = 7^k \cdot 7 - 5^k \cdot 5$

Podemos reescrever essa expressão: $(7^k - 5^k) \cdot 7 + 5^k \cdot (7-5)$

Pela nossa hipótese de indução, sabemos que $7^k - 5^k$ é um número par (visto que estamos assumindo que é verdade para k). Além disso, sabemos que $7-5=2$, que é um número par.

Agora, temos um número par $(7^k - 5^k)$ multiplicado por um número ímpar (7), somado a um número par $(5^k \cdot 2)$. O produto de um número par por um número ímpar resulta em um número par. Logo, a soma (nesse caso) é um número par.

Assim, para $k+1$, $7^{(k+1)} - 5^{(k+1)}$ é par. Com a base de indução, a hipótese de indução e o passo indutivo provados, podemos concluir que a afirmação é verdadeira para todos os naturais. Segue que, $7^n - 5^n$ é par para todo $n \in \mathbb{N}$.

(a) Para todo $n \in \mathbb{N}$, $6 \mid (n^3 - n)$.

i) Base: Para $(n=1)$: $(1^3 - 1) = 1 - 1 = 0$

Assim, vemos que $6 \mid (1^3 - 1)$ e como 6 não divide 0, a afirmação vale.

ii) Hipótese de Indução (H.I): Suponha que a afirmação seja verdadeira para um número natural k arbitrário, isto é, que $6 \mid (k^3 - k)$.

iii) Passo Indutivo (P.I): Queremos ver a expressão $(k+1)^3 - (k+1)$.

$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - (k+1)$ (*)

Agora, usando a H.I. de que $6 \mid (k^3 - k)$, o que significa que $k^3 - k$ é um múltiplo de 6. Vamos escrever isso como $k^3 - k = 6m$, tal que $m \in \mathbb{Z}$.

Podemos substituir $k^3 - k$ por $6m$ na expressão (*):

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

Substituindo $(k^3 - k)$ por $6m$: $(k^3 - k) + 3k^2 + 3k + 1 = 6m + 3k^2 + 3k + 1$

Agora, fatorando 3 fora da expressão: $6m + 3k^2 + 3k + 1 = 3(2m + k^2 + k) + 1$

Com isso, está claro o Passo Indutivo ao mostrar que com base na hipótese de indução, a afirmação é verdadeira para $k+1$. Logo, a prova por indução, estabelecemos que $6 \mid (n^3 - n)$, $\forall n \in \mathbb{N}$.

08 | 11 | 23

17 × 4 = 68

DOM SEG TER QUA QUI SEX SÁB

③ Encontre o inverso multiplicativo de 17 módulo 72 no intervalo $\{0,1,\dots,71\}$. (Dica: Use o algoritmo de Euclides estendido).

Para encontrar o inverso multiplicativo de 17 módulo 72, podemos usar o algoritmo de Euclides estendido. Esse algoritmo nos permite calcular o máximo divisor comum (MDC) de 17 e 72, bem como encontrar os coeficientes de Bézout que nos ajudarão a determinar o inverso multiplicativo. Aqui temos os passos da resolução:

i) Calculemos o MDC pelo algoritmo de Euclides

$$72 \mid 17 \qquad 17 \mid 4$$
$$-68 \quad 4 \qquad -16 \quad 4$$
$$4 \qquad 1$$

* Logo: $\begin{cases} 72 = 4 \cdot 17 + 4 \\ 17 = 4 \cdot 4 + 1 \Rightarrow MDC(17,72) \text{ é igual a } 1 \\ 4 = 4 \cdot 1 + 0 \end{cases}$

ii) Aplicando o algoritmo de Euclides Estendido

↳ Primeiro, devemos encontrar os coeficientes Bézout tais que:
$(\exists\, x, y \in \mathbb{Z} \mid 17x + 72y = 1)$

↳ Usando o algoritmo de Euclides estendido, temos:
$1 = 17 - 4 \cdot 4 \Rightarrow (1 = 17 - 4 \cdot (72 - 4 \cdot 17))$

↳ Agora, substituímos a primeira equação na segunda:
$1 = 17 - 4(72 - 4 \cdot 17) \Rightarrow 1 = 5 \cdot 17 - 4 \cdot 72$

↳ Assim, podemos ver que $5 \cdot 17$ é o inverso multiplicativo de 17 mod 72. Porém, devemos encontrá-lo no intervalo $\{0,1,\dots,71\}$, então precisamos reduzir $5 \cdot 17 \bmod 72$ para:
$5 \cdot 17 \equiv 85 \pmod{72}$

↳ Agora para obter o inverso multiplicativo no intervalo $\{0,1,\dots,71\}$ subtraí 72 até obter um número menor ou igual a 71: $85 - 72 = 13$

* Portanto, o inverso multiplicativo de 17 módulo 72 no intervalo $\{0,1,\dots,71\}$ é 13.

DOM SEG TER QUA QUI SEX SÁB

09 11 23

(4) Prove que a equação $14x^2 + 15y^2 = 7^{2000}$ não possui solução (x, y) inteira.

*Para provar que $14x^2 + 15y^2 = 7^{2000}$ não possui soluções $(x, y) \in \mathbb{Z}$, usarei o método da indução.

① Caso-base: quando $n = 0$, a equação torna-se $14x^2 + 15y^2 = 7^0 = 1$. A única solução inteira possível nesse caso seria $x = y = 0$, o que não é uma solução. Logo, a afirmação vale para $n = 0$.

② Hipótese de Indução: Vamos supor que a equação não possui soluções inteiras para $n = k$, $k \in \mathbb{N}$. Ou seja, suponha que a equação $14x^2 + 15y^2 = 7^k$ não tem soluções inteiras para x e y.

③ Passo Indutivo: Agora, queremos provar que a equação também não possui soluções inteiras para $n = k+1$. Considere a equação $14x^2 + 15y^2 = 7^{k+1}$. Vamos supor, por contradição, que existe uma solução inteira para $n = k+1$. Ou seja, existem inteiros (x, y) que satisfazem $14x^2 + 15y^2 = 7^{k+1}$.

Agora, podemos manipular essa equação considerando o lado esquerdo módulo 7. Isso é:

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

Esta expressão implica que $x^2 \equiv y^2 \pmod 7$. Agora, podemos testar todas as possíveis condições de x e y mod 7 para ver que isso não é possível:

i) $x \equiv y \pmod 7$: Neste caso, $x^2 \equiv y^2 \pmod 7$ é verdadeiro.

ii) $x \equiv -y \pmod 7$: Neste caso, também $x^2 \equiv y^2 \pmod 7$ também é verdadeiro.

Assim, não importa qual das duas condições seja verdadeira, teríamos $x^2 \equiv y^2 \pmod 7$, o que contradiz a nossa hipótese inicial. Portanto, não pode haver uma solução inteira para $n = k+1$.

Concluímos, por indução, que a equação apresentada ($14x^2 + 15y^2 = 7^n$) não possui soluções inteiras para x e y tal que $n \geq 0$.

09 11 23

DOM SEG TER QUA QUI SEX SÁB

(5) Prove, usando congruências, que $11^{(n+2)} + 12^{(2n+1)}$ é divisível por 133, para qualquer número natural n.

* Para provar que $11^{(n+2)} + 12^{(2n+1)} + 1$ é divisível por 133, para qualquer número natural n usando congruências, temos que:

i) Primeiro, observe que $133 = 11 \cdot 12 + 1$. Vamos dividir isso como $133 \equiv 1 \pmod{11}$ e $133 \equiv 1 \pmod{12}$

ii) Agora, vamos considerar a expressão $11^{(n+2)} + 12^{(2n+1)} + 1$ e analisar cada termo separadamente em termos de congruências

a) $11^{(n+2)}$: $11^{(n+2)} \equiv 11^2 \cdot 11^n \equiv 121 \cdot 11^n \equiv 1 \cdot 11^n \equiv 11^n \pmod{11}$

b) $12^{(2n+1)}$: $12^{(2n+1)} \equiv (12^2)^n \cdot 12 \equiv 144^n \cdot 12 \equiv 1^n \cdot 12 \equiv 12 \pmod{11}$

iii) Agora, somamos esses resultados e somamos 1:

$11^n + 12 + 1 \equiv 11^n + 1 + 1 \equiv 11^n + 2 \pmod{11}$

Como $11^n + 2$ é congruente a 2 módulo 11, temos que: $11 \mid (11^n + 2)$

Acabamos de dizer que $12^{(2n+1)} \equiv 12 \pmod{11}$, temos que:

$12^{(2n+1)} + 1 \equiv 13 \pmod{11}$. Logo, vemos que: $12 \mid (12^{(2n+1)} + 1)$

iv) Portanto, a expressão completa $11^{(n+2)} + 12^{(2n+1)} + 1$ é a soma de três termos, cada um dos quais é divisível por 11. Logo, a expressão total é divisível por 11. Acabamos de provar, também, que $133 \equiv 1 \pmod{12}$, então podemos dizer que $12^{(2n+1)} + 1$ é divisível por 12.

* Deste modo, como toda a expressão é divisível por 11 e 12, concluí-se que $11^{(n+2)} + 12^{(2n+1)} + 1$ é divisível por $11 \times 12 = 132$ $\forall n \in \mathbb{N}$.

(6) Prove que se $f: X \to Y$ e $g: Y \to Z$ são funções injetoras, então $g \circ f$ também é injetora.

* Para provar que $g \circ f$ é injetora, vamos abordar dois tópicos:

(1) Composição de funções: observa-se que se $f \subseteq X \times Y$ e $g \subseteq Y \times Z$ são funções, então a composição $g \circ f$ é uma função de X para Z.

(2) Função injetora: $f \subseteq X \times Y$ é injetora se $f(x) = f(x') \Rightarrow x = x'$.

Agora, vamos considerar a composição $g \circ f$ e mostrar que ela é injetora. Suponha que $g \circ f$ não seja injetora. Isso significa que existem x e x' em X tal que $g(f(x)) = g(f(x'))$ e $x \neq x'$.

DOM DOM | SEG LUN | TER MAR | QUA MIÉ | QUI JUE | SEX VIE | SÁB SÁB

10 | 11 | 23

* Pela definição de função, $g(f(x))$ e $g(f(x'))$ estão em $\mathbb{Z}$. Como $g(f(x)) = g(f(x'))$ o que implica que $f(x) = f(x')$
* Agora, pela definição de função injetora, isso implica que $x = x'$, o que é uma contradição com a suposição inicial de que $x \neq x'$. Portanto, chegamos a uma contradição, e nossa suposição de que gof não é injetora é falsa. Consequentemente, podemos concluir que gof é injetora.
* Assim, combinando o Teorema de Composição de Funções com a definição de função injetora, mostramos que a composição de duas funções injetoras resulta em uma função injetora.

(7) Considere a função $f(x) = \frac{x}{(3+x)}$, onde $Dom(f) = \mathbb{R} \setminus \{-3\}$.

a) Determine $Img(f)$ e diga se f é sobrejetora ou não.

* Para encontrar a imagem de f, precisamos analisar para quais valores de x a função $f(x)$ pode assumir diferentes valores:

$f(x) = \frac{x}{3+x}$ ⇒ Simplificando: $f(x) = \frac{x}{(3+x)}$, $1 = \frac{x}{(x+3)}$ a expressão

* A imagem $Img(f)$ é o conjunto de todos os valores que $f(x)$ pode assumir, sendo que $f(x)$ está definida para todo $x \in \mathbb{R} \setminus \{-3\}$. Porém, $f(x)$ não pode assumir o valor 1, já que isso faria o denominador $x+3$ ser igual a zero, o que não é permitido. Logo, $Img(f) = \mathbb{R} \setminus \{0\}$.

Logo, a função não é sobrejetora, já que não atinge todos os reais do $\mathbb{R}$.

a.) f é injetora?

* Uma função é injetora se para todos x_1 e x_2 em $Dom(f)$, $f(x_1) = f(x_2)$
* Vamos considerar $f(x_1) = f(x_2)$: $\frac{x_1}{(x_1+3)} = \frac{x_2}{(x_2+3)}$
* Agora, multiplicando ambos os lados por $(x_1+3)(x_2+3)$:

$\frac{x_1}{(x_1+3)}(x_1+3)(x_2+3) = \frac{x_2}{(x_2+3)}(x_1+3)(x_2+3) \Rightarrow x_1(x_2+3) = x_2(x_1+3)$

* Expandindo os termos: $x_1x_2 + 3x_1 = x_2x_1 + 3x_2 \Rightarrow 3x_1 = 3x_2$
* Dividindo por 3, obtemos: $x_1 = x_2$. Logo, f é injetora.

10 11 23

DOM SEG TER QUA QUI SEX SÁB

(8) A função piso associa a cada número real x o maior inteiro que é menor ou igual a x. Este inteiro é denotado por $\lfloor x \rfloor$. Observe que $\lfloor 1/3 \rfloor = \lfloor 2/3 \rfloor = 0$, $\lfloor -1/3 \rfloor = \lfloor -2/3 \rfloor = -1$ e $\lfloor 5 \rfloor = 5$.

A função teto associa a cada número real x o menor inteiro que é maior ou igual a x. Este inteiro é denotado por $\lceil x \rceil$. Observe que $\lceil 5/4 \rceil = \lceil 7/4 \rceil = 2$, $\lceil -1/4 \rceil = \lceil -3/4 \rceil = 0$ e $\lceil 4 \rceil = 4$.

Tanto o piso quanto o teto são funções do conjunto $\mathbb{R}$ para o conjunto $\mathbb{Z}$. Para todo $x \in \mathbb{R}$ e $n \in \mathbb{Z}$, as seguintes propriedades valem:

- $\lfloor x \rfloor = n$ se, e somente se, $n \leq x < (n+1)$.
- $\lceil x \rceil = n$ se, e somente se, $(x-1) < n \leq x$.
- $\lfloor x \rfloor = n$ se, e somente se, $(n-1) < x \leq n$.
- $\lceil x \rceil = n$ se, e somente se, $x \leq n < (x+1)$.
- $(x-1) < \lfloor x \rfloor \leq x \leq \lceil x \rceil < (x+1)$
- $\lfloor -x \rfloor = -\lceil x \rceil$
- $\lceil -x \rceil = -\lfloor x \rfloor$

Prove, ou dê um contra-exemplo para as seguintes afirmações:

a) $\forall x, y \in \mathbb{R}$, $\lfloor x+y \rfloor = \lfloor x \rfloor + y$ e $\lceil x+y \rceil = \lceil x \rceil + y$

b) $\forall (x,y) \in \mathbb{R} \times \mathbb{Z}$, $\lfloor x+y \rfloor = \lfloor x \rfloor + y$ e $\lceil x+y \rceil = \lceil x \rceil + y$

a) Vamos analisar a afirmação para o teto ($\lceil x+y \rceil = \lceil x \rceil + y$):

- Considere $x = 1,5$ e $y = 2$. Vemos $\lceil x+y \rceil = \lceil 3,5 \rceil = 4$ e $\lceil x \rceil + y = 1 + 2 = 3$. Portanto, a afirmação não é verdadeira.
- Agora, analisamos a afirmação para o piso ($\lfloor x+y \rfloor = \lfloor x \rfloor + y$):
- Considere $x = 1,5$ e $y = 2$. Vemos $\lfloor x+y \rfloor = \lfloor 3,5 \rfloor = 3$ e $\lfloor x \rfloor + y = 1 + 2 = 3$. Neste caso específico, a afirmação vale.

* Logo, vemos que a) não é verdadeira, pois encontramos um contra-exemplo.

b) Para analisar a afirmação, devemos levar em consideração tanto valores fracionários quanto inteiros.

- Considere $x = 1,5$ e $y = 2$. Vemos $\lfloor x+y \rfloor = \lfloor 3,5 \rfloor = 4$ e $\lfloor x \rfloor + y = 1 + 2 = 4$, o que é verdadeiro. Agora, considere que $x = 1,5$ e $y = -2$. Temos $\lfloor x+y \rfloor = \lfloor -0,5 \rfloor = -1$ e $\lfloor x \rfloor + y = 1 - 2 = -1$, o que também vale. Portanto, a afirmação b) é verdadeira para os exemplos dados.

DOM SEG TER QUA QUI SEX SÁB

11 11 23

(9) Seja ε um número real positivo. Considere a relação R_ε sobre $\mathbb{R}$ tal que: $(x,y) \in R_\varepsilon \Leftrightarrow [x/\varepsilon] = [y/\varepsilon]$ para quaisquer x e y em $\mathbb{R}$. Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

* Precisamos verificar se R_ε satisfaz as três propriedades de uma relação de equivalência: reflexividade, simetria e transitividade.

i) Reflexividade: $(x,x) \in R_\varepsilon$ para todo $x \in \mathbb{R}$.

↳ Vamos verificar se $[x/\varepsilon] = [x/\varepsilon]$ é sempre verdadeiro, o que vale para qualquer número real x. Logo, a relação é reflexiva.

ii) Simetria: $(x,y) \in R_\varepsilon \Rightarrow (y,x) \in R_\varepsilon$ para todo $x, y \in \mathbb{R}$.

↳ Se $[x/\varepsilon] = [y/\varepsilon]$, então $[y/\varepsilon] = [x/\varepsilon]$, pois a função piso é simétrica em relação a x e y. Portanto, R_ε é simétrica.

iii) Transitividade: $(x,y) \in R_\varepsilon$ e $(y,z) \in R_\varepsilon \Rightarrow (x,z) \in R_\varepsilon$ $\forall x,y,z \in \mathbb{R}$

↳ Se $[x/\varepsilon] = [y/\varepsilon]$ e $[y/\varepsilon] = [z/\varepsilon]$, então pela transitividade da função piso, $[x/\varepsilon] = [z/\varepsilon]$ e assim, $(x,z) \in R_\varepsilon$. Logo, R_ε é transitiva.

* Com essas três verificações, concluímos que R_ε é uma relação de equivalência. A classe de equivalência de um elemento x é o conjunto de todos os elementos que são equivalentes a x de acordo com a relação R_ε.

* Nesse caso, a classe de equivalência de x é dada por:

$$[x]_{R_\varepsilon} = \{y \in \mathbb{R} : [x/\varepsilon] = [y/\varepsilon]\}$$

* Essa classe de equivalência é composta por todos os números reais que têm o mesmo valor de $[x/\varepsilon]$ quando divididos por ε.