Folha **D** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Fevereiro de 2017

1. Resolva os seguintes equações:
   (a) $x \equiv 3 \pmod 7$ e $x \equiv 4 \pmod 9$.
   (b) $x \equiv 13 \pmod{71}$ e $x \equiv 41 \pmod{97}$.
   (c) $x \equiv 4 \pmod 7$, $x \equiv 5 \pmod 8$ e $x \equiv 11 \pmod{15}$.
2. Sejam $a, b \in \mathbb{Z}$ e n um número natural diferente de 1. Mostre que a equação $ax \equiv b \pmod n$ tem solução se, e somente se, $\mathrm{mdc}(a, n) \mid b$.
3. Sejam p e q primos ímpares distintos e $n = pq$. Mostre que o polinómio $x^2 - 1$ tem exatamente quatro raízes em $\mathbb{Z}/n\mathbb{Z}$.
4. Mostre que $n^5 - n$ é sempre divisível por 30. (Mostre que é sempre divisível por 2, 3 e 5.)
5. Sejam $n, k \in \mathbb{N}$ com $n > 1$. Dados $b, c \in \mathbb{Z}$ com $b \equiv c \pmod{n^k}$, mostre que $b^n \equiv c^n \pmod{n^{k+1}}$.
6. Para cada um dos primos p e números a, calcule $a^{-1} \pmod p$ usando o algoritmo de Euclides estendido: (a) $p = 47$ e $a = 11$; (b) $p = 587$ e $a = 345$; e (c) $p = 104801$ e $a = 78467$.
7. Sejam $n_1, n_2, \ldots, n_k$ números naturais maiores do que 1, co-primos dois a dois. Sejam $a_1, a_2, \ldots, a_k$ elementos de $\mathbb{Z}$. Mostre que existe $x \in \mathbb{Z}$ tal que $x \equiv a_i \pmod{n_i}$, para todo $1 \leq i \leq k$.
8. Calcule $\varphi(55)$, $\varphi(128)$, $\varphi(90)$, $\varphi(89)$ e $\varphi(105)$.
9. Use o método da repetição do quadrado para calcular $17^{183} \pmod{256}$, $2^{477} \pmod{1000}$ e $11^{507} \pmod{1237}$.
10. (a) Seja p um primo ímpar. Mostre que um polinómio $x^2 + bx + c \in \mathbb{Z}_p[x]$ tem raízes em $\mathbb{Z}_p$ se, e somente se, $b^2 - 4c$ é um quadrado módulo p.
    (b) Seja K um corpo de característica diferente de 2. Em que condições é que um polinómio $x^2 + bx + c \in K[x]$ tem raízes em K?
11. Mostre que $5^i \not\equiv -1 \pmod 8$ para todo $i \geq 0$.