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

(a) $91 \equiv_7 0$;

(b) $-2 \equiv_8 2$;

(c) $17 \not\equiv_2 13$.

Notação: $a \equiv_n b \iff a \equiv b \pmod n$
$\iff n \mid a-b$

a) $91 \overset{?}{\equiv} 0 \bmod 7 \iff 7 \mid 91$ verdadeiro

b) $-2 \overset{?}{\equiv} 2 \pmod 8 \iff 8 \mid -2-2 \iff 8 \mid -4$ Falso

c) $17 \overset{?}{\equiv} 13 \pmod 2 \iff 2 \mid 17-13 \iff 2 \mid 4$ Verdadeiro

Portanto $17 \not\equiv 13 \pmod 2$ Falso.

33. Prove que

(a) se $a \equiv_n b$ e $m \mid n$, então $a \equiv_m b$;

(b) se $a \equiv_n b$ e $c > 0$, então $ca \equiv_n cb$.

a) Suponhamos que $a \equiv b \pmod{n}$ e que $m \mid n$

Temos que $n \mid a-b$, então $a-b = nx$, para algum $x \in \mathbb{Z}$. Como $m \mid n$ então $n = my$, para algum $y \in \mathbb{Z}$.

Logo $a-b = (my)x = m(yx)$ e portanto $m \mid a-b$.

Assim $a \equiv b \pmod{m}$.

b) Suponhamos que $a \equiv b \pmod{n}$ então $n \mid a-b$, ou seja, $a-b = nx$, para algum $x \in \mathbb{Z}$.

Assim $c(a-b) = c(nx) = n(cx)$ logo $n \mid c(a-b)$ e portanto $ca \equiv cb \pmod{n}$.

34. Dê um exemplo que mostre que $a^2 \equiv_n b^2$ não implica que $a \equiv_n b$.

Queremos dar um exemplo que mostra que

$$n \mid a^2 - b^2 \quad \not\Rightarrow \quad n \mid a - b$$

Basta tomar $n = 3$ $a = 2$ $b = 1$

Temos $3 \mid 2^2 - 1$ mas $3 \nmid 2 - 1$

ou $n = 7$ $a = 4$ $b = 3$

$7 \mid 4^2 - 3^2$ mas $7 \nmid 4 - 3$

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

Queremos saber quais são os valores de n para os quais se tem $n \mid 25-4$ ou seja $n \mid 21$

Logo $n \in \{1, 3, 7, 21\}$.

37. Verifique se:

(a) o conjunto $\{-12, -4, 11, 13, 22, 32, 91\}$ é um sistema completo de resíduos módulo 7;

(b) o conjunto $\{-2, -1, 0, 1, 2\}$ é um sistema completo de resíduos módulo 5.

Fixado $n \in \mathbb{N}$, dado $x \in \mathbb{Z}$ então x é congruente com um e um só elemento do conjunto $\{0, 1, 2, \ldots, n-1\}$

(pelo Teorema do algoritmo da divisão, x é congruente com o seu resto na divisão por n)

<u>Definição:</u> Um conjunto de resíduos módulo n (ou um sistema completo de resíduos módulo n) é um conjunto com n elementos tal que dado $x \in \mathbb{Z}$ então x é congruente com um e um só elemento desse conjunto.

NOTA O conjunto $\{0, 1, \ldots, n-1\}$ é um sistema completo de resíduos módulo n.

a) $\{-12, -4, 11, 13, 22, 32, 91\}$ é um conjunto de resíduos módulo 7?

$-12 \equiv 2 \mod 7$ $\qquad$ $13 \equiv 6 \mod 7$

$-4 \equiv 3 \mod 7$ $\qquad$ $22 \equiv 1 \mod 7$

$11 \equiv 4 \mod 7$ $\qquad$ $32 \equiv 4 \pmod 7$

Temos $4 \equiv 11 \mod 7$ $\quad$ $4 \equiv 32 \mod 7$

Logo o conjunto apresentado não é um sistema completo de resíduos módulo 7.

b) $\{-2, -1, 0, 1, 2\}$ é um sistema de resíduos módulo 5?

$0 \equiv 0 \mod 5$ $\quad\quad$ $-1 \equiv 4 \mod 5$

$1 \equiv 1 \mod 5$ $\quad\quad$ $-2 \equiv 3 \mod 5$

$2 \equiv 2 \mod 5$

Sabemos que dado um qualquer inteiro $x \in \mathbb{Z}$ então x é congruente com um e um só elemento de $\{0, 1, 2, 3, 4\}$.

Logo pela transitividade da relação de congruência módulos então qualquer $x \in \mathbb{Z}$ vai ser congruente com um e um só dos elementos do conjunto $\{0, 1, 2, -2, -1\}$.

40. Indique quatro inteiros, dois positivos e dois negativos, na classe $[3]_6$:

A relação de congruência $\equiv_n$ é uma relação de equivalência

$[x]_n$ denota a classe de equivalência de x módulo n.

Ou seja $[x]_n = \{ y \in \mathbb{Z} : x \equiv y \pmod{n} \}$

$$= \{ y \in \mathbb{Z} : n \mid x - y \} =$$

$$= \{ y = x + tn : t \in \mathbb{Z} \}$$

$[3]_6 = \{ 3 + 6t : t \in \mathbb{Z} \}$

Dois inteiros positivos em $[3]_6$: $3, 9$ $(t=0, t=1)$

Dois inteiros negativos em $[3]_6$: $-3, -9$ $(t=-1, t=-2)$

41. Indique, justificando, caso existam:

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

(b) um número primo x tal que $x \equiv_{12} 6$;

(c) dois inteiros positivos em $[-182]_9$;

(d) o maior número par n tal que $-89 \equiv_n 5$;

(e) o maior inteiro x par, não positivo, tal que $x \equiv_{109} 50$.

a) $[-22]_{15} = \{-22 + 15t : t \in \mathbb{Z}\}$

Para $t = 3$ temos $-22 + 3 \times 15 = 23 \in [-22]_{15}$

e 23 é primo.

b) $[6]_{12} = \{6 + 12t : t \in \mathbb{Z}\} = \{6(1+2t) : t \in \mathbb{Z}\}$

qualquer $x \in [6]_{12}$ é um múltiplo de 6 logo

não é primo.

c) $[-182]_9 = \{-182 + 9t : t \in \mathbb{Z}\}$

$t = 21$ $\qquad 7 \in [-182]_9$

$t = 22$ $\qquad 16 \in [-182]_9$

d) Maior inteiro par n tal que $-89 \equiv 5 \mod n$

$-89 \equiv 5 \pmod n \iff n \mid -89-5 \iff n \mid -94$

Logo $n = 94$.

e) Maior inteiro x par, não positivo, $x \equiv 50 \pmod{109}$

$x \equiv 50 \pmod{109} \iff 109 \mid x - 50$

$\iff x = 50 + t\,109 \quad , t \in \mathbb{Z}$

$t = -2$ temos $x = 50 - 2 \times 109 = -168$ (par)

Note-se que se $t \leq -3$ então $x < -168$

se $t = -1$ então x é ímpar

se $t \geq 0$ então $x > 0$

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

Propriedade: $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$

$41 \equiv -1 \mod 7 \Rightarrow 41^{63} \equiv (-1)^{63} \pmod 7$

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

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

O resto da divisão de 41^{63} por 7 é 6.

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

$50 = 3 \times 16 + 2$

$(2^3)^{16} \equiv 1^{16} \pmod 7 \Leftrightarrow 2^{48} \equiv 1 \mod 7$

$\Rightarrow 2^{50} \equiv 2^2 \pmod 7 \Leftrightarrow 2^{50} \equiv 4 \pmod 7$

O resto da divisão de 2^{50} por 7 é 4.

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

$4^{215} = 2^{430}$

$430 = 3 \times 143 + 1$

$2^3 \equiv -1 \pmod 9 \implies (2^3)^{143} \equiv (-1)^{143} \bmod 9$

$\implies 2^{429} \equiv -1 \bmod 9$

$\implies 2^{430} \equiv -2 \bmod 9$

$\implies 2^{430} \equiv 7 \bmod 9$

Logo o resto da divisão de 2^{430} por 9 é 7.

44. Usando as propriedades das congruências, mostre que, para $n \geq 1$, se tem:

$$13 | 3^{n+2} + 4^{2n+1}$$

$4^2 \equiv 3 \pmod{13} \Rightarrow 4^{2n} \equiv 3^n \pmod{13}$

$\Rightarrow 4^{2n+1} \equiv 4 \times 3^n \pmod{13}$

$\Rightarrow 4^{2n+1} + 3^{n+2} \equiv 4 \times 3^n + 3^{n+2} \pmod{13}$

$\Rightarrow 4^{2n+1} + 3^{n+2} \equiv 3^n (4 + 3^2) \pmod{13}$

$\Rightarrow 4^{2n+1} + 3^{n+2} \equiv \underline{13 \times 3^n} \pmod{13}$

Temos $13 \times 3^n \equiv 0 \pmod{13}$ logo por transitividade

$4^{2n+1} + 3^{n+2} \equiv 0 \pmod{13}$, ou seja,

$13 \mid 4^{2n+1} + 3^{n+2}$.

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

$$p \equiv 3 \pmod 5 \implies \begin{array}{l} p^2 \equiv 9 \pmod 5 \\ p^2 \equiv 4 \pmod 5 \end{array}$$

$$p \equiv 3 \pmod 5 \implies \begin{array}{l} 2p \equiv 6 \pmod 5 \\ 2p \equiv 1 \pmod 5 \end{array}$$

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

Logo o resto da divisão de $p^2 + 2p - 1$ por 5 é 4.