Ficha 4:

35. Justifique, se é verdadeira ou falsa cada uma das afirmações seguintes:

(a) $91 \equiv 0 \pmod 7$;
(b) $-2 \equiv 2 \pmod 8$;
(c) $17 \not\equiv 13 \pmod 2$.

35) a) $7 \mid 91 - 0 \Rightarrow$ $91 = 7 \times 13$ ✓ Verdadeira

b) $8 \nmid 2+2$, Falsa

c) $2 \mid 17 - 13 \Rightarrow 2 \mid 4$ Falsa.

36. Para que valores de n se tem $25 \equiv 4 \pmod n$?

$n \mid 25 - 4 \Rightarrow n \mid 21$ $D_{21} = \{-21, -7, -3, -1, 1, 3, 7, 21\}$

Para -21 e 21 $25 \underline{\lfloor -21}$ 4 Resto 4 em ambos ✓

Para -7 e 7 $25 \underline{\lfloor 7}$ $25 \underline{\lfloor 7}$ $4 \underline{\lfloor 7}$ $4 \underline{\lfloor -7}$ ✓

4^{-3} 5^{-3} 4^{0} 4^{0}

Para -3 e 3

$25 \,\lfloor 3$, 1, 8

$4 \,\lfloor 3$, 1, 1

É possível para $n: \{-21, -7, -3, 3, 7, 21\}$

37. Prove que

(a) se $a \equiv b \,(\mathrm{mod}\, n)$ e $m \mid n$, então $a \equiv b \,(\mathrm{mod}\, m)$;

(b) se $a \equiv b \,(\mathrm{mod}\, n)$ e $c > 0$, então $ca \equiv cb \,(\mathrm{mod}\, n)$.

37)

a) $a \equiv b \pmod n \Rightarrow n \mid a - b$ $\quad ny = a - b$

$m \mid n \Leftrightarrow mx = n \longrightarrow mxy = a - b \rightarrow m \mid a - b$

então, $a \equiv b \pmod m$ c.q.m.

b) $a \equiv b \pmod n \Rightarrow ny = a - b$ $\quad c > 0$

$ca - cb = c(a - b) = c(ny) = n \times (y \times c) \longrightarrow$ então, $n \mid ca - cb$,

ou seja $ca \equiv cb \pmod n$

38. Dê um exemplo que mostre que $a^2 \equiv b^2 (\mathrm{mod}\, n)$ não implica que $a \equiv b \,(\mathrm{mod}\, n)$.

$n \mid a^2 - b^2$ mas $n \nmid a - b$

$n = 5$, $a = 4$, $b = 1$

$5 \mid 4^2 - 1^2 \Leftrightarrow 5 \mid 16 - 1 \Leftrightarrow 5 \mid 15 \rightarrow$ P.V pq $5 \times 3 = 15$

mas $5 \nmid 4 - 1 \Leftrightarrow 5 \nmid 3$.

39. Determine quais dos seguintes conjuntos são sistemas completos de resíduos módulo 5:

(a) $\{-2, -1, 0, 1, 2\}$;
(b) $\{0, 5, 10, 15, 20\}$;
(c) $\{5, 11, 2, 13, 29\}$;
(d) $\{-6, -3, 0, 3, 6\}$.

Restos na divisão por 5 : $\{0, 1, 2, 3, 4\}$

39) a)

$$\left.\begin{array}{l} -2 \equiv 3 \pmod 5 \\ -1 \equiv 4 \pmod 5 \\ 0 \equiv 0 \pmod 5 \\ 1 \equiv 1 \pmod 5 \\ 2 \equiv 2 \pmod 5 \end{array}\right\} \text{correto.}$$

b) $0 \equiv 0 \pmod 5$, $5 \equiv 5 \pmod 5$, $10 \equiv 10 \pmod 5$, $15 \equiv 15 \pmod 5$, $20 \equiv 20 \pmod 5$

errado.

c) $5 \equiv 0 \pmod 5$ $\qquad 29 \equiv 4 \pmod 5$

c) $5 \equiv 0 \pmod 5$

$11 \equiv 1 \pmod 5$

$2 \equiv 2 \pmod 5$

$13 \equiv 3 \pmod 5$

$29 \equiv 4 \pmod 5$

correto

d) $-6 \equiv 4 \pmod 5$, $-3 \equiv 2 \pmod 5$ $0 \equiv 0 \pmod 5$ $3 \equiv 3 \pmod 5$

$6 \equiv 1 \pmod 5$ correto.

40. Indique, justificando, caso existam:

(a) um inteiro primo x tal que $x \in [-22]_{15} \cap [8]_{15}$;

(b) dois elementos x, y em $[20]_{15} \times ([39]_{15} + [-80]_{15})$ tais que $-40 < x < 0$ e $y > 80$;

(c) um número primo x tal que $x \equiv 6 \pmod{12}$;

(d) dois elementos distintos em $[-182]_9 \cap [20]_9$;

(e) o maior número par n tal que $-89 \equiv 5 \pmod n$;

(f) o maior inteiro x par, não positivo, tal que $x \equiv 50 \pmod{109}$.

40) a) $x \in [-22]_{15} \cap [8]_{15}$

$x \equiv -22 \pmod{15} \Leftarrow 1$

$\wedge\ x \equiv 8 \pmod{15}$

$x \equiv 8 \pmod{15}$

$15 \mid x - 8 \longrightarrow x = 23$, que é inteiro e é primo.

b) $[20]_{15} \times ([39]_{15} + [-80]_{15}) =$

$= [20]_{15} \times [41]_{15} = [5]_{15} \times [11]_{15} = [55]_{15} = [10]_{15}$

$x \equiv 10 \pmod{15}$

$-40 < x < 0$ e $y > 80$

$\Downarrow$

$x = -5$

$15 \times (-1) + 10$

$y = 100$

$\Downarrow$

$15 \times 6 + 10$

c) $x \equiv 6 \pmod{12}$

$12 \mid 6 - x \Leftrightarrow 12k = 6 - x \Leftrightarrow$

$\Leftrightarrow 12k - 6 = -x \Leftrightarrow \boxed{x = 6 - 12k}$

$\Downarrow$

tem de ser primo, mas é par.

impossível

d) $182 \,\underline{|\; 9}$

$-7 \quad -21$

$x \equiv 7 \pmod 9$

$$\begin{cases} x \equiv 7 \pmod 4 \\ x \equiv 2 \pmod 9 \end{cases}$$ impossível.

e)

$n \mid 5+89 \Rightarrow n \mid 94 \qquad n = 94$

f)

$x \equiv 50 \pmod{109}$

Como -109 será impossível. Terá de ser como $-109 \times 2 = -218$

$-218 = x - 50 \Leftrightarrow \boxed{-268 = x}$

41. Determine o resto da divisão de $2357 \times 1036 + 499$ por 11.

$(2357 \times 1036 + 499) / 11$

$2357 \equiv \cancel{7} + 3 - \cancel{7} \pmod{11}$

$(2357 \times 1036 + 499) \equiv 3 \times 2 + 4 \pmod{11}$

$\Rightarrow (2357 \times 1036 + 499) \equiv 10 \pmod{11}$

$2357 \equiv \cancel{7}+3-\cancel{7} \pmod{11}$

$1036 \equiv 6-4 \pmod{11}$

$499 \equiv \cancel{9}+4-\cancel{9}$ (mod 11

42. Na divisão por 5, um inteiro p admite resto 3. Qual é o resto da divisão de p^2+2p-1 por 5?

42) $p \equiv 3 \pmod 5$ $\qquad p = 5q+3$

$(5q+3)^2 + 2(5q+3) - 1 = 5(5q^2+6q+2q) + 9 + 6 - 1 =$

$= 5a + \boxed{14}$ $\qquad p^2+2p-1 \equiv 14 \pmod 5 \Leftrightarrow$

ou também podíamos fazer assim: $\qquad \Leftrightarrow p^2+2p \equiv 4 \pmod 5)$

$p \equiv 3 \pmod 5 \Leftrightarrow p^2 \equiv 9 \pmod 5 \Leftrightarrow$

$\Leftrightarrow p^2+2p \equiv 9+6 \pmod 5 \Leftrightarrow p^2+2p-1 \equiv 9+6-1 \pmod 5 \Leftrightarrow$

$\Leftrightarrow p^2+2p-1 \equiv 4 \pmod 5$

43. Indique os restos das divisões de 2^{50} e 41^{63} por 7.

43)

$$2^3 \equiv 1 \pmod 7 \Leftrightarrow$$

$$2^{3\times 16} \equiv 1 \pmod 7 \Leftrightarrow$$

$$\Rightarrow 2^{3\times 16} \times 2^2 \equiv 1 \times 2^2 \pmod 7 \Leftrightarrow 2^{50} \equiv 4 \pmod 7$$

$\Downarrow$ resto 4

$41 = 35 + 6$

$$41 \equiv 6 \pmod 7 \Leftrightarrow \qquad 6 \equiv -1 \pmod 7$$

$$\Leftrightarrow 41 \equiv -1 \pmod 7 \Leftrightarrow$$

$$\Leftrightarrow 41^{63} \equiv -1 \pmod 7 \Leftrightarrow$$

$$\Leftrightarrow 41^{63} \equiv 6 \pmod 7$$

44. Calcule o resto da divisão de 4^{215} por 9.

44)

$$4^3 \equiv 1 \pmod 9 \Leftrightarrow$$

$$4^{3\times 71} \equiv 1 \pmod 9 \Leftrightarrow 4^{213} \times 4^2 \equiv 1 \times 4^2 \pmod 9 \Leftrightarrow$$

$$\Leftrightarrow 4^{215} \equiv 16 \pmod 9 \Leftrightarrow 4^{215} \equiv 7 \pmod 9$$

45. Mostre que $11^{10} \equiv 1 \pmod{100}$. Método da força bruta:

45. Mostre que $11^{10} \equiv 1 \pmod{100}$. Método da força bruta:

45) $(10+1)^{11} = (10+1)^4 (10+1)^4 (10+1)^2 = 10m + 1^{10} \rightarrow$ resto $= 1$

(utilizamos o binómio de Newton)

"todos os nºs desta conta acumulados"

Com as propriedades de mod n,

$11 \times 9 \equiv -1 \pmod{100}$

$\Rightarrow (11 \times 9)^{10} \equiv (-1)^{10} \pmod{100}$

logo, podemos cortar,

$\Rightarrow 11^{10} \equiv (-1)^{10} \pmod{\frac{100}{1}} \Rightarrow$

$\Rightarrow 11^{10} \equiv 1^{10} \pmod{100}$

c.q.m

$9^{4 \times 2} \equiv 1 \pmod{100}$

$\underbrace{9^8 \times 9^2 \equiv 81 \pmod{100}}$

$81 \times 81 =$

$= 6400 + 1600 + 1$

$\approx \underline{8000 + 1}$

$19 \times 4 = 76$

$$\begin{array}{r|l} 100 & 81 \\ \hline 19 & 1 \end{array} \quad \begin{array}{r|l} 81 & 19 \\ \hline 5 & 4 \end{array} \quad \begin{array}{r|l} 19 & 5 \\ \hline 4 & 3 \end{array}$$

$$\begin{array}{r|l} 5 & 4 \\ \hline 1 & 1 \end{array} \quad \begin{array}{r|l} 4 & 1 \\ \hline 0 & \end{array}$$

$m.d.c(9^{10}, 100) = 1$

Meio aldrabado, mas se formos ver, os divisores de 100 e os de 9^{10} (podemos fatorizar), veremos que o único divisor c.c. mum é 1.