SOCIEDADE BRASILEIRA DE MATEMÁTICA
MESTRADO PROFISSIONAL EM REDE NACIONAL
PROFMAT

GABARITO da 3ª Avaliação Nacional de Aritmética - MA14 - 21/12/2013

Questão 1. *(pontuação: 2)*

(1,0) a) Enuncie e demonstre o Teorema Fundamental da Aritmética.

(1,0) b) Encontre os possíveis valores de m, $n \in \mathbb{Z}$ tais que o número $9^m 10^n$ tenha 243 divisores.

Uma solução:

a) **Teorema Fundamental de Aritmética em** $\mathbb{N}$: Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

A demonstração é feita usando-se a segunda forma do Princípio de Indução Finita. Se $n = 2$, o resultado é óbvio, pois 2 é primo.

Suponhamos que o resultado seja válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1.n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$. Portanto $n = p_1...p_r.q_1...q_s$.

Vamos provar a unicidade da escrita: se $n = p_1...p_r = q_1...q_s$, sendo p_i e q_j números primos, $i = 1, ...r$, $j = 1, ..., s$, como $p_1|q_1...q_s$, segue que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto $p_2...p_r = q_2...q_s$. Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

Uma outra formulação deste teorema é a seguinte:

Teorema Fundamental de Aritmética em $\mathbb{Z}$: Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < p_2, ... < p_r$ e $\alpha_1, \alpha_2, ..., \alpha_r \in \mathbb{N}$, univocamente determinados, tais que

$$n = \pm p_1^{\alpha_1}...p_r^{\alpha_r}.$$

A demonstração é essencialmente a mesma do teorema anterior, agrupando os fatores primos repetidos e ordenando os primos em ordem crescente.

b) Temos que $9^m 10^n = 3^{2m} 2^n 5^n$. Desta forma, o número de divisores de $9^m 10^n$ é $(2m+1)(n+1)^2$: Como $243 = 3^5$; devemos encontrar os pares de soluções inteiras $(m; n)$ da equação $(2m+1)(n+1)^2 = 3^5$.

Em $\mathbb{Z}$, temos apenas as seguintes possibilidades:

$2m + 1 = 3$ e $(n + 1)^2 = 3^4$, ou seja, $m = 1$ e $n = 8$;

$2m + 1 = 3^3$ e $(n + 1)^2 = 3^2$, ou seja, $m = 13$ e $n = 2$;

$2m + 1 = 3^5$ e $(n + 1)^2 = 1$, ou seja, $m = 121$ e $n = 0$.

Logo os pares (m, n) são $(1, 8)$, $(13, 2)$ e $(121, 0)$.

Questão 2. *(pontuação: 2)*

(1,0) a) Enuncie e demonstre o Teorema Chinês dos Restos.

(1,0) b) Dispomos de uma quantia em reais menor do que $R\$\,3\,000,00$. Se distribuirmos essa quantia entre 11 pessoas, sobra $R\$\,1,00$. Se a distribuirmos entre 12 pessoas, sobram $R\$\,2,00$ e se a distribuirmos entre 13 pessoas, sobram $R\$\,3,00$. De quantos reais dispomos?

Uma solução:

a) **Teorema Chinês dos Restos**: O sistema

$$\begin{cases} X \equiv c_1 \bmod n_1 \\ X \equiv c_2 \bmod n_2 \\ \dots \\ X \equiv c_r \bmod n_r \end{cases}$$

em que $(n_i, n_j) = 1$, para todo par n_i, n_j, com $i \neq j$, possui uma única solução módulo $N = n_1 n_2 ... n_r$. Tal solução pode ser obtida por:

$$x = N_1 y_1 c_1 + \cdots + N_r y_r c_r,$$

sendo $N_i = \dfrac{N}{n_i}$ e y_i solução de $N_i Y \equiv 1 \bmod n_i$, $i = 1, ..., r$.

A demonstração é a seguinte:

Como $n_i | Nj$, se $i \neq j$, e $N_i y_i \equiv 1 \bmod n_i$ então

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + \cdots N_r y_r c_r + \equiv N_i y_i c_i \equiv c_i \bmod n_i$$

Isto mostra que x é solução do sistema.

Suponhamos agora que x' seja uma outra solução do sistema. Então

$$x \equiv x' \bmod n_i, \ \forall i, \ i = 1, \dots r.$$

Como $(n_i, n_j) = 1$, para $i \neq j$, segue que $[n_1, n_2, \dots, n_r] = n_1 n_2 \cdots n_r = N$ e, portanto, $x \equiv x' \bmod N$.

b)

Denote por x a quantia procurada. Usando os dados do problema, vemos que $x = 11n_1 + 1 = 12n_2 + 2 = 13n_3 + 3$.

Essa cadeia de equações é equivalente ao sistema de congruências lineares

$$\begin{cases} X \equiv 1 \bmod 11 \\ X \equiv 2 \bmod 12 \\ X \equiv 3 \bmod 13 \end{cases}$$

Como $(11, 12) = 1$, $(11, 13) = 1$, $(12, 13) = 1$; usando o Teorema Chinês dos Restos, vemos que as soluções do sistema de congruências acima são dadas por

$$X = 12.13.y_1 + 11.13.y_2 + 11.12.y_3 + 11.12.13.t = 156y_1 + 286y_2 + 396y_3 + 1716t, \quad t \in \mathbb{Z},$$

em que y_1, y_2 e y_3 são soluções das congruências $156Y \equiv 1 \bmod 11$, $143Y \equiv 1 \bmod 12$, $132Y \equiv 1 \bmod 13$, respectivamente. Resolvendo-as, encontramos as soluções respectivas: $y_1 = -5$, $y_2 = -1$ e $y_3 = -6$.

Desta forma, as soluções do sistema são

$$x = 156.(-5) + 286.(-1) + 396.(-6) + 1716t = -3442 + 1716t, \quad t \in \mathbb{Z}$$

Se $t \leq 2$, então $x < 0$, o que não nos fornece soluções válidas para o problema proposto. Para $t = 3$ temos $x = R\$\,1\,706,00$. Para $t \geq 4$ temos $x > 3\,000,00$, o que também não nos fornece soluções válidas para o problema. Logo a única solução possível é $x = R\$\,1\,706,00$. De fato,

$$1706 = 155.11 + 1$$

$$1706 = 142.12 + 2$$

$$1706 = 131.13 + 3$$

Logo $R\$\,1\,706,00$ é a quantia procurada.

Questão 3. *(pontuação: 2)*

Numa criação de galinhas e coelhos, contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?

Uma solução:

Denote por C o número de coelhos e por G o número de galinhas. Como cada coelho tem 4 pés e cada galinha tem 2 pés, temos $4C + 2G = 400$, que é equivalente à equação $2C + G = 200$. A equação diofantina $2C + G = 1$ tem, como uma das soluções, $C = 1$ e $G = -1$. Desta forma, as soluções de $2C + G = 200$ (logo de $4C + 2G = 400$), são:

$$C = 200 - t \quad \text{e} \quad G = -200 + 2t, \quad t \in \mathbb{Z}$$

Como $C \geq 0$ e $G \geq 0$; as soluções admissíveis ocorrem para $100 \leq t \leq 200$. A diferença entre C e G é

$$C - G = 400 - 3t.$$

Como $400 = 3.133 + 1$, segue que a diferença mínima ocorre para $t = 133$, para o qual $C - G = 1$. Neste caso, temos $C = 67$ coelhos e $G = 66$ galinhas.

Questão 4. *(pontuação: 2)*

Mostre que $n^7 - n$ é divisível por 7 para todo $n \in \mathbb{Z}$.

Uma solução:

Inicialmente, note que

$$n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = n(n - 1)(n^2 + n + 1)(n + 1)(n^2 - n + 1)$$

.

Basta analisar as possíveis congruências módulo 7:

Se $n \equiv 0 \bmod 7$, então, observando a decomposição acima, vemos que $n^7 - n \equiv 0 \bmod 7$.

Se $n \equiv 1 \bmod 7$, então $n-1 \equiv 0 \bmod 7$ e, novamente observando a decomposição acima, vemos que $n^7-n \equiv 0 \bmod 7$.

Analogamente, temos:

Se $n \equiv 2 \bmod 7$, então $n^2 + n + 1 \equiv 0 \bmod 7$ e, portanto, $n^7 - n \equiv 0 \bmod 7$.

Se $n \equiv 3 \bmod 7$, então $n^2 - n + 1 \equiv 0 \bmod 7$ e, portanto, $n^7 - n \equiv 0 \bmod 7$.

Se $n \equiv 4 \bmod 7$, então $n^2 + n + 1 \equiv 0 \bmod 7$ e, portanto, $n^7 - n \equiv 0 \bmod 7$.

Se $n \equiv 5 \bmod 7$, então $n^2 - n + 1 \equiv 0 \bmod 7$ e, portanto, $n^7 - n \equiv 0 \bmod 7$.

Se $n \equiv 6 \bmod 7$, então $n + 1 \equiv 0 \bmod 7$ e, portanto, $n^7 - n \equiv 0 \bmod 7$.

Em qualquer caso, $n^7 - n$ é divisível por 7, $n \in \mathbb{Z}$.

Questão 5. *(pontuação: 2)*

a) Seja u_n o n-ésimo termo da sequência de Fibonacci. Mostre que

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{bmatrix}$$

e conclua que $u_{n-1}u_{n+1} = u_n^2 + (-1)^n$.

Uma solução:

a)

Para $n = 2$, temos

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} u_3 & u_2 \\ u_2 & u_1 \end{bmatrix}$$

Suponhamos que a afirmação seja válida para algum $n \in \mathbb{N}$. Vamos mostrar a sua validade para $n + 1$. Usando a hipótese de indução, temos

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Logo

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n+1} = \begin{bmatrix} u_{n+1} + u_n & u_{n+1} \\ u_n + u_{n-1} & u_n \end{bmatrix} = \begin{bmatrix} u_{n+2} & u_{n+1} \\ u_{n+1} & u_n \end{bmatrix}$$

Desta forma, usando o Princípio de Indução, concluímos que

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = \begin{bmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{bmatrix}$$

é válido para todo $n \in \mathbb{N}$.

Vamos agora demonstrar a validade de $u_{n-1}u_{n+1} = u_n^2 + (-1)^n$.

Calculando o determinante das matrizes acima e usando o fato que $\det(A^n) = (\det A)^n$; vemos que

$$\det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n\right) = \det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)^n = \det \begin{bmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{bmatrix}$$

ou seja, $(-1)^n = u_{n+1}u_{n-1} - u_n^2$, como queríamos demonstrar.

b)

Prove a fórmula de Leibniz

$$(a_1 + a_2 + ... + a_m)^n = \sum_{i_1+i_2+...+i_m=n} \frac{n!}{i_1!i_2!...i_m!} a_1^{i_1} a_2^{i_2} ... a_m^{i_m}, \quad a_1, a_2, ..., a_m \in \mathbb{R}.$$

Observação: Se achar necessário, para facilitar, assuma a validade da fórmula do Binômio de Newton.

Uma solução:

Vamos aplicar indução em m: Para $m = 1$; a fórmula é óbvia. Suponhamos que a fórmula seja válida para m. Vamos mostrar sua validade para $m + 1$. Usando a Fórmula do Binômio de Newton, vemos que

$$(a_1 + a_2 + ... + a_{m+1})^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}(a_1 + a_2 + ... + a_m)^k a_{m+1}^{n-k}$$

e, a seguir, a hipótese de indução, obtemos:

$$(a_1 + a_2 + ... + a_{m+1})^n = \sum_{k=0}^{n} \quad \sum_{i_1+i_2+...+i_m=k} \frac{n!}{k!(n-k)!} \frac{k!}{i_1!i_2!...i_m!} a_1^{i_1} a_2^{i_2} ... a_m^{i_m} a_{m+1}^{n-k}$$

Como $i_1 + ... + i_m = k \Rightarrow i_1 + ... + i_m + (n-k) = n$ e como k assume todos os valores inteiros de 0 a n, denotando por $i_{m+1} = n - k$, temos

$$\begin{aligned}(a_1 + a_2 + ... + a_{m+1})^n &= \sum_{i_1+i_2+...+i_m+(n-k)=n} \frac{n!}{i_1!i_2!...i_m!(n-k)!} a_1^{i_1} a_2^{i_2} ... a_m^{i_m} a_{m+1}^{n-k} \\ &= \sum_{i_1+i_2+...+i_m+i_{m+1}=n} \frac{n!}{i_1!i_2!...i_m!i_{m+1}!} a_1^{i_1} a_2^{i_2} ... a_m^{i_m} a_{m+1}^{i_{m+1}}\end{aligned}$$

Desta forma, usando o Princípio de Indução, concluímos que a fórmula de Leibniz é verdadeira para todo $m \in \mathbb{N}$.