

CLASSI DI RESTO:

$[A]_n$ L'INSIEME DI TUTTI GLI INTERI CHE DIVISO "h" DANNO RESTO "A"

$$\begin{array}{ll}
 x \equiv_3 0 & [0]_3 \\
 x \equiv_3 1 & [1]_3 \\
 x \equiv_3 2 & [2]_3
 \end{array} \rightarrow \begin{array}{ll}
 x = 3k & \\
 x = 3k + 1 & \\
 x = 3k + 2 &
 \end{array} \rightarrow \begin{array}{ll}
 \{ \dots, 0, 3, 6, \dots \} \\
 \{ \dots, 1, 4, 7, \dots \} \\
 \{ \dots, 2, 5, 8, \dots \}
 \end{array} \quad \left([\alpha]_n \leftrightarrow x \equiv_n \alpha \right)$$

prendendo n : $[0]_n$

negli insiemi c'è distinguibili, non passaggono elementi degli altri.

\vdots
 \swarrow
 $[n-1]_n$

$\text{es. } n=5$ $[0]_5$ $[1]_5$ \vdots $[4]_5$	$(\text{dove il resto modulo } 5) \text{ (resto } 5)$ hanno tutti elementi diversi, insieme formano tutti i numeri possibili (\mathbb{Z}) se c'è forse un $[5]_5$ avrebbe gli stessi elementi di $[0]_5$
--	--

OPERAZIONI:

$$[A]_n + [B]_n = [(A+B) \bmod n]_n$$

$$[A]_n \cdot [B]_n = [(AB) \bmod n]_n$$

$$[A]_n - [B]_n = \begin{matrix} \text{forma trasforma} \\ \text{-}[B]_n \text{ in} \end{matrix} + [n-B]_n \quad \begin{matrix} \text{poi sommo} \end{matrix}$$

$$\begin{array}{l}
 [2]_5 + [1]_5 = [3]_5 \\
 [3]_5 + [4]_5 = [2]_5 \leftarrow (3+4=7) \\
 [2]_5 + [1]_5 = [0]_5 \\
 \hline
 [0]_5, [2]_5, [0]_5 \\
 [3]_5, [3]_5 = [4]_5 \leftarrow (3+3=6)
 \end{array}$$

PROPRIETÀ: SOMMA:

- associativa
- commutativa
- $[\alpha]_n + [0]_n = [\alpha]_n$
- $[\alpha]_n + [n-\alpha]_n = [0]_n$

$$[(\alpha + (n-\alpha)) \bmod n]_n = [n \bmod n]_n$$

PRODOTTO:

- commutativa ($[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$)
- associativa
- $[\alpha]_n \cdot [1]_n = [\alpha]_n$
- distributiva ($[\alpha]_n \cdot [b]_n = [b]_n \cdot [a]_n + [b]_n \cdot [a]_n$)

$$\bullet [a]_n \cdot [b]_n = [a]_n + [n-b]_n \quad \left([-4]_{13} = [9]_{13} \right)$$

$$\bullet [a]_n \cdot \text{se } a \text{ è multiplo di } n \cdot [a]_n = \left[\frac{a}{n} \right]_n$$

$$\bullet [a^m]_n = [\alpha]_n^m \rightarrow \left[\frac{\alpha}{n} \right]_n^m = [a^m]_n$$

EQUAZIONE: $[a]_n \cdot [x]_n = [r]_n$ se lavoriamo solo con gli interi. Non posso fare $x = \frac{r}{a}$

$[x]_n$ è l'inverso di $[a]_n$:

$$[(a \cdot x) \bmod n]_n$$

$$a \cdot x \bmod n = 1$$

$$a \cdot x = q \cdot n + 1$$

↑
INCognite

$$ax - ny = 1$$

DIOFANTEA

ammette soluzioni solo se $\text{MCD}(a, n) = 1$

Si risolve con l'algoritmo di Euclide esteso

a mente

$$\begin{aligned} [A]_n^{-1} &= x \\ x = tc &\exists \frac{(A \cdot x) - 1}{n} \end{aligned}$$

es)

trovo $[10]_{23}^{-1}$:

$$[10]_{23} \cdot [x]_{23} = [1]_{23}$$

$$10x - 23y = 1$$

$$x = 7 \rightarrow [7]_{23}$$

o $\varphi(23) = 22$

$$[10]_{23}^{22} = 2^4 \cdot 2 + 1$$

$\stackrel{2^4}{\rightarrow} [8]_{23}$
 $\stackrel{2}{\rightarrow} [16]_{23} \quad [8+16]_{23} = [7]_{23}$
 $\stackrel{2}{\rightarrow} [12]_{23} \quad [12+16]_{23} = [7]_{23}$
 $\stackrel{2}{\rightarrow} [4]_{23}$

(caso Particolare:

n è un numero primo: MCD sempre = 1, ammette sempre inverso

semplificare usando l'inversa:

$$3_n \equiv_{28} 17$$

trova l'inverso di 3 mod 28

$$3x - 28y = 1 = [40]_{28}$$

moltiplico entrambi per l'inversa:

$$10 \cdot 3_n \equiv_{28} 10 \cdot 17 \quad \underbrace{\text{per l'inversa}}_{1} \quad \rightarrow n \equiv_{28} 323 \quad \rightarrow n \equiv_{28} 15$$

$$[A] \cdot [A]^{-1} = 1$$

$\mathbb{Z}_{48} : [11]_{48} [x]_{48} = [6]_{48}$

$\left| \begin{array}{l} ([11]_{48}^{-1} \cdot [6]_{48})^* \\ [x]_{48} = [11]_{48}^{-1} + [6]_{48} \\ [x]_{48} = [35]_{48} + [6]_{48} \end{array} \right.$

$\text{MCD}(11, 48) = 1 ? \quad \rightarrow [11]_{48}^{-1}$
 $11y - 48q = 1 \quad \rightarrow 11(-13) - 48(-3) = 1$
 $11(-13) = 35 \quad \rightarrow [35]_{48}$

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

$\left| \begin{array}{l} 11x - 48y = 6 \\ 11x = [6]_{48} \end{array} \right.$

$\text{MCD}(11, 48) = \text{divisore di } 6$

$(x < 6)$

$11x - 48y = 6 \rightarrow \text{Facile Diofantea}$

$$[\alpha]_n [x]_n = [bx]_n$$

- se $\text{MCD}(\alpha, n) = 1$ 1 soluzione
- MCD non divide b 0 soluzioni
- MCD divide b (MCD) soluzioni

$$[26]_{80} [x]_{80} = [48]_{80}$$

- $\text{MCD}(26, 80) = 2$
- $\exists \frac{48}{2} ?$ Sí, ammette soluzione
- 2 soluzioni

$$26x - 80y = 48$$

$$\begin{matrix} \downarrow & \downarrow \\ 8 & 2 \\ \downarrow & \\ \end{matrix}$$

infinitamente soluzioni

$$X = 8 + Bk \quad B = \frac{80}{\text{MCD}} = 40$$

Z_{80} : valori in $\emptyset \dots 80$

quindi k può essere solo 0 o 1

$$\therefore X = 8$$

$$\text{1: } X = 48$$

$$[15]_{36} [x]_{36} = [6]_{36}$$

- $15x - 36y = 6$
- $\text{MCD}(15, 36) = 3$

DIOFANTICA: $x = -2$

INFINITESIME SOLUZIONI:

$$x = -2 + \frac{36}{3}k$$

$$x = -2 + 12k$$

quali valori di $(-2 + 12k)$ stanno in $\emptyset \dots 35$?

SOL.

$$\left\{ \begin{array}{l} k=0 \quad x = [-2] = [36-2] = [34] \\ k=1 \quad x = [12-2] = [10] \\ k=2 \quad x = [24-2] = [22] \end{array} \right\}$$

TRASFORMARE EQUAZIONE LUNGA in STANDARD

$$[3]_{13} [x]_{13} + [5]_{13} = [6]_{13} + [9]_{13} [x]_{13}$$

$$\boxed{[A][B] = [C] \rightarrow [B] = [C][A]^{-1}}$$

$$[A] + [B] = [C] \rightarrow [B] = [C] - [A]$$

- x da un lato
- raccordo
- trasformo = in +
- $[2]_{13} \cdot [2]_{13} = [4]_{13}$
- somig

$$[3][x] - [9][x] = [6] - [5]$$

$$[x] ([3] - [9]) = [6] - [5]$$

$$[3]_{13} = [73 - 5]_{13} = [68]_{13}$$

$$[5]_{13} = [73 - 9]_{13} = [64]_{13}$$

$$[x] ([3] + [4]) = [6] + [8]$$

$$[7]_{13} [x]_{13} = [14]_{13}$$

INCOGNITA:

- quando $[a+3]_{12}$ è invertibile ?

$$[a+3]_{12} [x]_{12} = [1]_{12}$$

$(a+3)x - 12y = 1$ DICHIARO HA SOLUZIONI SOLO SE $\exists \frac{c}{\text{MCD}(a,b)}$

$\frac{1}{\text{MCD}} = \text{per entrambi deve essere per forza} = 1$

- ① QUALI VALORI HANNO $\text{MCD}(\dots, 12) = 1$?

1, 5, 7, 11

- ② QUALE AL SERVE PER DARE quei NUMERI ?

$$a = 10 \quad [10+3]_{12} = 1$$

$$a = 2 \quad [2+3]_{12} = 5$$

$$a = 4 \quad [4+3]_{12} = 7$$

$$a = 8 \quad [8+3]_{12} = 11$$

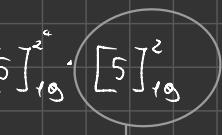
- È INVERTIBILE QUANDO $A = (10, 2, 4, 8)$

RISOLVERE ESPONENTI GRANDI

$$[5]_{10}^{1234}$$

① esponente in base 2: $1234 = 10011010010 = 2^{10} + 2^7 + 2^6 + 2^4 + 2^0$

$$[5]_{10}^{1234} = [5]_{10}^{2^{10}} \cdot [5]_{10}^{2^7} \cdot [5]_{10}^{2^6} \cdot [5]_{10}^{2^4} \cdot [5]_{10}^{2^0}$$



$$\textcircled{2} \quad [5]_{10}^2 = [5]_{10}$$

③ ALGORITMO

$$[m]_n^2 = [x_1]_n$$

$$[m]_n^{2^2} = [x_1]_n^2 = [x_2]_n$$

$$[m]_n^{2^3} = [x_2]_n^2 = [x_3]_n$$

$$[m]_n^{2^4} = [x_3]_n^2 = [x_4]_n$$

$$[m]_n^{2^5} = [x_4]_n^2 = [x_5]_n$$

$$[m]_n^{2^6} = [x_5]_n^2 = [x_6]_n$$

$$[m]_n^{2^7} = [x_6]_n^2 = [x_7]_n$$

$$[m]_n^{2^8} = [x_7]_n^2 = [x_8]_n$$

$$[m]_n^{2^9} = [x_8]_n^2 = [x_9]_n$$

$$[m]_n^{2^{10}} = [x_9]_n^2 = [x_{10}]_n$$

④ $[5]_{10}^{1234} = \text{PRODOTTO DI } \dots \text{ (←)}$