13/10/2025

$$\begin{cases} n \equiv_{28} 17 \\ n \equiv_{5} 3 \end{cases} \Longrightarrow \begin{cases} n = 17 + 28x & x \in \mathbb{Z} \\ n = 3 + 5y & y \in \mathbb{Z} \end{cases}$$

$$28x - 5y = -14 \qquad MCD(28, 5) = 1$$

QUINDI È RISOLUBILE

$r_0 = 28$

$r_1 = 5$

$r_2 = 28 \bmod 5 = 3 \qquad 28 = 5 \cdot 5 + 3 \Rightarrow 3 = 28 - 5 \cdot 5$

$r_3 = 5 \bmod 3 = 2 \qquad 5 = 3 + 2 \Rightarrow 2 = 5 - 3$

$$\Downarrow$$

$$2 = 5 - (28 - 5 \cdot 5) = 6 \cdot 5 - 28$$

$r_4 = 3 \bmod 2 = 1 \Rightarrow 3 = 2 + 1 \Rightarrow 1 = 3 - 2 \Rightarrow$

$$\Rightarrow 1 = (28 - 5 \cdot 5) - (6 \cdot 5 - 28) = 2 \cdot 28 - 11 \cdot 5$$

$$c = -14 \qquad \frac{c}{d} = -14$$

$$-28 \cdot 28 + 154 \cdot 5 = -14$$

$$x_0 = -28 \quad e \quad y_0 = -154$$

RICORDANDOCI CHE 5 IN REALTÀ È UN -5

QUINDI: $m_0 = -28 \cdot 28 + 17 = -767$

$$m = -767 + \text{MCM}(28, 5)K = -767 + \frac{28 \cdot 5}{1}K =$$

$$= -767 + 140K \qquad K \in \mathbb{Z}$$

CIOÉ $m \equiv_{140} -767 \implies \boxed{m \equiv_{140} 73}$

ES: PER QUALI VALORI DI $a \in \mathbb{Z}$, IL SISTEMA

$$\begin{cases} m \equiv_{180} 21 + a \\ m \equiv_{105} 2a - 1 \end{cases}$$

RISOLVERLO SE POSSIBILE CON $a = -68$.

MCD $(180, 105) = 15$, QUINDI AMMETTE CHE:

$2a - 1 - (21 + a)$ SIA MULTIPLO DI 15.

$$2a - a - 1 - 21 = 15K$$

$$a - 22 = 15K$$

$$a \equiv_{15} 22 \implies a \equiv_{15} 7$$

PERCHE SE $a \equiv_m b$ → $b \bmod m \neq b$ → SI PUÒ RIDURRE

$-68 - 7 = -75$ CHÉ MULTIPLO DI 15

QUINDI È RISOLVIBILE PER $a = -68$.

$$\begin{cases} m \equiv_{180} 21 + a \\ m \equiv_{105} 2a - 1 \end{cases} \implies \begin{cases} m \equiv_{180} -47 \\ m \equiv_{105} -137 \end{cases}$$

EQUAZIONE DIOFANTEA:

$$\begin{cases} n \equiv_a x \\ n \equiv_b y \end{cases} \Rightarrow a \cdot t - b \cdot s = y - x$$

$$\boxed{180t - 105s = -90}$$

DIVIDO PER 15.

$$12t - 7s = -6 \qquad MCD(12,7) = 1$$

$r_0 = 12 \quad r_1 = 7$

$r_2 = 12 \bmod 7 = 5 \Rightarrow 12 = 7 + 5 \Rightarrow 5 = 12 - 7$

$r_3 = 7 \bmod 5 = 2 \Rightarrow 7 = 5 + 2 \Rightarrow 2 = 7 - 5 \Rightarrow$

$\Rightarrow 2 = 7 - (12 - 7) = \underline{2 \cdot 7 - 12}$

$r_4 = 5 \bmod 2 = 1 \Rightarrow 5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 \Rightarrow$

$\Rightarrow 1 = (12 - 7) - 2(2 \cdot 7 - 12) = \underline{3 \cdot 12 - 5 \cdot 7}$

$$3 \cdot 12 - 5 \cdot 7 = 1$$

MOLTIPLO PER $\underline{-6}$:

$$-18 \cdot 12 + 30 \cdot 7 = -6$$

$t_0 = -18, \; s_0 = -30$ → 7 È IN REALTÀ −7

$$n \equiv_{180} -47 \Rightarrow n = 180K - 47$$

$$n_0 = -18 \cdot 180 - 47 = \underline{-3287}$$

QUINDI TUTTE LE SOLUZIONI SONO:

$$n = -3287 + MCM(180, 105)K = \underline{-3287 + 1260K}$$

CIOÈ $m \equiv_{1260} -3287 \Rightarrow m \equiv_{1260} 523$

CLASSI DI RESTO MODULO N:

È UTILE INTRODURRE IL CONCETTO DI CLASSE DI RESTO MOD. N, CIOÈ L'INSIEME DI TUTTI I NUMERI CHE HANNO LO STESSO RESTO QUANDO SONO DIVISI PER N. (O CONGRUI MOD N)

LE OPERAZIONI $+, \cdot$ POSSONO ESSERE ESTESE ALLE CLASSI DI RESTO.

GLI INSIEMI $\mathbb{Z}_m$

SIA m INTERO POSITIVO. NOTIAMO CHE $\mathbb{Z}$ PUÒ ESSERE SUDD. IN SOTTOINSIEMI. $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$.

$[0]_m$ CONTIENE TUTTI GLI INTERI K TALI CHE $K \equiv_m 0$

$$(0, m, 2m, -m, -2m, \dots)$$

$[1]_m$ " " " TALI CHE $K \equiv_m 1$

$$(1, m+1, 2m+1, -m+1, -2m+1, \dots)$$

$[2]_m$ " " " TALI CHE $K \equiv_m 2$

$$(2, m+2, 2m+2, -m+2, -2m+2)$$

$$[m]_m = [0]_m$$

SONO INSIEMI DISGIUNTI E OGNI INTERO APPARTIENE AD UNO DI QUESTI INSIEMI. (FORMANO UNA PARTIZIONE DI $\mathbb{Z}$)

PONIAMO: $\mathbb{Z}_m : \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$

ES: $\bullet\ \mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$[0]_5 = \{0, 5, -5, -10, \dots\}$ MULTIPLI DI 5

$[1]_5 = \{1, 6, -4, -9, \dots\}$

$[2]_5 = \{2, 7, -3, -8, \dots\}$

$[3]_5 = \{3, 8, -2, -7, \dots\}$

$[4]_5 = \{4, 9, -1, -6, \dots\}$

$-99\ ? \Rightarrow [1]_5 \Rightarrow -99-1 = \underline{-100}$

$\hookrightarrow$ DIVISIBILE PER 5.

$$[a]_m + [b]_m = [(a+b) \bmod m]_m$$

$$[a]_m \cdot [b]_m = [(a \cdot b) \bmod m]_m$$

ES: $[2]_5 + [1]_5 = [3]_5$ $\qquad \mathbb{Z}_5$

$[3]_5 + [4]_5 = [7 \bmod 5]_5 = [2]_5$

$[2]_5 \cdot [1]_5 = [2]_5$ $\qquad [3]_5 \cdot [3]_5 = [9 \bmod 5]_5 =$

$= [4]_5$

$[0]_5 \cdot [2]_5 = [0]_5$

$\mathbb{Z}_9 \Rightarrow [3]_9 + [4]_9 = [7]_9$

LE OPERAZIONI $+, \cdot$ IN $\mathbb{Z}_m$ SODDISFANO LE STESSE PROP. IN $\mathbb{Z}$:

1) $[a]_m + [b]_m = [b]_m + [a]_m$

2) $[a]_m + ([b]_m + [c]_m) = ([a]_m + [b]_m) + [c]_m$

3) $[a]_m + [0]_m = [a]_m$

4) $[a]_m + [m-a]_m = [0]_m \Rightarrow [(\cancel{a} + m - \cancel{a}) \bmod m]_m = [0]_m$

5) $[a]_m \cdot [b]_m = [b]_m \cdot [a]_m$

6) $[a]_m \cdot ([b]_m \cdot [c]_m) = ([a]_m \cdot [b]_m) \cdot [c]_m$

7) $[a]_m \cdot [1]_m = [a]_m$

8) $[a]_m \cdot ([b]_m + [c]_m) = [a]_m \cdot [b]_m + [a]_m \cdot [c]_m$

OSS: LA SOTTRAZIONE È DEFINITA COME:

$$[a]_m - [b]_m = [a]_m + [m-b]_m \quad \text{OPPURE}$$

$$[(a-b) \bmod m]_m$$

OSS: $9999^3 \bmod 7 = [9999^3]_7 = [9999]_7^3 = [3]_7^3 = [27 \bmod 7]_7 =$

$= [6]_7 \longrightarrow$ QUINDI POSSIAMO FARE OGNI OPERAZIONI CON MODULO N PER SAPERE IL RISULTATO.

NON C'È STATO BISOGNO DI CALCOLARE $\underline{9999^3}$.

L'INVERSO IN $\mathbb{Z}_m$:

IN $\mathbb{Z}$ ABBIAMO VISTO CHE TUTTI GLI ELEMENTI (A PARTE ± 1) NON AMMETTONO L'INVERSO RISPETTO AL PRODOTTO, CIOÈ DATO:

$$a \in \mathbb{Z},\ a \neq \pm 1 \quad \nexists\, b \in \mathbb{Z} \text{ t.c. } a \cdot b = 1$$

PERCHÉ $b = \frac{1}{a}$ CON $a \neq \pm 1$ $b \notin \mathbb{Z}$

N.B.: INVECE IN $\mathbb{Q}$ E $\mathbb{R}$ OGNI ELEMENTO AMMETTE L'INVERSO RISPETTO AL PRODOTTO.

CI PONIAMO IL PROBLEMA: ESISTE UN INVERSO RISPETTO AL PRODOTTO IN $\mathbb{Z}_m$? CIOÉ, SE DATA UNA CLASSE DI RESTO $[a]_m$ ESISTE $[x]_m$ t.c. $[a]_m \cdot [x]_m = [1]_m$

ES: SIA $[2]_3$ LA SUA CLASSE INVERSA É:

$$[2]_3 \cdot [2]_3 = [4]_3 = [1]_3$$

OPPURE SIA $[3]_5$:

$$[3]_5 \cdot [2]_5 = [6]_5 = [1]_5$$

L'EQUAZIONE:

$$[a]_m \cdot [x]_m = [1]_m$$

É COME DIRE:

$$[ax]_m = [1]_m$$

$ax,\ m+ax,\ 2m+ax$

$1,\ m+1,\ 2m+1$

CIOÉ $\exists q \in \mathbb{Z}$ t.c. $ax = q \cdot m + 1$

ax DEVE ESSERE UN q VOLTE $m+1$ PER ARRIVARE A $[1]_m$ PERCHÉ:

$$[m+1]_m = [1]_m$$

$ax - mq = 1$ $\longrightarrow$ EQUAZIONE DIOFANTEA.

CON a E m DATI.

$\longrightarrow MCD(a, m) = 1 \longrightarrow x$ E q POSSONO ESSERE TROVATI CON L'ALG. E. e.

TEO: SIA m UN INTERO POSITIVO, $[a]_m \in \mathbb{Z}_m$, $[a]_m \neq [0]_m$.
ALLORA L'EQUAZ.

$$[a]_m \cdot [x]_m = [1]_m$$

AMMETTE SOLUZIONE SOLO CON $\underline{MCD(a, x) = 1}$

OSS: IL PRECED. TEOREMA CI DICE CHE LE CLASSI DI RESTO DI $\mathbb{Z}_m$ CHE AMMETTONO UN INVERSO PER IL PRODOTTO SONO $[a]_m$ DOVE a È PRIMO CON m. IN PARTICOLARE SE m È PRIMO. TUTTI GLI ELEMENTI DI $\mathbb{Z}_m$ A PARTE LO $[0]_m$ AMMETTONO L'INVERSO.

SE $[a]_m$ AMMETTE INVERSO, LO DENOTIAMO CON $[a]_m^{-1}$.

ES: TROVARE L'INVERSO, SE ESISTE, DI $[5]_{22}$.
NOTIAMO CHE AMMETTE INVERSO DATO CHE $MCD(5, 22) = 1$

$$\Downarrow$$

$$[5]_{22} \cdot [x]_{22} = [1]_{22}$$

$$5x = 22q + 1 \Rightarrow 5x - 22q = 1$$

ALG. E. e.: $MCD(22, 5)$

$r_0 = 22 \quad r_1 = 5$

$r_2 = 22 \bmod 5 = 2 \quad \Rightarrow 22 = 5 \cdot 4 + 2 \Rightarrow 2 = 22 - 4 \cdot 5$

$r_3 = 5 \bmod 2 = 1 \quad \Rightarrow 5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 \Rightarrow$

$\Rightarrow 1 = 5 - 2 \cdot (22 - 4 \cdot 5) = \underline{9} \cdot 5 \underline{- 2} \cdot 22$

$$x_0 = 9, \quad q = 2$$

QUINDI L'INVERSO DI $[5]_{22}$ È $[9]_{22}$

$$[5]_{22}^{-1} = [9]_{22}$$

EQUAZIONI DI I GRADO IN $\mathbb{Z}_m$

DATO CHE SAPPIAMO MOLTIPLICARE E TROVARE L'INVERSO MOLTIPLICATIVO IN $\mathbb{Z}_m$, SIAMO IN GRADO DI RISOLVERE LE EQ. DI I GRADO.

ES: RISOLVERE IN $\mathbb{Z}_{48}$ L'EQUAZIONE:

$$[11]_{48} \cdot [x]_{48} = [6]_{48}$$

CI SONO 2 MODI:

1° MODO: CALCOLO L'INVERSO, SE ESISTE, DI $[11]_{48}$ E POI MOLTIPLICO AMBO I MEMBRI PER $[11]_{48}^{-1}$.
DATO CHE MCD$(11, 48) = 1$

$$[11]_{48} \cdot [y]_{48} = [1]_{48}$$

$$11y - 48q = 1$$

ALG. E. Q. MCD$(11, 48)$

$r_0 = 48 \quad r_1 = 11$

$r_2 = 48 \bmod 11 = 4 \Rightarrow 48 = 11 \cdot 4 + 4 \Rightarrow 4 = 48 - 4 \cdot 11$

$r_3 = 11 \bmod 4 = 3 \Rightarrow 11 = 2 \cdot 4 + 3 \Rightarrow 3 = 11 - 2 \cdot 4 \Rightarrow$

$\Rightarrow 3 = 11 - 2(48 - 4 \cdot 11) = 9 \cdot 11 - 2 \cdot 48$

$r_4 = 4 \bmod 3 = 1 \Rightarrow 4 = 3 + 1 \Rightarrow 1 = 4 - 3 \Rightarrow$

$\Rightarrow 1 = 48 - 4 \cdot 11 - (9 \cdot 11 - 2 \cdot 48) = -13 \cdot 11 + 3 \cdot 48$

$y_0 = -13, \quad q_0 = -3 \qquad -13 \cdot 11 \equiv_{48} 1$

LO VOGLIAMO POSITIVO QUINDI $-13 + 48 = 35$

$$[11]_{48}^{-1} = [35]_{48}$$

QUINDI:

$$\cancel{[11]_{48}} \cdot \cancel{[11]_{48}^{-1}} \cdot [x]_{48} = [6]_{48} \cdot [11]_{48}^{-1}$$

$$[x]_{48} = [6]_{48} \cdot [11]_{48}^{-1} =$$

$$= [6]_{48} \cdot [35]_{48} = [(6 \cdot 35) \bmod 48]_{48} = [210]_{48} = [18]_{48}$$

QUINDI: $[11]_{48} \cdot [18]_{48} = [198 \bmod 48]_{48} = [6]_{48}$

2° MODO:

$$[11]_{48} \cdot [x]_{48} = [6]_{48}$$

$$[11x]_{48} = [6]_{48}$$

$11x - 48q = 6$ $\qquad$ $MCD(11, 48) = \underline{-13} \cdot 11 + \underline{3} \cdot 48 = 1$

$11t - 48s = 1$ $\qquad$ $t = -13 \quad s = -3$

$11 \cdot (-13) - 48(-3) = 1$ MOLTIPLICO PER 6

$11 \cdot (-78) - 48(-18) = 6$

$11 \cdot (-78) \equiv_{48} 6$ $\qquad \Longrightarrow -78 + 48 = -30$

$-30 + 48 = \underline{\underline{18}}$