FMC2, 2017.1
(Turmas do Thanos)

Provinha 0
(points: 0; bonus: $0^\flat$; time: 60')

Alun∗: **Turma:**

15/02/2017

(Responda em todas as A, B, C, D, e **em apenas uma** das I e J.)

A

A1. Escreva uma definição certa e formal (em português matemático) da palavra "*par*". Não assume que o leitor já saiba o significado das palavras: "*sistema de numeração*", "*ímpar*", "*divisão*", "*divide*", "*módulo*".
DEFINIÇÃO.

Um inteiro n é *par* sse existe inteiro k tal que $n = 2k$.

A2. Usando uma fórmula, expresse o significado da frase *"o x é irracional"*.
Considere como universo o $\mathbb{R}$ e seus subconjuntos. Alem dos símbolos "padrão" de lógica, podes usar apenas os símbolos:

$$0, 1, 2, +, >, \cdot, \in, \mathbb{N}, \mathbb{Z}.$$

FÓRMULA: $x \in \mathbb{R} \land \neg\,\exists p \exists q\,[\,p \in \mathbb{Z} \land q \in \mathbb{Z} \land \neg(q = 0) \land x \cdot q = p\,]$

B

Considere os inteiros $1, 2, \ldots, 30$.

B1. De quantas maneiras podemos os permutar?

RESPOSTA: $30!$

B2. Quantas delas deixam cada múltiplo de 5 no seu lugar?

RESPOSTA: $(30 - 6)! = 24!$

C

Sejam $a, b, c \in \mathbb{Z}$. Prove que

(i) $a \mid a$;

(ii) $a \mid b \;\&\; a \mid c \implies a \mid b + c$;

(iii) $a \mid b \;\&\; b \mid c \implies a \mid c$.

PROVA.

(i) Como $a \cdot 1 = a$ e $1 \in \mathbb{Z}$, temos $a \mid a$.
(ii) Suponha que $a \mid b$ e $a \mid c$. Logo, temos $as = b$ e $at = c$ para alguns $s, t \in \mathbb{Z}$. Precisamos mostrar que $a \mid b + c$. Calculamos:

$$\begin{aligned} b + c &= as + at \\ &= a(s + t) \end{aligned}$$

e como $s + t \in \mathbb{Z}$, chegamos no desejado $a \mid b + c$.
(iii) Suponha que $a \mid b$ e $b \mid c$. Logo, temos $au = b$ e $bv = c$ para alguns $u, v \in \mathbb{Z}$. Precisamos mostrar que $a \mid c$. Realmente temos

$$\begin{aligned} c &= bv \\ &= (au)v \\ &= a(uv) \end{aligned}$$

que mostra que $a \mid c$, porque $uv \in \mathbb{Z}$.

D

Prove que para todo $n \in \mathbb{Z}$, se $3 \nmid n$ então $3 \mid n^2 - 1$.

PROVA.

Prova 1: Seja $n \in \mathbb{Z}$ tal que $3 \nmid n$. Observe que $n^2 - 1 = n^2 - 1^2 = (n+1)(n-1)$. Observe também que os inteiros $n - 1$, n, $n + 1$ são 3 inteiros consecutivos, então sabemos que o 3 divide exatamente um deles. Como 3 *não* divide o n (pela hipótese), concluimos que divide um dos $n - 1$ e $n + 1$, e logo divide o produto $(n + 1)(n - 1)$: $3 \mid (n + 1)(n - 1) = n^2 - 1$.

Prova 2: Seja $n \in \mathbb{Z}$ tal que $3 \nmid n$. Preciso mostrar que $3 \mid n^2 - 1$.
Como $3 \nmid n$, existem dois casos:

CASO 1: $n = 3k + 1$, para algum $k \in \mathbb{Z}$.

Logo, $$\begin{aligned} n^2 - 1 &= (3k + 1)^2 - 1 \\ &= (9k^2 + 6k + 1) - 1 \\ &= 9k^2 + 6k \\ &= 3(3k^2 + 2k). \end{aligned}$$

Como $3k^2 + 2k \in \mathbb{Z}$, temos que $3 \mid n^2 - 1$.

CASO 2: $n = 3k + 2$, para algum $k \in \mathbb{Z}$.

Logo, $$\begin{aligned} n^2 - 1 &= (3k + 2)^2 - 1 \\ &= (9k^2 + 12k + 4) - 1 \\ &= 9k^2 + 12k + 3 \\ &= 3(3k^2 + 4k + 1), \end{aligned}$$

e, como $3k^2 + 4k + 1 \in \mathbb{Z}$, temos que $3 \mid n^2 - 1$.

I

Os *números Fibonacci* são definidos recursivamente assim:

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

Prove que para todo $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1. \tag{$*$}$$

Prova.

Vou provar o teorema por indução no n.

Para $n = 0$ (base da indução), preciso verificar que os dois lados da $(*)$ são iguais. Realmente são:

$$\sum_{i=0}^{0} F_i = F_0 = 0$$

$$F_{0+2} - 1 = F_2 - 1 = (F_1 + F_0) - 1 = (1 + 0) - 1 = 0.$$

Seja $k \in \mathbb{N}$ tal que

$$\sum_{i=0}^{k} F_i = F_{k+2} - 1. \tag{H.I.}$$

Preciso provar que

$$\sum_{i=0}^{k+1} F_i = F_{(k+1)+2} - 1.$$

Realmente

$$\begin{aligned} \sum_{i=0}^{k+1} F_i &= \left(\sum_{i=0}^{k} F_i\right) + F_{k+1} && \text{(def. de somatório)} \\ &= (F_{k+2} - 1) + F_{k+1} && \text{(H.I.)} \\ &= (F_{k+2} + F_{k+1}) - 1 && \text{(associatividade e comutatividade de +)} \\ &= F_{k+3} - 1. && \text{(def. de } F_n\text{),} \end{aligned}$$

J

J1. Para cada um dos inteiros 24, 3, 1, e 0, escreve ele como produtório de prímos se é possível; senão, explique o porquê.

Resposta.

$24 = 2 \cdot 2 \cdot 2 \cdot 3$.
3 é um produtorio de primos, de tamanho 1! (Podemos escrever $3 = \prod_{i=1}^{1} 3$.)
1 é um produtorio (de primos!) de tamanho 0, o produtório vazio! (Podemos escrever $1 = \prod_{i=1}^{0} 3$.)

Mas o inteiro 0 não pode ser escrito como produtório de primos, porque um produtório é igual 0 sse pelo menos um termo dele é o 0; e o 0 não é primo.

J2. Prove que cada $n \in \mathbb{N}$ com $n > 1$ pode ser escrito como produtório de primos.

Dica: *Princípio da indução finita forte* (PIFF), ou *princípio da boa ordem* (PBO).

Prova.

Prova usando o PIFF: Caso que n seja primo, trivialmente ele mesmo é um produtório de primos (um produtório de tamanho 1).

Caso contrário, $n = ab$, para alguns $a, b \in \mathbb{N}$ com $1 < a < n$ e $1 < b < n$, logo podemos assumir (hipotese indutiva) que cada um deles pode ser escrito na forma desejada:

$$a = p_1 p_2 \cdots p_{k_a}, \qquad \text{para alguns } p_i\text{'s primos;}$$
$$b = q_1 q_2 \cdots q_{k_b}, \qquad \text{para alguns } q_j\text{'s primos.}$$

Então temos $n = ab = (p_1 p_2 \cdots p_{k_a})(q_1 q_2 \cdots q_{k_a}) = p_1 p_2 \cdots p_{k_a} q_1 q_2 \cdots q_{k_b}$,
que realmente é um produtório de primos.

Prova usando o POB: Considere o conjunto C de todos os inteiros $n > 1$ que *não* podem ser escritos como produtório de primos. Queremos mostrar que $C = \emptyset$.

Para chegar num absurdo, suponha que C tem elementos e (pelo PBO) seja $m = \min C$ o menor deles, ou seja, m é o menor natural que não pode ser escrito como produtório de primos. Então m com certeza não é primo: se fosse primo, ele mesmo seria um produtório de primos (de tamanho 1).

Logo, $m = ab$ para alguns $a, b \in \mathbb{N}$ com $1 < a < m$ e $1 < b < m$. Como m foi o menor natural que não pode ser escrito como produtório de primos, e ambos os naturais a e b são menores de m, então ambos podem ser escritos como produtórios de primos:

$$a = p_1 p_2 \cdots p_{k_a}, \qquad \text{para alguns } p_i\text{'s primos;}$$
$$b = q_1 q_2 \cdots q_{k_b}, \qquad \text{para alguns } q_j\text{'s primos.}$$

Agora conseguimos escrever o m como produtório de primos:

$$m = ab = (p_1 p_2 \cdots p_{k_a})(q_1 q_2 \cdots q_{k_a}) = p_1 p_2 \cdots p_{k_a} q_1 q_2 \cdots q_{k_b},$$

contradizendo sua definição. Chegando nesse absurdo podemos concluir que realmente $C = \emptyset$, que foi o que queriamos provar.