Monitoria:

Objetivo: Ex: 6, 10, 20, 23, 29, 30, 31, 32, 33

Ex 6) Dem: Queremos que $23 \mid 2^{11} - 1$, ou ainda, que $2^{11} \equiv 1 \pmod{23}$.

$2^{11} = 2^5 \cdot 2^5 \cdot 2 \equiv 9 \cdot 9 \cdot 2 \pmod{23}$, pois

$2^5 = 32 \equiv 9 \pmod{23}$. Como $81 \equiv 12 \pmod{23}$

temos que $81 \cdot 2 \equiv 12 \cdot 2 = 24 \pmod{23}$.

Portanto, $2^{11} \equiv 24 \pmod{23}$ e $24 \equiv 1 \pmod{23}$

logo, $2^{11} \equiv 1 \pmod{23}$

$\blacksquare$

Exercício 10:

2) $12x + 25y = 331$.

obs: $ax \equiv b \pmod{m} \Leftrightarrow m \mid ax - b \Leftrightarrow ax - b = my$

$\Leftrightarrow \quad ax + m(-y) = b$.

Veja que $\overset{(*)}{12x + 25y = 331} \iff$

$12x - 25(-y) = 331$ Pelo obs.

$12x \equiv 331 \pmod{25} \iff 24x \equiv 662 \pmod{25} \iff$

$x \equiv -662 \pmod{25} \iff x = -662 + 25t,\ t \in \mathbb{Z}$

Daí, usando $(*)$,

$$12(-662 + 25t) + 25y = 331 \Rightarrow$$

$$25y = (331 + 12 \cdot 662) - 12 \cdot 25t \Rightarrow$$

$$y = 331 - 12t,\ t \in \mathbb{Z}.$$

$\blacksquare$

Exercício 20:

1) Dem: Note que $2^8 = (2^4)^2$ e

$2^4 \equiv -1 \pmod{17}$. Assim, $(2^4)^2 \equiv 1 \pmod{17} \Rightarrow$

$2^8 \equiv 1 \pmod{17}$

$\rightarrow$ Observe que $2^{16} = (2^8)^2$ e pelo "item" anterior, $2^8 \equiv 1 \pmod{17}$. Daí,

$(2^8)^2 \equiv 1 \pmod{17} \Rightarrow 2^{16} \equiv 1 \pmod{17}$

$\blacksquare$

2) Pelo teorema de Fermat,

$a^{p-1} \equiv 1 \pmod{p}$. Como p é ímpar,

$p-1 = 2k$. Daí, $a^{2k} - 1 = (a^k)^2 - 1 =$

$(a^k - 1)(a^k + 1)$. Vejam ainda que

$k = \left(\frac{p-1}{2}\right)$. Logo, $p \mid (a^k - 1)(a^k + 1) \Rightarrow$

$p \mid (a^k + 1)$ ou $p \mid a^k - 1 \Rightarrow$

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\left(\frac{p-1}{2}\right)} \equiv -1 \pmod{p}$ $\boxed{}$

3) Dem: Pelo teo. de Fermat,

$$a^{p-1} \equiv 1 \pmod p$$

Assim $e \leq (p-1)$. Se $e = p-1$, não há o que fazer.

Se $e < p-1$, considere que

$$(p-1) = e \cdot k + r, \quad 0 < r < e$$

Então, $a^{p-1} = (a^e)^k \cdot a^r$. Como $a^{p-1} \equiv 1 \pmod p$ e $a^e \equiv 1 \pmod p$ temos que

Ex 23)

(i) $(p-1)! \equiv (p-1) \pmod{1 + \dots + p-1}$

Dem: Considere $p > 2$. Observe que

$1 + 2 + \dots + (p-1) = \dfrac{p(p-1)}{2}$. Veja que

$\operatorname{mdc}\left(p, \dfrac{(p-1)}{2}\right) = 1$. Daí, vamos provar

que

1) $(p-1)! \equiv (p-1) \pmod{p}$

2) $(p-1)! \equiv (p-1) \pmod{\dfrac{(p-1)}{2}}$

1) Pelo teo. de Wilson,

$$(p-1)! \equiv -1 \pmod{p} \quad e \quad -1 \equiv p-1 \pmod{p}$$

Daí, $(p-1)! \equiv (p-1) \pmod{p}$

2) Note $p-1 = 2k$. Queremos que

$\frac{p-1}{2} \mid (p-1)! - (p-1)$. Mas veja que

$\frac{p-1}{2} = k$, $(p-1)! = (2k)!$ e $(p-1) = 2k$,

Assim, é claro que $k \mid (2k)! - 2k$

$\boxed{\Xi}$

2) Vamos provar que

$$q \mid a^p + (p-1)!\,a$$

Temos que

$$a^p \equiv a \pmod p \quad \text{e} \quad (p-1)! \equiv -1 \pmod p$$

Daí, $p \mid a^p - a$ e $p \mid (p-1)! + 1$. Logo,

$$p \mid (a^p - \cancel{a}) + a(p-1)! + \cancel{a} = a^p + a(p-1)!$$

$\blacksquare$

Outro caso fica como ex.

3) Se p é ímpar, então $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

Dem: Observe que $\{0, 1, \ldots, p-1\}$ é um sistema completo de resíduos módulo p. Além disso, $p - x \equiv -x \pmod{p}$. Assim, considerando que x percorre os ímpares entre 1 e $p-1$, temos que

$$\{0, 1, -1, 3, -3, \ldots, (p-2), -(p-2)\}$$

Pelo teorema de Wilson,

$$(p-1)! \equiv -1 \pmod{p} \Rightarrow$$

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (-1) \pmod{p} \Rightarrow$$

$$1(-1) \cdot 3(-3) \cdots (p-2) \cdot (-(p-2)) \equiv (-1) \pmod{p} \quad (*)$$

Como p é ímpar, entre 1 e $p-1$ há

$p-1$ números, sendo que $\frac{p-1}{2}$ são ímpares.

Daí, por $(*)$,

$$(-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1) \pmod{p} \Rightarrow$$

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv \underbrace{(-1) \cdot (-1)^{\frac{p-1}{2}}} \pmod{p} \Rightarrow$$

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

$\blacksquare$

Ex 29) Dem: Como $a^p \equiv a \pmod{p} \Rightarrow$

$\overline{a^p} = \overline{a}$. $\overline{a^p} = \overline{\underbrace{a \cdots}_{p \text{ vezes}} a} = \overline{a} \cdots \overline{a} =$

$\overline{a}^p$. Portanto, $\overline{a}^p = \overline{a}$.

$\blacksquare$

Ex 30 Dem: Veja que $(a+b)^p \equiv a^p + b^p$ $(\mathrm{mod}\, p)$. De fato,

$$(a+b)^p \equiv (a+b) \pmod{p},$$

$$a^p \equiv a \pmod{p} \quad \text{e} \quad b^p \equiv b \pmod{p}.$$

Daí, $(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}$.

Logo, $\overline{(a+b)^p} = \overline{a^p + b^p} \Rightarrow$

$$\overline{(a+b)}^p = \overline{a^p} + \overline{b^p} = \overline{a}^p + \overline{b}^p$$

$\blacksquare$

Ex 31) Queremos que $\overline{(p-1)}! = \overline{(-1)}$. Pelo Teorema de Wilson,

$$(p-1)! \equiv -1 \mod p \Rightarrow$$

$$\overline{(p-1)!} = \overline{(-1)} \Rightarrow \overline{(p-1)\cdot(p-2)\cdots 1} = \overline{(-1)} \Rightarrow$$

$$\overline{(p-1)} \cdot \overline{(p-1)} \cdots \overline{1} = \overline{(-1)} \Rightarrow \overline{(p-1)}! = \overline{(-1)}.$$

$\blacksquare$

<u>obs</u> Vejam prop. 3.6.2.

Ex 32

2) $(\overline{2}x + \overline{3})^5 + (\overline{3}x + 2)^5 + \overline{5}x = \overline{0}$ em

$\mathbb{Z}_5$.

Veja que, $\overline{5}x = \overline{0}$ e $(\overline{2}x + \overline{3})^5 =$

$\overline{2}x + \overline{3}$, bem como $(\overline{3}x + \overline{2})^5 =$

$\overline{3}x + \overline{2}$. Daí, temos que

$\overline{2}x + \overline{3} + \overline{3}x + \overline{2} = \overline{0} \Rightarrow \overline{5}x + \overline{5} = \overline{0}$.

Como $\overline{5} = \overline{0}$, todo elemento de $\mathbb{Z}_5$ é solução. $\blacksquare$

→ Ex 33) Em $\mathbb{Z}_{14}$

$$\begin{cases} \overline{2}x - \overline{3}y = \overline{2} \\ \overline{3}x + \overline{2}y = \overline{3} \end{cases} \Rightarrow \begin{cases} \overline{6}x - \overline{9}y = \overline{6} \\ \overline{6}x + \overline{4}y = \overline{6} \end{cases} \Rightarrow$$

$$-\overline{9}y - \overline{4}y = \overline{0} \Rightarrow \overline{-13}y = 0 \Rightarrow$$

$y = \overline{0}$. Agora baste substituir y em em uma das eqs.

Ex 34) $aRa' \Leftrightarrow f(a) = f(a')$

1) Reflexiva

2) Simetrica $(aRb) \Rightarrow (bRa)$

3) transitiva

1) $f(a) = f(a) \Rightarrow aRa$.

2) Se aRb, então $f(a) = f(b) \Rightarrow$

$f(b) = f(a) \Rightarrow bRa$.

3) aRb e $bRc \Rightarrow f(a) = f(b)$ e

$f(b) = f(c) \Rightarrow f(a) = f(c) \Rightarrow aRc$.

$\blacksquare$

Ex 16 (Rascunho)

$$\mathrm{mdc}(m, n) \mid (b - a)$$

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \Rightarrow \quad x = a + nt$$

$$a + nt \equiv b \pmod{m} \Rightarrow nt \equiv (b - a) \pmod{m}$$

$$d \mid n \qquad d \mid (b - a)$$

$$m \mid nt - (b - a) \Rightarrow$$

$$mK = nt - (\underbrace{b - a}_{c \,=\, d c_1}) \Rightarrow \cancel{d} m_1 K = \cancel{d}(n_1 t - c_1)$$

$$n_1 t \equiv c_1 \pmod{m_1}$$

$$r m_1 + s n_1 = 1 \Rightarrow s n_1 \equiv 1 \pmod{m_1}$$