Números Inteiros & Criptografia 2022.2

Prova 1

24 de novembro de 2022

Você pode usar qualquer questão da prova para resolver outra, mesmo que você não tenha feito a questão que está usando! Você deve citar claramente qual questão está usando, e não pode criar dependências circulares.

Definição. Dados números inteiros a, b, c, vamos definir $\mathrm{mdc}(a, b, c)$ fazendo $\mathrm{mdc}(a, b, c) = 0$, se $0 = a = b = c$, e $\mathrm{mdc}(a, b, c) =$ o maior número inteiro que divide tanto a quanto b quanto c, nos outros casos.

Questão 1. Sejam a, b, c inteiros.

a (1 ponto)**.** Prove que $\mathrm{mdc}(a, b, c) \geq 1$ se, e somente se, ($a \neq 0$ ou $b \neq 0$ ou $c \neq 0$).

b (1 ponto)**.** Prove que $\mathrm{mdc}(a, b, c) = \mathrm{mdc}(a, \mathrm{mdc}(b, c))$.

c (1,5 ponto)**.** Descreva um algoritmo para encontrar inteiros x, y, z tais que

$$ax + by + cz = \mathrm{mdc}(a, b, c).$$

Você **não** precisa fazer provas formais de terminação e corretude para o seu algoritmo.

Questão 2. Considere o seguinte jogo.

Você é o piloto de um veículo que só se movimenta para frente e para trás. Antes do começo do jogo, são sorteados 3 números naturais v_A, v_B, v_C e um número inteiro $p \neq 0$. Um pote de ouro é colocado a $|p|$ metros de distância da posição inicial do veículo, sendo à frente do veículo se $p > 0$ e atrás se $p < 0$.

No painel de comando do veículo há 3 alavancas, rotuladas A, B, C. Cada alavanca pode ficar em duas posições, *para frente* ou *para trás*. No painel há também 3 botões, rotulados b_A, b_B, b_C, e um indicador de combustível. O veículo se movimenta de acordo com as seguintes regras:

- Ao apertar qualquer botão, exatamente 1 litro de combustível é usado.
- Quando o botão b_A é apertado e ainda há combustível no tanque, o veículo anda v_A metros para frente, se a alavanca A estiver na posição "para frente", ou v_A posições para trás, se a alavanca A estiver na posição "para trás".
- Analogamente para o botão b_B com a alavanca B e o número v_B, e para o botão b_C com a alavanca C e o número v_C.

Para começar o jogo, sabendo os valores sorteados v_A, v_B, v_C, p, você deve fazer as seguintes escolhas:

- as posições de cada uma das três alavancas A, B, C
- quantos litros de combustível devem ser colocados no tanque do veículo, com a única restrição de que essa quantidade seja um número natural.

A partir de então, seu objetivo é: apenas apertando os botões (sem tocar nas alavancas nem colocar mais combustível!), levar o veículo da origem até exatamente a posição do pote de ouro.

a (1 ponto)**.** Mostre como o jogo com $v_A = 30$, $v_B = 105$, $v_C = 42$, $p = -51$ pode ser vencido, i.e., quais escolhas você pode fazer no início, e depois em qual sequência apertar os botões, para vencer.

b (1,5 ponto)**.** Dependendo dos valores sorteados, pode ser impossível vencer o jogo. Dê uma condição suficiente e necessária (ou seja, uma condição do tipo "se e somente se") para que, dados os valores sorteados, seja possível vencer o jogo.

c (2,5 pontos)**.** Descreva uma estratégia que, recebendo os valores sorteados v_A, v_B, v_C, p como entrada e supondo que o jogo correspondente possa ser vencido, escolha as posições das alavancas e a quantidade de combustível, e também dê a sequência na qual os botões devem ser apertados para ganhar o jogo.

Questão 3 (2,5 pontos)**.** Considere um sistema de cifra multiplicativa com os seguintes 15 símbolos e números ("códigos") correspondentes:

símbolo	A	C	D	E	I	L	M	N	O	P	R	S	T	U	V
código	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Você recebe a mensagem **AUPRMVI** e sabe que ela foi encriptada com a chave 13. Explique como obter a chave de descriptação correspondente a esta chave de encriptação, e encontre a mensagem original.

Para facilitar seu trabalho, você pode usar a tabela abaixo. Nela, cada célula indica a "casa do ciclo" resultante de se partir de algum número na "casa do ciclo" indicada pela linha e multiplicar pelo número indicado na coluna. Por exemplo, partindo da casa do "N" no ciclo e multiplicando por 6, chegamos à casa do "T".

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
C	A	C	D	E	I	L	M	N	O	P	R	S	T	U	V
D	A	D	I	M	O	R	T	V	C	E	L	N	P	S	U
E	A	E	M	P	T	A	E	M	P	T	A	E	M	P	T
I	A	I	O	T	C	L	P	U	D	M	R	V	E	N	S
L	A	L	R	A	L	R	A	L	R	A	L	R	A	L	R
M	A	M	T	E	P	A	M	T	E	P	A	M	T	E	P
N	A	N	V	M	U	L	T	I	S	E	R	D	P	C	O
O	A	O	C	P	D	R	E	S	I	T	L	U	M	V	N
P	A	P	E	T	M	A	P	E	T	M	A	P	E	T	M
R	A	R	L	A	R	L	A	R	L	A	R	L	A	R	L
S	A	S	N	E	V	R	M	D	U	P	L	C	T	O	I
T	A	T	P	M	E	A	T	P	M	E	A	T	P	M	E
U	A	U	S	P	N	L	E	C	V	T	R	O	M	I	D
V	A	V	U	T	S	R	P	O	N	M	L	I	E	D	C

Boa prova!