

CALCOLARE L'INVERSA MULTIPLICATIVA DI

$$[28]_{125}$$

PER CALCOLARLO L'INVERSA MULTIPLICATIVA UNA  
CALCOLATA L'ID DI BETOUT. CALCOLARE L'AC

$$125 = 4 \cdot 28 + 13$$

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

$$13 = 6 \cdot 2 + 1 \quad = \text{MCD}(125, 28)$$

$$2 = 2 \cdot 1 + 0$$

CALCOLAMO L'ID DI BETOUT

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

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

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

$$= 28(-6) + (125 + 28(-1))(13)$$

$$= 125(13) + 28(-58)$$

OVRDI L'IDEA E' DI SCRIVERE IL

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

PER TORNARE ALL'INVERSA MULTIPLICATIVA.

$$D1 \quad [28]_{125} \in$$

$$[-58]_{125} = \boxed{[67]_{125}}$$

Calcolare l' inverse moltiplicativa rispettivamente

D1

$$[172]_{221} \in [221]_{172}$$

Calcolando rispettivamente l' mcj

$$221 = 1 \cdot 172 + 49$$

$$172 = 3 \cdot 49 + 25$$

$$49 = 1 \cdot 25 + 24$$

$$25 = 1 \cdot 24 + \textcircled{1} = \text{mcj}(221, 172)$$

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

Calcolando l' id di bezout

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

$$= 25(1) + (49 + 25(-1))(-1)$$

$$= 49(-1) + 25(1)$$

$$= 49(-1) + (172 + 49(-3))(1)$$

$$= 172(1) + 49(-7)$$

$$= 172(2) + (221 + 172(-1))(-7)$$

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

Quando l'10 di resto è

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

Pertanto l'inversa moltiplicativa di

$$[172]_{221} \text{ è } [9]_{221}$$

Mentre l'inversa moltiplicativa di

$$[221]_{172} \text{ è } [-7]_{172} = [165]_{172}$$


---

**Calcolare, se esiste, l'inversa moltiplicativa di**  $[56]_{34}$

Poiché calcolare l'inversa moltiplicativa abbiamo bisogno dell'10 di resto.

Imettiamo calcolatutto rcd {97, 56}

$$97 - 1 \cdot 56 + 41$$

$$S_6 = 1 \cdot 9 - 1S$$

$$q_1 = 2 \cdot 1S + 11$$

$$1S = 1 \cdot 11 + 9$$

$$\sim_1 = 2 \cdot 9 + 3$$

$$F = 1 \cdot 3 + 11 \Rightarrow \text{mcd}(97, S_6)$$

$$3 = 3 \cdot 1 + 0$$

Calculation mit SGBJT

$$1 = q(1) + 3(-1)$$

$$= q(-1) + (\sim_1 + F(-2))(-1)$$

$$= \sim_1(-1) + q(3)$$

$$\geq \sim_1(-1) + (1S + \sim_1 \cdot (-1))(2)$$

$$= 1S(2) + \sim_1(-q)$$

$$= 1S(2) + (q_1 + 1S(-2))(-q)$$

$$= q_1(-q) + 1S(-\sim_1)$$

$$= q_1(-q) + (S_6 + q_1(-1))(\sim_1)$$

$$= S_6(11) + g_1(-15)$$

$$= S_6(11) + (g_8 + S_6(-1))(-15)$$

$$= g_4(-15) + S_6(26)$$

Quasi L' INV-RSA multiplicazione.

$$\text{S1} \left[ g_6 \right]_{S7} \leftarrow [26]_{S7}$$

---

Calcola re scissione L' INV-RSA

moltiplicativa S1

$$[129]_{148}$$

Poi Calcola, re L' INV-RSA moltiplicazione

ABBIANO DISOGNUO S1 (188, 129) PCRN CALCOLA

L' 10 di 82000

$$194 = 1 \cdot 129 + 15$$

$$129 = 8 \cdot 15 + 9$$

$$15 = 1 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3 \Rightarrow \text{GCD}(144, 120)$$

$$6 = 2 \cdot 3 + 0$$

Ora calcoliamo l'1° si resto

$$\begin{aligned} 3 &= 9(1) + 6(-1) \\ &= 9(1) + (15 + 9(-1))(-1) \\ &= 15(-1) + 9(1) \\ &= -15(-1) + (120 + 15(-8))(1) \\ &= 120(1) + 15(-17) \\ &= 120(1) + (144 + 120(-1))(-1) \\ &= 144(-17) + 120(19) \end{aligned}$$

Quindi l'inversa moltiplicativa

$$9^{-1} \equiv [120]_{144}^{-1} \in [19]_{144}$$


---

CALCOLARE, SE ESISTE, L'inversa moltiplicativa di

[S6]  $\Rightarrow$

Più calcolare l'irreversibile moltiplicazione

abbiamo bisogno delle ID di  $36 \cdot 15$ , calcolando

PIVA  $(92, S6)$  utilizzando l'A.C.

$$97 = 1 \cdot S6 + f_1$$

$$S6 = 1 \cdot q_1 + r_1$$

$$q_1 = 3 \cdot 15 + 6$$

$$15 = 2 \cdot 6 + 3 \Rightarrow (94, S6)$$

$$6 = 2 \cdot 3 + 0$$

Ora calcoliamo l'ID di  $36 \cdot 15$

$$3 = 1S(1) + 6(-2)$$

$$= 1S(1) + (q_1 + _1S(-3))(-2)$$

$$= q_1(-2) + _1S(7)$$

$$= q_1(-2) + (56 + f_1(-1))(7)$$

$$= S6(7) + f_1(-2)$$

$$= 36(7) + (S6 + f_1(-1))(-2)$$

$$= 56(+)(9 + 7 \cdot 56(-1))(-1)$$

$$= 97(-1) + 56(16)$$

QUINDI L'INVERSA MOLTIPLICATIVA DI

$$\begin{bmatrix} 56 \\ 97 \end{bmatrix}_{131} \sigma \begin{bmatrix} 16 \\ ? \end{bmatrix}_{131}$$

---

CALCOLARE L'INVERSA MOLTIPLICATIVA DI

$$\begin{bmatrix} 4 \\ ? \end{bmatrix}_{131}$$

SAPPIAMO CHE TAKA, INVESSO MOLTIPLICATIVA

ESISTE SOLO SE  $\text{gcd}(131, 4) = 1$ .

CALCOLIAMO  $(131, 4)$  UTILIZZANDO L'A.E.

$$131 = 32 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1 \Rightarrow \text{rgd}(131, 4)$$

$$3 = 3 \cdot 1 + 0$$

DATO CHE  $(131, 4) = 1$  L'INVERSA

MOLTIPLICATIVA ESISTE. CALCOLIAMO

L'ID DI NGUARDI

$$1 = 4(1) + 3(-1)$$

$$= f(1) + (131 + 4 \cdot (-32))f_1$$

$$= 131(-1) + 4(33)$$

Quelques idées pour tout faire

$$1 = 131(-1) + 4(33)$$

Quelques idées pour résoudre le système

$$[f]_{131} \quad ; \quad [33]_{131}$$

Preuve :

$$[4 \cdot 33]_{131} = [132]_{131} - [1]_{131}$$

