# Segunda Prova de Aritmética - MA14

## GABARITO

## 2012/2º semestre

**Questão 1**

Sejam $n \in \mathbb{Z}$ e $p$ um número primo. Denota-se com $E_p(n)$ o expoente da maior potência de $p$ que divide $n$.

a) Justifique a seguinte afirmação sobre dois números naturais $m$ e $n$:

$$m = n \iff E_p(m) = E_p(n) \text{ para todo número primo } p.$$

b) Sejam $a, b, c \in \mathbb{N}$. Mostre que

$$[a, b, c]^2(a, b)(a, c)(b, c) = (a, b, c)^2[a, b][a, c][b, c]$$

**Sugestão:** *Note que dada a simetria dessa expressão em a, b e c, pode-se supor sem perda de generalidade que* $E_p(a) \leqslant E_p(b) \leqslant E_p(c)$.

**Uma solução:**

a) A menção ao Teorema Fundamental da Aritmética já deveria garantir metade da pontuação do ítem.

Se $n = m$ é óbvio que $E_p(m) = E_p(n)$ para todo número primo $p$. A seguir, provaremos a implicação contrária.

Pelo Teorema Fundamental da Aritmética, podemos escrever $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ e $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, com $\{p_1, \ldots, p_r\}$ e $\{q_1, \ldots, q_s\}$ dois conjuntos formados por números primos, dois a dois distintos em cada um dos conjuntos anteriores.

Como

$$\{p\,;p \text{ é primo e } E_p(m) > 0\} = \{p_1, \ldots, p_r\}$$

e

$$\{p\,;p \text{ é primo e } E_p(n) > 0\} = \{q_1, \ldots, q_s\},$$

segue-se que

$$\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}.$$

Assim, $r = s$ e, após reordenar os elementos $q_1, \ldots, q_r$, podemos supor $q_i = p_i$, para $i = 1, \ldots, r$. Como

$$\alpha_i = E_{p_i}(m) = E_{p_i}(n) = \beta_i, \quad i = 1, \ldots, r,$$

conclui-se que $n = m$.

b) Pelo fato desta expressão ser simétrica em $a$, $b$ e $c$, podemos supor que $E_p(a) \leqslant E_p(b) \leqslant E_p(c)$. Portanto,

$$E_p\big([a, b, c]^2(a, b)(a, c)(b, c)\big) = 2E_p(c) + 2E_p(a) + E_p(b). \tag{1}$$

Por outro lado,

$$E_p\big((a, b, c)^2[a, b][a, c][b, c]\big) = 2E_p(a) + E_p(b) + 2E_p(c). \tag{2}$$

O resultado segue de a), usando-se (1) e (2), já que, para todo $p$ primo,

$$E_p\big([a, b, c]^2(a, b)(a, c)(b, c)\big) = E_p\big((a, b, c)^2[a, b][a, c][b, c]\big).$$

**Questão 2**

Mostre que

a) $7|3^{2n+1}+2^{n+2}$ b) $37|3\underbrace{00\ldots0}_{3n}7$

**Uma solução:**

a) Como $9 \equiv 2 \mod 7$, temos que

$$3^{2n+1} = 3\cdot(3^2)^n \equiv 3\cdot 9^n \equiv 3\cdot 2^n \mod 7.$$

Por outro lado, como $2^{n+2} = 4\cdot 2^n$, segue-se que

$$3^{2n+1}+2^{n+2} \equiv 3\cdot 2^n + 4\cdot 2^n = 7\cdot 2^n \equiv 0 \mod 7.$$

b) Temos que

$$3\underbrace{00\ldots0}_{3n}7 = 3\cdot 10^{3n+1}+7 = 3\cdot 10\cdot 10^{3n}+7 = 30\cdot 10^{3n}+7.$$

Mas, como $10^3 \equiv 1 \bmod 37$, temos que

$$10^{3n} = (10^3)^n \equiv 1 \mod 37,$$

logo

$$3\underbrace{00\ldots0}_{3n}7 = 30\cdot 10^{3n}+7 \equiv 37 \equiv 0 \mod 37.$$

**Questão 3**

Considere os números da forma

$$\alpha_n = \frac{10^n-1}{9}.$$

a) Mostre que $9|\alpha_n \iff 9|n$.

b) Mostre que $11|\alpha_n \iff n$ é par.

**Uma solução:**

Podemos escrever

$$\alpha_n = \frac{10^n-1}{9} = \frac{10^n-1}{10-1} = 10^{n-1}+\cdots+10+1.$$

a) Como $10 \equiv 1 \mod 9$ temos que

$$\alpha_n = 10^{n-1}+\cdots+10+1 \equiv n \mod 9,$$

logo $\alpha_n \equiv 0 \bmod 9$ se, e somente se, $n \equiv 0 \bmod 9$.

b) Note que $10 \equiv -1 \mod 11$, logo $10^n \equiv (-1)^n$. Portanto,

$$\alpha_n = 1+10+\cdots+10^{n-1} \equiv 1-1+1\cdots+(-1)^{n-1} \mod 11.$$

Consequentemente, $\alpha_n \equiv 0 \mod 11$ se, e somente se, $n$ é par.

**Questão 4**

Ache todos os números que deixam resto 2, quando divididos por 7, deixam resto 3, quando divididos por 11 e deixam resto 5, quando divididos por 13. Aponte a menor solução positiva.

**Uma solução:**

Definindo $N = 7 \times 11 \times 13 = 1001$, $N_1 = 11 \times 13 = 143$, $N_2 = 7 \times 13 = 91$ e $N_3 = 7 \times 11 = 77$, temos que resolver cada uma das congruências: $143Y \equiv 1 \mod 7$, $91Y \equiv 1 \mod 11$ e $77Y \equiv 1 \mod 13$

Como $143 \equiv 3 \mod 7$, $91 \equiv 3 \mod 11$ e $77 \equiv 12 \equiv -1 \mod 13$, essas congruências são equivalentes às seguintes: $3Y \equiv 1 \mod 7$, $3Y \equiv 1 \mod 11$ e $Y \equiv -1 \mod 13$, que possuem as seguintes soluções: $y_1 = 5$, $y_2 = 4$ e $y_3 = 12$.

Assim, pelo Teorema Chinês dos Restos, uma solução é dada por

$$x = N_1 y_1 \times 2 + N_2 y_2 \times 3 + N_3 y_3 \times 5 = 1430 + 1092 + 4620 = 7142.$$

Essa solução é única módulo $N = 1001$. Assim, todas as soluções são

$$7142 + t1001, \quad t \in \mathbb{Z}.$$

A solução positiva mínima é o resto da divisão de 7142 por 1001, que é igual a 135.

**Questão 5**

Seja $\varphi$ a função de Euler que associa a cada número natural $m > 1$ o número de inteiros entre 0 e $m$ que são primos com $m$. Mostre que

a) Se $m > 2$, então $\varphi(m)$ é par. Conclua, nessas condições, que $\mathbb{Z}_m$ tem sempre um número par de elementos invertíveis.

b) O número de elementos invertíveis de $\mathbb{Z}_{2m}$ é igual ao número de elementos invertíveis de $\mathbb{Z}_m$, se $m$ é ímpar, e igual ao dobro desse número, se $m$ é par.

c) Mostre que o número de elementos invertíveis de $\mathbb{Z}_{m^2}$ é $m$ vezes o número de elementos invertíveis de $\mathbb{Z}_m$.

d) Relacione o número de elementos invertíveis de $\mathbb{Z}_{m^r}$ com o número de elementos invertíveis de $\mathbb{Z}_m$, sendo $r$ um inteiro positivo.

**Uma solução:**

Observe inicialmente que o número de elementos invertíveis de $\mathbb{Z}_m$ é igual a $\varphi(m)$. Sabemos que se $m = 2^r p_1^{r_1} \cdots p_s^{r_s}$, então

$$\varphi(m) = 2^{r-1}(2-1)p_1^{r_1-1} \cdots p_s^{r_s-1}(p_1 - 1) \cdots (p_s - 1).$$

a) Se $m > 2$, então $r > 2$ ou $s \geqslant 1$. Em qualquer das duas situações $\varphi(m)$ é par, pois uma das parcelas é par.

b) Segue da seguinte afirmação:

$$\varphi(2m) = \begin{cases} \varphi(m), & \text{se } m \text{ é ímpar} \\ 2\varphi(m), & \text{se } m \text{ é par.} \end{cases}$$

(basta escrever a expressão de $\varphi(2m)$).

c) é um caso particular de d).

d) Escrevendo a expressão de $\varphi(m^r)$, $r > 0$, segue imediatamente que

$$\varphi(m^r) = m^{r-1}\varphi(m).$$

Logo, o número de elementos invertíveis de $\mathbb{Z}_{m^r}$ é igual a $m^{r-1}$ vezes o número de elementos invertíveis de $\mathbb{Z}_m$.