MAT0164 - Números Inteiros: Uma Introdução à Matemática - 2019

Segunda Lista de Exercícios

1. Encontre todos os inteiros positivos a tais que
$$\begin{cases} \text{mmc}(120, a) = 360 \\ \text{mdc}(450, a) = 90 \end{cases}$$
2. Resolva em $\mathbb{Z}$ o sistema abaixo
$$\begin{cases} \text{mdc}(x, y) = 20 \\ \text{mmc}(x, y) = 420 \end{cases}$$
3. Seja $n > 1$ um inteiro. Mostre que se n divide $(n-1)! + 1$, então n é primo. (*Sugestão:* Tome um divisor primo p de n e mostre que $p \geq n$.)
4. Decida se cada uma das afirmações abaixo é verdadeira ou falsa, em que a e b são inteiros positivos e p é um primo positivo. Em cada caso, dê uma demonstração ou um contra-exemplo.
   (a) Se $\text{mdc}(a, p^2) = p$, então $\text{mdc}(a^2, p^2) = p^2$.
   (b) Se $\text{mdc}(a, p^2) = p$ e $\text{mdc}(b, p^2) = p^2$, então $\text{mdc}(ab, p^4) = p^3$.
   (c) Se $\text{mdc}(a, p^2) = p$ e $\text{mdc}(b, p^2) = p$, então $\text{mdc}(ab, p^4) = p^2$.
   (d) Se $\text{mdc}(a, p^2) = p$, então $\text{mdc}(a + p, p^2) = p$.
5. Sejam $a, b \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = p$, um inteiro primo. O que se pode dizer sobre $\text{mdc}(a^2, b)$ e $\text{mdc}(a^2, b^2)$?
6. Mostrar que três inteiros positivos ímpares consecutivos não podem ser todos primos, com exceção de 3, 5 e 7.
7. Sejam p, q primos tais que $p \geq q \geq 5$. Provar que $24 \mid p^2 - q^2$.
8. Seja n um inteiro positivo. Provar que
   (a) se $2^n - 1$ é primo, então n é primo;
   (b) $n^4 + 4$ é composto, para todo $n > 1$;
   (c) todo inteiro positivo da forma $3n + 2$ tem um fator primo dessa forma;
   (d) se $n^3 - 1$ é primo, então $n = 2$;
   (e) se n é primo e $3n + 1$ é um quadrado, então $n = 5$.
9. (a) Determinar a maior potência de 14 que divide 100!.
   (b) Determinar todos os primos que dividem 50!.
10. Mostre que existem infinitos primos da forma $3n + 2$, com $n \in \mathbb{Z}$.
11. Mostre que se $2^m + 1$ é primo para algum $m > 0$ então m é uma potência de 2.
12. Seja $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n, \ldots$ a seqüência dos números primos positivos em sua ordem natural.
    (a) Mostre que $p_{n+1} \leq p_1 p_2 \ldots p_n + 1$.
    (b) Mostre que $p_n \leq 2^{2^{n-1}}$, para todo $n \geq 1$. (Sugestão: use indução.)
    (c) Conclua que existem pelo menos $n + 1$ primos menores que 2^{2^n}.

13. Prove que um inteiro é divisível por 3 se, e somente se, a soma de seus algarismos for divisível por 3. Prove que um inteiro é divisível por 9 se, e somente se, a soma de seus algarismos for divisível por 9.
14. Prove que um inteiro é divisível por 11 se, e somente se, a diferença entre a soma dos seus algarismos nas posições ímpares e a soma dos seus algarismos nas posições pares for divisível por 11.
15. Para cada inteiro $n \geq 0$, seja $F(n) = 2^{2^n} + 1$ o n-ésimo número de Fermat.
    (a) Sejam $m, n \geq 0$ inteiros tais que $n > m$. Mostre que $F(n) - 2$ é divisível por $F(m)$.
    (b) Mostre que $F(n)$ e $F(m)$ são relativamente primos, se $n \neq m$.
    (c) Mostre que $F(n) - 2$ é divisível por pelo menos n primos distintos. (Sugestão: indução em n.)
16. (a) Seja $a > 1$ um inteiro e seja $k \geq 1$ um inteiro que não é divisível por 3.
        (i) Mostre que $\text{mdc}(1 + a + a^2, 1 + a + a^2 + \cdots + a^{k-1}) = 1$.
        (ii) Mostre que $1 + a + a^2$ divide $1 + a^k + a^{2k}$.(Sugestão: fatore $a^{3k} - 1$ de duas maneiras.)
    (b) Mostre que se $1 + 2^n + 4^n$ é primo então n é potência de 3. (Sugestão: escreva $n = 3^t k$ com k não divisível por 3.)
17. (a) Encontre $x \in \mathbb{Z}$, $0 \leq x \leq 6$, tal que $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv x \pmod 7$.
    (b) Encontre $x \in \mathbb{Z}$, $0 \leq x \leq 3$, tal que $(1 + 2 + 2^2 + ... + 2^{19}) \equiv x \pmod 4$.
18. Sejam a, b inteiros e r, s inteiros positivos. Prove que:

$$a \equiv b \pmod r \iff as \equiv bs \pmod{rs}.$$

19. Sejam a, b inteiros e d, m inteiros positivos. Mostre que se $a \equiv b \pmod m$ e d divide m então $a \equiv b \pmod d$.
20. Sejam a, b inteiros e r, s inteiros positivos. Mostre que se $a \equiv b \pmod r$ e $a \equiv b \pmod s$ então $a \equiv b \pmod{\text{mmc}(r, s)}$.
21. Sejam a, b inteiros e r, m inteiros positivos. Mostre que se $ra \equiv rb \pmod m$ e $\text{mdc}(r, m) = 1$ então $a \equiv b \pmod m$.
22. Sejam a, b inteiros, r, m inteiros positivos e $d = \text{mdc}(r, m)$. Escreva $m = m_1 d$ Mostre que se $ra \equiv rb \pmod m$ então $a \equiv b \pmod{m_1}$.
23. Mostre que se $n > 4$ não é primo então $(n-1)! \equiv 0 \pmod n$.
24. Mostre que se $x \equiv y \pmod m$ então $\text{mdc}(x, m) = \text{mdc}(y, m)$.
25. Mostre que $6 \cdot 4^m \equiv 6 \pmod 9$, para todo inteiro $m \geq 0$.
26. Mostre que $5^n + 6^n \equiv 0 \pmod{11}$, para todo inteiro ímpar n.
27. Seja a um inteiro. Demonstre as afirmações abaixo.
    (a) $a^2 \equiv 0, 1$ ou $4 \pmod 8$.
    (b) Se a é um cubo, então a^2 é congruente a $0, 1, 9$ ou 28 módulo 36.
    (c) Se $2 \nmid a$ e $3 \nmid a$ então $a^2 \equiv 1 \pmod{24}$.

28. Sejam m_1, m_2 inteiros positivos relativamente primos e seja a um inteiro arbitrário. Prove que:

$$a \equiv 0 \pmod{m_1 m_2} \iff a \equiv 0 \pmod{m_1} \text{ e } a \equiv 0 \pmod{m_2}$$

O que ocorre se $\mathrm{mdc}(m_1, m_2) \neq 1$?

29. Determine o resto das divisões de:
    (a) 2^{50} por 7;
    (b) 41^{65} por 7;
    (c) $(1^5 + 2^5 + \cdots + 100^5)$ por 4;
    (d) 57383^5 por 19.
30. Use congruências para verificar que:
    (a) $89 \mid 2^{44} - 1$;
    (b) $23 \mid 2^{11} - 1$.
31. Seja $\{a_1, a_2, \ldots, a_n\}$ um sistema completo de resíduos módulo n e seja a um inteiro tal que $\mathrm{mdc}(a, n) = 1$. Prove que $\{aa_1, aa_2, \ldots, aa_n\}$ é um sistema completo de resíduos módulo n.
32. Resolva as seguintes congruências lineares:
    (a) $25x \equiv 15 \pmod{29}$;
    (b) $140x \equiv 133 \pmod{301}$.
33. Usando congruências, resolva as seguintes equações diofantinas:
    (a) $4x + 51y = 9$;
    (b) $12x + 25y = 331$.
34. Determine todas as soluções das congruências abaixo:
    (a) $3x - 7y \equiv 11 \pmod{13}$;
    (b) $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$.
35. Resolva os seguintes sistemas de congruências lineares:
    (a) $x \equiv 1 \pmod{3}$; $x \equiv 2 \pmod{5}$; $x \equiv 3 \pmod{7}$
    (b) $x \equiv 5 \pmod{6}$; $x \equiv 4 \pmod{11}$; $x \equiv 3 \pmod{7}$.
36. Determine o menor inteiro a, maior que 100, tal que:

$$2 \mid a;\ \ 3 \mid (a+1);\ \ 4 \mid (a+2);\ \ 5 \mid (a+3);\ \ 6 \mid (a+4).$$

37. Se de uma cesta com ovos retiramos duas unidades por vez, sobra 1 ovo. O mesmo acontece se os ovos são retirados de 3 em 3, de 4 em 4, de 5 em 5 e de 6 em 6. Mas não resta nenhum ovo se retirarmos 7 unidades de cada vez. Qual o menor número possível de ovos na cesta?