Departamento de Matemática da Universidade de Coimbra
Teoria dos Números

Uma possível resolução do 2^o Teste — Prova B

10 de Dezembro de 2004 — Duração: 30m

---

1. (0.4 valores)
Sabendo que 3 é uma raíz primitiva módulo 19 determine, caso existam, todas as soluções de $x^{15} \equiv 18 \pmod{19}$.

O número 19 é primo, $(19, 18) = 1$ e $18^{\frac{19-1}{(15,19-1)}} = 18^{\frac{18}{3}} = 18^6 \equiv (-1)^6 \pmod{19} \equiv 1 \pmod{19}$, o que permite concluir que existem exactamente $(15, 18) = 3$ classes de congruência módulo 19 cujos elementos verificam a congruência dada.

Uma vez que 3 é uma raíz primitiva módulo 19, o conjunto $\{3, 3^2, \ldots, 3^{18}\}$ é um sistema reduzido de resíduos módulo 19. Assim, porque 18 é primo com 19, existe um e um só $k \in \{1, 2, \ldots, 18\}$ tal que $3^k \equiv 18 \pmod{19}$. De $3^1 \equiv 3 \pmod{19}$, $3^2 \equiv 9 \pmod{19}$, $3^3 \equiv 8 \pmod{19}$, $3^4 \equiv 24 \pmod{19} \equiv 5 \pmod{19}$, $3^5 \equiv 15 \pmod{19} \equiv -4 \pmod{19}$, $3^6 \equiv -12 \pmod{19} \equiv 7 \pmod{19}$, $3^7 \equiv 21 \pmod{19} \equiv 2 \pmod{19}$, $3^8 \equiv 6 \pmod{19}$ e $3^9 \equiv 18 \pmod{19}$ conclui-se que $k = 9$.

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 $x \equiv 3^i \pmod{19}$. Logo,

$$\begin{aligned} x^{15} \equiv 18 \pmod{19} &\Leftrightarrow 3^{15i} \equiv 3^9 \pmod{19} \\ &\Leftrightarrow 3^{15i} - 3^9 \equiv 0 \pmod{19} \\ &\Leftrightarrow 3^9 \left(3^{15i-9} - 1\right) \equiv 0 \pmod{19} \\ &\Leftrightarrow 3^{15i-9} \equiv 1 \pmod{19}, \end{aligned}$$

onde, na última equivalência, se usou o facto de 3 e 19 serem primos entre si. Uma vez que a ordem de 3 módulo 19 é 18 (3 é uma raíz primitiva módulo 19),

$$\begin{aligned} 3^{15i-9} \equiv 1 \pmod{19} &\Leftrightarrow 15i - 9 \equiv 0 \pmod{18} \\ &\Leftrightarrow 15i \equiv 9 \pmod{18} \\ &\Leftrightarrow 5i \equiv 3 \pmod{6} \\ &\Leftrightarrow i \equiv 3 \pmod{6}. \end{aligned}$$

Os inteiros que satisfazem a congruência $i \equiv 3 \pmod{6}$ são todos os inteiros pertencentes a $[3]_6$. Esta classe de congruência módulo 6 é a união de três classes de congruência módulo 18, $[3]_{18}$, $[3 + 6]_{18} = [9]_{18}$ e $[3 + 12]_{18} = [15]_{18}$.

Então as soluções de $x^{15} \equiv 18 \pmod{19}$ são as 3 classes de congruência módulo 19, $[3^3]_{19} = [8]_{19}$, $[3^9]_{19} = [18]_{19}$ e $[3^{15}]_{19} = [3^7 3^8]_{19} = [2 \times 6]_{19} = [12]_{19}$.

---

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) O sistema formado pelas congruências $x \equiv 4 \pmod{60}$ e $x \equiv 16 \pmod{42}$ tem solução e quaisquer duas soluções são congruentes módulo 420.

(b) Para quaisquer inteiros a, b e m, com m positivo, $a \equiv b \pmod{m} \Leftrightarrow (a, m) = (b, m)$.

(c) Para quaisquer números naturais a e b, se $a \mid b$ então $\varphi(a\, b) = a\, \varphi(b)$.

(a) A afirmação é **verdadeira**.
Uma vez que $(60, 42) = 6 \mid 16 - 4$, do teorema chinês dos resíduos conclui-se que o sistema tem solução e que o conjunto das soluções é uma classe de congruência módulo $[60, 42] = 420$. Assim, quaisquer duas soluções são congruentes módulo 420.

(b) A afirmação é **falsa**.
Por exemplo, $(2, 3) = 1 = (7, 3)$ e $2 \not\equiv 7 \pmod{3}$.

(c) A afirmação é **verdadeira**.
Se $a = 1$ ou $b = 1$ o resultado é óbvio. Suponha-se que $a > 1$ e $b > 1$. Uma vez que $a \mid b$, se a decomposição canónica de a é $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $k \in \mathbb{N}$, $p_1, p_2, \ldots, p_k$ números primos distintos dois a dois e $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, então $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} c$ com $(c, p_i) = 1$, $\beta_i \in \mathbb{N}$ e $\alpha_i \leq \beta_i$, para $i = 1, 2, \ldots, k$.

$$\begin{aligned}
\varphi(ab) &= \varphi\left(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_k^{\alpha_k+\beta_k} c\right) \\
&= \varphi\left(p_1^{\alpha_1+\beta_1}\right) \varphi\left(p_2^{\alpha_2+\beta_2}\right) \cdots \varphi\left(p_k^{\alpha_k+\beta_k}\right) \varphi(c) \\
&= \left(p_1^{\alpha_1+\beta_1} - p_1^{\alpha_1+\beta_1-1}\right)\left(p_2^{\alpha_2+\beta_2} - p_2^{\alpha_2+\beta_2-1}\right) \cdots \left(p_k^{\alpha_k+\beta_k} - p_k^{\alpha_k+\beta_k-1}\right) \varphi(c) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \left(p_1^{\beta_1} - p_1^{\beta_1-1}\right)\left(p_2^{\beta_2} - p_2^{\beta_2-1}\right) \cdots \left(p_k^{\beta_k} - p_k^{\beta_k-1}\right) \varphi(c) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \varphi\left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\right) \varphi(c) \\
&= a\varphi(b)\,.
\end{aligned}$$