

MAC 105 – Fundamentos de Matemática para Computação

Prova 2 — 22/6/2015

Instruções:

- Identifique sua prova na primeira página, com nome e número USP
- Numere as páginas, principalmente se usar mais de uma folha
- A prova pode ser feita a lápis
- As questões podem estar em qualquer ordem

1. (2,5 pts) Uma função $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ é *convexa* se, para todos vetores $\mathbf{u}, \mathbf{v}$ e todo real λ tal que $0 \leq \lambda \leq 1$, $f(\lambda \mathbf{u} + (1-\lambda)\mathbf{v}) \leq \lambda f(\mathbf{u}) + (1-\lambda)f(\mathbf{v})$. Prove que, se f é convexa, então, dados $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in \mathbb{R}^3$ e números reais não negativos $\lambda_1, \lambda_2, \dots, \lambda_n$ tais que $\lambda_1 + \lambda_2 + \dots + \lambda_n = 1$ então

$$f\left(\sum_{i=1}^n \lambda_i \mathbf{v}_i\right) \leq \sum_{i=1}^n \lambda_i f(\mathbf{v}_i).$$

2. (2,5 pts) Sobre equações modulares:

- (a) Considere uma equação $ax = b$ em $\mathbb{Z}_p$, onde p é um número primo dado, e a e b são inteiros. Mostre como se pode usar algoritmos conhecidos para encontrar uma solução x , representada por um inteiro entre 0 e $p-1$.
- (b) Resolva o seguinte sistema em $\mathbb{Z}_{17}$

$$\begin{aligned} 3x + 5y &= 1 \quad (4) \\ 7x - 4y &= 1 \quad (5) \end{aligned} \Rightarrow \begin{aligned} 12x + 20y &= 4 \quad (12x + 3y = 1) \\ 35x - 20y &= 1 \quad (-x - 3y = -1) \end{aligned}$$

Dando uma solução (x, y) com componentes entre 0 e 16.

3. (5,0 pts) Seja $\mathbb{N}_2$ o conjunto dos inteiros maiores que 1. Em $\mathbb{N}_2$, dizemos que n *divide potencialmente* m , e denotamos $n \uparrow m$ se existe um inteiro $k > 0$ tal que $n|m^k$.

- (a) Prove que $\uparrow$ é uma relação reflexiva e transitiva.

Para o que segue, $\sim$ é a relação de equivalência associada, isto é: $n \sim m$ sse $n \uparrow m$ e $m \uparrow n$.

- (b) Dê quatro números distintos a, b, c tais que: $a \sim b$, $a \uparrow c$, $d \uparrow b$ mas não vale que $c \uparrow a$ nem que $a \uparrow d$. Justifique todas as afirmativas.

- (c) Seja $Q = \mathbb{N}_2 / \sim$. Abaixo são definidas funções e operações sobre Q . Em cada caso, afirme se está bem definida ou não, e prove sua afirmação.

- $f([n]) =$ o menor número primo que divide n .
- $f : Q \rightarrow \mathbb{Z}_3$, dada por $f([n]) = n \% 3$.
- $s([n], [m]) = [n + m]$ (permitiria definir: $[n] + [m] = [n + m]$).
- $p([n], [m]) = [nm]$ (permitiria definir: $[n][m] = [nm]$).