FMC1, 2022.1 (Turma N12 do Thanos)

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

Nome: Θάνος **Gabarito**

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 D, E, F, G, H.[3]

Lembram-se:

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

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

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.

Sejam p inteiro primo e a, b inteiros.
Suponha $p \mid ab$.
Caso $p \mid a$:
    Imediato.
Caso $p \nmid a$:
    Logo $(p, a) = 1$. [Pelo Lemma-prime-coprime.]
    Logo sejam x, y inteiros tais que $1 = px + ay$ Lemma-Bézout.
    Logo $b = bpx + bay = pbx + aby$ (1).
    Como $p \mid p$ Lemma-div-refl e $p \mid ab$, logo $p \mid bpx + aby$ Lemma-div-lincomb.
    Logo $p \mid b$.

(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.

Sejam c, c', a, m inteiros tais que $c \equiv_m c'$, ou seja, $m \mid c - c'$ (1).

Parte (i).
    Preciso demonstrar que $m \mid (a + c) - (a + c')$.
    Mas $(a + c) - (a + c') = c - c'$, e já temos que $m \mid c - c' = 0$, pelo Lemma-div-zero.

Parte (ii).
    Preciso demonstrar que $m \mid ac - ac' = a(c - c')$.
    Como $m \mid c - c'$, logo $m \mid a(c - c')$, pelo Lemma-div-mult.

Parte (iii).
    Preciso demonstrar que $m \mid (-c) - (-c') = -c + c' = (-1)(c - c')$.
    Imediato pela (1) e o Lemma-div-mult.

(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.

Suponha $(a, m) = 1$.
Logo sejam x, y inteiros tais que $1 = ax + my$ Lemma-Bézout.
Calculamos:

$$\begin{aligned} 1 = &\quad ax + my \\ &\equiv_m ax + my \\ &\equiv_m ax + 0y && \text{[pela } \mathbf{E}\text{]} \\ &\equiv_m ax + 0 \\ &\equiv_m ax. \end{aligned}$$

Logo x é um inverso módulo m de a, e logo a é invertível módulo m.

(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.

Suponha a invertível módulo m e logo seja a' um inverso de a, ou seja,

$$aa' \equiv_m 1.$$

Logo $m \mid aa' - 1$.
Logo seja u tal que $mu = aa' - 1$.
Logo $1 = mu + a(-a')$, e logo 1 é uma combinação linear dos m, a.
Logo $(m, a) \mid 1$ pelo Lemma-Bézout, e logo $(m, a) = 1$, pelo Lemma-div-one.

(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.

Sejam a', a'' inversos módulo m de a.
Preciso demonstrar que $a' \equiv_m a''$.
Como $aa' \equiv_m 1$ e $aa'' \equiv_m 1$, logo $aa' \equiv_m aa''$.
Logo $a'(aa') \equiv_m a'(aa'')$.
Logo $(a'a)a' \equiv_m (a'a)a''$.
Logo $1a' \equiv_m 1a''$.
Logo $a' \equiv_m a''$.

(Qual a justificativa de cada «Logo...» mesmo, aqui?)

Só isso mesmo.

LEMMATA

Lemma-div-refl.
Para todo inteiro a, $a \mid a$.

DEMONSTRAÇÃO.
Seja a inteiro.
Como $a1 = a$, logo $a \mid a$.

Lemma-div-one.
Para todo inteiro a, (i) $1 \mid a$; (ii) $-1 \mid a$; (iii) se $a \mid 1$, $a = 1$ ou $a = -1$.

DEMONSTRAÇÃO.
Seja a inteiro.
(i) Como $1a = a$, logo $1 \mid a$.
(ii) Como $(-1)(-a) = a$, logo $-1 \mid a$.
(iii) Suponha $a \mid 1$. Logo seja u inteiro tal que $au = 1$. Logo $a = 1$ ou $a = -1$.

Lemma-div-zero.
Para todo inteiro a, $a \mid 0$.

DEMONSTRAÇÃO.
Seja a inteiro.
Como $a0 = 0$, logo $a \mid 0$.

Lemma-cong-refl.
Para quaisquer inteiros a, m, $a \equiv_m a$.

DEMONSTRAÇÃO.
Sejam a, m inteiros.
Pelo Lemma-div-zero, $m \mid 0 = a - a$.

Lemma-div-add.
Para quaisquer inteiros d, a, b, se $d \mid a$ e $d \mid b$, então $d \mid a + b$.

DEMONSTRAÇÃO.
Sejam d, a, b inteiros tais que $d \mid a$ e $d \mid b$.
Logo sejam u, v tais que $du = a$ e $dv = b$.
Calculamos:

$$\begin{aligned} a + b &= du + b && \text{[Pela escolha de } u.\text{]} \\ &= du + dv && \text{[Pela escolha de } u.\text{]} \\ &= d(u + v). \end{aligned}$$

Logo $d \mid a + b$.

Lemma-div-mult.
Para quaisquer inteiros d, a, se $d \mid a$, então para todo x inteiro, $d \mid ax$.

DEMONSTRAÇÃO.
Sejam d, a inteiros tais que $d \mid a$.
Logo seja u inteiro tal que $du = a$.
Seja x inteiro.
Calculamos:

$$\begin{aligned} ax &= (du)x && \text{[Pela escolha de } u.\text{]} \\ &= d(ux). \end{aligned}$$

Logo $d \mid ax$.

Lemma-div-lincomb.
Para quaisquer inteiros d, a, b, se $d \mid a$ e $d \mid b$, então para quaisquer x, y inteiros, $d \mid ax+by$.

DEMONSTRAÇÃO.
Sejam d, a, b inteiros tais que $d \mid a$ e $d \mid b$, e sejam x, y inteiros.
Pelo Lemma-div-mult, temos $d \mid ax$ e $d \mid by$.
Pelo Lemma-div-add, temos $d \mid ax + by$.

Lemma-prime-coprime.
Sejam p inteiro primo e a inteiro. Se $p \nmid a$, então $(a, p) = 1$.

DEMONSTRAÇÃO.
Suponha $p \nmid a$.
Como p primo, seus únicos divisores são os $1, -1, p, -p$.
Como $p \nmid a$, logo os divisores em comum dos a, p são os $1, -1$.
Logo $(a, p) = 1$.