FMC1, 2022.2 (Turma N12 do Thanos)

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

Nome: Θάνος **Gabarito**

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:

> Sejam a, b, m inteiros. Dizemos que a é congruente ao b módulo m sse $m \mid a - b$.
> Em símbolos:
> $$a \equiv b \pmod{m} \overset{\text{def}}{\iff} m \mid a - b.$$

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.

> Seja y inteiro tal que $x \equiv_0 y$, ou seja $0 \mid x - y$.
> Logo $x - y = 0$, pois 0 é o único inteiro dividido por 0, e logo $x = y$.
> Seja $m \geq 0$. Preciso demonstrar que $m \mid x - y$.
> Como todo inteiro divide o 0, logo $m \mid 0$, e logo $m \mid x - y$.

(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:

> Seja m coprimo com n.
> Temos que d é inverso de e módulo $\varphi(n)$, ou seja:
>
> $$ed \equiv 1 \pmod{\varphi(n)},$$
>
> ou seja, $\varphi(n) \mid ed - 1$.
> Logo seja k tal que $k\varphi(n) = ed - 1$, e logo $ed = \varphi(n)k + 1$ (1).
> Calculamos:
>
> $$\begin{aligned}
> (m^e)^d &= m^{ed} \\
> &= m^{\varphi(n)k+1} && \text{(pela (1))} \\
> &= m^{\varphi(n)k} m \\
> &= (m^{\varphi(n)})^k m \\
> &\equiv_n 1^k m && \text{(pelo Teorema de Euler, pois } (m, n) = 1) \\
> &\equiv_n 1m \\
> &\equiv_n m.
> \end{aligned}$$

(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.)

$(\forall b_1, b_2)\,(\exists x)\,[\,x \equiv_{m_1} b_1 \;\&\; x \equiv_{m_2} b_2\,]$

(9) Demonstração de **I1**.

Observe que para qualquer inteiro k, o inteiro $m_1 k + b_1$ satisfaz a primeira congruência. Basta achar um k tal que $m_1 k + b_1$ satisfaz a segunda; ou seja, tal que

$$m_1 k + b_1 \equiv b_2 \pmod{m_2}.$$

Basta achar k tal que $m_1 k \equiv b_2 - b_1 \pmod{m_2}$.
Seja m_1' um inverso de m_1 módulo m_2.
Verificarei que o inteiro $m_1'(b_2 - b_1)$ é um testemunha válido:

$$\begin{aligned} m_1(m_1'(b_2 - b_1)) &= (m_1 m_1')(b_2 - b_1) \\ &\equiv_{m_2} 1(b_2 - b_1) && \text{(pela escolha de } m_1') \\ &\equiv_{m_2} b_2 - b_1. \end{aligned}$$

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

$(\forall b_1, b_2, x, x')\,[\,x \equiv_{m_1} b_1 \;\&\; x \equiv_{m_2} b_2 \;\&\; x' \equiv_{m_1} b_1 \;\&\; x' \equiv_{m_2} b_2 \implies x \equiv_{m_1 m_2} x'\,]$

(8) Demonstração de **I2**.

Sejam b_1, b_2, x, x' tais que

$$x \equiv_{m_1} b_1 \;\&\; x \equiv_{m_1} b_2 \qquad \& \qquad x' \equiv_{m_2} b_1 \;\&\; x' \equiv_{m_2} b_2.$$

Logo

$$x \equiv_{m_1} x' \qquad \& \qquad x \equiv_{m_2} x',$$

ou seja,

$$m_1 \mid x - x' \qquad \& \qquad m_2 \mid x - x'.$$

Logo $m_1 m_2 \mid x - x'$ (pois m_1, m_2 coprimos), ou seja $x \equiv x' \pmod{m_1 m_2}$.

Só isso mesmo.

congruência-mesmo.
Para todo m, $(\equiv_m)$ é uma congruência para as operações $(+), (-), (-), (\cdot)$ dos inteiros.

DEMONSTRAÇÃO.
Sejam a, a', b, b' tais que $a \equiv_m a'$ e $b \equiv_m b'$. Logo $m \mid a-a'$ e $m \mid b-b'$. Logo $m \mid (a-a')+(b-b')$, e logo $m \mid (a+b)-(a'+b')$. Ou seja, $a+b \equiv_m a'+b'$. As outras operações: similar.

coprime-inv.
Sejam a, m inteiros com $(a, m) = 1$. Logo a é invertível (e logo cancelável) módulo m.

DEMONSTRAÇÃO.
Pelo Bézout sejam u, v tais que $1 = au + mv$. Logo $1 - au = mv$, e logo $m \mid 1 - au$, ou seja, $au \equiv_m 1$, ou seja, a é invertível (e logo cancelável) módulo m.

congruências-pow.
Para todo m, e para todo $n \in \mathbb{N}$, $(\equiv_m)$ é compatível com a operação unária $(x \mapsto x^n)$.

DEMONSTRAÇÃO.
Seja m inteiro. Por indução. A BASE é trivial.
PASSO INDUTIVO. Suponha k tal que $(\equiv_m)$ é compatível com a $(x \mapsto x^k)$ (HI). Vou mostrar que $(\equiv_m)$ é compatível com a $(x \mapsto x^{k+1})$ também. Sejam a_1, a_2 tais que $a_1 \equiv_m a_2$. Calculamos:

$$a_1^{k+1} = a_1^k a_1 \equiv_m a_2^k a_1 \equiv_m a_2^k a_2 \equiv_m a_2^{k+1}.$$

(pelas: def. de a_1^{k+1}, H.I., $(\equiv_m)$ compatível com $(\cdot)$, def. de a_2^{k+2})

Teorema de Euler.
Para quaisquer a, m coprimos, temos $a^{\varphi(m)} \equiv_m 1$.

DEMONSTRAÇÃO.
Sejam a, m coprimos. Seja $R = \{r_1, \ldots, r_{\varphi(m)}\}$ um s.r.r. módulo m. Temos: (i) para quaisquer i, j t.q. $ar_i \equiv_m ar_j$, temos $r_i \equiv_m r_j$ (cancelando o a pois é coprimo com m), e logo $i = j$ (pois R s.r.r.); (ii) $(r, m) = 1$ & $(a, m) = 1$ implica $(ar, m) = 1$ e logo todos os membros do aR são coprimos com o m. Pelas (i),(ii) segue que aR também é um s.r.r., e logo:

$$\prod_{r\in R}{}^{1} r \equiv_m \prod_{r\in R} ar \equiv_m a^{\varphi(m)} \prod_{r\in R}{}^{1} r$$

Como todos os membros do R são canceláveis módulo m (pois são coprimos com m), logo seu produto também é. Logo $1 \equiv_m a^{\varphi(m)}$.

product-of-invertibles.
Sejam m inteiro, $n \in \mathbb{N}$ e $u_1, \ldots, u_n$ inteiros invertíveis módulo m. Logo $\prod_{k=1}^{n} i_k$ também é invertível módulo m.

DEMONSTRAÇÃO.
Por indução. BASE: imediato pois $\prod_{k=1}^{0} i_k = 1$ e 1 é invertível.
PASSO INDUTIVO. Seja w tal que $\prod_{k=1}^{w} i_k$ é invertível, e logo seja j o seu inverso módulo m. Vou demonstrar que $\prod_{k=1}^{w+1} i_k$ também é invertível. Seja j_{w+1} um inverso de i_{w+1}. Basta mostrar que $j_{w+1}j$ é um inverso de $\prod_{k=1}^{w+1} i_k$. Calculamos:

$$\begin{aligned}
(\prod_{k=1}^{w+1} i_k)(j_{w+1}j) &\equiv_m (\prod_{k=1}^{w} i_k) i_{w+1} j_{w+1} j && \text{(def. de } \prod_{k=1}^{w} i_k \text{; assoc.)} \\
&\equiv_m (\prod_{k=1}^{w} i_k) j && \text{(pela escolha do } j_{w+1}\text{)} \\
&\equiv_m 1. && \text{(pela escolha do } j\text{)}
\end{aligned}$$