Monitoria:

Ex 4) $42 \mid n^7 - n \iff n^7 \equiv n \pmod{42}$

Prop. 2.39: Sejam a e b inteiros relativamente primos entre si ($mdc(a,b) = 1$) e seja c outro inteiro tal que $a \mid c$ e $b \mid c$. Então $ab \mid c$.

Dem: pág 69.

—//—

$42 = 6 \cdot 7 = 2 \cdot 3 \cdot 7$. Vamos mostrar que

$2 \mid n^7 - n$, $3 \mid n^7 - n$, $7 \mid n^7 - n$

. $2 \mid n^7 - n$.

Repare que n^7 e n tem a mesma paridade.

Note que se dois números tem a mesma paridade então a diferença é par. Daí,

$2 \mid n^7 - n$.

- $3 \mid n^7 - n$

Vamos fatorar $n^7 - n$.

$$n^7 - n = n(n^6 - 1) = n\left((n^3)^2 - 1^2\right) =$$

$$n(n^3 - 1)(n^3 + 1) = n(n^3 - 1^3)(n^3 + 1^3) =$$

$$n \cdot (n-1)(n^2 + n + 1)(n+1)(n^2 - n + 1),$$

Veja que $n = 3k + r$, $r = 0, 1, 2$. (Alg. da Divisão)

→ Se $n = 3k$. Como $n^7 - n = \underline{n}(n-1)(n^2+n+1)(n+1)$.

$(n^2 - n + 1) = 3 \cdot k(\_\_\_\_) \Rightarrow 3 \mid n^7 - n$.

→ Se $n = 3k + 1 \Rightarrow n - 1 = 3k \Rightarrow 3 \mid n^7 - n$.

→ Se $n = 3k + 2 \Rightarrow n + 1 = 3(k+1) \Rightarrow 3 \mid n^7 - n$.

—.—

Agora vamos mostrar que $7 \mid n^7 - n$. Usaremos a fatoração acima: $n^7 - n = n(n-1)(n+1)(n^2+n+1)$ $(n^2 - n + 1)$. Pelo teorema da Divisão,

$n = 7k + r$, onde $r \in \{0, \ldots, 6\}$

Indicações (fim do ex 4):

$n = 7k$ ✓

$n = 7k+1 \Rightarrow n-1 = 7k \Rightarrow 7 \mid n^7 - n$

$n = 7k+2 \Rightarrow n^2 + n + 1$ é múltiplo de 7

$n = 7k+3 \Rightarrow n^2 - n + 1$ é múltiplo de 7

$n = 7k+4 \Rightarrow n^2 + n + 1$ é múltiplo de 7

$n = 7k+5 \Rightarrow n^2 - n + 1$ é múltiplo de 7

$n = 7k+6 \Rightarrow n+1$ é múltiplo de 7

Façam as contas.

Ex 1(ii) $1 + 2 + \dots + 2^{19} \equiv x \pmod 4$ e

$x = 0, 1, 3$. Considere $a > 1$, a expoente de 2^a, então $a = 2k$ (par) ou é $2k+1$ (ímpar).

Caso $a = 2k \Rightarrow 2^a = 2^{2k} = 4^k$ Como $4 \equiv 0 \pmod 4$,

$4^k \equiv 0^k = 0 \pmod 4$. (*)

Se $a = 2k+1 \Rightarrow 2^a = 2^{2k+1} = 2 \cdot 4^k$. Como

$4^k \equiv 0 \pmod 4 \Rightarrow 2 \cdot 4^k \equiv 2 \cdot 0 = 0 \pmod 4$.

Então,

$$1 + 2 + \underbrace{2^2 + \ldots + 2^{19}}_{\equiv 0 \pmod 4} \equiv 1 + 2 + 0 \pmod 4$$

Logo $\sum_{i=0}^{19} 2^i \equiv 3 \pmod 4$

Ex 5 (Dica) $a^{2^n} \equiv 1 \pmod{2^{n+2}}$

1) Indução em n. Se $n=1$

$a^{2^n} - 1 = a^2 - 1 = (a-1)(a+1)$. Como a é ímpar, $a = 2k+1$. Daí, $(a-1)(a+1) = (2k)\,2(k+1) = 4k(k+1)$. Note k e $k+1$ tem paridades diferentes então, suponha (S.P.G), k é par $\Rightarrow k = 2l$. Logo $a^2 - 1 = 8 \cdot l \cdot (k+1)$.

Assim $8 = 2^3 \mid a^2 - 1$.

Suponha que $a^{2^n} \equiv 1 \pmod{2^{n+2}} \Rightarrow$

$2^{n+2} \mid a^{2^n} - 1$. Vamos mostrar que

$2^{(n+1)+2} \mid a^{2^{(n+1)}} - 1$. Repare que

$2^{n+1} = 2^n \cdot 2$. Então,

$$a^{2^{(n+1)}} - 1 = a^{2 \cdot 2^n} - 1 = (a^{2^n})^2 - 1^2 =$$

$(a^{2^n} + 1)(a^{2^n} - 1) \ldots$ (continuem).

Ex 8 (Dica)

$$17x \equiv 3 \pmod{\underbrace{2 \cdot 3 \cdot 5 \cdot 7}_{210}} \iff$$

$$17x \equiv 3 \pmod{210} \iff 210 \mid 17x - 3 \iff$$

$$17x - 3 = 210y \iff 17x - 210y = 3 \quad (*)$$

Agora basta resolver (*) para x.