ESEMPIO 4: "Calcolare il resto della divisione per 62 del numero 6^{755}"

- $\varphi(n) = 62$ non è primo $= \varphi(62) = \varphi(2)\cdot\varphi(31) = 1\cdot 30 = 30$
- MCD dech: $MCD(62,6)$: $62 = 6\cdot 6 + 2$ ② — non è possibile usare Eulero e $\varphi(n)$
  $6 = 3\cdot 2 + 0$ — In questo caso conviene scomporre il membro in elementi più piccoli in cui 1 sia compatibile con MCD
- $6^{755} = (3\cdot 2)^{755} = 3^{755}\cdot 2^{755}$
  - Risoluzione per 3^{755} $MCD(62,3)$: $62 = 20\cdot 3 + 2$ sono coprimi, procedere con Eulero
    $3 = 1\cdot 2 + 1$ ①
    $2 = 2\cdot 1 + 0$
    $755 = 30\cdot 25 + 5$
    $3^{755} = 3^{30\cdot 25 + 5} = (3^{30})^{25}\cdot 3^5$
    $3^{755} \equiv 3^5 \bmod 62 = 57 \bmod 62$
  - Risoluzione per 2^{755} $MCD(62,2)$ $62 = 2\cdot 31 + 0$ Non si può usare Eulero, allo stesso tempo 62 non è rappresentabile come 2^n
    Per ciò è possibile semplificare la potenza Modulo
    $2^{755} = (2^6)^{125}\cdot 2^5 \Rightarrow 2^{125}\cdot 2^5 \Rightarrow (2^6)^{20}\cdot 2^5\cdot 2^5$ *
    $2^6 \equiv 2^{\square} \bmod 62$ * $2^{20}\cdot 2^5\cdot 2^5 \bmod 62 \Rightarrow 2^{30} \bmod 62$
    $2^{30} \equiv 2^{6\cdot 5}\ 2^5 \bmod 62$
    $32 \bmod 62$
    Costruendo il "giro" di $[a]_{62}$ con 2:
    $2^0 \equiv 1 \bmod 62$, $2^1 \equiv 2 \bmod 62$, $2^2 = 4 \bmod 62$
    $2^3 = 8 \bmod 62$, $2^4 \equiv 16 \bmod 62$, $2^5 \equiv 32 \bmod 62$
    $2^6 \equiv 2 \bmod 62$
    $32\cdot 2 = 64 = 62 + 2$

$3^{755}\cdot 2^{755} \bmod 62 = 57\cdot 32 \bmod 62$
$= 26 \bmod 62$

ESEMPIO 5 "Dato il gruppo $\mathbb{Z}_{12}$, si considerino i sottogruppi ciclici $\langle\bar{3}\rangle$ $\langle\bar{6}\rangle$. Scegliere una risposta"

A) $\langle\bar{3}\rangle \subseteq \langle\bar{6}\rangle$
B) $\langle\bar{3}\rangle \cap \langle\bar{6}\rangle = \{\bar{6}\}$
C) $|\langle\bar{6}\rangle| \geq |\langle\bar{3}\rangle|$
D) $\langle\bar{3}\rangle \cup \langle\bar{6}\rangle \equiv \mathbb{Z}_{12}$
E) $\langle\bar{3}\rangle \setminus \langle\bar{6}\rangle = \{\bar{3},\bar{9}\}$

$\langle\bar{3}\rangle = \{\bar{0},\bar{3},\bar{6},\bar{9}\}$ $\langle\bar{6}\rangle = \{\bar{0},\bar{6}\}$

A) FALSO, è vero il contrario
B) $\langle\bar{3}\rangle \cap \langle\bar{6}\rangle = \{\bar{0},\bar{6}\}$ FALSO
C) $2 \geq 4$ FALSO
D) FALSO
E) VERO