Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do 2^o Teste — Prova A

10 de Dezembro de 2004 — Duração: 30m

---

1. (0.4 valores)
Sabendo que 2 é uma raíz primitiva módulo 19 determine, caso existam, todas as soluções de $x^{14} \equiv 7 \pmod{19}$.

O número 19 é primo, $(19, 7) = 1$ e $7^{\frac{19-1}{(14,19-1)}} = 7^{\frac{18}{2}} = 7^9 \equiv (7^3)^3 \pmod{19} \equiv 77^3 \pmod{19} \equiv 1 \pmod{19}$, o que permite concluir que existem exactamente $(14, 18) = 2$ classes de congruência módulo 19 cujos elementos verificam a congruência dada.

Uma vez que 2 é uma raíz primitiva módulo 19, o conjunto $\{2, 2^2, \ldots, 2^{18}\}$ é um sistema reduzido de resíduos módulo 19. Assim, porque 7 é primo com 19, existe um e um só $k \in \{1, 2, \ldots, 18\}$ tal que $2^k \equiv 7 \pmod{19}$. De $2^1 \equiv 2 \pmod{19}$, $2^2 \equiv 4 \pmod{19}$, $2^3 \equiv 8 \pmod{19}$, $2^4 = 16 \equiv -3 \pmod{19}$, $2^5 \equiv -6 \pmod{19}$ e $2^6 \equiv -12 \pmod{19} \equiv 7 \pmod{19}$, conclui-se que $k = 6$.

Se $x \in \mathbb{Z}$ verifica a congruência dada então $(x, 19) = 1$ e portanto existe um e um só $i \in \{1, 2, \ldots, 18\}$ tal que $x \equiv 2^i \pmod{19}$. Logo,

$$\begin{aligned} x^{14} \equiv 7 \pmod{19} &\Leftrightarrow 2^{14i} \equiv 2^6 \pmod{19} \\ &\Leftrightarrow 2^{14i} - 2^6 \equiv 0 \pmod{19} \\ &\Leftrightarrow 2^6 \left(2^{14i-6} - 1\right) \equiv 0 \pmod{19} \\ &\Leftrightarrow 2^{14i-6} \equiv 1 \pmod{19}. \end{aligned}$$

onde, na última equivalência, se usou o facto de 2 e 19 serem primos entre si. Uma vez que a ordem de 2 módulo 19 é 18 (2 é uma raíz primitiva módulo 19),

$$\begin{aligned} 2^{14i-6} \equiv 1 \pmod{19} &\Leftrightarrow 14i - 6 \equiv 0 \pmod{18} \\ &\Leftrightarrow 14i \equiv 6 \pmod{18} \\ &\Leftrightarrow 7i \equiv 3 \pmod{9} \\ &\Leftrightarrow i \equiv 3 \pmod{9}. \end{aligned}$$

Os inteiros que satisfazem a congruência $i \equiv 3 \pmod{9}$ são todos os inteiros pertencentes a $[3]_9$. Esta classe de congruência módulo 9 é a união de duas classes de congruência módulo 18, $[3]_{18}$ e $[3 + 9]_{18} = [12]_{18}$.

Então as soluções de $x^{14} \equiv 7 \pmod{19}$ são as 2 classes de congruência módulo 19, $[2^3]_{19} = [8]_{19}$ e $[2^{12}]_{19} = [2^6 2^6]_{19} = [7 \times 7]_{19} = [11]_{19}$.

---

v.s.f.f.

2. (0.6 valores)
Em cada uma das alíneas seguintes diga, sem justificar, se a afirmação feita é verdadeira ou falsa.

(a) Para quaisquer $a, b, c \in \mathbb{Z} \setminus \{0\}$ e qualquer $m \in \mathbb{N}$, $ab \equiv ac \pmod{m} \Leftrightarrow b \equiv c \pmod{m}$.

(b) O sistema formado pelas congruências $x \equiv 9 \pmod{12}$ e $x \equiv 12 \pmod{15}$ tem solução e quaisquer duas soluções são congruentes módulo 180.

(c) Para quaisquer números naturais a e b, se $a \mid b$ então $\varphi\left(\frac{b}{a}\right) = \frac{\varphi(b)}{a}$.

(a) A afirmação é **falsa**.
Por exemplo, $2 \times 4 \equiv 2 \times 3 \pmod{2}$ e $4 \not\equiv 3 \pmod{2}$.

(b) A afirmação é **falsa**.
Uma vez que $(12, 15) = 3 \mid 12 - 9$, do teorema chinês dos resíduos conclui-se que o sistema tem solução e que o conjunto das soluções é uma classe de congruência módulo $[12, 15] = 60$. Se x_0 é uma solução também $x_0 + 60$ é uma solução. No entanto, $x_0 + 60 \not\equiv x_0 \pmod{180}$.

(c) A afirmação é **falsa**.
Por exemplo, $3 \mid 6$ e $\varphi\left(\frac{6}{3}\right) = \varphi(2) = 1 \neq \frac{2}{3} = \frac{\varphi(6)}{3}$.