FMC1, 2022.1 (Turma N12 do Thanos)

Prova 1.3 (points: 52; bonus: $0^\flat$; time: 42')

Nome:

2022-05-27

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. Escolhe até 2 dos $\mathbf{D}, \mathbf{E}, \mathbf{F}, \mathbf{G}, \mathbf{H}$.[3]

Lembram-se:

Definição. Sejam a, b, m inteiros. Dizemos que a, b são congruentes módulo m sse $m \mid a - b$:

$$a \equiv_m b \iff^{\text{def}} m \mid a - b.$$

Esclarecimento:

Suas demonstrações/refutações precisam ser escritas em português matemático (linguagem "mid-level" que temos elaborado nas aulas).
Considere como conhecidas *apenas as propriedades que temos demonstrado sobre as operações e a ordem dos inteiros* (ou seja, nenhuma propriedade que envolve divisibilidade é considerada como conhecida), e também considere conhecido o lema de Bézout:

Lemma-Bézout.
Para quaisquer inteiros a, b, existem inteiros x, y tais que $(a, b) = ax + by$.
Ainda mais, o (a, b) divide qualquer combinação linear dos a, b.

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).

(26) **D**

O lema de Euclides.
Para todo primo p e quaisquer inteiros a, b, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.
Demonstração.

(12) **E**

A congruência da relação $\equiv_m$ para qualquer inteiro m.
Para quaisquer inteiros c, c', a, m,

$$\text{se } c \equiv_m c', \text{ então } \begin{cases} \text{(i)} & a + c \equiv_m a + c'; \\ \text{(ii)} & a \cdot c \equiv_m a \cdot c'; \\ \text{(iii)} & -c \equiv_m -c'. \end{cases}$$

Demonstração.

(26) **F**

A invertibilidade de inteiros módulo um inteiro (suficiência).
Sejam a, m inteiros. Se $(a, m) = 1$, então a é invertível módulo m.
DEMONSTRAÇÃO.

(26) **G**

A invertibilidade de inteiros módulo um inteiro (necessidade).
Sejam a, m inteiros. Se a é invertível módulo m, então $(a, m) = 1$.
DEMONSTRAÇÃO.

(26) **H**

A unicidade de inversos módulo um inteiro.
Sejam a, m inteiros tais que a é invertível módulo m. Logo o inverso de a é único módulo m.
Demonstração.

Só isso mesmo.

Lemmata

Rascunho