FMC1, 2022.2 (Turma N12 do Thanos)

Prova 1.4 (points: 36; bonus: $0^\flat$; time: 42')

Nome:

2022-10-26

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. $(\forall x)\,[\,\mathrm{Colar}(x) \implies \neg\mathrm{Passar}(x, \mathrm{FMC1})\,]$.[2]

VI. Responda dentro das caixas indicadas, escrevendo em forma clara e facilmente legível.

VII. Nenhuma prova será aceita depois do fim do tempo—mesmo se for atraso de 1 segundo.

VIII. Escolha até 1 dos G, H, I.[3]

Dados. Os inteiros $(\mathbb{Z}; 0, 1, +, -, \cdot, \mathrm{Pos})$ com tipos:

$$0, 1 : \mathsf{Int} \qquad (+), (\cdot) : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int} \qquad (-) : \mathsf{Int} \to \mathsf{Int} \qquad \mathrm{Pos} : \mathsf{Int} \to \mathsf{Prop}.$$

Axiomas.

`(ZA-Ass)`, `(ZA-IdR)`, `(ZA-Com)`, `(ZA-InvR)`, `(ZM-Ass)`, `(ZM-IdR)`, `(ZM-Com)`, `(Z-DistR)`, `(Z-NZD)`, `(Z-NZero)`, `(ZP-ACl)`, `(ZP-MCl)`, `(ZP-Tri)`, `(Z-PBO)`.

Esclarecimento: Tuas demonstrações/refutações precisam ser na linguagem mid-level que temos elaborado nas aulas. *Não inclua* os Dados/Alvo nem outros rascunhos no teu texto! Os teoremas que demonstramos na disciplina "pré-congruência" são considerados dados, e podes usar nas suas respostas. Para citá-los, escreva apenas os seus enunciados (sem demonstrar) no Lemmata.

Boas provas!

[1] Ou seja, *desligue antes* da prova.

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

[3] Provas violando essa regra (com respostas em mais problemas) não serão corrigidas (tirarão 0 pontos).

(12) # G

Neste problema, escreva tua definição **em português matemático** que "compila" e que defina mesmo a noção correta. Tua definição, além de correta, precisa ser capaz de deixar a proposição que segue *demonstrável*.

(6) Definição de congruência módulo um inteiro:

Teorema. Seja x inteiro. Para qualquer y inteiro,

$$x \equiv y \pmod 0 \implies (\forall m \geq 0)\,[\, x \equiv y \pmod m \,]\,.$$

(6) Demonstração.

(36) # H

Sejam e, d, n inteiros tais que $e, \varphi(n)$ coprimos e d inverso de e módulo $\varphi(n)$.
Demonstre que para todo m com $(m, n) = 1$,

$$(m^e)^d \equiv m \pmod n.$$

Dica: *Não tenha medo aplicar as definições das relações envolvidas.*

Demonstração:

(24) # I

Sejam m_1, m_2 inteiros coprimos.

(12) **I1.** O sistema de congruências seguinte possui resolução:

$$x \equiv b_1 \pmod{m_1} \qquad\qquad x \equiv b_2 \pmod{m_2}$$

(12) **I2.** Ainda mais, tal resolução é única módulo $m_1 m_2$.

(3) Enunciado de **I1**. (Podes escrever em português matemático ou usando fórmula mesmo.)

(9) Demonstração de **I1**.

(4) Enunciado de **I2**. (Podes escrever em português matemático ou usando fórmula mesmo.)

(8) Demonstração de **I2**.

Só isso mesmo.

Rascunho