FMC1, 2016.2
(Turmas do Thanos)

Prova 2
(points: 120/100; bonus: $18^{\flat}$; time: 100')

Nome: Θάνος **Gabarito**

23/11/2016

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

VI. Use caneta para tuas respostas.

VII. Escreva teu nome em *cada* folha de rascunho antes de usá-la.

VIII. Entregue *todas* as folhas de rascunho juntas com tua prova.

IX. Nenhuma prova será aceita depois do fim do tempo.

X. Os pontos bônus duma unidade são considerados apenas para quem consiga passar sem.[3]

Boas provas!

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

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

[3] Por exemplo, 25 pontos bonus podem aumentar uma nota final de 5,2 para 7,7 ou de 9,2 para 10,0, mas de 4,9 nem para 7,4 nem para 5,0. A 4,9 ficaria 4,9 mesmo.

(14) # A

(4) **A0.** Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$. Defina formalmente (com fórmulas de lógica) as relações "a divide b" e "a congruente b módulo m". Considere como universo o conjunto de inteiros $\mathbb{Z}$.

DEFINIÇÕES.

$$a \mid b \overset{\triangle}{\iff} \boxed{(\exists k)\,[\,a \cdot k = b\,]}$$

$$a \equiv b \pmod{m} \overset{\triangle}{\iff} \boxed{m \mid a - b}$$

(10) **A1.** Sejam $a, b, c \in \mathbb{Z}$. Considere as proposições:

$$a \mid b + c \;\&\; a \mid b - c \implies a \mid b\,; \tag{i}$$

$$a \mid b + c \;\&\; a \mid b + 2c \implies a \mid b\,. \tag{ii}$$

Para cada uma, se ela é verdadeira, prova-la; se não, ache um contraexemplo.

RESPOSTA.

A (i) é falsa: um contraexemplo seria o $a = 2$, $b = c = 1$. Realmente, temos

$$2 \mid 1 + 1 = 2 \;\&\; 2 \mid 1 - 1 = 0, \qquad \text{mas} \qquad 2 \nmid 1.$$

A (ii) é verdadeira:

$$\left.\begin{matrix} a \mid b + c \implies a \mid 2b + 2c \\ a \mid \;\; b + 2c \end{matrix}\right\} \implies a \mid \underbrace{(2b + 2c) - (b + 2c)}_{b}\,.$$

(42) B

(18) **B1.** Sejam $a, b \in \mathbb{Z}$. Prove que

$$(a, b) = (a, a + b).$$

Dica: *Lembre a definição de m.d.c. e que para $x, y \in \mathbb{N}$, $x \mid y$ e $y \mid x \implies x = y$.*

PROVA.

Sejam $d = (a, b)$ e $d' = (a, a + b)$.
Pela definição, d é divisor comum dos a e b, então $d \mid a$ e $d \mid b$, e logo $d \mid a + b$.
Temos então que d é um divisor comum dos a e $a + b$, e, pela definição de mdc, como $d' = (a, b + c)$, temos $d' \mid d$. Similarmente, $d \mid d'$.
Então $|d| = |d'|$ e como ambós são naturais (parte da definição de (x, y)), temos:

$$(a, b) = d = d' = (a, a + b).$$

(24) **B2.** Prove que para todo $n \in \mathbb{N}$, $(F_n, F_{n+1}) = 1$, onde F_n é o n-ésimo termo da sequência Fibonacci. Lembra-se a definição:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n. \end{aligned}$$

PROVA.

Vamos provar o pedido por indução. Para $n = 0$ temos

$$(F_0, F_1) = (0, 1) = 1.$$

Seja $k \in \mathbb{N}$ tal que $(F_k, F_{k+1}) = 1$.
Precisamos mostrar que $(F_{k+1}, F_{k+2}) = 1$.
Calculando,

$$\begin{aligned} (F_{k+1}, F_{k+2}) &= (F_{k+1}, F_{k+1} + F_k) && \text{(pela definição da } F_n) \\ &= (F_{k+1}, F_k) && \text{(pela } \mathbf{B1}, \text{ com } a \coloneqq F_{k+1},\ b \coloneqq F_k) \\ &= (F_k, F_{k+1}) && \text{(propriedade de mdc)} \\ &= 1 && \text{(pela hipótese indutiva).} \end{aligned}$$

$(50 + 6^\flat)$ # C

(24) **C1.** Prove que para todo $n \in \mathbb{Z}$,

$$13 \mid n(n^6 - 1)(n^6 + 1).$$

Prova.

Seja $n \in \mathbb{Z}$. Calculamos:

$$n(n^6 - 1)(n^6 + 1) = n((n^6)^2 - 1^2) = n(n^{12} - 1) = n^{13} - n.$$

Logo, precisamos mostrar que

$$n^{13} - n \equiv 0 \pmod{13},$$

que, como 13 é primo, segue diretamente pelo teorema de Fermat:

$$\begin{aligned} n^{13} - n &\equiv n - n \pmod{13} \\ &\equiv 0 \pmod{13}. \end{aligned}$$

(26 + 6♭) **C2.** Seja $f : \mathbb{Z}^3 \to \mathbb{Q}$ a função recursiva definida pela equação

$$f(c,x,y) = \begin{cases} c^2 + x + 2y, & \text{se } c \equiv 0 \pmod 3 \\ 2cx + 10y, & \text{se } c \equiv 1 \pmod 3 \\ f(c^2, x^y, y^x), & \text{senão.} \end{cases}$$

(5) (i) Calcule os valores: $f(3,3,8)$, $f(25,8,9)$, $f(-5,2,3)$.

(6♭) (ii) Explique curtamente porque a f sempre termina.

(21) (iii) Prove que para todos $c, x \in \mathbb{Z}$,

$$3 \mid f(c,x,x).$$

Dica: $a \mid b \iff b \equiv 0 \pmod a$.

Resolução.

(i) Calculamos:

$$\begin{aligned} f(3,3,8) &= 3^2 + 3 + 2 \cdot 8 &&= 9 + 3 + 16 = 28 \\ f(25,8,9) &= 2 \cdot 25 \cdot 8 + 10 \cdot 9 &&= 400 + 90 \quad = 490 \\ f(-5,2,3) &= 2 \cdot (-5) \cdot 2 + 10 \cdot 3 = -20 + 30 \quad &&= 10. \end{aligned}$$

(ii) Porque $2^2 \equiv 1 \pmod 3$: a única chamada recursiva da $f(c,x,y)$ é quando o seu primeiro argumento c é congruente 2 módulo 3, e nesse caso ela se-chama com primeiro argumento c^2, que será congruente 1 módulo 3, e a função retorna diretamente o seu valor.

(iii) Sejam $c, x \in \mathbb{Z}$. Vamos provar que $f(c,x,x) \equiv 0 \pmod 3$.
Consideramos os casos:

Caso $c \equiv 0 \pmod 3$: Calculamos:

$$\begin{aligned} f(c,x,x) &= c^2 + x + 2x \\ &= c^2 + 3x \\ &\equiv 0^2 + 0x \pmod 3 \\ &\equiv 0 \pmod 3. \end{aligned}$$

Caso $c \equiv 1 \pmod 3$: Calculamos:

$$\begin{aligned} f(c,x,x) &= 2cx + 10x \\ &\equiv 2x + 10x \pmod 3 \\ &\equiv 12x \pmod 3 \\ &\equiv 0 \pmod 3. \end{aligned}$$

Caso $c \equiv 2 \pmod 3$: Temos

$$\begin{aligned} f(c,x,x) &= f(c^2, x^x, x^x) && \text{(pela definição da } f) \\ &\equiv f(2^2, x^x, x^x) \pmod 3 && (c \equiv 2 \pmod 3) \\ &\equiv f(4, x^x, x^x) \pmod 3 \\ &\equiv 0 \pmod 3 && \text{(pelo caso anterior).} \end{aligned}$$

Em todos os casos, $f(c,x,x) \equiv 0 \pmod 3$, ou seja, $3 \mid f(c,x,x)$.

(10) **D**

Ache um inteiro *positivo* $z > 0$ que satisfaz a congruência:

$$13z \equiv 1 \pmod{50}.$$

Dica: *Euclides!*

Resolução.

Usando o algoritmo (extendido) de Euclides, temos:

$$\begin{aligned} 50 &= 3 \cdot 13 + 11 \\ 13 &= 1 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 \ \ + 1 \\ 2 &= 2 \cdot 1 \ \ + 0. \end{aligned}$$

Então $(50, 13) = 1$ e temos:

$$\begin{aligned} 1 &= \underline{11} - 5 \cdot \underline{2} \\ &= \underline{11} - (\underline{13} - \underline{11}) \cdot 5 \\ &= 6 \cdot \underline{11} - 5 \cdot \underline{13} \\ &= 6 \cdot (\underline{50} - 3 \cdot \underline{13}) - 5 \cdot \underline{13} \\ &= 6 \cdot \underline{50} - 18 \cdot \underline{13} - 5 \cdot \underline{13} \\ &= 6 \cdot \underline{50} - 23 \cdot \underline{13}. \end{aligned}$$

Logo,

$$\begin{aligned} 1 &\equiv 6 \cdot 50 - 23 \cdot 13 \pmod{50} \\ &\equiv 6 \cdot 0 \ \ - 23 \cdot 13 \pmod{50} \\ &\equiv \qquad - 23 \cdot 13 \pmod{50}, \end{aligned}$$

e o inteiro -23 satisfaz a congruência desejada, mas ele é negativo. Então escolhemos como z qualquer positivo congruente com ele, por exemplo o $z := -23 + 50 = 27$:

$$1 \equiv 27 \cdot 13 \pmod{50}.$$

(4 + 12♭) # E

Seja $C \subseteq \mathbb{Z}$ um conjunto cujos elementos são coprimos dois a dois.

(4) **E0.** Descreva formalmente (com uma fórmula de lógica) o que significa a frase:

"*os elementos do C são coprimos dois a dois*".

FÓRMULA: $(\forall x, y \in C)\,[\,x \neq y \to (x, y) = 1\,]$

(12♭) **E1.** Ache uma infinidade de conjuntos infinitos com essa propriedade.

RESOLUÇÃO.

Seja $P = \{p_0, p_1, p_2, \dots\}$ onde

$$p_0 < p_1 < p_2 < \dots$$

a sequência de todos os primos, e defina a sequência de conjuntos

$$C_i \triangleq \{p_j \mid j \in \mathbb{N}, j \geq i\}\,.$$

Assim, temos a sequência infinita de tais conjuntos:

$$\begin{aligned} C_0 &= \{p_0, p_1, p_2, p_3, \dots\} = P \\ C_1 &= \{p_1, p_2, p_3, p_4, \dots\} \\ C_2 &= \{p_2, p_3, p_4, p_5, \dots\} \\ C_3 &= \{p_3, p_4, p_5, p_6, \dots\} \\ &\vdots \end{aligned}$$

Como o conjunto dos primos é infinito, cada um dos C_i's é infinito também e obviamente satisfaz a propriedade desejada.

Outra infinidade de tais conjuntos ganhamos se, para $i \in \mathbb{N}$ definir

$$P_i \triangleq P \setminus \{p_i\}\,.$$

Assim temos outra sequência infinita de tais conjuntos:

$$\begin{aligned} P_0 &= \{\quad p_1, p_2, p_3, p_4, \dots\} \\ P_1 &= \{p_0, \quad p_2, p_3, p_4, \dots\} \\ P_2 &= \{p_0, p_1, \quad p_3, p_4, \dots\} \\ P_3 &= \{p_0, p_1, p_2, \quad p_4, \dots\} \\ &\vdots \end{aligned}$$

Só isso mesmo.