Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do Exame da Época Normal

24 de Janeiro de 2006

---

1. (3 valores)
Considere-se o conjunto $\mathcal{S} = \{b - ax : x \in \mathbb{Z}\}$. Se $x \in \mathbb{Z}$ é tal que $x \leq \frac{b-1}{a}$ então, porque $a > 0$, $b - ax \geq 1$. Assim, $\mathcal{S} \cap \mathbb{N} \neq \emptyset$ e, pelo princípio de boa ordenação, tem um mínimo. Seja r o elemento de $\mathcal{S}$ definido por

$$r = \begin{cases} \min(\mathcal{S} \cap \mathbb{N}) \text{ se } 0 \notin \mathcal{S} \\ 0 \text{ se } 0 \in \mathcal{S} \end{cases} .$$

Isto é, r é o mínimo de $\mathcal{S} \cap \mathbb{N}_0$. Como $r \in \mathcal{S}$, existe $q \in \mathbb{Z}$ tal que $r = b - aq$ e portanto $b = aq + r$, com $q \in \mathbb{Z}$.

Por construção, $r \geq 0$. Falta apenas provar que $r < a$. Suponha-se que $r \geq a$. Então $r - a \in \mathbb{N}_0$. Por outro lado, $r - a = b - aq - a = b - a(q+1)$, concluindo-se que $r - a \in \mathcal{S}$, porque $q + 1 \in \mathbb{Z}$.

Tem-se assim que $r - a \in \mathcal{S} \cap \mathbb{N}_0$ e $r - a < r$ (porque $a > 0$), o que entra em contradição com o facto de r ser o mínimo de $\mathcal{S} \cap \mathbb{N}_0$. Essa contradição resultou de termos suposto que $r \geq a$. Então $r < a$.

---

2. (2,5 valores)
Se $m = 1$ ou $k = 1$ o resultado é óbvio. Suponha-se que $m > 1$ e $k > 1$. Uma vez que $(m, k) = 1$, nas factorizações canónicas de m e k não há primos em comum, isto é,

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{e} \quad k = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s} ,$$

com $r, s \in \mathbb{N}$, $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_r$, $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{N}$. Assim, em

$$mk = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

temos mk escrito como produto de potências de primos distintos dois a dois. Uma vez que mk é um quadrado perfeito os expoentes $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_s$ são números pares. Então $\frac{\alpha_1}{2}, \frac{\alpha_2}{2}, \ldots, \frac{\alpha_r}{2}, \frac{\beta_1}{2}, \frac{\beta_2}{2}, \ldots, \frac{\beta_s}{2}$ são números naturais, resultando que

$$p_1^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \cdots p_r^{\frac{\alpha_r}{2}} , \; q_1^{\frac{\beta_1}{2}} q_2^{\frac{\beta_2}{2}} \cdots q_s^{\frac{\beta_s}{2}} \in \mathbb{N}$$

e, portanto,

$$m = \left(p_1^{\frac{\alpha_1}{2}} p_2^{\frac{\alpha_2}{2}} \cdots p_r^{\frac{\alpha_r}{2}} \right)^2 \quad \text{e} \quad k = \left(q_1^{\frac{\beta_1}{2}} q_2^{\frac{\beta_2}{2}} \cdots q_s^{\frac{\beta_s}{2}} \right)^2$$

são quadrados perfeitos.

---

3. (2 valores)
Uma vez que 13 é primo e $(6, 13) = 1$, aplicando o Teorema de Fermat, obtém-se que $6^{12} \equiv 1 \pmod{13}$. Além disso, $194 = 16 \times 12 + 2$ e, assim,

$$6^{194} = \left(6^{12}\right)^{16} 6^2 \equiv 1^{16} 6^2 \pmod{13} \equiv 36 \pmod{13} \equiv 10 \pmod{13}.$$

Por outro lado, aplicando o Teorema de Wilson, obtém-se que $12! = (13-1)! \equiv -1 \pmod{13}$, ou seja, $12 \times 11! \equiv -1 \pmod{13}$, o que é equivalente a $11! \equiv 1 \pmod{13}$.

Então

$$6^{194} - 11! \equiv 10 - 1 \pmod{13} \equiv 9 \pmod{13}$$

e o resto da divisão inteira de $6^{194} - 11!$ por 13 é 9.

---

4. (2,5 valores)
Uma vez que $(a, b) = 1$, do Teorema de Euler conclui-se que $a^{\varphi(b)} \equiv 1 (\mathrm{mod}\, b)$. Por outro lado, $\varphi(a)$ é um número natural, logo $b^{\varphi(a)} \equiv 0 (\mathrm{mod}\, b)$. Então

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 + 0 (\mathrm{mod}\, b) \equiv 1 (\mathrm{mod}\, b). \tag{1}$$

De modo análogo (trocando os papéis de a e b), obtém-se que

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 (\mathrm{mod}\, a). \tag{2}$$

De (1) e (2) resulta que $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 (\mathrm{mod}\, [a, b])$. Uma vez que $(a, b) = 1$, tem-se $[a, b] = ab$ e, portanto, $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 (\mathrm{mod}\, ab)$.

---

5. (3,5 valores)
O número 7 é primo, $(7, 4) = 1$ e $4^{\frac{7-1}{(8,7-1)}} = 4^{\frac{6}{2}} = 4^3 \equiv 2 \times 4 \pmod{7} \equiv 1 \pmod{7}$, o que permite concluir que existem exactamente $(8, 6) = 2$ classes de congruência módulo 7 cujos elementos verificam a congruência dada.

Uma vez que 3 é uma raíz primitiva módulo 7, o conjunto $\{3, 3^2, \ldots, 3^6\}$ é um sistema reduzido de resíduos módulo 7. Assim, porque 4 é primo com 7, existe um e um só $k \in \{1, 2, \ldots, 6\}$ tal que $3^k \equiv 4 \pmod{7}$. De $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 18 \pmod{7} \equiv 4 \pmod{7}$, conclui-se que $k = 4$.

Se $x \in \mathbb{Z}$ verifica a congruência dada então $(x, 7) = 1$ e portanto existe um e um só $i \in \{1, 2, \ldots, 6\}$ tal que $x \equiv 3^i \pmod{7}$. Logo,

$$\begin{aligned} x^8 \equiv 4 \pmod{7} &\Leftrightarrow 3^{8i} \equiv 3^4 \pmod{7} \\ &\Leftrightarrow 3^{8i} - 3^4 \equiv 0 \pmod{7} \\ &\Leftrightarrow 3^4 \left(3^{8i-4} - 1\right) \equiv 0 \pmod{7} \\ &\Leftrightarrow 3^{8i-4} \equiv 1 \pmod{7}, \end{aligned}$$

onde, na última equivalência, se usou o facto de 3 e 7 serem primos entre si. Uma vez que a ordem de 3 módulo 7 é 6 (3 é uma raíz primitiva módulo 7),

$$\begin{aligned} 3^{8i-4} \equiv 1 \pmod{7} &\Leftrightarrow 8i - 4 \equiv 0 \pmod{6} \\ &\Leftrightarrow 8i \equiv 4 \pmod{6} \\ &\Leftrightarrow 4i \equiv 2 \pmod{3} \\ &\Leftrightarrow i \equiv 2 \pmod{3}. \end{aligned}$$

Os inteiros que satisfazem a congruência $i \equiv 2 \pmod 3$ são todos os inteiros pertencentes a $[2]_3$. Esta classe de congruência módulo 3 é a união de duas classes de congruência módulo 6, $[2]_6$ e $[2+3]_6 = [5]_6$.

Então as soluções de $x^8 \equiv 4 \pmod 7$ são as 2 classes de congruência módulo 7, $[3^2]_7 = [2]_7$ e $[3^5]_7 = [3^4 \times 3]_7 = [4 \times 3]_7 = [5]_7$.

---

6. (3 valores)
Designe-se por n um qualquer número natural nas condições do enunciado, isto é, tal que $100 \mid n$, $\tau(n) = 18$ e $\varphi(n) = 480$. 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 $100 = 2^2 \times 5^2$, n é múltiplo de 100 se e só se $r \geq 2$, $2, 5 \in \{p_1, \ldots, p_r\}$ e os expoentes de 2 e 5 na factorização canónica de n são superiores a 1. Suponha-se que $p_1 = 2$ e $p_2 = 5$. Então $\alpha_1 \geq 2$ e $\alpha_2 \geq 2$.

O número de divisores positivos de n é $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$. Como $\alpha_1 + 1 \geq 3$ e $\alpha_2 + 1 \geq 3$,

$$\begin{aligned}
\tau(n) = 18 &\Leftrightarrow (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1) = 18 \\
&\Leftrightarrow \left\{ \begin{array}{l} r = 2 \\ \alpha_1 + 1 = 3 \\ \alpha_2 + 1 = 6 \end{array} \right. \vee \left\{ \begin{array}{l} r = 2 \\ \alpha_1 + 1 = 6 \\ \alpha_2 + 1 = 3 \end{array} \right. \vee \left\{ \begin{array}{l} r = 3 \\ \alpha_1 + 1 = 3 \\ \alpha_2 + 1 = 3 \\ \alpha_3 + 1 = 2 \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{l} r = 2 \\ \alpha_1 = 2 \\ \alpha_2 = 5 \end{array} \right. \vee \left\{ \begin{array}{l} r = 2 \\ \alpha_1 = 5 \\ \alpha_2 = 2 \end{array} \right. \vee \left\{ \begin{array}{l} r = 3 \\ \alpha_1 = 2 \\ \alpha_2 = 2 \\ \alpha_3 = 1 \end{array} \right. .
\end{aligned}$$

Há assim 3 hipóteses: $n = 2^2 5^5$, $n = 2^5 5^2$ ou $n = 2^2 5^2 p_3$, com p_3 um número primo, distinto de 2 e 5.

Uma vez que $\varphi(2^2 5^5) = (2^2 - 2)(5^5 - 5^4) = 2 \times 5^4 \times 4 > 480$ e $\varphi(2^5 5^2) = (2^5 - 2^4)(5^2 - 5) = 16 \times 20 = 320 \neq 480$, só resta a terceira hipótese.

$$\varphi(2^2 5^2 p_3) = 480 \Leftrightarrow (2^2 - 2)(5^2 - 5)(p_3 - 1) = 480 \Leftrightarrow 40(p_3 - 1) = 480 \Leftrightarrow p_3 = 13 \,.$$

Uma vez que 13 é primo pode, de facto, escolher-se $p_3 = 13$. Assim, há um único número nas condições do enunciado, $n = 2^2 5^2 13 = 1300$.

---

7. (3,5 valores)
Uma vez que $(12, 16) = 4$ é um divisor de 96, a equação tem soluções inteiras. De $4 = 16 - 12$ resulta que

$$96 = 24 \times 4 = 12 \times (-24) + 16 \times 24$$

e portanto $x_0 = -24$ e $y_0 = 24$ são inteiros que verificam a equação $12\,x + 16\,y = 96$. Sejam x e y inteiros tais que $12\,x + 16\,y = 96$. Então

$$12\,x + 16\,y = 12\,x_0 + 16\,y_0 \Leftrightarrow 12(x - x_0) = 16(y_0 - y) \Leftrightarrow 3(x - x_0) = 4(y_0 - y)\,,$$

concluindo-se, porque $(3,4)=1$, que $4 \mid x-x_0$ e $3 \mid y_0-y$. Isto é, existem $q,t \in \mathbb{Z}$ tais que $x=x_0+4q$ e $y=y_0-3t$. Uma vez que

$$\begin{aligned} 12\,x+16\,y=96 &\Leftrightarrow 12\,x_0+12\times 4\times q+16\,y_0-16\times 3\times t=96 \\ &\Leftrightarrow 96+48(q-t)=96 \\ &\Leftrightarrow q=t\,, \end{aligned}$$

as soluções inteiras de $12\,x+16\,y=96$ são dadas por

$$\left\{\begin{array}{l} x=x_0+4q=-24+4q \\ y=y_0-3q=24-3q \end{array}\right. , \quad q\in\mathbb{Z}\,.$$