Monitoria: (lista 6)

1) i $ax \equiv b \pmod{p}$. Considere $x = a^{p-2} \cdot b$,

então $a(a^{p-2}b) \equiv a^{p-1}b \pmod{p}$. (*)

Note que como $p \nmid a$, pelo teorema de

fermat, $a^{p-1} \equiv 1 \pmod{p}$. Daí, por (*),

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

e, portanto

$a \cdot x \equiv b \pmod{p}$, i.e, $x = a^{p-2} \cdot b$ é solução da

equação.

(ii) Vamos resolver $2x \equiv 1 \pmod{31}$. Veja que 31 é primo. Além disso, $mdc(2, 31) = 1$. Assim, pelo Teo. de Fermat, $2^{30} \equiv 1 \pmod{31}$. Daí,

$$2x \equiv 1 \pmod{p} \iff 2^{29} \cdot 2x \equiv 2^{29} \pmod{31} \iff$$

$$x \equiv 2^{29} \pmod{31} \iff x = 2^{29} + 31t, \; t \in \mathbb{Z}.$$

→ Ex 2:

Queremos que $1^p + 2^p + \dots + (p-1)^p \equiv 0 \pmod{p}$, p primo. Note $p \nmid 1$, $p \nmid 2$, ..., $p \nmid (p-1)$

Então pelo cor. do teo. de Fermat

($a^p \equiv a \pmod p$, p primo, $a \in \mathbb{Z}$)

$$1^p \equiv 1 \pmod p, \ \ldots, \ (p-1)^p \equiv (p-1) \pmod p$$

Vamos somar as congruências acima, então:

$$1^p + \ldots + (p-1)^p \equiv \underbrace{1 + \ldots + (p-1)}_{\frac{p(p-1)}{2} \in \mathbb{Z}} \pmod p$$

Logo $\frac{p(p-1)}{2} \equiv 0 \pmod p$. Portanto,

$$1^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$$

$\blacksquare$

↳ Ex 4

(i) $a^{37} \equiv a \pmod{1729}$

$1729 = 7 \cdot 13 \cdot 19$.

Repare que $a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19} \iff$

$7 \cdot 13 \cdot 19 \mid \underbrace{a^{37} - a}$. Vamos mostrar que

$\underbrace{7 \mid a^{37} - a}_{(1)}$, $\underbrace{13 \mid a^{37} - a}_{(2)}$ e que $\underbrace{19 \mid a^{37} - a}_{(3)}$

(1) $7 \mid a^{37} - a \iff a^{37} \equiv a \pmod 7$

Pelo alg. da divisão, $37 = 7 \cdot 5 + 2$. Daí

$a^{37} = a^{7 \cdot 5 + 2} = (a^7)^5 \cdot a^2$. Note que pelo

cor. do teo de fermat, $a^7 \equiv a \pmod 7$. Logo,

$(a^7)^5 \, a^2 \equiv a^5 \, a^2 = a^7 \equiv a \pmod 7$.

(Escrevam cuidadosamente)

(2) $13 \mid a^{37} - a \iff a^{37} \equiv a \pmod{13}$

Pelo alg. da divisão, $37 = 2 \cdot 13 + 11$. Assim,

$a^{37} = a^{2 \cdot 13 + 11} = (a^{13})^2 \cdot a^{11}$. Agora, pelo cor. do teo. de fermat, $a^{13} \equiv a \pmod{13}$ e portanto,

$$(a^{13})^2 \cdot a^{11} \equiv a^2 \cdot a^{11} = a^{13} \equiv a \pmod{13}.$$

Logo, $a^{37} \equiv a \pmod{13}$.

(3) Para vocês.

Ex 5:

obs/ Teo. de Euler: Sejam a e n inteiros, $n \geq 1$, tais que $mdc(a,n) = 1$. Então

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

— / —

Queremos que $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$. Do teo de Euler,

$$m^{\phi(n)} \equiv 1 \pmod{n} \quad (1)$$

$$n^{\phi(m)} \equiv 1 \pmod{m} \quad (2)$$

De (1), vem que $n \mid m^{\phi(n)} - 1$ e por (2)

$m \mid n^{\phi(m)} - 1$. Então,

$$mn \mid \underbrace{\left(m^{\phi(n)} - 1\right)}_{*} \left(n^{\phi(m)} - 1\right)$$

(*) $\left(m^{\phi(n)} - 1\right)\left(n^{\phi(m)} - 1\right) =$

$$m^{\phi(n)} \cdot n^{\phi(m)} - \left(m^{\phi(n)} + n^{\phi(m)}\right) + 1$$

Veja que na linguagem de congruências

temos que

$$\underbrace{m^{\phi(n)} \cdot n^{\phi(m)}} - \left(m^{\phi(n)} + n^{\phi(m)}\right) + 1 \equiv 0 \pmod{mn} \quad (3)$$

Agora perceba que para um inteiro a qualquer $\phi(a) \geq 1$ (porque no conjunto $\{1, \ldots a\}$, pelo menos $mdc(1, a) = 1$)

Logo, $\phi(n)$ e $\phi(m)$ são maiores ou iguais a 1

e $mn \mid m^{\phi(n)} \cdot n^{\phi(m)} \iff m^{\phi(n)} \cdot n^{\phi(m)} \equiv 0 \pmod{mn}$

Portanto, por (3)

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

Ex 6 (i) $a = 15!$ e $b = 17$ (Dico)

Queremos encontrar r tal que

$$15! = 17q + r, \quad 0 \leq r < 17 \quad (*)$$

Repare que na linguagem de congruências (*) é equivalente a

$$15! \equiv r \pmod{17}$$

Perceba que 17 é primo e use o teorema de Wilson,

$$(17-1)! \equiv -1 \pmod{17} \Rightarrow 16! \equiv -1 \pmod{17}$$

(...)

Ex 7: (1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, ...)

obs/ Deram os lemas 3.5.9 e 3.5.10.

Queremos associar os elementos do conj. $\{2, \ldots, 21\}$ em pares tais $a, a' \in \{1, \ldots, 21\}$, $a \neq a'$ e $a \cdot a' \equiv 1 \pmod{23}$

1) $2X \equiv 1 \pmod{23} \iff 12 \cdot 2X \equiv 12 \pmod{23} \iff$

$X \equiv 12 \pmod{23}$. Então, 2 e 12 estão associados.

2) $3X \equiv 1 \pmod{23} \Leftrightarrow 8 \cdot 3X \equiv 8 \pmod{23} \Leftrightarrow$

$X \equiv 8 \pmod{23}$. Assim, 3 e 8 estão associados.

(...) continuem.