

# Appunti di Algebra

Quel ragazzo con la maglia blu

## Contents

<b>1</b>	<b>Divisione nei numeri naturali e nei numeri interi</b>	<b>2</b>
1.1	Divisione in $\mathbb{N}$ . . . . .	2
1.2	Divisione in $\mathbb{Z}$ . . . . .	2
1.3	Divisibilità in $\mathbb{N}$ e $\mathbb{Z}$ . . . . .	3
1.4	Massimo Comun Divisore in $\mathbb{N}$ ed in $\mathbb{Z}$ . . . . .	3
1.5	Calcolo MCD in $\mathbb{N}$ : Algoritmo di Euclide . . . . .	5
1.5.1	In $\mathbb{N}$ . . . . .	5
1.5.2	In $\mathbb{Z}$ . . . . .	6
<b>2</b>	<b>Polinomi</b>	<b>7</b>
2.1	Somma di polinomi . . . . .	7
2.2	Prodotto di polinomi . . . . .	7
2.3	Divisioni di polinomi . . . . .	8
2.4	Radici di un polinomio . . . . .	8
2.4.1	Teorema di Ruffini . . . . .	8
2.4.2	Radici di polinomi di 2° grado a coefficienti reali . . . . .	8
2.5	Teorema fondamentale dell'algebra . . . . .	9
2.6	Identità di Bezout (teorema) . . . . .	10
<b>3</b>	<b>Classi di Congruenza</b>	<b>12</b>
3.1	Invertibili in $\mathbb{Z}_n$ e il loro calcolo . . . . .	15
3.2	La funzione di Eulero . . . . .	15
3.3	Sistema di congruenze . . . . .	16
3.4	Il teorema cinese dei resti . . . . .	17
3.4.1	Metodo di Newton . . . . .	17
3.5	Ridurre un generico sistema di congruenze . . . . .	20
3.6	Esercizio tipo . . . . .	22
<b>4</b>	<b>Matrici e loro operazioni</b>	<b>24</b>
4.1	Operazioni . . . . .	24
4.1.1	Prodotto di una matrice per uno scalare . . . . .	24
4.2	Somma di due matrici . . . . .	25
4.3	Prodotto di un vettore riga per un vettore colonna . . . . .	26
4.4	Prodotto di due matrici (riga per colonna) . . . . .	27
4.5	La trasposta . . . . .	29
4.6	La coniugata . . . . .	30
4.7	Tipi di matrici . . . . .	31
4.8	Scrittura matriciale di un sistema lineare . . . . .	32



**NB2**  $q, r$  sono unici perché si richiede  $0 \leq r < |b|$

**NB3**  $a, b \in \mathbb{Z}, b \neq 0$  in  $\mathbb{Z} : a = bq_1 + r_1, 0 \leq r_1 < |b|$   
 $|a|, |b| \in \mathbb{N}, |b| \neq 0$  in  $\mathbb{N} : |a| = |b| \cdot q_2 + r_2, 0 \leq r_2 < |b|$

**ATTENZIONE** Non c'è un nesso tra il quoziente ed il resto della divisione di  $a$  e  $b$  in  $\mathbb{Z}$  ed il quoziente ed il resto della divisione di  $|a|$  e  $|b|$  in  $\mathbb{N}$

**Ad esempio**

$$\begin{array}{lcl} a = -137 & -137 = 55(-3) + 28 & |a| = 137 \\ b = 55 & \begin{array}{c} \text{a} \quad \text{b} \quad q_1 \quad r_1 \end{array} & \begin{array}{c} |a| = 137 \\ |b| = 55 \end{array} \end{array} \quad \left| \quad \begin{array}{lcl} 137 = 55 \cdot 2 + 27 & & \\ \begin{array}{c} |a| \quad |b| \quad q_2 \quad r_2 \end{array} & & \end{array} \right.$$

### 1.3 Divisibilità in $\mathbb{N}$ e $\mathbb{Z}$

**Divisibilità in  $\mathbb{N}$**   $a, b \in \mathbb{N}, b \neq 0$

$$\begin{array}{ll} b|a \text{ se } a = bq \exists q \in \mathbb{N}^1 & b \nmid a \\ \text{divide} & \text{non divide} \\ \text{Es. } 6|18 & \text{Es. } 4|18 \end{array}$$

Per esempio  $6|18$

**Divisibilità in  $\mathbb{Z}$**   $a, b \in \mathbb{Z}, b \neq 0$

$$b|a \text{ se } \exists q \in \mathbb{Z} | a = bq \quad \text{altrimenti } b \nmid a$$

$$\text{NB} \quad a, b \in \mathbb{N}, b \neq 0, a \neq 0 \quad \begin{cases} b|a \\ a|b \end{cases} \implies a \in \{b, -b\}$$

### 1.4 Massimo Comun Divisore in $\mathbb{N}$ ed in $\mathbb{Z}$

**MCD In  $\mathbb{N}$**   $\forall a, b \in \mathbb{N}, (a, b) \neq (0, 0)$

(almeno uno dei due deve essere diverso da 0)

Un  $d \in \mathbb{N}$  è un  $MCD(a, b)$  se

1.  $d|a$  e  $d|b$  (è un divisore comune di  $a$  e  $b$ )
2. se  $z|a$  e  $z|b \implies z|d$

Ossia, se  $d$  è un divisore comune di  $a$  e  $b$  CHE

**NB 1**  $MCD(a, b)$  è ! in  $\mathbb{N}$  è il  $MCD(a, b)$

$$\begin{array}{ll} 60 = 2^2 \cdot 3 \cdot 5 & 18 = 2 \cdot 3^2 \\ \\ \begin{array}{l} 60|2 \\ 30|2 \\ 15|3 \\ 5|5 \end{array} & \begin{array}{l} 18|2 \\ 9|3 \\ 3|3 \end{array} \\ & d = 2 \cdot 3 = 6 \end{array}$$

**NB 2**  $MCD(a, b) = MCD(b, a)$

**NB 3**

$$\begin{cases} b|a \\ b \neq 0 \end{cases} \implies MCD(a, b) = b \quad (1)$$

**NB 4**  $a, b \in \mathbb{N} \quad b \neq 0 \quad \exists q, r \in \mathbb{N}$   
 $a = bq + r^2 \quad 0 \leq r < b$

Perciò

$$MCD(a, b) = MCD(b, r)$$

Per provarlo, proviamo che i due insiemi  $A$  e  $B$  sono uguali:

$A = \{z \mid z|a \text{ e } z|b\}$  = insieme dei divisori comuni di  $a$  e  $b$   
 $B = \{w \mid w|b \text{ e } w|r\}$  = insieme dei divisori comuni di  $b$  e  $r$

$$z \in A \implies \begin{cases} z|a \\ z|b \end{cases} \quad \begin{cases} z|a - bq = r \\ z|b \end{cases} \implies z \in B \implies A \subseteq B$$

$$w \in B \implies \begin{cases} w|b \\ w|r \end{cases} \quad \begin{cases} w|b \\ w|bq + r = a \end{cases} \implies w \in A \implies B \subseteq A$$

In  $\mathbb{Z} \quad \forall a, b \in \mathbb{Z}$  con  $(a, b) \neq (0, 0) \quad d \in \mathbb{Z}$  è un  $MCD(a, b)$  se

1.  $d|a$  e  $d|b$   $d$  è un divisore comune di  $a$  e  $b$

2.  $\begin{cases} z|a \\ z|b \end{cases} \implies z|d$   $d$  è un multiplo di ogni divisore comune di  $a$  e  $b$

Abbiamo già visto che  $d = MCD(a, b)$  è unico in  $\mathbb{N}$

Anche in  $\mathbb{Z}$  scrivo  $d = MCD(a, b)$  anche se la nozione è “impropria”.

**NB** In  $\mathbb{Z}$   $d$  è individuale e **non ha segno**.

Se  $d$  è un massimo comun divisore di  $a$  e  $b$  allora anche  $-d$  è un massimo comun divisore di  $a$  e  $b$ .

Quindi in  $\mathbb{Z}$   $MCD(a, b)$  non indica un solo numero, ma 2:  $d$  e  $-d$ .

Es.  $-6 = MCD(-12, 18) = +6$

**Perché per parlare di  $MCD(a, b)$  è necessario supporre  $(a, b) \neq (0, 0)$**

---


$$^2r = a - bq$$

$$\begin{array}{lcl} \text{NB} & \frac{2|0}{b \ a} & \frac{0}{a} = \frac{2 \cdot 0}{b \ q} \\ 3|0 & 142|0 & \forall b \neq 0 \quad b|0 \end{array}$$

Ecco perchè è importante quando si parla di  $\text{MCD}(a, b)$   
**se fosse**  $(a, b) = (0, 0)$  allora  $\forall z \neq 0 \ z|0$

L'insieme dei divisori comini di  $(a, b) = (0, 0)$  è

$$\{z|z \in \mathbb{Z}, z \neq 0\}$$

Dunque non c'è un  $MCD(a, b)$  nel casi in cui  $(a, b) = (0, 0)$

$$\begin{array}{ll} \mathbf{NB} & a, b \in \mathbb{Z}, b \neq 0 \\ & a = bq + r \quad 0 \leq r < |b| \end{array}$$

$$\implies MCD(a, b) = MCD(b, r)$$

è la stessa osservazione che abbiamo fatto per  $MCD(a, b)$  nel caso  $a, b \in \mathbb{N}$ ,  $b \neq 0$

**NB**  $a, b \in \mathbb{Z}$ , **non entrambi nulli** allora  
 $MCD(a, b) = MCD(-a, b) = MCD(a, -b) = MCD(-a, -b)$

### 1.5 Calcolo MCD in $\mathbb{N}$ : Algoritmo di Euclide

### 1.5.1 In $\mathbb{N}$

$$a, b \in \mathbb{N}, b \neq 0 \neq a$$

**1° passaggio**  $a = bq_1 + r_1$   $0 \leq r_1 < b$

**SE**  $r_1 = 0$   $MCD(a, b) = MCD(b, r_1) = MCD(b, 0) = b$   
**STOP**

Esempio 1       $\text{MCD}(\underset{a}{36}, \underset{b}{12}) =$

$$\mathbf{P1} \quad \underset{a}{36} = \underset{b}{12} \cdot \underset{q_1}{3} + \underset{r_1}{0} \implies MCD(36, 12) = MCD(12, 0) = 12$$

$$1^o \mathbf{P} \ a = bq_1 + r_1 \qquad 0 \leq r_1 < b$$

**SE  $r_1 \neq 0$  continua.**

**2° passaggio SI DIVIDE  $b$  per  $r_1$**

$$b = r_1 q_2 + r_2 \quad =_{\leq} r_2 < r_1$$

**SE  $R_2 = 0$  STOP**

$$\begin{array}{ccccccc} \text{MCD}(a, b) & = & \text{MCD}(b, r_1) & = & \text{MCD}(r_1, r_2) & = & \text{MCD}(r_1, 0) = r_1 \\ & & \uparrow & & \uparrow & & \\ & & b = r_1 q_2 + r_2 & & \text{se } r_2 = 0 & & \end{array}$$

Potevo vederlo così: se  $r_2 = 0$  allora  $b = r_1q_2 + r_2 = r_1q_2$   
 per cui  $\text{MCD}(b, r_1) = r_1$  quindi  $\text{MCD}(a, b) = \text{MCD}(b, r_1) = r_1$

Esempio 2      $\text{MCD}(\underset{a}{42}, \underset{b}{12} = 6)$

$$\frac{r_1 \neq 0}{\frac{1^{\circ}p}{2^{\circ}p}} \quad \frac{42 = 12 \cdot 3 = 6}{\frac{a}{b} \quad \frac{q_1}{r_1} \quad \frac{r_2}{q_2} \quad \frac{r_1}{r_2}} \quad \text{SE } r_2 \neq 0 \text{ continuo...}$$

$MCD(A, B)$  è l'ultimo resto non nullo della sequenza di divisioni successive

**Es 1**  $MCD(36, 28) = 4$

$$\begin{array}{lcl} \underline{1^o p} & 36 = 28 \cdot 1 + 8 & \\ \underline{2^o p} & 28 = 8 \cdot 3 + 4 & \\ \underline{3^o p} & 8 = 4 \cdot 2 + 0 & r_3 = 0 \implies r_2 = MCD \end{array}$$

**Es 2**  $MCD(2420, 1386) = 22$

$$\begin{array}{lcl} \underline{1^o p} & 2420 = 1386 \cdot 1 + 1034 & \\ \underline{2^o p} & 1386 = 1034 \cdot 1 + 352 & \\ \underline{3^o p} & 1034 = 352 \cdot 2 + 330 & \\ \underline{4^o p} & 352 = 330 \cdot 1 + 22 & \\ \underline{5^o p} & 330 = 22 \cdot 15 + 0 & \end{array}$$

### 1.5.2 In $\mathbb{Z}$

**1° modo** consigliato

- $|a|, |b| \in \mathbb{N}$
- $MCD(|a|, |b|) = d \in \mathbb{N}$
- $d, -d$  boh illeggibile  $MCD(a, b)$  in  $\mathbb{Z}$

**2° modo** Algoritmo di Euclide in  $\mathbb{Z}$

**Esempio**  $MCD(-274, 110)$

$$\begin{aligned} |a| &= |-274| = 274 \\ |b| &= |110| = 110 \end{aligned}$$

**1° Modo** svolgimento

$$\begin{array}{lcl} \underline{1^o p} & 274 = 110 \cdot 2 + 54 & \\ \underline{2^o p} & 110 = 54 \cdot 2 + 2 & \\ \underline{3^o p} & 54 = 2 \cdot 27 + 0 & \\ & & MCD(|a|, |b|) = d = 2 \implies 2 \text{ e } -2 \text{ sono i } MCD(-274, 110) \end{array}$$

**2° Modo** Algoritmo di Euclide in  $\mathbb{Z}$

$$\begin{array}{lcl} \underline{1^o p} & 274 = 110 \cdot (-3) + 56 & |b| > r_1 \geq 0 \\ \underline{2^o p} & 110 = 56 \cdot 1 + 54 & \\ \underline{3^o p} & 56 = 54 \cdot 1 + 2 & 2 \text{ e } -2 \text{ sono i due massimi comuni divisori di } -274 \text{ e } 110 \\ \underline{4^o p} & 54 = 2 \cdot 27 + 0 & \end{array}$$

## 2 Polinomi

$$S \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$$

$S[x]$  = Insieme dei polinomi a coefficienti in  $S$  nella indeterminata  $x$

$f(x) \in S[x]$  se  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  Robette che non ho capito bene bene bene

Se  $a_n \neq 0$  IL GRADO DI  $f(x)$  è

$n = \deg f(x)$ ;  $a_n$  si chiama **coefficiente direttore** di  $f(x)$ ,  $a_0$  si chiama **termine noto** di  $f(x)$

$$\text{NB 1} \quad \begin{cases} c \in S \\ c \neq 0 \end{cases} \longrightarrow \deg c = 0$$

$$\text{NB 2} \quad c = 0 \in S \quad \text{per convenzione di pone } \deg 0 = -\infty$$

### 2.1 Somma di polinomi

$\forall f(x), g(x) \in S[x]$  definisco  $f(x) + g(x) \in S[x]$

$$\text{Es} \quad f(x) = 2 - x^3 + 3x^2 \quad g(x) = 7x + x^3 + 12$$

$$\begin{array}{rcl} 2 + 0x + 3x^2 - x^3 + & \deg f(x) = 3 & \\ 12 + 7x + 0x^2 + x^3 = & \deg g(x) = 3 & \\ \hline 14 + 7x + 3x^2 & \deg(f(x) + g(x)) \leq 3 & \end{array}$$

$$\begin{array}{lcl} f(x) = a_0 + a_1x + \dots + a_nx^n = \sum_{i=0}^n a_i x^i & a_n = 0, \deg f(x) = n & \\ g(x) = b_0 + b_1x + \dots + b_mx^m = \sum_{i=0}^m b_i x^i & b_m = 0, \deg g(x) = m & \end{array}$$

Per fissare le idee si ponga che  $m \leq n$

$$f(x) + g(x) = \sum_{i=0}^m (a_i + b_i)x^i + \sum_{i=m+1}^n a_i x^i$$

$$\text{NB} \quad \deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

### 2.2 Prodotto di polinomi

$\forall f(x), g(x) \in S[x]$  definisco  $f(x) \cdot g(x) \in S[x]$

nel seguente modo:

se  $f(x) = \sum_{i=0}^n a_i x^i$  e  $g(x) = \sum_{i=0}^m b_i x^i$  allora

$$\begin{aligned} f(x)g(x) &= \left( \sum_{i=0}^n a_i x^i \right) \left( \sum_{i=0}^m b_i x^i \right) = \\ &= (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) = \\ &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots = \sum_{i=0}^i a_k b_{i-k} \left( \sum_{k=0}^i a_k b_{i-k} \right) x^i \end{aligned}$$

$$\text{NB} \quad \deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$$

$$\begin{array}{lcl} \text{Esempio} & f(x) = 2 - x + 6x^2 & g(x) = 1 + 4x \\ & (2 - x + 6x^2)(1 + 4x) = \dots = 2 + 7x - 4x^2 + 6x^4 + 24x^5 & \end{array}$$

$$\text{DA QUESTO MOMENTO } S \neq \mathbb{Z} : \quad S \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$$

## 2.3 Divisioni di polinomi

$\forall f(x), g(x) \in S[x], g(x) \neq 0 \exists! q(x), r(x) \in S[x]$  tale che  $\begin{cases} f(x) = g(x)q(x) + r(x) \\ \deg r(x) < \deg g(x) \end{cases}$

**Esempio** Divido  $f(x) = 7x^4 + 3x - 2 \in \mathbb{Q}[x]$  per  $g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$

$$\begin{array}{r|l} 7x^4 & x^2 + x + 1 \\ -7x^4 - 7x^3 - 7x^2 & \\ \hline & -7x^3 - 7x^2 \\ & 7x^3 + 7x^2 + 7x \\ \hline & 7x \end{array}$$

## 2.4 Radici di un polinomio

Sia  $f(x) \in S[x]$ .

Un numero  $x_0 \in S$  si dice una **radice**<sup>3</sup> di  $f(x)$  se  $f(x_0) = 0$ <sup>4</sup>

Quindi  $x_0$  è una radice di  $f(x)$  se e solo se  $x_0$  è una soluzione dell'equazione  $f(x) = 0$

**Esempio**  $f(x) = x^2 + 2x + 1 = (x + 1)^2$   
 $x_0 = -1$  è una radice di  $f(x)$ :  $f(-1) = (-1 + 1)^2 = 0$   
 $x_0 = 1$  è soluzione dell'equazione  $x^2 + 2x + 1 = 0$ <sup>5</sup>

### 2.4.1 Teorema di Ruffini

Se  $f(x) \in S[x]$  ed  $x_0 \in S$

$(x_0 \text{ è una radice di } f(x)) \iff (x - x_0) \mid f(x) \iff f(x) = (x - x_0)q(x)$   
(divide)  $\exists q(x) \in S[x]$

dividendo  $f(x)$  per  $x - x_0$  si ha  $r(x) = 0$

### 2.4.2 Radici di polinomi di 2° grado a coefficienti reali

$ax^2 + bx + c = 0$   $a, b, c \in \mathbb{R}$   $a \neq 0$

$\Delta = b^2 - 4ac$  è il discriminante dell'equazione

- SE  $\Delta > 0$  ci sono due soluzioni REALI distinte

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

- SE  $\Delta = 0$  l'equazione ha UNA soluzione REALE  
 “contata due volte”

$$(x^2 + 2x + 1) = (x + 1)(x + 1) \quad x_1 = x_2 = \frac{-b}{2a}$$

- SE  $\Delta < 0$  l'equazione non ha soluzioni reali, ma ha 2 soluzioni complesse

$$x_1 = \frac{-b + i\sqrt{-\Delta}}{2a} \quad x_2 = \frac{-b - i\sqrt{-\Delta}}{2a}$$

Poiché  $\sqrt{-\Delta} \neq 0 \implies x_1 \neq x_2$

L'equazione ha 2 soluzioni complesse **coniugate** (l'una coniugata dell'altra)

$$x_1 = \overline{x_2}$$

<sup>3</sup>oppure uno zero

<sup>4</sup>“f valutato in  $x_0 = 0$ ”

<sup>5</sup>ovvero  $f(x)$



$$x_2 = \overline{x_1}$$

**Equivalentemente** dato  $f(x) = ax^2 + bx + c$ ,  $a, b, c \in \mathbb{R}$ ,  $a \neq 0$   
 $f(x) = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right)$  e  $x^2 + \frac{b}{a}x + \frac{c}{a}$  ha due radici complesse  $x_1, x_2$

$$x^2 + \frac{b}{a}x + \frac{c}{a} = (x - x_1)(x - x_2)$$

e quindi

$$f(x) = ax^2 + bx + c = a(x - x_1)(x - x_2)$$

$$\exists x_1, x_2 \in \mathbb{C} \quad a, b, c \in \mathbb{R}, a \neq 0$$

## 2.5 Teorema fondamentale dell'algebra

$$\forall f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$a_0, a_1, a_2, \dots, a_n \in \mathbb{C}$$

$$\text{polinomio di grado } n > 0 \quad (a_n \neq 0)$$

$\exists z_1, z_2, \dots, z_n \in \mathbb{C}$  tale che

$$f(x) = a_n(x - z_1)(x - z_2)\dots(x - z_n)$$

potrebbero esserci ripetizioni

**Ad esempio** se  $f(x) = (x-1)^n = (x-1)(x-1)\dots(x-1)$  allora  $z_1 = z_2 = \dots = z_n = 1$   
**Ogni polinomio di grado  $n > 0$  e coefficienti complessi è prodotto di  $n$  polinomi di grado 1**

Se  $z_0, z_1, \dots, z_x$  <sup>6</sup> sono quegli  $z_i$  **DISTINTI**, allora

$$f(x) = a_n(x - z_1)^{m_1}(x - z_2)^{m_2}\dots(x - z_k)^{m_k}$$

**$m_i$  = la molteplicità algebrica di  $z_i$**

È equivalente a:  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$

L'equazione  $f(x) = 0$  <sup>7</sup> ha  $n$  soluzioni:

$z_1$  contata  $m_1$  volte

$z_2$  contata  $m_2$  volte

$z_3$  contata  $m_3$  volte

...

...

$z_k$  contata  $m_k$  volte

$$m_1 + m_2 + \dots + m_k = n$$

**Esempio**  $f(x) = (x^2 + 2x + 1)(x - 3) = (x - 1)^2(x - 3)$

$z_1 = -1$   $m_1 = 2$

$z_2 = 3$   $m_2 = 1$

**Ogni equazione a coefficienti complessi di grado  $n$  ha  $n$  soluzioni complesse contate con le loro molteplicità**

---

<sup>6</sup>sono le radici di  $f(x)$

<sup>7</sup>cioè  $a(x - z_1)^{m_1}(x - z_2)^{m_2}\dots(x - z_k)^{m_k} = 0$

### Ritorniamo alle divisioni in $\mathbb{Z}$

Se  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ ,  $d = MCD(a, b)$  Vogliamo trovare  $m, n \in \mathbb{Z}$  tali che

$$d = ma + nb$$

**Esempio**  $a = 10$   $b = 4$   $d = 2$

cerco  $m, n \in \mathbb{Z}$  tali che

$$\frac{d}{2} = \frac{a}{10}m + \frac{b}{4}n$$

Calcolo  $d$  usando l'algoritmo di Euclide:

$$\begin{aligned} 10 &= 4 \cdot 2 + 2 \\ \frac{a}{10} &= \frac{b}{4} \cdot \frac{q_1}{2} + \frac{r_1}{2} \\ 4 &= 2 \cdot 2 + 0 \\ \frac{a}{4} &= \frac{b}{2} \cdot \frac{q_1}{2} + \frac{r_1}{2} \end{aligned} \quad d = 2 = \frac{10}{a} + \frac{4}{b} \cdot \frac{(-2)}{n}$$

$m = 1$

**NB**  $m, n$  non sono univocamente individuati da  $a$  e  $b$

**Esempio**  $2 = m10 + n4$  ma anche  $2 = \frac{10}{a} \cdot \frac{3}{m} + \frac{4}{b} \cdot \frac{(-7)}{n}$   
 $m = 1, n = -2$

## 2.6 Identità di Bezout (teorema)

$\forall a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ , posto  $d = (a, b)$   $\exists m, n \in \mathbb{Z}$  tali che

$$d = ma + nb$$

**NB**  $m, n$  non sono unici

Per trovarli posso:

1. Applico l'algoritmo di Euclide in  $\mathbb{Z}$  e lo "ripercorro" all'indietro"  
OPPURE
2. (a) calcolo  $|a|, |b| \in \mathbb{N}$   
(b) osservo  $MCD(a, b) = MCD(|a|, |b|)$   
(c) prendo  $d$  il  $MCD(|a|, |b|)$  **positivo**  
calcolato con l'algoritmo di Euclide in  $\mathbb{N}$   
Lo ripercorro all'indietro e ottengo  $m^*, n^* \in \mathbb{Z}$

$$d = m^*|a| + n^*|b|$$

- (d) se  $a \geq 0 \Rightarrow |a| = a$  e  $m = m^*$ , se  $a \leq 0 \Rightarrow |a| = -a$  e  $m = -m^*$   
se  $b \geq 0 \Rightarrow |b| = b$  e  $n = n^*$ , se  $b \leq 0 \Rightarrow |b| = -b$  e  $n = -n^*$

**Esempio**  $a = -36$   $b = 28$  se  $d = MCD(a, b)$ , cerco  $m, n \in \mathbb{Z}$  tale che  $d = ma + nb$

1° Modo Algoritmo di Euclide in  $\mathbb{Z}$  e calcolo  $d$

$$\frac{-36}{a} = \frac{28}{b} \cdot \frac{(-2)}{q_1} + \frac{20}{r_1} \Rightarrow \boxed{20 = -36 + 2 \cdot 28}$$

$$\text{N.B. } 0 \leq r_1 < |b| = 28$$

$$\frac{28}{b} = \frac{20}{r_1} \cdot \frac{q_2}{1} + \frac{8}{r_2} \Rightarrow 8 = 28 + 20 \cdot (-1)$$

$$\frac{20}{r_1} = \frac{8}{r_2} \cdot \frac{q_3}{2} + \frac{4}{r_3} \Rightarrow d = 4 = 20 + 8 \cdot (-2) = 20 + (-2)[28 + 20 \cdot (-1)] =$$

$$\begin{aligned}
&= 20 + (-2) \cdot 28 + 20 \cdot 2 = \\
&= 3 \cdot 20 + (-2) \cdot 28 = \\
&\quad 3 \cdot [-36 + 2 \cdot 28] + (-2) \cdot 28 \\
&= 3 \cdot (-36) + 6 \cdot 28 + (-2) \cdot 28 = 3 \cdot (-36) + 4 \cdot 28
\end{aligned}$$

**2° Modo** Cerco  $m, n \in \mathbb{Z}$  tali che  $d = am + bn$  dove  $d = MCD(a, b)$   $|a| = |-36| = 36$

**NB**  $MCD(|a|, |b|) = MCD(a, b) = d$

$|b| = |28| = 28$  Intanto (PAOLO) l'algoritmo di Euclide a  $|a|$  e  $|b|$  e trovo  $m^*, n^* \in \mathbb{Z}$

tali che  $d = |a| \cdot m^* + |b| \cdot n^*$

PAOLO

### 3 Classi di Congruenza

Siano  $a, b \in \mathbb{Z}$ ,  $n \in \mathbb{N}$ ,  $n > 0$

Si dice che  $a$  è **congruo** (o congruente) a  $b$  modulo  $n$  se

$$n|(a-b)$$

Si scrive  $a \equiv b \pmod{n}$ ; oppure  $a \equiv b \pmod{n}$  oppure  $a \equiv_n b$

**NB**  $a \equiv b \pmod{n} \iff \begin{array}{c} \text{il resto della divisione} \\ \text{di } a \text{ per } n \end{array} = \begin{array}{c} \text{il resto della divisione} \\ \text{di } b \text{ per } n \end{array}$

**Dimostrazione** ipotesi:  $a \equiv b \pmod{n}$  tesi: i due resti sono uguali

divido  $a$  per  $n$ :  $a = nq_1 + r_1$ ,  $0 \leq r_1 < n$

divido  $b$  per  $n$ :  $b = nq_2 + r_2$ ,  $0 \leq r_2 < n$

So che  $a \equiv b \pmod{n} \implies n|(a-b)$

Da  $a-b = nq_1 + r_1 - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2)$

$$\begin{array}{l} \uparrow \\ a = nq_1 + r_1 \\ b = nq_2 + r_2 \end{array}$$

Si ottiene:  $r_1 - r_2 = (a-b) - n(q_1 - q_2)$

$$\begin{cases} n|n(q_1 - q_2) \\ n|a-b \end{cases} \implies n|(a-b) - n(q_1 - q_2) \implies n|r_1 - r_2$$

Perché per ipotesi  $a \equiv b \pmod{n}$

$$\text{se } r_1 \geq r_2 \implies \begin{cases} 0 \leq r_1 - r_2 < n \\ n|r_1 - r_2 \end{cases} \implies r_1 - r_2 = 0 \implies r_1 = r_2$$

$$\text{se } r_2 \geq r_1 \implies \begin{cases} 0 \leq r_2 - r_1 < n \\ n|(r_1 - r_2) \implies n|(r_2 - r_1) \end{cases} \implies r_2 - r_1 = 0 \implies r_2 = r_1$$

**Viceversa**

**Ipotesi** Considero

$$a = nq_1 + r_1 \quad 0 \leq r_1 < n$$

$$b = nq_2 + r_2 \quad 0 \leq r_2 < n$$

$$r_2 = r_1$$

**Tesi**  $a \equiv b \pmod{n}$

**Dimostrazione** Voglio arrivare a dire che  $n|(a-b)$

$$\begin{cases} a = nq_1 + r_1 \\ r_1 = r_2 \end{cases} \implies a = nq_1 + r_2 \implies$$

$$\begin{aligned} a-b &= (nq_1 + r_2) - (nq_2 + r_2) = nq_1 + \cancel{r_2} - nq_2 - \cancel{r_2} = nq_1 - nq_2 = \\ &= n(q_1 - q_2) \implies n|(a-b) \end{aligned}$$

**NB 2** Fisso  $n \in \mathbb{N}$ 

La relazione di congruenza gode delle seguenti proprietà:

1. **è riflessiva:**  $a \equiv a \pmod n \forall a$   
(infatti  $n|(a-a) = 0$ )

2. **è simmetrica:**  $a \equiv b \pmod n \implies b \equiv a \pmod n$   
(infatti  $n|(a-b) \implies n|(b-a)$ )

3. **è transitiva:**  $\begin{cases} a \equiv b \pmod n \\ b \equiv c \pmod n \end{cases} \implies a \equiv c \pmod n$

$$\text{Infatti } \begin{cases} a \equiv b \pmod n \implies n|(a-b) \\ b \equiv c \pmod n \implies n|(b-c) \end{cases} \implies n|[(a-b) + (b-c)] = (a-c) \implies a \equiv c \pmod n$$

Ogni relazione che gode delle proprietà 1., 2., 3. si dice una **relazione di equivalenza**.

Fissato  $n \in \mathbb{N}$ ,  $n > 0$ ,  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$

4.  $\begin{cases} a_1 \equiv b_1 \pmod n \\ a_2 \equiv b_2 \pmod n \end{cases} \implies (a_1 + a_2) \equiv (b_1 + b_2) \pmod n$

le congruenze modulo  $n$  si possono “sommare”

5.  $\begin{cases} a_1 \equiv b_1 \pmod n \\ a_2 \equiv b_2 \pmod n \end{cases} \implies a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod n$

le congruenze modulo  $n$  si possono “moltiplicare” PAOLO qui però ho copiato parecchio dalle slide vecchie

In generale

1.  $\forall n \in \mathbb{N}, \forall a, k \in \mathbb{Z}$

$$[a]_n = [a + kn]_n$$

2.  $c \in [a]_n \implies [a]_n = [c]_n$

3. In particolare (dividevo)  $a$  per:

$$a = qn + r \text{ con } 0 \leq r < n$$

$$\text{Si ha } [a]_n = [r]_n$$

Perché, essendo  $r = a + n \cdot (-q)$ , si ha che  $r \in [a]_n$ , quindi si può usare  $[z]_{??}$  con  $c = r$

**Def.**  $a \in \mathbb{Z}, n \in \mathbb{Z}, n > 0$ , si chiama

**classe di congruenza  $a$  modulo  $n$**  e si indica  $[a]_n$  oppure  $[a] \pmod n$

$$\begin{aligned} [a]_n &= \text{insieme di tutti i numeri interi che sono congrui ad } a \text{ modulo } n \\ &= \{b \in \mathbb{Z} | b \equiv a \pmod n\} \end{aligned}$$

**NB 1**  $\forall b \in \mathbb{N}, n > 0, a, b \in \mathbb{Z}$   $[a]_n, [b]_n$

Voglio vedere che  $[a]_n = [b]_n$  oppure che  $[a]_n \cap [b]_n = \emptyset$ <sup>8</sup>

Infatti o  $[a]_n = [b]_n$

Oppure  $[a]_n \neq [b]_n$ . Suppongo  $[a]_n \cap [b]_n \neq \emptyset$

$$\implies \exists c \in [a]_n \cap [b]_n \implies \begin{cases} c \in [a]_n \implies [a]_n = [c]_n \\ c \in [b]_n \implies [b]_n = [c]_n \end{cases}$$

$$\implies [a]_n = [c]_n = [b]_n \implies [a]_n = [b]_n \text{ è una contraddizione}$$

<sup>8</sup> $[a]_n$  e  $[b]_n$ , pensati come insiemi di numeri interi, sono **insiemi disgiunti**

**NB 2**  $\forall n, n > 0$

Considero le classi di congruenza  $[a]_n$  con  $0 \leq a < n$

se  $b \in \mathbb{Z}$ , dividendo  $b$  su  $n$  si ha:  $b = nq + r$  con  $0 \leq r < n \implies [b]_n = [r]_n \implies b \in [r]_n$

Quindi

$$\mathbb{Z} = [0]_n \cup [1]_n \cup [2]_n \cup \dots \cup [n-1]_n$$

$$\mathbb{Z} = \bigcup_{0 \leq a < n} [a]_n$$

Queste classi sono a due a due **disgiunte**, l'insieme delle classi  $[0]_n, [1]_n, \dots, [n-1]_n$  sono una **partizione** di  $\mathbb{Z}$

**Def.** L'insieme degli **interi modulo  $n$** , indicato con il simbolo  $\mathbb{Z}_n$  è:

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$$

In  $\mathbb{Z}_n$  si definiscono  $+$  e  $\cdot$  nel seguente modo:

DA QUI RIPRENDO LEZIONE LIVE 6

**Teorema 1**  $(*)$  ha soluzione  $\iff d = MCD(a, n) | b$

se  $d|b$  una soluzione  $x_0 = \alpha q$  dove  $\begin{cases} d = \alpha a + bn \\ b = \alpha q \text{ per cui } q = \frac{b}{d} \end{cases}$

**Teorema 2** se  $(*)$  ha soluzione e  $x_0$  è una soluzione allora l'insieme di **tutte** le soluzioni è:

$\{x_k = x_0 + k \cdot \frac{n}{d} | k \in \mathbb{Z}\}$  si ripartiscono nelle classi:  $[x_0]_n, [x_1]_n, \dots, [x_{d-1}]_n$

### ESERCIZI

1.  $2x \equiv 5 \pmod{8}$

(a) Calcolo  $d = MCD(a, n) = MCD(2, 8) = 2$

(b)  $d|b$  **PAOLO**

2.  $3 \equiv 4 \pmod{7}$

(a) Calcolo  $d = MCD(a, n) = MCD(3, 7) = 1$

(b)  $d|b$   $1|4$

La congruenza ha  $\infty$  numeri come soluzioni:

$\{x_0 + 7k | x \in \mathbb{Z}\} = [x_0]_7$  dove  $x_0$  è una particolare soluzione.

Soluzione:

$$d = \alpha a + \beta n$$

$$1 = \alpha \cdot 3 + \beta \cdot 7$$

Bezout:

$$7 = 3 \cdot 2 + 1 \implies d = 1$$

$$1 = \underset{d}{7} + \underset{\beta=1}{3} \cdot (-2) \implies \alpha = -2$$

$$4 = 7 \cdot 4 + 3 \cdot (-2) \cdot 4$$

Le soluzioni sono tutte nella classe

$$[(-2) \cdot 4]_7 \implies [-8]_7 = [-8 + 7]_7 = [-1]_7 = [-1 + 7]_7 = [6]_7$$

**PAOLO**

3.  $2x \equiv 10 \pmod{12}$

**PAOLO** La congruenza ha infiniti numeri interi come soluzioni, che si ripartiscono in  $d = 2$  classi di congruenza modulo  $n = 12$

(a) calcolo  $x_0$  (poi prendo anche  $x_1 = x_0 + 6$ )

$$2x \equiv 10 \pmod{12} \quad d = \alpha \cdot 2 + \beta \cdot 12$$

$$2 = \alpha \cdot 2 + \beta \cdot 12$$

$$2 = 12 \cdot 0 + 2 \implies \text{Continua}$$

$$2 = 2 \cdot \alpha 1 + 12 \cdot 0 \quad \text{Moltiplico per } 5 = \frac{b}{d}$$

$$5 \cdot 2 = 5 \cdot 2 \cdot 1 + 5 \cdot 12 \cdot 0 \quad \text{Continua}$$

L'insieme delle soluzioni della congruenza è:

$$\{5 + 12k | k \in \mathbb{Z}\} \cup \{11 + 12k | k \in \mathbb{Z}\}$$

### 3.1 Invertibili in $\mathbb{Z}_n$ e il loro calcolo

$n \in \mathbb{Z}$ ,  $n > 0$ ,  $a \in \mathbb{Z}$  si dice **invertibile modulo  $n$**  se la congruenza  $ax \equiv 1 \pmod{n}$  ha soluzioni.

quindi  $\iff MCD(a, n) = d | b = 1 \iff MCD(a, n) = 1$

Si dice **PAOLO**.

**Def.**  $n \in \mathbb{N}$ ,  $n > 0$

$[a]_n \in \mathbb{Z}_n$  si dice **invertibile** in  $\mathbb{Z}_n$  se

$\exists [b]_n \in \mathbb{Z}_n$  tale che  $[a]_n [b]_n = [1]_n$

In questo caso  $[b]_n$  si dice **un inverso** di  $[a]_n$

$[a]_n = [1]_n \quad ax \equiv 1 \pmod{n} \quad d = MCD(a, n) = 1$  Essendo  $[b]_n$  **unico** (Perché  $d = 1$ )

Allora  $[b]_n$  è l'**inverso** di  $[a]_n$  **PAOLO**

**Esempio 1** 6 non è invertibile modulo 9 perché  $MCD(6, 9) \neq 1$

( $6x \equiv 1 \pmod{9}$  non ha soluzioni)

**Esempio 2** 4 è invertibile modulo 9 perché  $MCD(4, 9) = 1$

(4 e 9 sono coprimi)

$4x \equiv 1 \pmod{9}$  ha soluzione

$$\exists [4]_9^{-1}$$

Calcolo l'inverso di  $[4]_9$ , cioè calcolo  $[4]_9^{-1}$

$$d = \alpha a + \beta n$$

$$9 = 4 \cdot 2 + 1$$

$1 = 9 + 4 \cdot (-2)$  colorred $\mathbb{Z}_p$  (con  $p$  un numero primo) Sia  $p$  un numero primo e  $[a]_p \in \mathbb{Z}_p$

Posso supporre  $0 \leq a < p$

se  $a = 0$  allora  $[a]_p = [0]_p$

$$\nexists [b]_p | [0]_p [b]_p = [1]_p$$

$$\exists [0]_p^{-1}$$

se  $a \neq 0$  **Siccome  $p$  è un numero primo PAOLO**

Di  $\mathbb{Z}_p$  **tutti di elementi**  $\neq [0]_p$  sono **invertibili**.

Quanti sono? Sono  $p - 1$

Il numero degli elementi invertibili in  $\mathbb{Z}_p$  è  $p - 1$

Quanti sono gli invertibili in  $\mathbb{Z}_n$ ?

**PAOLO**

### 3.2 La funzione di Eulero

La funzione di Eulero  $\phi$  li "conta"

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

è definita da  $\phi(n)$  = il numero dei naturali  $k$  tali che  $\begin{cases} 0 \leq k < n \\ MCD(k, n) = 1 \end{cases}$  Se  $p$  è un numero primo (PAOLO)  $\phi(p) = p - 1$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \implies \phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right)$$

Finisci slide

### 3.3 Sistema di congruenze

UN sistema di congruenze è

$$a_1 x \equiv c_1 \pmod{m_1}$$

$$a_2 x \equiv c_2 \pmod{m_2}$$

...

$$a_k x \equiv c_k \pmod{m_k}$$

Dove  $a_i, c_i \in \mathbb{Z}$   $i = 1, \dots, k$

PAOLO

“Risolvere” il sistema significa

- Dire se ha soluzioni oppure no
- nel caso le abbia, trovarle tutte

Un  $x_0 \in \mathbb{Z}$  è UNA SOLUZIONE del sistema se è **contemporaneamente soluzione** di **ogni congruenza** del sistema.

**NB 1** Se una congruenza non ha soluzioni allora l'intero sistema non ne ha.<sup>9</sup>

**NB 2** Anche se tutte le congruenze del sistema hanno soluzione, non è detto che il sistema abbia soluzione.

Ad esempio

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{6} \end{cases} \quad \text{non ha soluzioni anche se ogni sua configurazione ha soluzioni}$$

---

<sup>9</sup>come avviene in tutti i sistemi



### 3.4 Il teorema cinese dei resti

Il teorema cinese dei resti da una condizione **sufficiente** affinché **particolari** sistemi di congruenze abbiano soluzioni.

Dati  $n_1, n_2, \dots, n_k \in \mathbb{N}, n_i > 0 \quad i = 1, \dots, k$   
**a due a due coprimi**<sup>10</sup>

$\forall b_1, b_2, \dots, b_k \in \mathbb{Z}$  si ha che  $\exists$  infinite soluzioni del sistema

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \dots \\ x \equiv b_k \pmod{n_k} \end{cases} \quad \begin{array}{l} \text{Esse si trovano tutte nella stessa classe} \\ \text{di congruenze modulo } n = n_1 \cdot n_2 \cdot \dots \cdot n_k \end{array}$$

**NB** La condizione che gli  $n_i$  siano a due a due coprimi non è una condizione necessaria affinché il sistema abbia soluzioni:

**Esempio 1**  $\begin{cases} 5x \equiv 3 \pmod{7} \\ 3x \equiv 6 \pmod{7} \end{cases} \quad \begin{array}{l} n_1 = n_2 \implies MCD(n_1, n_2) \neq 0 \\ \text{Però il sistema ha soluzione } [2]_7 \end{array}$

**Esempio 2**  $\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 2 \pmod{4} \end{cases} \quad \begin{array}{l} MCD(n_1, n_2) \neq 0 \\ \text{Però il sistema ha soluzione in } [2]_4 \end{array}$

**Cominciamo a studiare Il caso  $k = 2$**

$$\begin{cases} A \rightarrow \\ B \rightarrow \end{cases} \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases} \quad MCD(n_1, n_2) = 1$$

#### 3.4.1 Metodo di Newton

1.  $x_1 = b_1$
2. Cerco  $t_2 \in \mathbb{Z}$  tale che  $x_1 + t_2 n_1 \equiv x_2$  sia soluzione di  $B$   
 Così cerco  $t_2 \in \mathbb{Z}$  tale che  
 $b_1 = t_2 n_1 \equiv b_2 \pmod{n_2}$   
 $t_2 n_1 \equiv (b_2 - b_1) \pmod{n_2}$   
 dove  $t_2$  è il numero intero che cerco in modo tale che:  
 $x_2 \equiv b_2 \pmod{4}$  (siccome cerco  $t_2$ )  
 $x_2 = x_1 + t_2 n_1 \equiv x - 1 = b_1 \pmod{n_1}$
3.  $x_2$  è una soluzione di  $\begin{cases} A \\ B \end{cases}$
4. Per il teorema cinese dei resti, le soluzioni del sistema sono esattamente tutti i numeri interi nella classe  $[x_2]_n = \{ \}$  **PAOLO**

**Esempio**  $\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{5} \end{cases} \quad \begin{array}{l} b_1 \quad n_1 \\ b_2 \quad n_2 \end{array}$   
 $MCD(n_1, n_2) = MCD(6, 5) = 1$

Posso applicare il teorema cinese dei resti e concludere che il sistema ha infinite soluzioni: tutti i numeri in  $[x_2]_{30} = \{x_2 + 30k | k \in \mathbb{Z}\}$

<sup>10</sup>cioè se  $i \neq j$  allora  $MCD(n_i, n_j) = 1$

1.  $x_1 = 4$
2. cerco  $t_2 \in \mathbb{Z}$  tale che  $x_2 = x_1 + t_2 n_1 \equiv b_2 \pmod{n_2}$ , ovvero  
 $4 + t_2 \cdot 6 \equiv 3 \pmod{5}$   
 Facendo i conti in  $\mathbb{Z}_5$ :  $[4]_5 + t_2[6]_5 = [3]_5$   
 $t_2 \cdot 6 \equiv 3 - 4 \pmod{5}$   
 $6t_2 \equiv -1 \pmod{5} \implies t_2 \equiv 4 \pmod{5}$
3. ad esempio prendo  $t_2 = 4 \implies$   
 $\implies x_2 = x_1 + t_2 n_1 = 4 + 4 \cdot 6 = 28$

Per il teorema cinese dei resti tutte le soluzioni di  $\begin{cases} A \\ B \end{cases}$  sono gli interi nell'insieme  
 $[28]_{30} = \{28 + 30k | k \in \mathbb{Z}\}$

**Il caso  $k = 3$**  Consideriamo

$$\begin{aligned} A &\longrightarrow \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ x \equiv b_3 \pmod{n_3} \end{cases} \\ B &\longrightarrow \\ C &\longrightarrow \end{aligned}$$

E lo risolviamo col teorema cinese dei resti con l'ipotesi:

$$\begin{aligned} MCD(n_1, n_2) &= 1 \\ MCD(n_1, n_3) &= 1 \\ MCD(n_2, n_3) &= 1 \end{aligned}$$

Per trovare  $x_3$ :

1. Scelgo una soluzione di  $A : x_1 = b_1$
2. Cerco  $t_2 \in \mathbb{Z}$  tale che  $x_2 = x_1 + t_2 n_1 \equiv b_2 \pmod{n_2}$
3.  $x_2$  è soluzione di  $\begin{cases} A \\ B \end{cases}$
4. Cerco  $t_3 \in \mathbb{Z}$  tale che  $x_2 + t_3(n_1 \cdot n_2) \equiv b_3 \pmod{n_3}$   $x_3$  è soluzione di  $\begin{cases} A \\ B \\ C \end{cases}$

$$\begin{aligned} x_3 &\equiv x_2 \pmod{n_1} \text{ è soluzione di } A \\ x_3 &\equiv x_2 \pmod{n_2} \text{ è soluzione di } B \end{aligned}$$

$$n = n_1 \cdot n_2 \cdot n_3$$

5.  $x_3$  è una soluzione del sistema  $\begin{cases} A \\ B \\ C \end{cases}$

Per il teorema cinese dei resti la soluzione del (\*) sono i numeri interi nell'insieme  
 $\{x_2 + nk | k \in \mathbb{Z}\}$

**Esempio 2** considero

$$\begin{cases} x \equiv 10 \pmod{11} & MCD(11, 6) = 1 \\ x \equiv 5 \pmod{6} & MCD(11, 7) = 1 \\ x \equiv 10 \pmod{7} & MCD(6, 7) = 1 \end{cases}$$

$$n = 11 \cdot 6 \cdot 7 = 462$$

1.  $x_1 = 10$
2. Cerco  $t_2 \in \mathbb{Z}$  tale che  $x_2 = x_1 + t_2 n_1 \equiv b_2 \pmod{n_2}$   
 $10 = t_2 \cdot 11 \equiv 5 \pmod{6}$   
 $11t_2 \equiv 5 - 10 \pmod{6}$   
 $11t_2 \equiv -5 \pmod{6}$   
 $[1]_6 = [5]_6$   
 $[-5]_6 = [1]_6$  **PAOLO**, e anche bello grosso
3. Cerco  $t_3 \in \mathbb{Z}$  tale che  $x_3 = x_2 + t_3(n_1 \cdot n_2)$  sia soluzione di  $C: x \equiv 5 \pmod{7}$   
 $x_2 + t_3(n_1 \cdot n_2) \equiv 5 \pmod{7}$   
 $65 + t_3(11 \cdot 6) \equiv 5 \pmod{7}$   
 $66t_3 \equiv -60 \pmod{7} \quad 3t_3 \equiv 3 \pmod{7}$

$$\begin{aligned} x_3 &= x_2 + t_3 \cdot n_1 \cdot n_2 \\ &= 65 + 1 \cdot 11 \cdot 6 \\ &= 65 + 66 = 131 \end{aligned}$$

**PAOLO**

In generale se  $k \geq 4$  e  $\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ x \equiv b_k \pmod{n_k} \end{cases}$  Con  $MCD(n_i, n_j) = 1 \quad \forall i \neq j$

Itero di procedimento

- $x_1 = b_1$  è una soluzione di 1
- impongo che  $x_1 + n_1 t_2 = x_2$  Sia soluzione di 2 **PAOLO** Cerco  $t_2 \dots$
- Impongo che  $x_2 + n_1 n_2 t_3 = x_3$  sia soluzione di 3  
 $(\text{Cerco } t_3 \in \mathbb{Z} \text{ tale che } \dots) \text{ allora } x_3 \text{ è soluzione di } \begin{cases} 1 \\ 2 \\ 3 \end{cases}$
- Impongo che  $x_3 + n_1 n_2 n_3 t_4 = x_4$  sia soluzione di 4  
 $(\text{Cerco } t_4 \in \mathbb{Z} \text{ tale che } \dots) \text{ allora } x_4 \text{ è soluzione di } \begin{cases} 1 \\ 2 \\ 3 \\ 4 \end{cases}$

**PAOLO**

Torniamo al caso  $k = 2$   $\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases}$  Metodo di Lagrange  $MCD(n_1, n_2) =$   
1

Da  $MCD(n_1, n_2) = 1$ , usando Bezout trovo:  $\alpha_1, \alpha_2 \in \mathbb{Z}$  tali che

$$\alpha_1 n_1 + \alpha_2 n_2 = 1$$

Allora  $z = \alpha_1 n_1 b_2 + \alpha_2 n_2 b_1$  è una **PAOLO** ..

..

..

$$z = \alpha_1 n_1 b_2 + \alpha_2 n_2 b_1$$

$$z \equiv b_1 \pmod{n_1} \quad \alpha_1 n_1 + \alpha_2 n_2 \implies \alpha_2 n_2 = 1 - \alpha_1 n_1$$

$$z = \alpha_1 n_1 b_2 + (1 - \alpha_1 n_1) b_1 \quad (2)$$

$$= \alpha_1 n_1 b_2 \quad (3)$$

**PAOLO**, c'è da finire la slide

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases} \quad MCD\left(\begin{smallmatrix} 6 \\ n_1 \end{smallmatrix}, \begin{smallmatrix} 5 \\ n_2 \end{smallmatrix}\right) = 1 \text{ cerco } \alpha_1, \alpha_2 \in \mathbb{Z}$$

**PAOLO**

### 3.5 Ridurre un generico sistema di congruenze

Vediamo come “ridurre”, se si può, un generico sistema di congruenze:

$$\begin{cases} a_1 x \equiv c_1 \pmod{m_1} \\ a_2 x \equiv c_2 \pmod{m_2} \\ \dots \\ a_k x \equiv c_k \pmod{m_k} \end{cases} \quad \text{ad un sistema nella forma} \quad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \dots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

$a_i, c_i \in \mathbb{Z}, m_i \in \mathbb{N}, m_i > 0$   $b_i \in \mathbb{Z}, n_i \in \mathbb{Z}, n_i > 0$

**Ridurre** significa “sostituire con un sistema equivalente”

**Equivalente** significa “con le stesse soluzioni”

**Motivazione** Abbiamo

$$\begin{aligned} A &\rightarrow \begin{cases} 2x \equiv 4 \pmod{8} \\ 3x \equiv 6 \pmod{9} \end{cases} \\ B &\rightarrow \end{aligned}$$

$$A = MCD(2, 8) = d = 2 \mid 4 \begin{cases} [2]_8 & 2 \cdot 2 = 4 \equiv 4 \pmod{8} \\ [6]_8 & 2 \cdot 6 = 12 \equiv 4 \pmod{8} \end{cases}$$

$$A \begin{cases} x \equiv 2 \pmod{8} & \text{C} \\ x \equiv 6 \pmod{8} & \text{D} \end{cases}$$

$$B : MCD(3, 9) = d = 3 \mid 6 \begin{cases} [2]_9 & 3 \cdot 2 = 6 \equiv 6 \pmod{9} \\ [5]_9 & 3 \cdot 5 = 15 \equiv 6 \pmod{9} \\ [8]_9 & 3 \cdot 8 = 24 \equiv 6 \pmod{9} \end{cases}$$

$$B \begin{cases} x \equiv 2 \pmod{9} & E \\ x \equiv 5 \pmod{9} & F \\ x \equiv 8 \pmod{9} & G \end{cases}$$

Quindi le soluzioni di  $\begin{cases} A \\ B \end{cases}$  sono l'unione delle soluzioni di 6 sistemi:

$$\begin{cases} C \\ E \end{cases} \cup \begin{cases} C \\ F \end{cases} \cup \begin{cases} C \\ G \end{cases} \cup \begin{cases} D \\ E \end{cases} \cup \begin{cases} D \\ F \end{cases} \cup \begin{cases} D \\ G \end{cases}$$

E noi vorremmo non dover risolvere sei sistemi.

**Passaggio 1** Calcolo  $d_i = MCD(a_i, m_i) \forall i = 1, \dots, k$

- $\exists d_i$  tale che  $d_i \nmid c_i$  allora  $a_i x \equiv c_i \pmod{m_i}$  Non ha soluzioni, allora (\*) non ha soluzioni.
- se  $d_i | c_i \forall i = 1, \dots, k$  allora ogni congruenza di (\*) ha soluzione e
  - se  $d_i = 1$  **mantengo** la congruenza  $a_i x \equiv c_i \pmod{m_i}$
  - se  $d_i \neq 1$  **sostituisco** la congruenza  $a_i x \equiv c_i \pmod{m_i}$  con la congruenza

$$\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}}$$

**NB 1** La congruenza  $\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}}$  è **equivalente** alla congruenza  $a_i x \equiv c_i \pmod{m_i}$

**NB 2** La congruenza  $a_i x \equiv c_i \pmod{m_i}$

Infatti

Sia  $z \in \mathbb{Z}$

$$\begin{array}{ccc} \boxed{z \text{ è soluzione di } a_i x \equiv c_i \pmod{m_i}} & \iff & \boxed{\exists k \in \mathbb{Z} \text{ tale che } a_i z = c_i + m_i k} \\ \text{divido per } d_i & & \\ \implies & & \\ \iff & & \\ \text{moltiplico per } d_i & & \\ \boxed{\exists k \in \mathbb{Z} \text{ tale che } \frac{a_i}{d_i} z = \frac{c_i}{d_i} + \frac{m_i}{d_i} k} & \iff & \boxed{z \text{ è soluzione di } \frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}}} \end{array}$$

**NB 3** Siccome  $d_i = MCD(a_i, m_i)$  allora

$$MCD\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1$$

Quindi le soluzioni della congruenza  $\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}}$  stanno tutte in un'unica classe di congruenza modulo  $\frac{m_i}{d_i}$

Alla fine del **passaggio 1** ottengo che (\*) non ha soluzioni, oppure che (\*) è equivalente a

$$(**) \begin{cases} \frac{a_1}{d_1} x \equiv \frac{c_1}{d_1} \pmod{\frac{m_1}{d_1}} \\ \vdots \\ \frac{a_k}{d_k} x \equiv \frac{c_k}{d_k} \pmod{\frac{m_k}{d_k}} \end{cases}$$

**Passaggio 2** Risolvo ciascuna congruenza di (\*\*)

$$\frac{a_i}{d_i} x \equiv \frac{c_i}{d_i} \pmod{\frac{m_i}{d_i}} \implies x \equiv b_i \pmod{\frac{m_i}{d_i}}$$

Dove  $[b_i]_{\frac{m_i}{d_i}} = \{b_i + \frac{m_i}{d_i} t \mid t \in \mathbb{Z}\}$  è l'insieme delle soluzioni della congruenza

Posto  $n_i = \frac{m_i}{d_i}$  ottengo un sistema

$$(***) \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \dots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

SE  $MCD(n_i, n_j) = 1 \forall i \neq j$  posso applicare il Teorema cinese dei resti. In tal caso:

**Passaggio 3** Con newton trovo  $x_k$  una particolare soluzione di (\*\*\*) e per il teorema cinese dei resti l'insieme di tutte le soluzioni (\*\*\*), e quindi anche di (\*) è  $[x_k]_n = \{x_k + nt \mid t \in \mathbb{Z}\}$

$$\text{dove } n = n_1 \cdot n_2 \cdot \dots \cdot n_k$$

### 3.6 Esercizio tipo

Risolvere il sistema

$$\begin{cases} 3x \equiv 4 \pmod{5} \\ 2x \equiv 4 \pmod{6} \end{cases}$$

**Passaggio 1**  $a_1 = MCD(a_1, m_1) = MCD(3, 5) = 1 \mid 4 = c_1$   
 $a_2 = MCD(a_2, m_2) = MCD(2, 6) = 2 \mid 4 = c_2$

$a_1 = 1 \implies$  mantengo  $3x \equiv 4 \pmod{5}$   
 $a_2 = 2 \neq 1$  **sostituisco**  $2x \equiv 4 \pmod{6}$   
 Con  $\frac{2}{2}x \equiv \frac{4}{2} \pmod{\frac{6}{2}}$ :  $x \equiv 2 \pmod{3}$

$$\text{arrivo a } (**) \begin{cases} 3x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases}$$

**Passaggio 2** Risolvo ciascuna congruenza **PAOLO**

$$3x \equiv 4 \pmod{5}$$

$$d = MCD(a, n) = 1 \mid 4 = b$$

$$d = 1 = \alpha a + \beta n$$

$$1 = \alpha + \beta \cdot 5$$

$$\alpha = 2$$

$$x_0 = \alpha q = 2 \cdot 4 = 8$$

$$5 = 3 \cdot 1 + 2 \implies 2 = 5 + 3 \cdot (-1)$$

$$3 = 2 \cdot 1 + 1$$

$$\implies 1 = 3 + 3 \cdot (-1) = 3 + (-1)[5 + 3 \cdot (-1)] = 3x \equiv 4 \pmod{5}$$

$$[8]_5 = [8 - 5]_5 = [3]_5$$

Sostituisco  $3x \equiv 4 \pmod{5}$  con  $x \equiv 3 \pmod{5}$

Per puro caso la congruenza  $x \equiv 2 \pmod{3}$  è già risolta.

$$(***) \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases}$$

Siccome  $MCD(n_1, n_2) = MCD(5, 3) = 1$ ,

Allora posso applicare il teorema cinese dei resti e concludere che  $(***)$  e quindi anche il sistema da cui sono partiti ha infinite soluzioni (numeri interi) tutte nella stessa classe di congruenza modulo

$$n = n_1 \cdot n_2 = 5 \cdot 3 = 15$$

**Passaggio 3** Trovo  $x_2$  una particolare soluzione di  $(***)$

**1° Modo** per trovare  $x_2 \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases}$

1.  $x_1 = 3$

2. cerco  $t_2 \in \mathbb{Z}$  tale che  $x_2 = x_1 + t_2 n_1 \equiv 2 \pmod{3}$   
 $x_2 \rightarrow 3 + t_2 \cdot 5 \equiv 2 \pmod{3}$

$$5t_2 \equiv (2 - 3) \pmod{3}$$

$$5t_2 \equiv -1 \pmod{3} \equiv 2 \pmod{3}$$

$$[5]_3 = [2]_3 \rightarrow 5t_2 = 2t_2$$

$$2t_2 \equiv 2 \pmod{3}$$

Ad esempio  $t_2 = 1$   $x_2 = 3 + 1 \cdot 5 = 3 + 5 = 8$

**tutte le soluzioni del (\*) sono  $[8]_5 = \{8 + 15k | k \in \mathbb{Z}\}$**

**2° Modo** per trovare  $x_2 = z$   $MCD(n_1, n_2) = 1 \exists \alpha_1, \alpha_2 \in \mathbb{Z}$  tale che

$$\alpha_1 n_1 + \alpha_2 n_2 = 1$$

$$\alpha_1 \cdot 5 + \alpha_2 \cdot 3 = 1$$

$$z = \alpha_1 n_1 + \alpha_2 n_2$$

$$= -5 \cdot 2 + 6 \cdot 3$$

$$= -10 + 18 = 8$$

$$[z]_n = [8]_{15} = \{8 + 15k | k \in \mathbb{Z}\}$$

## 4 Matrici e loro operazioni

Una **matrice** è una tabella di numeri (o di simboli) disposti in righe e colonne, detti **coefficienti** della matrice

$$A = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{bmatrix} \quad A = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{pmatrix} \quad A = \begin{matrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{matrix}$$

Altri tipi di notazioni sono sbagliati, inoltre:

$$\begin{bmatrix} 2 \\ 1 & 4 \end{bmatrix} \text{ non è una matrice}$$

Il numero che si trova nella  $i$ -esima riga e nella  $j$ -esima colonna si chiama **coefficiente** di posto  $(i, j)$

$A$  è  $m \times n$  se ha  $m$  righe e  $n$  colonne

( $A$  ha “dimensioni  $m \times n$ ”)

$$A = \begin{matrix} \xrightarrow{\text{red}} \\ \xrightarrow{\text{blue}} \end{matrix} \begin{bmatrix} 2 & \downarrow 3 & \downarrow 0 \\ 1 & 4 & 1 \end{bmatrix} \text{ è } 2 \times 3 \quad \xrightarrow{\text{green}} \begin{bmatrix} 1 & \downarrow 2 \\ i & 7 \\ 0 & 3 \end{bmatrix} \text{ è } 3 \times 2$$

Le posizioni sono:

$$(2, 2) \quad (1, 3) \quad (3, 2)$$

Le matrici si indicano con lettere latine **maiuscole in stampatello**

$$A, B, C, \dots$$

I Coefficienti si indicano con le lettere latine **minuscole** in corsivo

$$a_{ij} = \text{il coefficiente di posti } (i, j) \text{ di } A$$

Per scrivere in modo compatto la matrice:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{bmatrix}$$

**La indico:**

$$A_{m \times n} = (a_{ij}) \text{ oppure } A = (a_{ij})_{i=1, \dots, m, j=1, \dots, n} \text{ PAOLO}$$

### 4.1 Operazioni

#### 4.1.1 Prodotto di una matrice per uno scalare

Dato  $A = (a_{ij}), m \times n$  e dato uno scalare  $\alpha$ , si definisce **Prodotto dello scalare  $\alpha$  per la matrice  $A$**  la matrice  $B_{m \times n} = (b_{ij})$  dove  $b_{ij} = \alpha \cdot a_{ij}$

$$\text{si indica } B = \alpha \cdot A$$



**Esempio**  $\alpha = 1 - i$   $A = \begin{bmatrix} 7 & 0 & 3i \\ 1+2i & -i & -4 \end{bmatrix}$

$$\Rightarrow \alpha A = (1 - i) \begin{bmatrix} 7 & 0 & 3i \\ 1+2i & -i & -4 \end{bmatrix} =$$

$$= \begin{bmatrix} (1-i)7 & (1-i) \cdot 0 & (1-i) \cdot 3i \\ (1-i)(1+2i) & (1-i)(-i) & (1-i)(-4) \end{bmatrix} = \begin{bmatrix} 7-7i & 0 & 3+3i \\ 3+i & 1-i & -4+4i \end{bmatrix}$$

$$\left. \begin{array}{l} (1-i)7 = 7-7i \\ (1-i) \cdot 3i = 3i-3i^2 \\ = -3i-3(-1) \\ = 3i+3 \end{array} \right| \begin{array}{l} (1-i)(1+2i) = 1-i+2i+2i^2 = 1-i+2i+2 = 3+i \\ (1-i)(-i) = -i+i^2 = -i-1 \\ (1-i)(-4) = -4+4i \end{array}$$

**NB 1** vale la legge di cancellazione

$$\alpha \cdot A = || \Rightarrow \alpha = 0 \text{ oppure } A = ||$$

Indico con  $||$  la matrice con tutti i coefficienti  $= 0$

**NB 2**

1.  $\alpha A = A\alpha$   $\forall \alpha \text{ scalare } \forall A$
2.  $1 \cdot A = A$   $\forall A$
3.  $0 \cdot A = ||$   $\forall A$
4.  $(\alpha \cdot \beta) \cdot A = \alpha(\beta A)$   
 $\forall \alpha, \beta \text{ scalari } \forall A$

**Notazioni**  $(-1) \cdot A = -A$

$A = [a_{ij}]$   $(-1) \cdot A = [(-1)a_{ij}]$   $-A$  si chiama **la matrice opposta della matrice A**

## 4.2 Somma di due matrici

Date almeno due matrici  $A = (a_{ij})_{m \times n}$  e  $B = (b_{ij})_{r \times s}$  **aventi le stesse dimensioni**,

cioè  $\begin{cases} r = m \\ s = n \end{cases}$  si definisce  $A + B = (a_{ij} + b_{ij})_{m \times n}$  **la somma delle due matrici**

**Esempio** Siano  $A = \begin{bmatrix} 1+i & 3 & 2 \\ i & 0 & 7 \end{bmatrix}$ ,  $B = \begin{bmatrix} 7 & 2 \\ 3i & 0 \end{bmatrix}$ ,  $C = \begin{bmatrix} 0 & i & 2-i \\ i & 7+i & i \end{bmatrix}$

Non posso sommare A con B, né B con C, ma posso sommare A con C:

$$A+C = \begin{bmatrix} 1+i & 3+i & 2+2-i \\ i+i & 7+i & 7+i \end{bmatrix} = \begin{bmatrix} 1+i & 3+i & 4-i \\ 2i & 7+i & 7+i \end{bmatrix}$$

**Proprietà della somma** Siano  $A, B, C$   $m \times n$ ,  $\alpha, \beta$  scalari

1.  $A+(B+C) = (A+B)+C$
2.  $A+B=B+A$
3.  $A+|| = A$
4.  $A+(-A) = ||$
5.  $\alpha(A+B) = \alpha A + \alpha B$
6.  $(\alpha + \beta)A = \alpha A + \beta A$

### 4.3 Prodotto di un vettore riga per un vettore colonna

Sono chiamati **vettori riga** matrici con una sola riga e **vettori colonna** matrici con una sola colonna.

In notazione:

$$\underline{u} = \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_m \end{bmatrix}$$

$$\underline{u}^T = [u_1 \quad u_2 \quad \dots \quad u_n]$$

**Il prodotto (riga per colonna)** di  $\underline{v}^T = [v_1 \quad v_2 \quad \dots \quad v_n]$  per  $\underline{u} = \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_n \end{bmatrix}$  è

$$\underline{v}^T \underline{u} = [v_1 \quad v_2 \quad \dots \quad v_n] \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_n \end{bmatrix} = v_1 u_1 + v_2 u_2 + \dots + v_n u_n$$

**La riga deve necessariamente avere tanti elementi quanti ne ha la colonna**

**Esempio**  $[7 \quad 1+i \quad 3] \begin{bmatrix} -1 \\ 1-i \end{bmatrix}$  non esiste

$$\begin{aligned} [7 \quad 1+i \quad 3] \begin{bmatrix} -1 \\ 1-i \\ 2i \end{bmatrix} &= -7 + (1+i)(1-i) + 3 \cdot 2i \\ &= -7 + 1^2 - i^2 + 6i \\ &= -7 + 1 - (-1) + 6i \\ &= -7 + 1 + 1 + 6i \\ &= -5 + 6i \end{aligned}$$

**NB 1**

1.  $\underline{v}^T \cdot \underline{0}$

$$\begin{aligned}
2. \quad \underline{u} &= \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_n \end{bmatrix}, \underline{v}^T = [v_1 \quad v_2 \quad \dots \quad v_n] \\
\underline{v} &= \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix}, \underline{u}^T = [u_1 \quad u_2 \quad \dots \quad u_n] \\
\\
\underline{v}^T \underline{u} &= [v_1 \quad v_2 \quad \dots \quad v_n] \begin{bmatrix} u_1 \\ u_2 \\ \dots \\ u_n \end{bmatrix} = v_1 u_1 + v_2 u_2 + \dots + v_n u_n = \\
\\
&= u_1 v_1 + u_2 v_2 + \dots + u_n v_n = [u_1 \quad u_2 \quad \dots \quad u_n] \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix}
\end{aligned}$$

**NB 2 non vale la legge di cancellazione**

Ossia

$$\begin{aligned}
\underline{u} \neq \underline{0} \text{ e } \underline{v}^T \underline{u} = 0 &\nRightarrow \underline{v}^T = \underline{0}^T \\
\text{ed anche } \underline{v}^T \neq \underline{0}^T \text{ e } \underline{v}^T \underline{u} = 0 &\nRightarrow \underline{u} = \underline{0}
\end{aligned}$$

**Esempio**  $\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1 \cdot 0 + 0 \cdot 1 = 0$

#### 4.4 Prodotto di due matrici (riga per colonna)

$A_{m \times n}$ ,  $B_{r \times s}$  Il prodotto di A e B è possibile solo se

$$n = r$$

$$A_{m \times n} B_{r \times s}$$

In tal caso il prodotto  $A_{m \times n} \cdot B_{r \times s} = C_{m \times s}$

dove

$c_{ij} = (i\text{-esima riga di A}) \cdot (j\text{-esima colonna di B})$  **PAOLO**

**Esempio**  $A_{2 \times 3} = \begin{bmatrix} 2 & 3 & 7 \\ 6 & 0 & 5 \end{bmatrix}$ ,  $B_{2 \times 2} = \begin{bmatrix} 7 & 4 \\ 2 & 3 \end{bmatrix}$ ,  $C_{2 \times 3} = \begin{bmatrix} 7 & 6i & 1 \\ 3 & 4 & -2 \end{bmatrix}$ ,

$$E_{3 \times 3} = \begin{bmatrix} 1 & 1 & -2 \\ 4 & 3i & 3 \\ 0 & -1 & 2 \end{bmatrix}, F_{3 \times 2} = \begin{bmatrix} 7i & 6+i \\ -2 & 5 \\ 4 & -3 \end{bmatrix}$$

Non esiste AB, come non esiste AC.

Esiste però  $AE_{2 \times 3}$  perché il numero delle colonne di A coincide col numero di righe di E.

Per la stessa ragione esiste anche  $AF_{2 \times 2}$

$$AF = \begin{bmatrix} 22 + 14i & 6 + 2i \\ 20 + 42i & 21 + 6i \end{bmatrix}$$

Calcoliamo AE

$$\begin{bmatrix} 2 & 3 & 7 \\ 6 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 & 1 & -2 \\ 4 & 3i & 3 \\ 0 & -1 & 2 \end{bmatrix} = \begin{array}{|c|c|c|} \hline 14 & -5+9i & 19 \\ \hline 6 & 1 & -2 \\ \hline \end{array}$$

$$c_{11} = \begin{bmatrix} 2 & 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix} = 2 + 12 = 14$$

$$c_{12} = \begin{bmatrix} 2 & 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 3i \\ -1 \end{bmatrix} = 2 + 9i - 7 = -5 + 9i$$

$$c_{13} = \begin{bmatrix} 2 & 3 & 7 \end{bmatrix} \begin{bmatrix} -2 \\ 3 \\ 2 \end{bmatrix} = -4 + 9 + 14 = 19$$

$$c_{21} = \begin{bmatrix} 6 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix} = 6$$

$$c_{22} = \begin{bmatrix} 6 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 3i \\ -1 \end{bmatrix} = 6 - 5 = 1$$

$$c_{23} = \begin{bmatrix} 6 & 0 & 5 \end{bmatrix} \begin{bmatrix} -2 \\ 3 \\ 2 \end{bmatrix} = -12 + 10 = -2$$

### Proprietà di cui gode il prodotto

Supponiamo che tutte le operazioni seguenti si possano fare con A, B, C matrici e  $\alpha$  scalare

1.  $\begin{matrix} r \times m & m \times n \\ s \times r & r \times n \end{matrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{matrix} s \times r & r \times m \\ s \times m & m \times n \end{matrix}$  proprietà associativa
2.  $\begin{matrix} r \times m & m \times n \\ r \times m & m \times n \end{matrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{matrix} r \times m & m \times n \\ r \times m & m \times n \end{matrix}$
3. Se  $I_n$  indica la matrice  $n \times n$  allora la matrice

$$I_n = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Si chiama **matrice identica di ordine  $n$**

$$I_2 = \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}$$

$$I_3 = \begin{array}{|c|c|c|} \hline 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ \hline \end{array}$$

Eccetera...

$$I_M \cdot \begin{matrix} A \\ m \times n \end{matrix} = A = \begin{matrix} I_n \\ m \times n \end{matrix}$$

4.  $A(B+C) = AB+AC$

5.  $(A+B)C=AC+BC$
6.  $\alpha(AB) = (\alpha \cdot A)B = A(\alpha \cdot B)$   
Questo perché  $\alpha$  è uno scalare.

#### Proprietà di cui il prodotto non gode

1. **non vale la legge di cancellazione**

$$\begin{aligned} \text{ossia } \begin{cases} AB = \mathbb{I} \\ A \neq \mathbb{I} \end{cases} &\not\Rightarrow B = \mathbb{I} \\ \text{anche } \begin{cases} AB = \mathbb{I} \\ B \neq \mathbb{I} \end{cases} &\not\Rightarrow A = \mathbb{I} \end{aligned}$$

#### Esempio

$$AB = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix} \begin{bmatrix} 6 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 2 \cdot 6 + 3 \cdot (-4) & 2 \cdot (-3) + 3 \cdot 2 \\ 4 \cdot 6 + 6 \cdot (-4) & 4 \cdot (-3) + 6 \cdot 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Dunque  $AB = \mathbb{I}$  che  $A \neq 0$  e  $B \neq 0$   
(ed anche sia A che B sono “quadrate”)

2. **Il prodotto (righe per colonne) NON è commutativo**

Cioè  $AB \neq BA$

- $\exists AB \not\Rightarrow BA$

$$\begin{cases} A_{x \times n} \\ B_{n \times k} \end{cases} \Rightarrow \exists AB_{m \times k}, \text{ ma se } k \neq m \text{ allora } \nexists BA$$

- $\begin{cases} \exists AB \\ \exists BA \end{cases} \not\Rightarrow AB \text{ e } BA \text{ hanno le stesse dimensioni}$

dunque

$$A_{m \times n} \text{ e } B_{n \times m} \Rightarrow \begin{matrix} \exists AB \text{ ed è } m \times m \\ \exists BA \text{ ed è } n \times n \end{matrix} \Rightarrow \begin{matrix} \text{se } n \neq m \text{ allora} \\ AB \neq BA \end{matrix}$$

- Ma anche se A e B sono entrambe  $m \times m$  per cui  $\exists AB_{m \times m}$  ed  $\exists BA_{m \times m}$ ,  
ma non è detto che AB sia uguale a BA

#### Esempio

$$AB = \begin{bmatrix} 2 & 3 \\ -1 & 6 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 6 \end{bmatrix} = \begin{array}{|c|c|} \hline 8+6 & 6+18 \\ \hline -4+2 & -3+36 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 14 & 24 \\ \hline 8 & 32 \\ \hline \end{array}$$

$$BA = \begin{bmatrix} 4 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ -1 & 6 \end{bmatrix} = \begin{array}{|c|c|} \hline 8-3 & 12+18 \\ \hline 4-6 & 6+36 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 5 & 30 \\ \hline -2 & 42 \\ \hline \end{array}$$

## 4.5 La trasposta

Sia  $A = (a_{ij})$   $m \times n$ , la **trasposta di A** è  $B = (b_{ij})$   $n \times m$  tale che

$$b_{ij} = a_{ji}$$

E si indica con  $B=A^T$

**Esempio**  $A = \begin{bmatrix} 1 & 2+3i & 1-i \\ \textcolor{red}{7} & \textcolor{red}{0} & \textcolor{red}{4} \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 1 & \textcolor{red}{7i} \\ 2+3i & \textcolor{red}{0} \\ 1-i & \textcolor{red}{4} \end{bmatrix}$

Per questo  $\underline{v} = \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix} \Rightarrow \underline{v}^T = [v_1 \quad v_2 \quad \dots \quad v_n]$

## 4.6 La coniugata

Sia  $A = (a_{ij})_{m \times n}$

La **coniugata di A** è  $B = (b_{ij})_{m \times n}$  tale che  $b_{ij} = a_{ij}$

Si indica  $B = \bar{A}$

**Esempio**  $A = \begin{bmatrix} 1 & 2+3i & 1+i \\ 7i & 0 & 4 \end{bmatrix} \Rightarrow \bar{A} = \begin{bmatrix} \bar{1} & \overline{2+3i} & \overline{1+i} \\ \overline{7i} & \bar{0} & \bar{4} \end{bmatrix} = \begin{bmatrix} 1 & 2+3i & 1-i \\ 7i & 0 & 4 \end{bmatrix} \begin{bmatrix} \bar{1} & \overline{7i} \\ \overline{2+3i} & \bar{0} \\ \overline{1-i} & \bar{4} \end{bmatrix} \begin{bmatrix} 1 & 2+3i \\ 2+3i & 0 \\ 1-i & 4 \end{bmatrix}$

**PAOLO**

**Proprietà delle trasposte, delle coniugate e delle H-trasposte**

Siano A, B matrici,  $\alpha$  scalare, supponiamo che tutte le operazioni scritte siano possibili.

### Trasposte

1.  $(\alpha A)^T = \alpha \cdot A^T$
2.  $(A+B)^T = A^T + B^T$
3.  $(A^T)^T = \text{PAOLO}$
4.  $(AB)^T = B^T A^T$

### Coniugate

1.  $\overline{\alpha A} = \bar{\alpha} \cdot \bar{A}$
2.  $\overline{A+B} = \bar{A} + \bar{B}$
3.  $\overline{\bar{A}} = A$
4.  $\overline{AB} = \bar{A} \cdot \bar{B}$

### H-trasposte

1.  $(\alpha A)^H = \bar{\alpha} \cdot A^H$
2.  $(A+B)^H = A^H + B^H$
3.  $(A^H)^H = A$
4.  $(AB)^H = B^H A^H$

## 4.7 Tipi di matrici

L'insieme di tutte le matrici  $m \times n$  a coefficienti in  $\mathbb{R}$  viene indicato

$$M(\mathbb{R})_{m \times n} \text{ oppure } M(\mathbb{R})_{m,n}$$

Stessa cosa per quanto riguarda in  $\mathbb{C}$ :

$$M(\mathbb{C})_{m \times n} \text{ oppure } M(\mathbb{C})_{m,n}$$

Sia  $A \in M_{m \times n}(\mathbb{C})$  Diro: “una matrice” invece di “una matrice complessa”, specificherò “una matrice **reale**” per dire che i coefficienti sono reali.

(cioè nel caso  $A \in M_{m \times n}(\mathbb{R})$ )

1. A si dice **quadrata** se  $n = m$

In  $A_{n \times n}$ ,  $n$  indica l'**ordine delle matrice quadrata di A**

$M_n(\mathbb{C})$  è preferibile a  $M_{n \times n}(\mathbb{C})$

$M_n(\mathbb{R})$  è preferibile a  $M_{n \times n}(\mathbb{R})$

$M_{2 \times 3}(\mathbb{C})$  e  $M_{2,3}(\mathbb{C})$  = matrici  $2 \times 3$

$$M_{23}(\mathbb{C}) = \text{matrici } 23 \times 23 \text{ Esempio } A = \begin{bmatrix} 7 & 3 & 1-i \\ 0 & 2+3i & 4 \\ 5 & 1 & 2 \end{bmatrix} \in M_3(\mathbb{C})$$

**Diagonale principale**

I coefficienti diagonali di A sono 7,  $2 + 3i$ , 2

2. A si dice **diagonale** se

- è quadrata ( $n \times n$ )
- tutti i coefficienti che non sono diagonali sono uguali a 0  
(cioè:  $a_{ij} = 0 \forall i \neq j$ )

**Esempi**  $\begin{bmatrix} 3 & 0 & 0 \\ 0 & 7 & 0 \end{bmatrix}$ ,  $\begin{bmatrix} 3 & 0 \\ 0 & 7 \end{bmatrix}$ ,  $\begin{bmatrix} 3 & 1 \\ 0 & 7 \end{bmatrix}$ ,  $\begin{bmatrix} 0 & 0 \\ 0 & 7 \end{bmatrix}$   
Non è quadrata   È diagonale   Non è diagonale   È diagonale

3.  $A = (a_{ij})$  si dice **scalare** se  $m \times n$

$$A = \text{Diag}(d, d, \dots, d)$$

$$A = \begin{bmatrix} d & 0 & 0 & 0 & 0 & 0 \\ 0 & d & 0 & 0 & 0 & 0 \\ 0 & 0 & d & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 \\ 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = d \cdot I_n$$

$dI_n$  si chiama **scalare** perché

$$dI_n B_{n \times k} = d(I_n B) = dB$$

$$C_{m \times n}(dI_n) = C(I_n d) = (CI_n) \cdot d = C \cdot d$$

Moltiplicare per la matrice scalare individuata dallo scalare  $d$  equivale a moltiplicare per lo scalare  $d$

4.  $\underline{v} = \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_n \end{bmatrix}$  è un **vettore colonna**

Un vettore colonna con  $n$  elementi si indica  $\mathbb{C}^n$  o  $\mathbb{R}^n$

Analogamente  $\underline{v}^T = [v_1 \ v_2 \ \dots \ v_n]$

Un vettore riga di  $n$  elementi si indica  $\mathbb{C}_n$  o  $\mathbb{R}_n$

5. Caso particolare: i vettori coordinati

**PAOLO**

6. A si dice **simmetrica** se  $A^T = A$

NB  $A_{m \times n} \implies A_{n \times m}^T$

Se  $A_{n \times m}^T = A_{m \times n} \implies A$  è **quadrata**

**Esempio**  $A = \begin{bmatrix} 1 & 3+i \\ 3+i & 2 \end{bmatrix}$

7. A si dice **Hermitana** se  $A^H = A$

NB se  $A^H = A \implies A$  quadrata

**Esempio:**  $A = \begin{bmatrix} 1 & 3+i \\ 3+i & 2 \end{bmatrix}$

8. A si dice **antisimmetrica** se

$A^T = -A$

Se  $A^T = -A \implies A$  è quadrata.

**Esempio:**  $A = \begin{bmatrix} 0 & 3+i \\ -3-i & 0 \end{bmatrix}$

9. A si dice **antihermitana** se

$A^H = -A$

Se  $A^H = -A \implies A$  è quadrata

**Esempio:**  $A = \begin{bmatrix} 2i & 3+i \\ -3+i & 7i \end{bmatrix}$

## 4.8 Scrittura matriciale di un sistema lineare

Dato un sistema lineare<sup>11</sup>

$$(*) \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 \quad a_{13}x_3 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 \quad a_{23}x_3 + \dots + a_{2n}x_n = b_2 \\ \dots \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 \quad a_{m3}x_3 + \dots + a_{mn}x_n = b_m \end{array} \right.$$

La matrice  $A_{m \times n} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$

Si chiama la  
**matrice dei coefficienti**  
di (\*)

<sup>11</sup>ovvero ogni equazione ha grado 1



$$\begin{array}{l} \text{Il vettore } \underline{b} = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ \dots \\ b_n \end{bmatrix} \in \mathbb{C}^m \end{array} \quad \begin{array}{l} \text{Si chiama il} \\ \textbf{vettore dei termini noti} \\ \text{di (*)} \end{array}$$

$$\begin{array}{l} \text{Il vettore } \underline{x} = \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ \dots \\ x_n \end{bmatrix} \end{array} \quad \begin{array}{l} \text{Si chiama il} \\ \textbf{vettore delle incognite} \\ \text{di (*)} \end{array}$$