PROVA 2

MAC105 FUNDAMENTOS DE MATEMÁTICA PARA A COMPUTAÇÃO

1o. SEMESTRE DE 2018

Nome:
Número USP:

Instruções:

(*1*) Esta prova é individual.
(*2*) A prova consiste de **4** questões (contando a Questão 0 nesta página). Note que é possível tirar mais de 100 pontos nessa prova `:-)`
(*3*) Para ter nota integral em uma questão, **a escrita de sua solução deve estar muito boa**, tanto do ponto de vista **matemático** como do ponto de vista de **apresentação**.
(*4*) As respostas devem estar nos locais indicados.
(*5*) Não é permitido o uso de aparelhos eletrônicos de qualquer natureza.
(*6*) Não destaque as folhas deste caderno.
(*7*) Não use folhas avulsas para rascunho. Não é necessário apagar seus rascunhos.
(*8*) Não é permitido consultar nenhum material nem consultar colegas.

Assinatura:

Sua assinatura acima atesta a autenticidade e originalidade de seu trabalho e que você compromete-se a seguir o código de ética da USP em todas as suas atividades, incluindo esta prova.

Boa sorte!

Q	0	1	2	3	**Total**
Nota					

Q0. [**5 pontos**] Leia o conteúdo desta página e preencha os itens requisitados. Assine acima, e atente ao significado de sua assinatura.

Data: 2018/7/16, 6:44pm

Q1. [50 pontos]

(i) Seja x um número real. Prove que $\lceil \lceil x \rceil / 3 \rceil = \lceil x/3 \rceil$.

Resposta:

(ii) Seja x um número real e $k \geq 1$ um inteiro. Prove que

$$\underbrace{\lceil \lceil \ldots \lceil \lceil \lceil x \rceil / 3 \rceil / 3 \rceil \ldots \rceil / 3 \rceil}_{k \text{ vezes}} = \lceil x/3^k \rceil. \tag{1}$$

Resposta:

(*iii*) Seja $x > 1/2$ um número real. Prove que $\lceil \log_2 \lceil x \rceil \rceil = \lceil \log_2 x \rceil$.
Resposta:

(*iv*) Prove que se $0 < x \leq 1/2$, então $\lceil \log_2 \lceil x \rceil \rceil \neq \lceil \log_2 x \rceil$.
Resposta:

(*v*) Seja x um número real e $k \geq 1$ um inteiro. Suponha que

$$x \geq \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{k-1 \text{ vezes}}. \tag{2}$$

(Por exemplo, para $k = 1$, supomos $x \geq 1$, para $k = 2$, supomos $x \geq 2$ e, para $k = 3$, supomos $x \geq 2^2$.) Prove que

$$\underbrace{\lceil \log_2 \lceil \dots \lceil \log_2 \lceil \log_2 \lceil x \rceil \rceil \rceil \dots \rceil \rceil}_{k \text{ vezes}} = \lceil \log_2^{(k)} x \rceil, \tag{3}$$

onde

$$\log_2^{(k)} x = \underbrace{\log_2 \log_2 \dots \log_2}_{k \text{ vezes}} x. \tag{4}$$

Isto é, $\log_2^{(1)} x = \log_2 x$ e, para $k > 1$, temos $\log_2^{(k)} x = \log_2 \log_2^{(k-1)} x$.

Resposta:

Q2. **[40 pontos]** Dado um conjunto não-vazio de inteiros A, seja

$$\operatorname{Div} A = \{d \in \mathbb{N} \colon \text{ para todo } a \in A, \text{ vale que } d \mid a\}. \tag{5}$$

Isto é, $\operatorname{Div} A$ é o conjunto dos divisores não-negativos comuns dos elementos em A.

(*i*) Sejam a e b inteiros. Prove que $\operatorname{Div}\{a, b\} = \operatorname{Div}\{\operatorname{mdc}(a, b)\}$.

Resposta:

(*ii*) (Generalização de (*i*)) Sejam $a_1, \ldots, a_n$ inteiros ($n \geq 2$). Prove que

$$\operatorname{Div}\{a_1, \ldots, a_n\} = \operatorname{Div}\{a_1, \ldots, a_{n-2}, \operatorname{mdc}(a_{n-1}, a_n)\}. \tag{6}$$

Resposta:

(*iii*) Seja A um conjunto não-vazio de inteiros, e suponha que A contenha um elemento não-nulo. Definimos o *máximo divisor comum* $\operatorname{mdc} A$ de A como sendo o elemento máximo de $\operatorname{Div} A$, isto é, $\operatorname{mdc} A = \max \operatorname{Div} A$. (Se $A = \{0\}$, pomos $\operatorname{mdc} A = 0$.) Determine $\operatorname{mdc}\{a + 3, a + 5, a + 7\}$, onde a é um inteiro ímpar.

Resposta:

(*iv*) Seja $A = \{a_1, \dots, a_n\}$ um conjunto de inteiros com $n \geq 1$ e seja $d = \operatorname{mdc} A$. Prove que d é uma combinação linear inteira de elementos de A. Isto é, prove que existem $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ tais que

$$d = \sum_{1 \leq i \leq n} \alpha_i a_i. \tag{7}$$

Resposta:

Q3. [**40 pontos**] Fixe $n \in \mathbb{N}$ com $n > 0$. Seja R^* um sistema reduzido completo de resíduos módulo n, isto é, seja $R^* \subset \mathbb{Z}$ tal que $\mathrm{mdc}(r, n) = 1$ para todo $r \in R^*$ e tal que, para todo $x \in \mathbb{Z}$ com $\mathrm{mdc}(x, n) = 1$, vale que existe um único $r \in R^*$ tal que $x \equiv r \pmod{n}$. Fixe $a \in \mathbb{Z}$ com $\mathrm{mdc}(a, n) = 1$.

(*i*) Suponha que r e r' pertençam a R^*. Prove que $\mathrm{mdc}(rr', n) = 1$. Deduza que $\mathrm{mdc}(\prod_{r \in R^*} r, n) = 1$.

Resposta:

(*ii*) Prove que

$$aR^* = \{ar \colon r \in R^*\} \tag{8}$$

é também um sistema reduzido completo de resíduos módulo n.

Resposta:

(*iii*) Deduza que

$$\prod_{r \in R^*} r \equiv \prod_{r \in R^*} ar \pmod{n}. \tag{9}$$

Resposta:

(*iv*) Deduza o teorema de Euler dos itens (*i*) e (*iii*) acima. Isto é, prove que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Resposta: