Folhas de exercícios III

Fernando Ferreira

Introdução à Teoria dos Números
2018/2019

1. Dados $a, b \in \mathbb{N}$ e $n \in \mathbb{N}$. Mostre que $a \equiv b \pmod{n}$ se, e somente se, o resto da divisão de a por n é igual ao resto da divisão de b por n.

2. Será que $b \equiv c \pmod{n}$ implica sempre $a^b \equiv a^c \pmod{n}$? (Aqui, a, b, c e n são números naturais.)

3. (a) Construa as tabelas de adição e multiplicação de $\mathbb{Z}/6\mathbb{Z}$ e de $\mathbb{Z}/7\mathbb{Z}$.
   (b) Construa as tabelas de multiplicação de $(\mathbb{Z}/8\mathbb{Z})^*$, $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/10\mathbb{Z})^*$ e $(\mathbb{Z}/15\mathbb{Z})^*$.
   (c) Diga quais são as ordens dos elementos de $(\mathbb{Z}/8\mathbb{Z})^*$. Faça o mesmo para $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/10\mathbb{Z})^*$ e $(\mathbb{Z}/15\mathbb{Z})^*$.

4. Calcule $347 + 513 \pmod{763}$, $3274 + 1238 + 7231 + 6437 \pmod{9254}$, $153 \cdot 287 \pmod{353}$, $357 \cdot 862 \cdot 193 \pmod{943}$, $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \pmod{8157}$, $137^4 \pmod{327}$ e $373^6 \pmod{581}$.

5. Resolva as equações: (a) $x + 17 \equiv 23 \pmod{37}$; (b) $x + 42 \equiv 19 \pmod{51}$; (c) $x^2 \equiv 3 \pmod{11}$; (d) $x^2 \equiv 2 \pmod{13}$; (e) $x^2 \equiv 1 \pmod{8}$ e (f) $x^3 - x^2 + 2x - 2 \equiv 0 \pmod{11}$. Apresente os resultados no sistema completo de resíduos canónico e no sistema menor.

6. Mostre que $n^5 - n$ é sempre divisível por 30. (Mostre que é sempre divisível por 2, 3 e 5.)

7. Mostre que um número é divisível por 9 se, e somente se, a soma dos seus dígitos (notação decimal) é divisível por 9. Apresente critérios semelhantes para a divisibilidade por 3, 5 e 11.

8. Mostre que $5^i \not\equiv -1 \pmod{8}$ para todo $i \geq 0$.

9. Sejam $n, k \in \mathbb{N}$ com $n > 1$. Dados $b, c \in \mathbb{Z}$ com $b \equiv c \pmod{n^k}$, mostre que $b^n \equiv c^n \pmod{n^{k+1}}$.

10. Seja p um número primo. Mostre que $(a + b)^p \equiv a^p + b^p \pmod{p}$, para todos $a, b \in \mathbb{Z}$. Será que este facto ainda é verdade caso p não seja primo?

11. Mostre que se $n > 4$ é um número composto então $(n-1)! \equiv 0 \pmod{n}$.

12. Seja $n \in \mathbb{N}$. Mostre que se n e $n^2 + 2$ são primos então $n = 3$. (Veja o problema 2.18 do livro e a sua solução.)

13. Para cada um dos seguintes pares de números naturais, encontre o seu máximo divisor comum e exprima-o como combinação linear inteira dos dois números. Encontre as soluções de duas maneiras: trabalhando o algoritmo de Euclides de baixo-para-cima e de cima-para-baixo: (a) 26, 19; (b) 187, 34; (c) 841, 160; (d) 2613, 2171.

14. Encontre um inteiro x tal que $37x \equiv 1 \pmod{101}$.

15. 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 $a = 78467$.

16. Resolva as equações: (a) $6x \equiv 9 \pmod{15}$; (b) $10x \equiv 15 \pmod{35}$; (c) $198x \equiv 90 \pmod{252}$.

17. 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, $\text{mdc}(a, n) \mid b$.

18. Sejam a e b números naturais e $d = \text{mdc}(a, b)$. Considere a equação nos inteiros $ax + by = d$.

    (a) Mostre que se o par de inteiros x_0, y_0 é solução da equação acima então, para todo $z \in \mathbb{Z}$, o par $x_0 + z\frac{b}{d}$, $y_0 - z\frac{a}{d}$, também é solução da equação.

    (b) Mostre que todas as soluções da equação são da forma da alínea anterior.

19. Use o algoritmo estendido de Euclides para encontrar inteiros x e y tais que $2261x + 1275y = 17$. Usando o problema (18), encontre todas as soluções inteiras da equação dada.

20. Obtenha $x, y, z \in \mathbb{Z}$ tais que $35x + 55y + 77z = 1$. (Sugestão: primeiro escreva 5 como combinação linear inteira de 35 e 55; depois escreva 1 como combinação linear inteira de 5 e 77.)

21. Dados $a_1, a_2, \ldots a_k$ elementos de $\mathbb{N}$, defina-se $\text{mdc}(a_1, a_2, \ldots, a_k)$ como o máximo dos divisores comuns a todos os $a_1, a_2, \ldots, a_k$.

    (a) Mostre que $\text{mdc}(a_1, a_2, a_3 \ldots, a_k) = \text{mdc}(\text{mdc}(a_1, a_2), a_3, \ldots, a_k)$.

    (b) Mostre que existem elementos $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ tais que

    $$\text{mdc}(a_1, a_2, \ldots, a_k) = x_1a_1 + x_2a_2 + \cdots + x_ka_k.$$

22. 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 $x \equiv 11 \pmod{15}$.

23. (a) Exiba concretamente o isomorfismo de anéis (da aula teórica) entre $\mathbb{Z}/15\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(b) Exiba concretamente o isomorfismo de grupos (da aula teórica) entre $(\mathbb{Z}/15\mathbb{Z})^*$ e $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$.

24. Seja $n \in \mathbb{N}$, $n \neq 1$, tal que n não é primo. Mostre que $\mathbb{Z}/n\mathbb{Z}$ não é um corpo.

25. Encontre um número de três dígitos (notação decimal) que deixa resto 4 quando dividido por 7, 9 e 11.

26. Encontre $x \in \mathbb{Z}$ tal que $x \equiv -4 \pmod{17}$ e $x \equiv 3 \pmod{23}$.

27. Seja A um anel com identidade e. Define-se $A^* := \{a \in A : \exists b\,(a \cdot b = e)\}$ (portanto, A^* é o conjunto dos elementos invertíveis de A). Mostre que A^* munido da operação de multiplicação do anel é um grupo.

28. Seja p um primo tal que $p \equiv 3 \pmod{4}$. Mostre que não há nenhum inteiro a tal que $p \mid (a^2 + 1)$. (Use o pequeno teorema de Fermat.)

29. Sejam p e q primos distintos. Mostre que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. (Use o pequeno teorema de Fermat.)

30. (a) Sejam p e q números primos ímpares. Mostre que se $2^p \equiv 1 \pmod{q}$, então $q \equiv 1 \pmod{p}$. (Sugestão: note que p é a ordem de 2 no grupo $(\mathbb{Z}/q\mathbb{Z})^*$.)

(b) Mostre que, na alínea acima, se tem mesmo que $q \equiv 1 \pmod{2p}$.

(c) Use a alínea (a) para mostrar o teorema de Euclides de que há um número infinito de primos. (Sugestão: dado um primo p, os primos que dividem $2^p - 1$ são maiores do que p.)

31. Calcule $\varphi(55)$, $\varphi(128)$, $\varphi(90)$, $\varphi(89)$ e $\varphi(105)$.

32. Será que existem números naturais n e m com $\varphi(nm) \neq \varphi(n)\varphi(m)$?

33. Para que valores de n é que $\varphi(n)$ é ímpar?

34. Sejam A e B dois anéis comutativos com identidade. Mostre que o grupo das unidades $(A \times B)^*$ do anel produto $A \times B$ é o produto $A^* \times B^*$ dos grupos de unidades de A e de B.

35. Sejam $m_1, m_2, \ldots, m_k$ números naturais diferentes de 1, coprimos dois a dois. Dados $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, mostre que existe $x \in \mathbb{Z}$ tal que

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \quad \ldots \quad \ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

Mostre também que x é único módulo o produto $m_1 \cdot m_2 \cdot \ldots \cdot m_k$. (Sugestão: para a parte da existência argumente por indução e use o teorema chinês dos restos.)

36. Sejam p e q primos ímpares distintos e $n = pq$. Mostre que o polinómio $x^2 - 1$ tem exatamente quatro raízes em $\mathbb{Z}/n\mathbb{Z}$. Encontre as quatro raízes de equação $x^2 - 1 \equiv 0 \pmod{35}$.

37. Sejam $p_1, p_2, \ldots, p_r$ primos ímpares distintos e considere-se $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$.

    (a) Seja $F \subseteq \{1, 2, \ldots, r\}$. Mostre que existe $x_F \in \mathbb{Z}$ tal que $x_F \equiv 1 \pmod{p_i}$, for $i \in F$, and $x_F \equiv -1 \pmod{p_j}$, for $j \notin F$ $(1 \leq j \leq r)$.

    (b) Mostre que a equação $x^2 \equiv 1 \pmod{n}$ tem exatamente 2^r soluções.

    (c) Encontre as oito soluções de $x^2 \equiv 1 \pmod{105}$.

38. Use o método da repetição do quadrado para calcular $17^{183} \pmod{256}$, $2^{477} \pmod{1000}$, $11^{507} \pmod{1237}$, $17^{5386} \pmod{26}$ e $2^{35687} \pmod{38521}$.

39. Diga quais são os dois últimos dígitos de 3^{35}.

40. Mostre que $2^{11} - 1$ $(= 2047)$ é um número composto usando o pequeno teorema de Fermat com base 3. (Faça mesmo as contas...)

41. Calcule $2^{246082372} \pmod{246082373}$ e use a sua resposta para concluir que 246082373 não é um número primo.