FMC1, 2019.2
(Turma N12 do Thanos)

Prova 3.x
(points: 24; bonus: $0^\flat$; time: 32')

Nome: Θάνος **Gabarito**

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!

[1] Ou seja, *desligue antes* da prova.
[2] Se essa regra não faz sentido, melhor desistir desde já.
[3] Por 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.

Como $ed \equiv 1 \pmod{\varphi(N)}$, logo seja $k \in \mathbb{Z}$ tal que

$$ed = k\varphi(N) + 1.$$

Calculamos:

$$\begin{aligned}
(x^e)^d &= x^{ed} \\
&= x^{k\varphi(N)+1} && \text{(pela escolha do } k\text{)} \\
&= x^{k\varphi(N)}x && \text{(def. de exponenciação)} \\
&= \left(x^k\right)^{\varphi(N)} x \\
&\equiv x \pmod{N}, && \text{(por teorema de Euler)}
\end{aligned}$$

onde no último passo precisamos a hipótese que x e $\varphi(N)$ são coprimos e logo, x^k e $\varphi(N)$ também são: $(x, \varphi(N)) = (x^k, \varphi(N)) = 1$.

Só isso mesmo.