MAT0164 - Números Inteiros: Uma Introdução à Matemática - 2019

Terceira Lista de Exercícios

1. Seja a um inteiro. Demonstre as afirmações abaixo.
   (a) $a^{21} \equiv a \pmod{15}$ e $a^7 \equiv a \pmod{42}$
   (b) Se $\text{mdc}(a, 35) = 1$ então $a^{12} \equiv 1 \pmod{35}$
   (c) Se $\text{mdc}(a, 42) = 1$ então $(3 \cdot 7 \cdot 8) \mid (a^6 - 1)$
2. (a) Sejam a, b inteiros e seja p um primo positivo tal que $\text{mdc}(a, p) = 1$. Mostre que $x = a^{p-2}b$ é solução da congruência $ax \equiv b \pmod{p}$.
   (b) Resolva as congruências $6x \equiv 5 \pmod{11}$ e $3x \equiv 17 \pmod{29}$.
3. (a) Sejam p um inteiro primo e sejam a, b inteiros arbitrários. Mostre que se $a^p \equiv b^p \pmod{p}$ então $a \equiv b \pmod{p}$.
   (b) Seja $p > 2$ um primo. Mostre que
   $$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$
4. Mostre que $2^8 \equiv 1 \pmod{17}$ e que $2^{16} \equiv 1 \pmod{17}$. Sejam, agora, p um primo e a um inteiro tal que $p \nmid a$. Prove que
   (a) se $p > 2$, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;
   (b) o menor inteiro positivo e tal que $a^e \equiv 1 \pmod{p}$ é divisor de $p - 1$;
   (c) se e é o inteiro acima e x é um inteiro tal que $a^x \equiv 1 \pmod{p}$ então $e \mid x$.
5. (a) Sejam p, q primos positivos distintos e seja a um inteiro tal que $a^p \equiv a \pmod{q}$ e $a^q \equiv a \pmod{p}$. Mostre que $a^{pq} \equiv a \pmod{pq}$.
   (b) Mostre que $2^{341} \equiv 2 \pmod{341}$.
6. Sejam a, m inteiros com $m > 1$. Prove que existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{m}$ se, e somente se, $\text{mdc}(a, m) = 1$. Mostre que, neste caso, o inteiro b é único, módulo m.
7. (a) Sejam p, q primos positivos distintos e ímpares tais que $(p-1) \mid (q-1)$. Mostre que se $\text{mdc}(a, pq) = 1$ então $a^{q-1} \equiv 1 \pmod{pq}$.
   (b) Seja a um inteiro. Prove que $a^{37} \equiv a \pmod{1729}$; $a^{79} \equiv a \pmod{158}$.
8. Sejam a um inteiro e n um inteiro positivo tais que $\text{mdc}(a, n) = \text{mdc}(a-1, n) = 1$. Prove que
   $$1 + a + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}.$$
9. Sejam m, n inteiros positivos relativamente primos. Prove que
   $$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$
10. Determine o resto da divisão de a por b nos casos
    (a) $a = 15!$ e $b = 17$;
    (b) $a = 2 \cdot (26)!$ e $b = 29$.
11. Reúna os inteiros $2, 3, \ldots, 21$ em pares (a, b) tais que $ab \equiv 1 \pmod{23}$.
12. Mostre que $18! \equiv -1 \pmod{437}$.
13. Calcule $\phi(n)$ para $n = 1, 2, \ldots, 12$.

14. Para que valores de n, $\phi(n)$ é ímpar?
15. Mostre que existem inteiros n para os quais $\phi(n) = 2, 4, 6, 8, 10, 12$, mas não existe n tal que $\phi(n) = 14$.
16. Encontre o menor inteiro positivo n tal que $\phi(n) = 6$.
17. Mostre que se m e n são inteiros positivos tais que m divide n, então $\phi(m)$ divide $\phi(n)$.
18. Mostre que se f é uma função multiplicativa, então $f(1) = 1$.
19. Seja f uma função multiplicativa e sejam m e n inteiros tais que $m \mid n$ e $\text{mdc}(m, n/m) = 1$. Mostre que $f(n/m) = f(n)/f(m)$.
20. Mostre que se f e g são funções multiplicativas tais que $g(n) \neq 0$ para todo inteiro positivo n, então $F(n) = f(n)g(n)$ e $G(n) = f(n)/g(n)$ são multiplicativas.
21. Sejam f e g funções multiplicativas tais que $f(p^k) = g(p^k)$ para todos os primos p e inteiros positivos k. Mostre que $f(n) = g(n)$, para todos os inteiros positivos n.
22. Dado um inteiro positivo n, considere as funções

$$\tau(n) = \text{número de divisores positivos de } n$$
$$\sigma(n) = \text{soma dos divisores positivos de } n$$

    (a) Calcule $\tau(n)$ e $\sigma(n)$ para $n = 1, 2, \ldots, 12$.
    (b) Mostre que se $n = 2^k$, então $\sigma(n) = 2n - 1$.
    (c) Encontre o menor inteiro n para o qual $\tau(n) = 6$.
    (d) Encontre o menor inteiro m para o qual não existe n satisfazendo $\sigma(n) = m$.
    (e) Mostre que um inteiro positivo p é primo se, e somente se, $\tau(p) = 2$.
    (f) Mostre que um inteiro positivo p é primo se, e somente se, $\sigma(p) = p + 1$.
    (g) Dado um inteiro $M > 1$, mostre que existem infinitos inteiros positivos n para os quais $\tau(n) = M$.
    (h) Dado um inteiro M, mostre que existe apenas uma quantidade finita de inteiros positivos n tais que $\sigma(n) = M$.
23. Dado um inteiro positivo n, considere a função

$$\chi(n) = \begin{cases} 0 & \text{se } n \text{ é par} \\ 1 & \text{se } n \equiv 1 \pmod 4 \\ -1 & \text{se } n \equiv 3 \pmod 4 \end{cases}$$

    Mostre que χ é uma função multiplicativa.
24. Construa as tabelas de adição e de multiplicação de $\mathbb{Z}_5$ e $\mathbb{Z}_6$.
25. Em $\mathbb{Z}_{20}$, determine
    (a) os menores representantes positivos de $\overline{-10}$ e $\overline{-6}$;
    (b) todos os divisores de zero;
    (c) todos os elementos inversíveis com seus inversos;
    (d) repita os itens (b) e (c) para $\mathbb{Z}_8$.

26. Mostre que o número de elementos inversíveis de $\mathbb{Z}_m$ é $\phi(m)$.
27. Seja $\overline{a} \in \mathbb{Z}_m$ não nulo. Prove que $\overline{a}$ é um divisor de zero ou $\overline{a}$ é um elemento inversível.
28. Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ com $\text{mdc}(c, m) = 1$. Prove que se $\overline{a} \cdot \overline{c} = \overline{b} \cdot \overline{c}$ então $\overline{a} = \overline{b}$.
29. Sejam p um primo positivo e $a, b \in \mathbb{Z}$. Prove que
    (a) $\overline{a}^p = \overline{a}$;
    (b) $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$.
30. Resolva em $\mathbb{Z}_m$ as equações abaixo.
    (a) $\overline{3}x + \overline{2} = \overline{6}x + \overline{7}, \ \ m = 8$;
    (b) $(\overline{2}x + \overline{3})^5 + (\overline{3}x + \overline{2})^5 + \overline{5}x = \overline{0}, \ \ m = 5$;
    (c) $\overline{4}x - \overline{7} + \overline{6}x + \overline{2} = \overline{3}x + \overline{5}x, \ \ m = 12$;
    (d) $x^{21} - x = \overline{0}, \ \ m = 5$;
    (e) $x^{12} - \overline{1} = \overline{0}, \ \ m = 5$;
    (f) $x^7 - x = \overline{0}, \ \ m = 4$.
31. Resolva em $\mathbb{Z}_5$ o sistema abaixo.
$$\begin{cases} \overline{4}x + y = \overline{1} \\ x - \overline{2}y = \overline{4} \end{cases}$$
32. Resolva em $\mathbb{Z}_4$, o sistema abaixo.
$$\begin{cases} x + y + z = \overline{0} \\ \overline{2}x + \overline{3}y + \overline{3}z = \overline{3} \\ x + y + \overline{3}z = \overline{0} \end{cases}$$