
Nome:

29/11/2019

Regras:

- I. Não vires esta página antes do começo da prova.
- II. Nenhuma consulta de qualquer forma.
- III. Nenhum aparelho ligado (por exemplo: celular, tablet, notebook, *etc.*).¹
- IV. Nenhuma comunicação de qualquer forma e para qualquer motivo.
- V. $(\forall x) [\text{Colar}(x) \implies \neg \text{Passar}(x, \text{FMC1})]$.²
- VI. Use caneta para tuas respostas.
- VII. Responda dentro das caixas indicadas.
- VIII. Escreva teu nome em *cada* folha de rascunho extra *antes de usá-la*.
- IX. Entregue *todas* as folhas de rascunho extra, juntas com tua prova.
- X. Nenhuma prova será aceita depois do fim do tempo—mesmo se for atraso de 1 segundo.
- XI. Os pontos bônus podem ser usados para aumentar uma nota de qualquer unidade, dado que a nota original é pelo menos 5,0.³

Boas provas!

¹Ou seja, *desligue antes* da prova.

²Se essa regra não faz sentido, melhor desistir desde já.

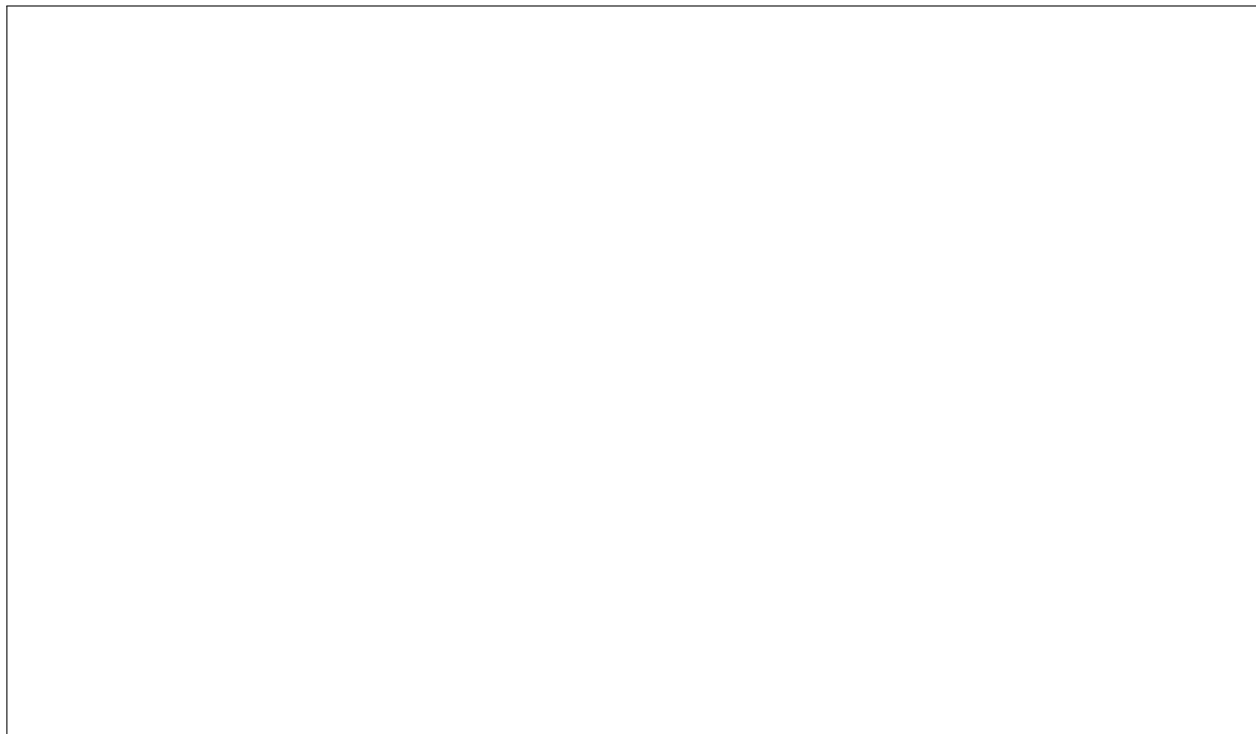
³Por exemplo, 25 pontos bonus podem aumentar uma nota de 5,2 para 7,7 ou de 9,2 para 10,0, mas de 4,9 nem para 7,4 nem para 5,0. A 4,9 ficaria 4,9 mesmo.

(24) **D**

Sejam $e, N \in \mathbb{Z}$ com $(e, \varphi(N)) = 1$, e seja d um inverso de e módulo $\varphi(N)$: $ed \equiv 1 \pmod{\varphi(N)}$. Para cada x com $(x, N) = 1$,

$$(x^e)^d \equiv x \pmod{N}.$$

DEMONSTRAÇÃO.



Só isso mesmo.

RASCUNHO

RASCUNHO