Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução da 1ª Frequência

16 de Novembro de 2005

---

1. (4,5 valores)

Seja $P(n)$ a afirmação de variável natural n indicada no enunciado.

- A afirmação $P(1)$ é verdadeira porque

$$1 \times 2 \times 3 = 6 = \frac{1 \times 2 \times 3 \times 4}{4}\,.$$

- Seja $k \in \mathbb{N}$ e suponha-se que $P(k)$ é verdadeira, isto é, suponha-se que

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + k(k+1)(k+2) = \frac{k(k+1)(k+2)(k+3)}{4}\,.$$

Pretende provar-se que $P(k+1)$ é verdadeira, isto é, que

$$1{\times}2{\times}3{+}2{\times}3{\times}4{+}\cdots{+}k(k{+}1)(k{+}2){+}(k{+}1)(k{+}2)(k{+}3) = \frac{(k+1)(k+2)(k+3)(k+4)}{4}\,.$$

Usando a hipótese de indução obtém-se

$$\begin{aligned} 1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + k(k+1)(k+2) + (k+1)(k+2)(k+3) = & \\ = \ & \frac{k(k+1)(k+2)(k+3)}{4} + (k+1)(k+2)(k+3) \\ = \ & (k+1)(k+2)(k+3)\left(\frac{k}{4}+1\right) \\ = \ & (k+1)(k+2)(k+3)\frac{k+4}{4} \\ = \ & \frac{(k+1)(k+2)(k+3)(k+4)}{4}\,. \end{aligned}$$

Mostrou-se assim que $P(1)$ é uma afirmação verdadeira e que, para $k \in \mathbb{N}$, qualquer, se $P(k)$ é uma afirmação verdadeira então também o é a afirmação $P(k+1)$. O princípio de indução matemática permite concluir que a afirmação $P(n)$ é verdadeira, para todo o $n \in \mathbb{N}$.

---

2. (4 valores)
Use-se o algoritmo de Euclides para calcular $(2124, 396)$.

Tem-se $2124 = 5 \times 396 + 144$, $396 = 2 \times 144 + 108$, $144 = 1 \times 108 + 36$ e $108 = 3 \times 36$. Então $(2124, 396) = 36$ e, das igualdades anteriores, obtém-se

$$\begin{aligned} 36 &= 144 - 108 \\ &= 144 - (396 - 2 \times 144) \\ &= 3 \times 144 - 396 \\ &= 3(2124 - 5 \times 396) - 396 \\ &= 3 \times 2124 + (-16) \times 396\,. \end{aligned}$$

Assim $72 = 6 \times 2124 + (-32) \times 396$ e os inteiros $x = 6$ e $y = -32$ satisfazem o pedido.

---

3. (4,5 valores)

(a)
Um número $p \in \mathbb{N}$, $p > 1$, diz-se um número primo se os seus únicos divisores positivos são 1 e p.

(b)
Seja $n \in \mathbb{N}$, $n > 1$. Se n é primo nada há a provar. Suponha-se que n é composto. Então n tem um divisor pertencente a $\{2, \ldots, n-1\}$, isto é, $D = \{d \in \mathbb{N} : 1 < d < n \wedge d \mid n\} \neq \emptyset$. Pelo princípio de boa ordenação este conjunto tem um mínimo, m. Suponha-se que m é composto. Então existe $q \in \mathbb{N}$, $1 < q < m$, tal que $q \mid m$. Atendendo à transitividade da relação de divisibilidade, de $q \mid m$ e $m \mid n$ conclui-se que $q \mid n$. Por outro lado, $1 < q < m < n$ e portanto $q \in D$, o que é absurdo porque $q < m$ e m é o mínimo de D. O absurdo resultou de se ter suposto que m é composto. Então m é primo. Designe-se m por p_1. Tem-se então que

$$n = p_1 n_1 \text{ com } n_1 \in \mathbb{N}\,,\ \ p_1 \text{ primo e } 1 < n_1 < n\,.$$

Se n_1 é primo então n é o produto de dois primos e nada mais há a provar. Suponha-se que n_1 é composto. Repetindo o processo descrito anteriormente conclui-se que $n_1 = p_2 n_2$, com $n_2 \in \mathbb{N}$, p_2 primo e $1 < n_2 < n_1$. Então

$$n = p_1 p_2 n_2 \text{ com } n_2 \in \mathbb{N}\,,\ \ p_1, p_2 \text{ primos e } 1 < n_2 < n_1 < n\,.$$

Repetindo este processo constrói-se uma sequência, estritamente decrescente, de números naturais superiores a 1, $n > n_1 > n_2 > \cdots$, onde, para cada i,

$$n = p_1 p_2 \cdots p_i n_i\,,\ \text{com } p_1, p_2, \ldots, p_i \text{ primos}\,.$$

Uma vez que $\{x \in \mathbb{N} : 1 < x < n\}$ é finito tal sequência é finita, isto é, ao fim de um número finito de passos, digamos k, o processo descrito anteriormente termina, ou seja, n_k é primo e portanto em $n = p_1 p_2 \cdots p_k n_k$ tem-se n escrito como o produto de $k+1$ números primos.

---

4. (4 valores)
Seja n um inteiro positivo que é múltiplo de 30 e tem 12 divisores positivos. Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a sua decomposição canónica. Isto é, $r \in \mathbb{N}$, $p_1, p_2, \ldots, p_r$ são números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$. Uma vez que $30 = 2 \times 3 \times 5$, n é múltiplo de 30 se e só se $r \geq 3$ e $2, 3, 5 \in \{p_1, \ldots, p_r\}$. Suponha-se que $p_1 = 2$, $p_2 = 3$ e $p_3 = 5$.

O número de divisores positivos de n é $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$. Uma vez que $r \geq 3$,

$$\begin{aligned} \tau(n) = 12 &\Leftrightarrow (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1) = 2 \times 2 \times 3 \\ &\Leftrightarrow \left\{ \begin{array}{l} r = 3 \\ \alpha_1 = 1 \\ \alpha_2 = 1 \\ \alpha_3 = 2 \end{array} \right. \vee \left\{ \begin{array}{l} r = 3 \\ \alpha_1 = 1 \\ \alpha_2 = 2 \\ \alpha_3 = 1 \end{array} \right. \vee \left\{ \begin{array}{l} r = 3 \\ \alpha_1 = 2 \\ \alpha_2 = 1 \\ \alpha_3 = 1 \end{array} \right. . \end{aligned}$$

Conclui-se assim que há três inteiros positivos que são múltiplos de 30 e têm 12 divisores positivos: $2 \times 3 \times 5^2 = 150$, $2 \times 3^2 \times 5 = 90$ e $2^2 \times 3 \times 5 = 60$.

---

5. (3 valores)
Seja $d = (a, m)$. Uma vez que $d \neq 0$ obtém-se

$$\begin{aligned} ab \equiv ac \,(\mathrm{mod}\, m) &\Leftrightarrow m \mid ab - ac \\ &\Leftrightarrow m \mid a(b - c) \\ &\Leftrightarrow \exists q \in \mathbb{Z} : a(b - c) = qm \\ &\Leftrightarrow \exists q \in \mathbb{Z} : \frac{a}{d}(b - c) = q\frac{m}{d} . \end{aligned}$$

Atendendo a que $d \mid a$ e $d \mid m$ conclui-se assim que

$$ab \equiv ac \,(\mathrm{mod}\, m) \Leftrightarrow \frac{m}{d} \mid \frac{a}{d}(b - c) .$$

Por outro lado, $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, logo,

$$\frac{m}{d} \mid \frac{a}{d}(b - c) \Leftrightarrow \frac{m}{d} \mid b - c$$

e, portanto,

$$\begin{aligned} ab \equiv ac \,(\mathrm{mod}\, m) &\Leftrightarrow \frac{m}{d} \mid b - c \\ &\Leftrightarrow b \equiv c \left(\mathrm{mod}\, \frac{m}{d}\right) . \end{aligned}$$