ES.: CALCOLARE L'INVERSA MOLTIPLICATIVA DI

$$[28]_{125}.$$

DOBBIAMO CALCOLARE L'ID. DI BEZOUT. CALCOLIAMO A.E.:

$$125 = 4 \cdot 28 + 13 \qquad 2 = 2 \cdot 1 + 0$$

$$28 = 2 \cdot 13 + 2$$

$$13 = 6 \cdot 2 + \boxed{1}$$

QUINDI $(125, 28) = 1$ ($\Rightarrow$ L'INVERSA MOLTIPLICATIVA ESISTE ED È UNICA).

CALCOLIAMO BEZOÚT:

$$1 = 13 + 2(-6)$$

$$= 13 + \big(28 + 13(-2)\big) \cdot (-6)$$

$$= 13 \cdot (13) + 28 \cdot (-6)$$

$$= \big(125 + 28 \cdot (-4)\big) \cdot (13) + 28 \cdot (-6)$$

$$= 125 \cdot (13) + 28\,(-58)$$

QUINDI L'ID. DI BEZOÚT È

$$1 = 125 \cdot (13) + 28 \cdot (-58)$$

PERTANTO L'INVERSA MOLTIPLICATIVA DI $[28]_{125}$ È

$$[-58]_{125} = [67]_{125}.$$

ES. : CALCOLARE LE INVERSE MOLTIPLICATIVE DI

$$[172]_{221} \quad E \quad [221]_{172}$$

RISPETTIVAMENTE.

CALCOLIAMO $(221, 172)$ CON A.E.:

$$221 = 1 \cdot 172 + 49 \qquad (1)$$

$$172 = 3 \cdot 49 + 25 \qquad (2)$$

$$49 = 1 \cdot 25 + 24 \quad (3)$$

$$25 = 1 \cdot 24 + \boxed{1} \quad (4)$$

$$24 = 24 \cdot 1 + 0$$

$\Rightarrow (221, 172) = 1$ ($\Rightarrow$ QUINDI $\exists !$ LE INVERSE).

CALCOLIAMO BEZOÚT

$$1 = 25 + 24 \cdot (-1)$$

(4) ↗

$$= 25 + \left(49 + 25 \cdot (-1)\right) \cdot (-1)$$

(3) ↗

$$= 25 \cdot (2) + 49 \cdot (-1)$$

$$= \left(172 + 49 \cdot (-3)\right) \cdot (2) + 49 \cdot (-1)$$

(2) ↗

$$= 172 \cdot (2) + 49 \cdot (-7)$$

(1) ↘

$$= 172 \cdot (2) + \left(221 + 172 \cdot (-1)\right) \cdot (-7)$$

$$= 172(9) + 221 \cdot (-7)$$

QUINDI L'I.D. DI BEZOUT È

$$1 = 172 \cdot (9) + 221 \cdot (-7)$$

PERTANTO L'INVERSA MOLTIPLICATIVA DI $[172]_{221}$ È

$$[9]_{221}$$

QUELLA DI $[221]_{172}$ È

$$[-7]_{172} = [165]_{172}.$$

ES. : CALCOLARE LE ULTIME DUE CIFRE DECIMALI DI

$$3^{100}.$$

SI CHIEDE DI CALCOLARE

$$\left[3^{100} \right]_{100}.$$

POICHÈ $(100,3)=1$ $\Rightarrow$ POSSO APPLICARE IL TEO. DI EULERO $(k=3,\ m=100)$

$\Rightarrow$ SAPPIAMO CHE

$$\left[3^{\Phi(100)} \right]_{100} = \left[1 \right]_{100}.$$

DALLA TEORIA SAPPIAMO CHE

$$\Phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$(100 = 2^2 \cdot 5^2)$

$$= 40.$$

PERTANTO

$$\left[3^{40} \right]_{100} = \left[1 \right]_{100}.$$

QUINDI

$$[3^{100}]_{100} = [3^{40}]_{100} \cdot [3^{40}]_{100} \cdot [3^{20}]_{100}$$

$$= [1]_{100} \cdot [1]_{100} \cdot [3^{20}]_{100}$$

$$= [3^{20}]_{100}.$$

CALCOLIAMO $[3^{20}]_{100}$. ABBIAMO CHE

$$20 = 16 + 4$$

E

$$[3^2]_{100} = [9]_{100}$$

$$[3^4]_{100} = \left([3^2]_{100}\right)^2 = \left([9]_{100}\right)^2 = [81]_{100}$$

$$[3^8]_{100} = \left([3^4]_{100}\right)^2 = \left([81]_{100}\right)^2 = [81^2]_{100}$$

$$= [6561]_{100} = [61]_{100}$$

$$[3^{16}]_{100} = \left([3^8]_{100}\right)^2 = \left([61]_{100}\right)^2 = [61^2]_{100}$$

$$= [3721]_{100} = [21]_{100}.$$

PERTANTO

$$[3^{20}]_{100} = [3^{16}]_{100} \cdot [3^4]_{100} = [21]_{100} \cdot [81]_{100}$$

$$= [21 \cdot 81]_{100} = [1701]_{100} = [1]_{100}.$$

CONCLUDENDO

$$[3^{100}]_{100} = [3^{20}]_{100} = [1]_{100}$$

$\Rightarrow$ ULTIME DUE CIFRE DI 3^{100} SONO 01.