FMC1, 2022.2
(Turma N12 do Thanos)

Prova 1.3
(points: 24; bonus: $0^\flat$; time: 36')

Nome: Θάνος **Gabarito**

2022-09-28

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. Respeite as restrições dos problemas que têm escolha.[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)`	$(a+b)+c = a+(b+c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	`(ZM-Ass)`
`(ZA-IdR)`	$a + 0 = a$	$a \cdot 1 = a$	`(ZM-IdR)`
`(ZA-Com)`	$a + b = b + a$	$a \cdot b = b \cdot a$	`(ZM-Com)`
`(ZA-InvR)`	$a + (-a) = 0$	$(a+b) \cdot c = a \cdot c + b \cdot c$	`(Z-DistR)`
`(Z-NZD)`	$a \cdot b = 0 \implies a = 0$ ou $b = 0$	$0 \neq 1$	`(Z-NZero)`
`(ZP-ACl)`	Pos é $(+)$-fechado	Pos é $(\cdot)$-fechado	`(ZP-MCl)`
`(ZP-Tri)`	e.u.d.: $a \in \mathrm{Pos}$; $a = 0$; $-a \in \mathrm{Pos}$.	Pos é bem ordenado.	`(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! Em uns problemas, certos teoremas são considerados dados. Se quiser citar (e usar) tais teoremas, 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] Respostas violando essa regra (respondendo em mais questões) tirarão 0 pontos.

(8) **D**

Neste problema, escreva tua definição em português matemático que "compila" e que defina mesmo a noção correta. Não use nada que depende da positividade.

Defina **exatamente uma das**:

(4) DEFINIÇÃO DE $(|)$:

Sejam a, b inteiros. Dizemos que a divide b sse existe inteiro k tal que $ak = b$. Em símbolos:

$$a \mid b \overset{\text{def}}{\iff} (\exists k)\,[\,ak = b\,]\,.$$

(8) DEFINIÇÃO DE M.D.C.:

Sejam a, b, d inteiros. Dizemos que d é um m.d.c. dos a, b sse d é um divisor comum dos a, b e para qualquer divisor d' em comum dos a, b, temos $d' \mid d$. Em símbolos:

$$d \text{ m.d.c. dos } a, b \overset{\text{def}}{\iff} d \mid a \ \ \& \ \ d \mid b \ \ \& \ \ (\forall d')\,[\,d' \mid a \ \ \& \ \ d' \mid b \implies d' \mid d\,]\,.$$

(8) **E**

Demonstre:

$$(\forall x)\left[\,x^2 \text{ par} \implies x \text{ par}\,\right].$$

Considere dado tudo que demonstramos incluindo as conseqüências (wishlist) do (Z-PBO).
Aviso: se usar "magias", teus pontos finais deste problema serão divididos por 2 (rounded up).
Dica: *Euclides is your friend.*

DEMONSTRAÇÃO.

Seja x inteiro tal que x^2 par.
Logo seja k tal que $x^2 = 2k$.
Divide x por 2 para obter q, r tais que $x = 2q + r$ e $0 \leq r < 2$.
Como $0 \leq r < 2$, separo em casos:
Caso $r = 0$:
    Imediato pois $x = 2q$.
Caso $r = 1$:
    Logo $x^2 = (2q+1)^2 = 2(2q^2 + 2q) + 1$.
    Mas $x^2 = 2k + 0$.
    Logo $0 = 1$ pela unicidade dos restos e logo chegamos numa contradição.

(8) **F**

Escolhe **até uma** das **F1**, **F2**.

(4) **F1.** Demonstre pelos axiomas:

para qualquer inteiro x, $-x = x(-1)$.

DEMONSTRAÇÃO.

Seja x inteiro. Calculamos:

$$
\begin{aligned}
x + x(-1) &= x1 + x(-1) && ((\text{ZM-IdR})\ x)\\
&= x(1 + (-1)) && ((\text{Z-DistL})\ 1\ (-1)\ x)\\
&= x0 && ((\text{ZA-InvR})\ 1)\\
&= 0 && ((\text{Z-AnnR})\ x)
\end{aligned}
$$

Como $x + (-x) = 0$ (pela (ZA-InvR) x), logo $-x = x(-1)$ pela (Z-ResR).

(8) **F2.** Demonstre o princípio da indução para os inteiros positivos:

para qualquer $P \subseteq \mathbb{Z}$, se $1 \in P$ e P é $(+1)$-fechado, então $\mathrm{Pos} \subseteq P$.

De teoremas e definições, podes considerar dado tudo que obtemos antes de adicionar (Z-PBO) na nossa lista de axiomas.
DEMONSTRAÇÃO:

Seja $P \subseteq \mathbb{Z}$ tal que $1 \in P$ $^{(1)}$ e P é $(+1)$-fechado.
Seja $x \in \mathrm{Pos}$.
Vou demonstrar que $x \in P$.
Suponha que $x \notin P$.
Aplicamos a (Z-PBO) no conjunto $P' \stackrel{\text{def}}{=} \{ p' \mid p' \notin P \}$ habitado pelo positivo x, e logo seja m o menor positivo tal que $x \notin P$.
Pela (1) temos que $m \neq 1$ e como m positivo, logo $m > 1$.
Logo $m - 1 > 0$.
Como $m - 1 < m$ e $m - 1$ positivo, logo $m - 1 \in P$ (pela escolha de m).
Como P é $(+1)$-fechado, logo $(m-1) + 1 \in P$, ou seja $m \in p$, contradição.

Só isso mesmo.

Z-DistL.
$(\forall a, b, c)\,[\,c(a+b) = ca + cb\,]$.

DEMONSTRAÇÃO.
Sejam a, b, c inteiros.
Calculamos:

$$\begin{aligned} c(a+b) &= (a+b)c && \text{((ZM-Com))} \\ &= ac + bc && \text{((Z-DistR))} \\ &= ca + bc && \text{((ZM-Com))} \\ &= ca + cb. && \text{((ZM-Com))} \end{aligned}$$

ZA-IdL.
$(\forall a)\,[\,0 + a = a\,]$.

DEMONSTRAÇÃO.
Similar.

ZA-InvL.
$(\forall a)\,[\,(-a) + a = 0\,]$.

DEMONSTRAÇÃO.
Similar.

Z-AnnR.
$(\forall a)\,[\,a0 = 0\,]$.

DEMONSTRAÇÃO.
Seja a inteiro.
Calculamos:

$$\begin{aligned} a0 &= a(0+0) && \text{((ZA-IdR))} \\ &= a0 + a0. && \text{((Z-DistL))} \end{aligned}$$

Logo $a0 = 0$ pela (Z-ResR), já que $a0 + 0 = a0$.

Z-ResR.
$(\forall a, b)\,(\exists! x)[\,a + x = b\,]$.

DEMONSTRAÇÃO.
Existência.
Testemunho $(-a) + b$.
Calculamos:

$$\begin{aligned} a + ((-a) + b) &= (a + (-a)) + b && \text{((ZA-Ass))} \\ &= 0 + b && \text{((ZA-InvR))} \\ &= b + 0 && \text{((ZA-Com))} \\ &= b. && \text{((ZA-IdR))} \end{aligned}$$

Unicidade.
Seja x tal que $a + x = b$.
Calculamos:

$$\begin{aligned} (-a) + b &= (-a) + (a + x) && \text{(pela escolha de } x\text{)} \\ &= ((-a) + a) + x && \text{((ZA-Ass))} \\ &= 0 + x && \text{((ZA-InvL))} \\ &= x. && \text{((ZA-IdL))} \end{aligned}$$