Monitoria:

Ex 4 (item 5) $x^{4p-4} - x^{2p-2} = \bar{5}$

① Dem:

$$x^{4(p-1)} - x^{2(p-1)} = \bar{5} \iff$$

$$(x^{(p-1)})^4 - (x^{p-1})^2 = \bar{5}$$

Se $x \neq \bar{0}$, pelo teo. de fermat,

$x^{p-1} = \bar{1}$. ① Daí, $1^4 - 1^2 = \bar{0} = \bar{5}$ (*)

Se $x = 0$, então $\bar{0} = \bar{5}$

Daí, se $p = 5$, todo elemento é solução.

Se $p \neq 5$, a eq. não tem solução

□

Ex 3) Considere um anel finito A, não trivial, i.e. $A \neq \{0\}$. Suponhamos por absurdo que exista uma rel. de ordem total, que satisfaça

$$\forall a,b,c \; (a \leq b \Rightarrow a+c \leq b+c) \quad (*)$$

Seja $A = \{a_1 \leq \dots \leq a_m\}$. Tome $a_k \in A$

$$a_m + a_k \leq a_m \Rightarrow (-a_m + a_m) + a_k \leq (-a_m + a_m)$$

$$\Rightarrow a_k \leq 0, \quad k = 1, 2, \dots, m$$

Ou seja, concluímos que todo elemento de A satisfaz $a_k \leq 0$. ←

Veja que se $a_k \neq 0$ se $a_k \leq 0 \Rightarrow$ $-a_k \geqslant 0$. De fato,

$$a_k \leq 0 \Rightarrow \underbrace{-a_k + a_k}_{0} \leq -a_k \Rightarrow$$

$$0 \leq -a_k$$

→ Lista de Revisão:

Ex 16

Dem: Suponhamos que $X \equiv a \pmod{n}$ e $X \equiv b \pmod{m}$. Assim, $n \mid (x-a)$ e $m \mid (x-b)$. Já sabemos que $mdc(m,n) \mid n$ e $mdc(m,n) \mid m$. Então $mdc(m,n) \mid (x-a)$ e $mdc(m,n) \mid (x-b)$.

Com isso,

$$mdc(m, n) \mid -(x-a) + (x-b) = (a-b).$$

Reciprocamente, considere as eqs.

1) $x \equiv a \pmod{n}$

2) $x \equiv b \pmod{m}$

Da eq 1, temos $x = a + ny$. Substituindo essa exp. em (2), vem que

$$a + ny \equiv b \pmod{m} \Leftrightarrow ny \equiv (b-a) \pmod{m}$$

Como $mdc(m,n) \mid (a-b) \Rightarrow$

$mdc(m,n) \mid (b-a)$, a eq.

$$ny \equiv (b-a) \pmod{m}$$

tem solução. Logo o sistema tem solução.

∎

Ex 23 (item 3) Queremos que se p é ímpar. $1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

Dem:

Note que $\{0, 1, \ldots, (p-1)\}$ é um sistema comp. de resíduos mod p.

obs/ Ex 5 - pág 133 (relerm)

Veja que $\{0, 1, -1, \ldots, (p-2), -(p-2)\}$ é um sistema completo de resíduos módulo p.

(Depois - monitoria (20/05))

Ex 21: Queremos provar que

$$\underbrace{1 + a + \cdots +}_{\text{soma de PG (razão } a)} a^{\phi(n)-1} \equiv 0 \pmod{p}$$

Veja que $1 + \cdots + a^{\phi(n)-1} = \dfrac{1\,(a^{\phi(n)} - 1)}{(a-1)} \Rightarrow$

$(a^{\phi(n)} - 1) = (a-1) \mid \underbrace{a^{\phi(n)-1} + \cdots +}\ 1)$ Pelo

Teo. de Euler, $n \mid (a^{\phi(n)} - 1)$

Então, $n \mid (a-1)(1 + \ldots + a^{\phi(n)-1})$. Pelo

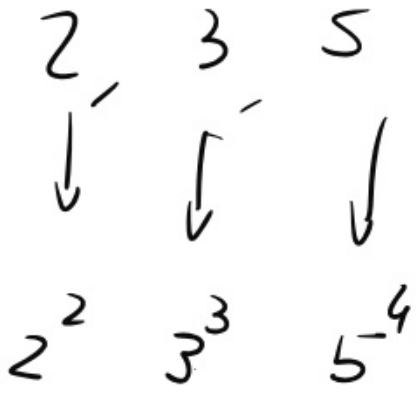
lema de Euclides, como $mdc(a-1, n) = 1$,

$n \mid 1 + \ldots + a^{\phi(n)-1}$

Ex 15 (esbozo)

$a,\ a+1,\ a+2$

$$\begin{cases} a \equiv 0 \pmod 4 \\ a \equiv -1 \pmod 5 \\ a \equiv -2 \pmod 7 \end{cases}$$



Ex 22: (Dicas)

1) Observe que podemos encarar cada termo da seq. $(1, 11, 111, \ldots)$ como soma de PG.

$a_1 \quad a_2 \quad a_3$

$$a_{n-1} = \underbrace{11\ldots1}_{n-1 \text{ vezes}} = \underbrace{10^{n-2} + \ldots + 10^0}_{\text{soma de PG (razão 10)}}$$

Então $10^{n-2} + \dots + 10^0 = 1\dfrac{(10^{n-1}-1)}{(10-1)}$ $\Rightarrow$

$9\underbrace{(10^{n-2} + \dots + 10^0)}_{a_{n-2}} = (10^{n-1}-1)$

$p \mid (10^{p-1}-1)$, $p-1 \mid n-1$ (suposição)

$(10^{p-1}) \equiv 1 \pmod p \Rightarrow (10^{p-1})^c \equiv 1 \pmod p$

$\Rightarrow 10^{n-1} \equiv 1 \pmod p$

Então, $p \mid 9(10^{n-2} + \dots + 10^0)$

Se $p \neq 3$, $p \mid \underbrace{10^{n-2} + \dots + 10^0}_{a^{n-2}}$

Note que supusemos que $p-1 \mid n-1$.

Logo $n-1 = c(p-1) \Rightarrow n = c(p-1)+1$,

$\forall c \in \mathbb{N}$, (vejam de $n > 2$)

Se $p = 3$ (escrevam com detalhes)

Ex 3

Dem: Se $a \equiv 0 \pmod{m_1 \cdot m_2} \Rightarrow$

$m_1 \cdot m_2 \mid a$ e como $m_i \mid m_1 \cdot m_2$, $i = 1, 2$,

temos que $m_i \mid a \Rightarrow a \equiv 0 \pmod{m_i}$

$i = 1, 2$.

Reciprocamente, se $a \equiv 0 \pmod{m_1}$ e

$a \equiv 0 \pmod{m_2}$ então $m_1 \mid a$ e $m_2 \mid a$.

Como $mdc(m_1, m_2) = 1 \Rightarrow$

$$m_1 \cdot m_2 \mid a \Rightarrow a \equiv 0 \pmod{m_1 \cdot m_2}$$