Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do Exame de Recurso

16 de Fevereiro de 2005

---

1. (2 valores)
Uma vez que $(a, b) = 1$, p não pode dividir simultaneamente a e b. Há assim 3 casos possíveis:

1. $p \nmid a$ e $p \nmid b$
   Neste caso, porque p é primo, $(a, p) = (b, p) = 1$. Ainda por p ser primo,
   $$p \nmid a \wedge p \nmid b \Rightarrow p \nmid ab \Rightarrow (ab, p) = 1\,,$$
   obtendo-se $(ab, p) = (a, p)(b, p)$.
2. $p \mid a$ e $p \nmid b$
   Se $p \mid a$ então também $p \mid ab$ e portanto $(ab, p) = p = p \times 1 = (a, p)(b, p)$.
3. $p \nmid a$ e $p \mid b$
   Este caso é análogo ao anterior.

---

2. (3 valores)
Teorema de Euler: Dados $m \in \mathbb{N}$ e $a \in \mathbb{Z}$, se $(a, m) = 1$ então $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Demonstração: Seja $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Uma vez que $(a, m) = 1$, também $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m. Então, cada um dos elementos de $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ é congruente módulo m a um e um só elemento de $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$. Isto é, existe uma aplicação bijectiva, $f : \{1, 2, \ldots, \varphi(m)\} \to \{1, 2, \ldots, \varphi(m)\}$, tal que $r_i \equiv ar_{f(i)} \pmod{m}$, para $i = 1, 2, \ldots, \varphi(m)$. Multiplicando membro a membro estas $\varphi(m)$ congruências obtém-se que

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv \left(ar_{f(1)}\right)\left(ar_{f(2)}\right) \cdots \left(ar_{f(\varphi(m))}\right) \pmod{m}\,.$$

Mas, porque f é bijectiva,

$$\left(ar_{f(1)}\right)\left(ar_{f(2)}\right) \cdots \left(ar_{f(\varphi(m))}\right) = a^{\varphi(m)} r_{f(1)} r_{f(2)} \cdots r_{f(\varphi(m))} = a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)}$$

e assim,

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}\,. \tag{1}$$

Por definição de sistema reduzido de resíduos módulo m, $r_1, r_2, \ldots, r_{\varphi(m)}$ são primos com m, o mesmo acontecendo portanto com o seu produto. Assim, de (1), conclui-se que $a^{\varphi(m)} \equiv 1 \pmod{m}$.

---

3. (3 valores)
O último dígito de um inteiro é o resto da sua divisão inteira por 10. Claro que o último dígito de 5^{2005} é 5, isto é, $5^{2005} \equiv 5 \pmod{10}$.

Uma vez que $(3,10) = (7,10) = (9,10) = 1$, aplicando o Teorema de Euler conclui-se que $a^{\varphi(10)} \equiv 1 \pmod{10}$, para $a \in \{3,7,9\}$, ou seja, $a^4 \equiv 1 \pmod{10}$, para $a \in \{3,7,9\}$. Então, para $a \in \{3,7,9\}$,

$$a^{2005} = \left(a^4\right)^{501} \; a \equiv 1^{501} \; a \pmod{10} \equiv a \pmod{10}$$

e $1^{2005} + 3^{2005} + 5^{2005} + 7^{2005} + 9^{2005} \equiv 1 + 3 + 5 + 7 + 9 \pmod{10} \equiv 5 \pmod{10}$. O último dígito de $1^{2005} + 3^{2005} + 5^{2005} + 7^{2005} + 9^{2005}$ é 5.

---

4. (3 valores)
Uma vez que 2, 5 e 9 são primos dois a dois, o Teorema chinês dos resíduos garante que o sistema

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv -2 \pmod 5 \\ x \equiv 5 \pmod 9 \end{cases} \tag{2}$$

tem solução, sendo o conjunto das soluções uma classe de congruência módulo $2 \times 5 \times 9 = 90$. Resolvam-se as congruências auxiliares $\frac{90}{2} b_1 \equiv 1 \pmod 2$, $\frac{90}{5} b_2 \equiv 1 \pmod 5$ e $\frac{90}{9} b_3 \equiv 1 \pmod 9$.

$\frac{90}{2} b_1 \equiv 1 \pmod 2 \Leftrightarrow 45 b_1 \equiv 1 \pmod 2 \Leftrightarrow b_1 \equiv 1 \pmod 2$
$\frac{90}{5} b_2 \equiv 1 \pmod 5 \Leftrightarrow 18 b_2 \equiv 1 \pmod 5 \Leftrightarrow 3 b_2 \equiv 1 \pmod 5 \Leftrightarrow 6 b_2 \equiv 2 \pmod 5$
$\Leftrightarrow b_2 \equiv 2 \pmod 5$.
$\frac{90}{9} b_3 \equiv 1 \pmod 9 \Leftrightarrow 10 b_3 \equiv 1 \pmod 9 \Leftrightarrow b_3 \equiv 1 \pmod 9$

Considerem-se $b_1 = 1$, $b_2 = 2$ e $b_3 = 1$.

Então $1 \times \frac{90}{2} b_1 + (-2) \times \frac{90}{5} b_2 + 5 \times \frac{90}{9} b_3 = 45 \times 1 - 2 \times 18 \times 2 + 5 \times 10 \times 1 = 23$ é uma solução de (2) e (Teorema chinês dos resíduos) o conjunto das soluções de (2) é $[23]_{90} = \{23 + 90k : k \in \mathbb{Z}\}$. Uma vez que $23 - 90 = -67$, o maior inteiro negativo que é solução de (2) é -67.

---

5. (a) (1 valor)
Para $m \in \mathbb{N}$, uma raíz primitiva módulo m é um inteiro a, primo com m, e com ordem módulo m igual a $\varphi(m)$, isto é, o menor inteiro positivo k tal que $a^k \equiv 1 \pmod m$ é $k = \varphi(m)$.

(b) (3 valores)
O número 17 é primo, $(17,16) = 1$ e $16^{\frac{17-1}{(10,17-1)}} = 16^{\frac{16}{2}} = 16^8 \equiv (-1)^8 \pmod{17} \equiv 1 \pmod{17}$, o que permite concluir que existem exactamente $(10,16) = 2$ classes de congruência módulo 17 cujos elementos verificam a congruência dada.

Uma vez que 5 é uma raíz primitiva módulo 17, o conjunto $\{5, 5^2, \ldots, 5^{16}\}$ é um sistema reduzido de resíduos módulo 17. Assim, porque 16 é primo com 17, existe um e um só $k \in \{1, 2, \ldots, 16\}$ tal que $5^k \equiv 16 \pmod{17}$. De $5^1 \equiv 5 \pmod{17}$, $5^2 \equiv 8 \pmod{17}$, $5^3 \equiv 40 \pmod{17} \equiv 6 \pmod{17}$, $5^4 \equiv 30 \pmod{17} \equiv -4 \pmod{17}$, $5^5 \equiv -3 \pmod{17}$, $5^6 \equiv 2 \pmod{17}$, $5^7 \equiv 10 \pmod{17}$ e $5^8 \equiv 50 \pmod{17} \equiv -1 \pmod{17} \equiv 16 \pmod{17}$, conclui-se que $k = 8$.

Se $x \in \mathbb{Z}$ verifica a congruência dada então $(x, 17) = 1$ e portanto existe um e um só $i \in \{1, 2, \ldots, 16\}$ tal que $x \equiv 5^i \pmod{17}$. Logo,

$$\begin{aligned} x^{10} \equiv 16 \pmod{17} &\Leftrightarrow 5^{10i} \equiv 5^8 \pmod{17} \\ &\Leftrightarrow 5^{10i} - 5^8 \equiv 0 \pmod{17} \\ &\Leftrightarrow 5^8 \left(5^{10i-8} - 1\right) \equiv 0 \pmod{17} \\ &\Leftrightarrow 5^{10i-8} \equiv 1 \pmod{17}, \end{aligned}$$

onde, na última equivalência, se usou o facto de 5 e 17 serem primos entre si. Uma vez que a ordem de 5 módulo 17 é 16 (5 é uma raíz primitiva módulo 17),

$$\begin{aligned} 5^{10i-8} \equiv 1 \pmod{17} &\Leftrightarrow 10i - 8 \equiv 0 \pmod{16} \\ &\Leftrightarrow 10i \equiv 8 \pmod{16} \\ &\Leftrightarrow 5i \equiv 4 \pmod{8} \\ &\Leftrightarrow i \equiv 4 \pmod{8}. \end{aligned}$$

Os inteiros que satisfazem a congruência $i \equiv 4 \pmod{8}$ são todos os inteiros pertencentes a $[4]_8$. Esta classe de congruência módulo 8 é a união de duas classes de congruência módulo 16, $[4]_{16}$ e $[4+8]_{16} = [12]_{16}$.

Então as soluções de $x^{10} \equiv 16 \pmod{17}$ são as 2 classes de congruência módulo 17, $[5^4]_{17} = [-4]_{17} = [13]_{17}$ e $[5^{12}]_{17} = [5^6 5^6]_{17} = [2 \times 2]_{17} = [4]_{17}$.

---

6. (2,5 valores)
Uma vez que $p^k \mid a$ e $p^{k+1} \nmid a$, existe $b \in \mathbb{N}$, primo com p, tal que $a = p^k b$. Então, porque a função σ é multiplicativa,

$$\sigma(p\,a) = \sigma\left(p^{k+1} b\right) = \sigma\left(p^{k+1}\right)\ \sigma(b).$$

Sendo p primo, os divisores positivos de p^{k+1} são $1, p, \ldots, p^k, p^{k+1}$, obtendo-se que $\sigma\left(p^{k+1}\right) = 1 + p + \cdots + p^k + p^{k+1}$. Então

$$\begin{aligned} \sigma(p\,a) &= \left(1 + p + \cdots + p^k + p^{k+1}\right) \sigma(b) \\ &= \left(1 + p + \cdots + p^k\right) \sigma(b) + p^{k+1} \sigma(b) \\ &= \sigma\left(p^k\right) \sigma(b) + p^{k+1} \sigma(b) \\ &= \sigma\left(p^k b\right) + p^{k+1} \sigma\left(\frac{a}{p^k}\right) \\ &= \sigma(a) + p^{k+1} \sigma\left(\frac{a}{p^k}\right). \end{aligned}$$

---

7. (2,5 valores)
Seja $k \in \mathbb{N}$ verificando $k \geq 2$. Pretendem determinar-se todos os trios pitagóricos primitivos que têm 2^k como um dos elementos. Um trio pitagórico primitivo (x, y, z), em que y é par, é da forma

$$x = a^2 - b^2, \quad y = 2ab \quad \text{e} \quad z = a^2 + b^2,$$

onde a e b são inteiros positivos, primos entre si, de paridades diferentes e $a > b$. Uma vez que a e b são de paridades diferentes, $a^2 - b^2$ e $a^2 + b^2$ são ímpares. Então terá de ser $2^k = 2ab$, ou seja, $2^{k-1} = ab$. Daqui resulta, porque $(a, b) = 1$ e $a > b$, que $a = 2^{k-1}$ e $b = 1$. Observe-se que 2^{k-1} é par porque $k \geq 2$. Então

$$\begin{aligned} x &= a^2 - b^2 = \left(2^{k-1}\right)^2 - 1^2 = 2^{2k-2} - 1 \\ y &= 2ab = 2^k \\ z &= a^2 + b^2 = \left(2^{k-1}\right)^2 + 1^2 = 2^{2k-2} + 1\,. \end{aligned}$$

Para $k \in \mathbb{N}$, com $k \geq 2$, se um dos catetos de um triângulo rectângulo mede 2^k unidades então o outro cateto mede $2^{2k-2} - 1$ unidades e a hipotenusa mede $2^{2k-2} + 1$ unidades.