Appunti di Algebra

Quel ragazzo con la maglia blu

Contents

1 Divisione nei numeri naturali e nei numeri interi **2**
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

2 Polinomi **7**
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^o grado a coefficienti reali 8
2.5 Teorema fondamentale dell'algebra 9
2.6 Identità di Bezout (teorema) 10

3 Classi di Congruenza **12**
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

4 Matrici e loro operazioni **21**
4.1 Operazioni 21
4.1.1 Prodotto di una matrice per uno scalare 21

1 Divisione nei numeri naturali e nei numeri interi

Insieme dei numeri **naturali**:

$$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$$

Insieme dei numeri **interi**:

$$\mathbb{Z} = \{... - 4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$$

1.1 Divisione in $\mathbb{N}$

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

$$\exists ! q, r \in \mathbb{N} \qquad | \qquad \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

$q =$ quoziente
$r =$ resto
$| =$ tale che

Esempio 1 $a = 137$ $b = 55$ $\quad \underset{a}{137} = \underset{b}{55} \cdot \underset{q}{2} + \underset{r}{27}$

Esempio 2 $a = 137$ $b = 142$ $\quad \underset{a}{137} = \underset{b}{142} \cdot \underset{q}{0} + \underset{r}{137}$

NB1 per provare che q ed r **esistono** si usa il principio di induzione

NB2 q ed r **sono unici** significa:

$$\begin{cases} a = bq_1 + r_1 \\ a = bq_2 + r_2 \end{cases} \qquad \begin{matrix} 0 \leq r_1 < b \\ 0 \leq r_2 < b \end{matrix} \quad \Longrightarrow \begin{cases} q_2 = q_1 \\ r_2 = r_1 \end{cases}$$

1.2 Divisione in $\mathbb{Z}$

La definizione è uguale per i numeri interi
$\forall a,\ b \in \mathbb{Z},\ b \neq 0\ \exists ! q,\ r \in \mathbb{Z}$ tali che $a = bq + r$
con unica differenza $0 \leq r < |b|$

$$|r| = \begin{cases} r \text{ se } r \geq 0 \\ -r \text{ se } r < 0 \end{cases}$$

NB Se non si impone la condizione $\begin{cases} r \geq 0 \\ r < |b| \end{cases}$ non si ha l'unicità di q e r

Ad esempio
$a = 137$ $b = -55$ $\quad \underset{a}{137} = \underset{b}{(55)}\ \underset{q}{-2} + \underset{r}{27}$ $\quad$ ma anche $\underset{a}{137} = \underset{b}{(-55)}\ \underset{q}{-3} + \underset{r}{-28}$

NB1 la dimostrazione dell'esistenza di q ed r è simile a quella che si fa in $\mathbb{N}$, ottenuta sempre col principio di induzione.

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 divizione di a e b in $\mathbb{Z}$ ed il quoziente ed il resto della divizione di $|a|$ e $|b|$ in $\mathbb{N}$

Ad esempio

$$\begin{array}{ll|ll} a = -137 & \underset{a}{-137} = \underset{b}{55}\underset{q_1}{(-3)} + \underset{r_1}{28} & |a| = 137 & \underset{|a|}{137} = \underset{|b|}{55} \cdot \underset{q_2}{2} + \underset{r_2}{27} \\ b = 55 & & |b| = 55 & \end{array}$$

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

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

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

Per esempio 6|18

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

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

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

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

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

$$60 = 2^2 \cdot 3 \cdot 5 \qquad\qquad 18 = 2 \cdot 3^2$$

$$\begin{array}{c} 60|2 \\ 30|2 \\ 15|3 \\ 5|5 \end{array} \qquad\qquad \begin{array}{c} 18|2 \\ 9|3 \\ 3|3 \end{array}$$

$$d = 2 \cdot 3 = 6$$

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

NB 3

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

NB 4 $a,\, b \in \mathbb{N}\; b \neq 0$ $\exists q,\, r \in \mathbb{N}$
$a = bq + r$ [2] $0 \leq r < b$

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 $\mathbb{Z}$ $\forall a,\, b \in \mathbb{Z}$ con $(a,b) \neq (0,0)$ $d \in \mathbb{Z}$ 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 $(a,b) \neq (0,0)$

[2] $r = a - bq$

NB $\underset{b}{2}|\underset{a}{0}$ $\quad \underset{a}{0} = \underset{b}{2} \cdot \underset{q}{0}$
$3|0 \qquad 142|0 \qquad \forall b \neq 0 \quad b|0$

Ecco perché è importante quando si parla di MCD(a, b)
se fosse $(a, b) = (\underset{a}{0}, \underset{b}{0})$ 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 $(a, b) = (0, 0)$

NB $a, b \in \mathbb{Z},\ b \neq 0$
$a = bq + r \qquad 0 \leq r < |b|$

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

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^o **passaggio** $a = bq_1 + r_1 \qquad 0 \leq r_1 < b$

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

Esempio 1 $\quad$ MCD$(\underset{a}{36}, \underset{b}{12}) =$
P1 $\underset{a}{36} = \underset{b}{12} \cdot \underset{q_1}{3} + \underset{r_1}{0} \Longrightarrow MCD(36, 12) = MCD(12, 0) = 12$
1^oP $a = bq_1 + r_1 \qquad 0 \leq r_1 < b$

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

2^o **passaggio SI DIVIDE** b **per** r_1

$b = r_1q_2 + r_2 \qquad =\leq r_2 < r_1$

SE $R_2 = 0$ **STOP**

$$\text{MCD}(a, b) = \text{MCD}(b, r_1) \underset{\substack{\uparrow \\ b = r_1q_2 + r_2}}{=} \text{MCD}(r_1, r_2) \underset{\substack{\uparrow \\ \text{se } r_2 = 0}}{=} \text{MCD}(r_1, 0) = r_1$$

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

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

1^op $\quad \underset{a}{42} = \underset{b}{12} \cdot \underset{q_1}{3} = \underset{r_1}{6}$
$r_1 \neq 0 \quad 2^o p \quad \underset{b}{12} = \underset{r_1}{6} \cdot \underset{q_2}{2} + \underset{r_2}{0}$ $\quad$ **SE** $r_2 \neq 0$ continuo...

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

Es 1 $\quad MCD(\underset{a}{36}, \underset{b}{28}) = 4$

$\underline{1^o p} \quad \underset{a}{36} = \underset{b}{28} \cdot \underset{q_1}{1} + \underset{r_1}{8}$

$\underline{2^o p} \quad \underset{b}{28} = \underset{r_1}{8} \cdot \underset{q_2}{3} + \underset{r_2}{4}$

$\underline{3^o p} \quad \underset{r_1}{8} = \underset{r_2}{4} \cdot \underset{q_3}{2} + \underset{r_3}{0} \qquad r_3 = 0 \Longrightarrow r_2 = \text{MCD}$

Es 2 $\quad MCD(\underset{a}{2420}, \underset{b}{1386}) = 22$

$\underline{1^o p} \quad \underset{a}{2420} = \underset{b}{1386} \cdot \underset{q_1}{1} + \underset{r_1}{1034}$

$\underline{2^o p} \quad \underset{b}{1386} = \underset{r_1}{1034} \cdot \underset{q_2}{1} + \underset{r_2}{352}$

$\underline{3^o p} \quad \underset{r_1}{1034} = \underset{r_2}{352} \cdot \underset{q_3}{2} + \underset{r_3}{330}$

$\underline{4^o p} \quad \underset{r_2}{352} = \underset{r_3}{330} \cdot \underset{q_3}{1} + \underset{r_4}{22}$

$\underline{5^o p} \quad \underset{r_3}{330} = \underset{r_4}{22} \cdot \underset{q_3}{15} + \underset{r_5}{0}$

1.5.2 In $\mathbb{Z}$

1^o modo consigliato

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

2^o modo Algoritmo di Euclide in $\mathbb{Z}$

Esempio $\quad MCD(\underset{a}{-274}, \underset{b}{110})$

$|a| = |-274| = 274$
$|b| = |110| = 110$

1^o Modo svolgimento

$\underline{1^o p} \quad \underset{a}{274} = \underset{b}{110} \cdot \underset{q_1}{2} + \underset{r_1}{54}$

$\underline{2^o p} \quad \underset{b}{110} = \underset{r_1}{54} \cdot \underset{q_2}{2} + \underset{r_2}{2}$

$\underline{3^o p} \quad \underset{r_1}{54} = \underset{r_2}{2} \cdot \underset{q_3}{27} + \underset{r_3}{0}$

$MCD(|a|, |b|) = d = 2 \Longrightarrow 2$ e -2 sono i $MCD(-274, 110)$

2^o Modo Algoritmo di Euclide in $\mathbb{Z}$

$\underline{1^o p} \quad \underset{a}{274} = \underset{b}{110} \cdot \underset{q_1}{(-3)} + \underset{r_1}{56} \qquad \underset{110}{|b|} > r_1 \geq 0$

$\underline{2^o p} \quad \underset{b}{110} = \underset{r_1}{56} \cdot \underset{q_2}{1} + \underset{r_2}{54}$

$\underline{3^o p} \quad \underset{r_1}{56} = \underset{r_2}{54} \cdot \underset{q_3}{1} + \underset{r_3}{2} \qquad$ 2 e -2 sono i due massimi comuni divisori di -274 e 110

$\underline{4^o p} \quad \underset{r_2}{54} = \underset{r_3}{2} \cdot \underset{q_3}{27} + \underset{r_4}{0}$

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 $f(x) = a_o + a_1x + a_2x^2 + ... + a_nx^n$ 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 $f(x)$

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

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

2.1 Somma di polinomi

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

Es $f(x) = 2 - x^3 + 3x^2$ $g(x) = 7x + x^3 + 12$

$2 + 0x + 3x^2 - x^3 +$	$\deg f(x) = 3$
$12 + 7x + 0x^2 + x^3 =$	$\deg g(x) = 3$
$14 + 7x + 3x^2$	$\deg\big(f(x) + g(x)\big) \leq 3$

$f(x) = a_0 + a_1x + ... + a_nx^n = \sum_{i=0}^{n} a_ix^i$ $a_n = 0, \deg f(x) = n$
$g(x) = b_0 + b_1x + ... + b_mx^m = \sum_{i=0}^{m} b_ix^i$ $b_n = 0, \deg g(x) = m$
Per fissare le idee si ponga che $m \leq n$

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

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

2.2 Prodotto di polinomi

$\forall f(x), g(x) \in S[x]$ definisco $f(x), g(x) \in S[x]$
nel seguente modo:
se $f(x) = \sum_{i=0}^{n} a_ix^i$ e $g(x) = \sum_{i=0}^{m} b_ix^i$ allora

$$f(x)g(x) = \left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{i=0}^{m} b_ix^i\right) =$$

$= (a_0 + a_1x + a_2x^2 + ... + a_nx^n)(b_0 + b_1x + b_2x^2 + ... + b_mx^m) =$
$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_a + a_2b_0)x^2 + ... = = \sum_{i=0}^{i} a_kb_{i-k}\left(\sum_{k=0}^{i} a_kb_{i-k}\right)x^i$

NB $\deg\big(f(x) \cdot g(x)\big) = \deg f(x) + \deg g(x)$

Esempio $f(x) = 2 - x + 6x^2$ $g(x) = 1 + 4x$
$(2 - x + 6x^2)(1 + 4x) = ... = 2 + 7x - 4x^2 + 6x^4 + 24x^5$

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

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 $g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$

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

2.4 Radici di un polinomio

Sia $f(x) \in S[x]$.
Un numero $x_0 \in S$ si dice una **radice** [3] di $f(x)$ se $f(x_0) = 0$ [4]
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 $x^2 + 2x + 1 = 0$ [5]

2.4.1 Teorema di Ruffini

Se $f(x) \in S[x]$ ed $x_0 \in S$
(x_0 è una radice di $f(x)$) $\iff (x - x_0) \underset{(divide)}{|} f(x) \iff \underset{\exists q(x) \in S[x]}{f(x) = (x - x_0)q(x)}$
dividendo $f(x)$ per $x - x_0$ si ha $r(x) = 0$

2.4.2 Radici di polinomi di 2^o grado a coefficienti reali

$ax^2 + bx + c = 0 \qquad a, b, c \in \mathbb{R} \qquad a \neq 0$
$\Delta = b^2 - 4ac$ è il discriminante dell'equazione

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

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

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

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

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

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

  Poiché $\sqrt{-\Delta} \neq 0 \Longrightarrow x_1 \neq x_2$
  L'equazione ha 2 soluzioni complesse **coniugate** (l'una coniugata dell'altra)

$$x_1 = \overline{x_2}$$

[3] oppure uno *zero*
[4] "f valutato in $x_0 = 0$"
[5] 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

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

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

2.5 Teorema fondamentale dell'algebra

$$\forall f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

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

$$\text{polinomio di grano } n > 0 \qquad (a_n \neq 0)$$

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

$$f(x) = a_n(x - z_1)(x - z_2)...(x - z_n)$$

potrebbero esserci ripetizioni

Ad esempio se $f(x) = (x-1)^n = (x-1)(x-1)...(x-1)$ allora $z_1 = z_2 = ... = z_n = 1$
Ogni polinomio di grado $n > 0$ e coefficienti complessi è prodotto di n polinomi di grado 1
Se $z_0, z_1, ..., z_x$ [6] sono quegli z_i DISTINTI, allora

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

$m_i =$ **la molteplicità algebrica di** z_i
È equivalente a: $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$
L'equazione $f(x) = 0$ [7] 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

$$m_1 + m_2 + ... + m_k = n$$

Esempio $f(k) = (x^2 + 2x + 1)(x - 3) = (x - 1)^2(x - 3)$
$z_1 = -1$ $m_1 = 2$
$z_2 = 3$ $m_2 = 1$

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

[6] sono le radici di $f(x)$
[7] cioè $a(x - z_n)^{m_1}(x - z_2)^{m_2}...(x - z_k)^{m_k} = 0$

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

Calcolo d usando l'algoritmo di Euclide:

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

. $m = 1$

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

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

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

1^o Modo Algoritmo di Euclide in $\mathbb{Z}$ e calcolo d
$\underset{a}{-36} = \underset{b}{28} \cdot \underset{q_1}{(-2)} + \underset{r_1}{20} \Rightarrow \boxed{20 = -36 + 2 \cdot 28}$
N.B. $0 \leq r_1 < |b| = 28$
$\underset{b}{28} = \underset{r_1}{20} \cdot \underline{q_2}1 + \underline{r_2}8 \Longrightarrow 8 = 28 + 20 \cdot (-1)$
$\underset{r_1}{20} = \underset{r_2}{8} \cdot q_3 2 + \underset{r_3}{4} \Longrightarrow d = 4 = 20 + 8 \cdot (-2) = 20 + (-2)[28 + 20 \cdot (-1)] =$

$= 20 + (-2) \cdot 28 + 20 \cdot 2 =$
$= 3 \cdot 20 + (-2) \cdot 28 =$
$3 \cdot [-36 + 2 \cdot 28] + (-2) \cdot 28$
$= 3 \cdot (-36) + 6 \cdot 28 + (-2) \cdot 28 == 3 \cdot (-36) + 4 \cdot 28$

2^o 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 $a \equiv b \mod n$; oppure $a \equiv b(\mod n)$ oppure $a \equiv_n b$

NB $a \equiv b \mod n \iff$ il resto della divisione di a per n = il resto della divisione di b per n

Dimostrazione ipotesi: $a \equiv b \mod n$ 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 $a \equiv b \mod n \implies n|(a-b)$
Da $a - b \underset{\uparrow}{=} nq_1 + r_1 - (nq_2 + r_2) = n(q_1 - q_2) + (r_1 - r_2)$
$a = nq_1 + r_1$
$b = nq_2 + r_2$

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 $a \equiv b \mod n$

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

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

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 $a \equiv b \mod n$

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

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

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

NB 2 Fisso $n \in \mathbb{N}$
La relazione di congruenza gode delle seguenti proprietà:

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

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

3. **è transitiva**: $\begin{cases} a \equiv b \mod n \\ b \equiv c \mod n \end{cases} \Longrightarrow a \equiv c \mod n$
Infatti $\begin{cases} a \equiv b \mod n \Longrightarrow n|(a-b) \\ b \equiv c \mod n \Longrightarrow n|(b-c) \end{cases} \Longrightarrow n|[(a-b)+(b-c)] = (a-c) \Longrightarrow$
$\Longrightarrow a \equiv c \mod n$
Ogni relazione che dove 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. $\begin{cases} a_1 \equiv b_1 \mod n \\ a_2 \equiv b_2 \mod n \end{cases} \Longrightarrow (a_1 + a_2) \equiv (b_1 + b_2) \mod n$
le congruenze modulo n si possono "sommare"

5. $\begin{cases} a_1 \equiv b_1 \mod n \\ a_2 \equiv b_2 \mod n \end{cases} \Longrightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod n$
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. $c \in [a]_n \Longrightarrow [a]_n = [c]_n$

3. In particolare (dividevo) a per:
$a = qn + r$ con $0 \leq r < n$
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 $[a] \mod n$

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

NB 1 $\forall b \in \mathbb{N}$, $n > 0$, $a, b \in \mathbb{Z}$ $\quad [a]_n, [b]_n$
Voglio vedere che $[a]_n = [b]_n$ oppure che $[a]_n \cap [b]_n = \varnothing$ [8]
Infatti o $[a]_n = [b]_n$
Oppure $[a]_n \neq [b]_n$. Suppongo $[a]_n \cap [b]_n \neq \varnothing$
$\Longrightarrow \exists c \in [a]_n \cap [b]_n \Longrightarrow \begin{cases} c \in [a]_n \Longrightarrow [a]_n = [c]_n \\ c \in [b]_n \Longrightarrow [b]_n = [c]_n \end{cases}$
$\Longrightarrow [a]_n = [c]_n = [b]_n \Longrightarrow [a]_n = b_n$ è una **contraddizione**

[8] $[a]_n$ 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 $0 \le a < n$
se $b \in \mathbb{Z}$, dividendo b su n si ha: $b = nq + r$ con $0 \le r < n \Longrightarrow [b]_n = [r]_n \Longrightarrow b \in [r]_n$
Quindi

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

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

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

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

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

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

DA QUI RIPRENDO LEZIONE LIVE 6

Teorema 1 (*) ha soluzione $\Longleftrightarrow d = MCD(a,n)|b$
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 ripartiscomno nelle classi: $[x_0]_n, [x_1]_n, ..., [x_{d-1}]_n$
ESERCIZI

1. $\underset{a}{2}x \equiv \underset{b}{5} \mod \underset{n}{8}$
   (a) Calcolo $d = MCD(a,n) = MCD(2,8) = 2$
   (b) $d|b$ PAOLO
2. $\underset{x}{3} \equiv \underset{b}{4} \mod \underset{n}{7}$
   (a) Calcolo $d = MCD(a,n) = MCD(3,7) = 1$
   (b) $d|b$ $1|4$
   La congruenza ha ∞ 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:
   $\underset{n}{7} = \underset{a}{3} \cdot \underset{q_1}{2} + \underset{r_1}{1} \Longrightarrow d = 1$
   $\underset{d}{1} = \underset{\beta=1}{7} + 3 \cdot (-2) \Longrightarrow \alpha = -2$
   $4 = 7 \cdot 4 + 3 \cdot (-2) \cdot 4$
   Le soluzioni sono tutte nella classe
   $[(-2) \cdot 4]_7 \Longrightarrow [-8]_7 = [-8+7]_7 = [-1]_7 = [-1+7]_7 = [6]_7$
   PAOLO
3. $\underset{a}{2}x \equiv \underset{b}{10} \mod \underset{n}{12}$
   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 prendero anche $x_1 = x_0 + 6$)
$\underset{a}{2}x \equiv \underset{b}{10} \mod \underset{n}{12}$ $d = \alpha \cdot 2 + \beta \cdot 12$
$2 = \alpha \cdot 2 + \beta \cdot 12$
$\underset{a}{2} = \underset{n}{12} \cdot \underset{q_1}{0} + \underset{r_1}{2} \Longrightarrow$ *Continua*
$\underset{d}{2} = \underset{a}{2} \cdot \alpha 1 + \underset{n}{12} \cdot \underset{\beta}{0}$ Moltiplico per $5 = \frac{b}{d}$
$\underset{b=10}{5 \cdot 2} = 5 \cdot 2 \cdot 1 + 5 \cdot \underset{n}{12} \cdot 0$ 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 $ax \equiv 1 \mod n$ ha soluzioni.
quindi $\Longleftrightarrow MCD(a, n) = d | b = 1 \Longleftrightarrow MCD(a, n) = 1$
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 case $[b]_n$ si dice **un inverso** di $[a]_n$
$[a]_n = [1]_n$ $ax \equiv 1 \mod n$ $d = MCD(a, n) = 1$ Essendo $[b]_n$ **unico** (Perché $d = 1$)
Allora $[b]_n$ è l'**inverso** di $[a]_n$ PAOLO

Esempio 1 6 non è iunvertibile modulo 9 perché $MCD(6, 9) \neq 1$
($6x \equiv 1 \mod 9$ non ha soluzioni)

Esempio 2 4 è invertibile modulo 9 perché $MCD(4, 9) = 1$
(4 e 9 sono coprimi)
$underseta4x \equiv \underset{b}{1} \mod \underset{n}{1}$ ha soluzione
$\exists [4]_q^{-1}$
Calcolo l'inverso di $[4]_q$, cioè calcolo $[4]_q^{-1}$
$\underset{1}{d} = \alpha \underset{4}{a} + \underset{1}{\beta} \underset{9}{n}$
$\underset{n}{9} = \underset{a}{4} \cdot \underset{q_1}{2} + \underset{r_1}{1}$
$1 = 9 + 4 \cdot (-2)$ colorred$\mathbb{Z}_p$ (con p un numero primo) Sia p un numero primo e $[a]_p \in \mathbb{Z}_p$
Posso supporre $0 \leq a < p$A

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 elemtni 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 ϕ 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) $\phi(p) = p - 1$

$$n = p_1^{\alpha_1} p_2^{a_2} ... p_m^{a_m} \Longrightarrow \phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}...(1 - \frac{1}{p_m})$$

Finisci slide

3.3 Sistema di congruenze

UN sistema di congruenze è
$a_1 x \equiv c_1 \mod m_1$
$a_2 x \equiv c_2 \mod m_2$
...
$a_k x \equiv c_k \mod m_k$
Dove $a_i, c_i \in \mathbb{Z}$ $i = 1, ..., k$
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.[9]

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

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

[9]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 $n_1, n_2, ..., n_k \in \mathbb{N}, n_i > 0 \qquad i = 1, ..., k$
a due a due coprimi[10]

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

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ ... \\ x \equiv b_k \mod n_k \end{cases} \qquad \begin{matrix} \text{Esse si trovano tutte nella stessa classe} \\ \text{di congruenze modulo } n = n_1 \cdot n_2 \cdot ... \cdot n_k \end{matrix}$$

NB La condizione che gli n_1 siano a due a due coprimi non è una condizione necessaria affinché il sistema abbia soluzioni:

Esempio 1 $\begin{cases} 5x \equiv 3 \mod \underset{n_1}{7} \\ 3x \equiv 6 \mod \underset{n_2}{7} \end{cases}$ $\qquad n_1 = n_2 \Longrightarrow MCD(n_1, n_2) \neq 0$
Però il sistema ha soluzione $[2]_7$

Esempio 2 $\begin{cases} x \equiv 0 \mod \underset{n_1}{2} \\ x \equiv 2 \mod \underset{n_2}{4} \end{cases}$ $\qquad MCD(n_1, n_2) \neq 0$
Però il sistema ha soluzione in $[2]_4$

Cominciamo a studiare Il caso $k = 2$

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

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
   $b_1 = t_2 n_1 \equiv b_2 \mod n_2$
   $t_2 n_1 \equiv (b_2 - b_1) \mod n_2$
   dove t_2 è il numero intero che cerco in modo tale che:
   $x_2 \equiv b_2 \mod 4$ (siccome cerco t_2)
   $x_2 = x_1 + t_2 n_1 \equiv x - 1 = b_1 \mod n_1$
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 $\begin{cases} x \equiv \underset{b_1}{4} \mod \underset{n_1}{6} \\ x \equiv \underset{b_2}{3} \mod \underset{n_2}{5} \end{cases}$
$MCD(n_1, n_2) = MCD(6, 5) = 1$
Posso applicare il teorema dinese dei resti e concludere che il sistema ha infinite soluzioni: tutti i numeri in $[x_2]_30 = \{x_2 + 30k | k \in \mathbb{Z}\}$

[10] 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 $\quad x_2 = \quad x_1 + t_2 n_1 \equiv b_2 \mod n_2$, ovvero
$$4 + t_2 \cdot 6 \equiv 3 \mod 5$$
Facendo i conti in $\mathbb{Z}_5$: $[4]_5 + t_2[6]_5 = [3]_5$
$t_2 \cdot 6 \equiv 3 - 4 \mod 5$
$6t_2 \equiv -1 \mod 5 \Longrightarrow t_2 \equiv 4 \mod 5$

3. ad esempio prendo $t_2 = 4 \Longrightarrow$
$\Longrightarrow x_2 = x_1 + t_2 n_1 = 4 + 4 \cdot 6 = 28$

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

$$\begin{array}{l} A \longrightarrow \\ B \longrightarrow \\ C \longrightarrow \end{array} \begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ x \equiv b_3 \mod n_3 \end{cases}$$

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

$MCD(n_1, n_2) = 1$
$MCD(n_1, n_3) = 1$
$MCD(n_2, n_3) = 1$

Per trovare x_3:

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

   $\underset{\text{mod } n_1}{x_3} \equiv x_2$ è soluzione di A
   $\underset{\text{mod } n_2}{x_3} \equiv x_2$ è soluzione di B

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

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

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

$$\begin{cases} x \equiv 10 \mod \underset{n_1}{11} \\ x \equiv 5 \mod \underset{n_2}{6} \\ x \equiv 10 \mod \underset{n_3}{7} \end{cases} \qquad \begin{array}{c} MCD(11,6) = 1 \\ MCD(11,7) = 1 \\ MCD(6,7) = 1 \end{array}$$

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

1. $x_1 = 10$
2. Cerco $t_2 \in \mathbb{Z}$ tale che $x_2 = x_1 + t_2 n_1 \equiv b_2 \mod n_2$
   $10 = t_2 \cdot 11 \equiv 5 \mod n$
   $11t_2 \equiv 5 - 10 \mod 6$
   $11t_2 \equiv -5 \mod 6$
   $[1]_6 = [5]_6$
   $[-5]_6 = [1]_6$ 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: $x \equiv 5 \mod 7$
   $x_2 + t_3(n_1 \cdot n_2) \equiv 5 \mod 7$
   $65 + t_3(11 \cdot 6) \equiv 5 \mod 7$
   $66t_3 \equiv -60 \mod 7$ $3t_3 \equiv 3 \mod 7$

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

FINISCI

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

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 FINISCI Cerco t_2...
- Impongo che $x_2 + n_1 n_2 t_3 = x_3$ sia soluzione di 3

  (Cerco $t_3 \in \mathbb{Z}$ tale che ...) allora x_3 è soluzione di $\begin{cases} 1 \\ 2 \\ 3 \end{cases}$
- Impongo che $x_3 + n_1 n_2 n_3 t_4 = x_3$ sia soluzione di 4

  (Cerco $t_4 \in \mathbb{Z}$ tale che ...) allora x_4 è soluzione di $\begin{cases} 1 \\ 2 \\ 3 \\ 4 \end{cases}$

PAOLO

Torniamo al caso $k=2$ $\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \end{cases}$ 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 ..
..
..
$z = \alpha_1 n_1 b_2 + \alpha_2 n_2 b_1$
$z \equiv b_1 \mod n_1$ $a_1 n_1 + \alpha_2 n_2 \implies \alpha_2 n_2 = 1 - \alpha_1 n_1$

$$z = \alpha_1 n_1 b_2 + (1 - \alpha_1 n_1) b_1 \tag{2}$$
$$= \alpha_1 n_1 b_2 \tag{3}$$

PAOLO, c'è da finire la slide

$\begin{cases} x \equiv \underset{b_1}{4} \mod \underset{n_1}{6} \\ x \equiv \underset{b_2}{4} \mod \underset{n_2}{6} \end{cases}$
$MCD(\underset{n_1}{6}, \underset{n_2}{5}) = 1$ cerco $\alpha_1, \alpha_2 \in \mathbb{Z}|$

PAOLO

Come "ridurre", se si può, un generico sistema di congruenze

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

PAOLO ma proprio una riga **Ridurre** significa "sostituire con un sistema equivalente"
Equivalente significa "con le stesse soluzioni"

4 Matrici e loro operazioni

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

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

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 $m \times n$")

$$\mathrm{A} = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 4 & 1 \end{bmatrix} \text{ è } 2 \times 3 \qquad \begin{bmatrix} 1 & 2 \\ i & 7 \\ 0 & 3 \end{bmatrix} \text{ è } 3 \times 2$$

Le posizioni sono:
$(2, 2)$ $(1, 3)$ $(3, 2)$

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

A, B, C, ...

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:

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

PAOLO

4.1 Operazioni

4.1.1 Prodotto di una matrice per uno scalare

Dato A$= (aij), m \times n$ e dato uno scalare α, si definisce **Prodotto dello scalare $\boldsymbol{\alpha}$ per la matrice A** la matrice $\underset{m \times n}{\mathrm{B}} = (bij)$ dove $b_{ij} = \alpha \cdot a_{ij}$

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

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

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

$$= \begin{array}{|c|c|c|} \hline (1-i)7 & (1-i)\cdot 0 & (1-i)\cdot 3i \\ \hline (1-i)(1+2i) & (1-i)(-i) & (1-i)(-4) \\ \hline \end{array} = \begin{array}{|c|c|c|} \hline 7-7i & 0 & 3+3i \\ \hline 3+i & 1-i & -4+41 \\ \hline \end{array}$$

$$\begin{array}{c|c} (1-i)7 = 7-7i & (1-i)(1+2i) = 1-i+2i+2i^2 = 1-i+2i+2 = 3+i \\ (1-i)\cdot 3i = 3i - 3i^2 & (1-i)(-i) = -i+i^2 = -i-1 \\ = -3i-3(-1) & (1-i)(-4) = -4+4i \\ = 3i+3 & \end{array}$$

NB 1 vale la legge di cancellazione

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

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

NB 2

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