# A1 BASIC Numeri complessi e polinomi — Maria —

Titolo nota 04/09/2012

## Numeri complessi

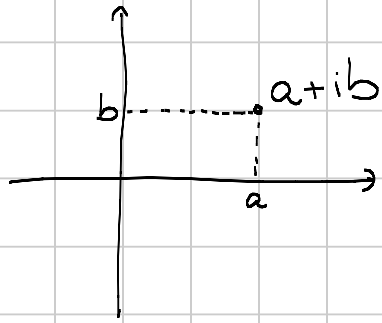
$\mathbb{C} = \{ a+ib : a, b \in \mathbb{R} \}$

$i$ è un segnaposto

Dato $z \in \mathbb{C}$, $z = a+ib$, diciamo $a = \mathrm{Re}\, z$ $b = \mathrm{Im}\, z$.

## Piano di Gauss

Associamo ad $a+ib$ il punto $(a, b)$.




$z \in \mathbb{R} \iff \mathrm{Im}\, z = 0 \iff z$ sta sull'asse $x$.

## Operazioni

Somma: $a+ib + c+id = (a+c) + i(b+d)$

Prodotto: $\boxed{i^2 = -1}$.

$$(a+ib)(c+id) = ac + ibc + iad + i^2 bd$$
$$= ac - bd + i(bc + ad).$$

Divisione: $\frac{a+ib}{c+id} = \frac{a+ib}{c+id} \cdot \frac{c-id}{c-id} = \frac{(ac+bd)+i(bc-ad)}{c^2-(id)^2}$

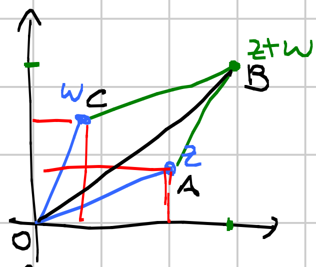
$$= \frac{ac+bd+i(bc-ad)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i \, \frac{bc-ad}{c^2+d^2}$$

È ben definito $c+id \neq 0$ (0 è $0 + i \cdot 0$)

Coniugio $\overline{a+ib} = a - ib$

Modulo $|a+ib| = \sqrt{a^2+b^2}$

## Operazioni nel piano di Gauss

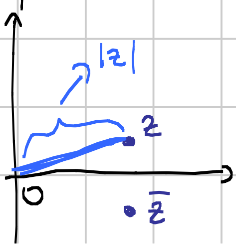



Somma: regola del parallelogramma

Prodotto e divisione: dopo

Coniugio: simmetria rispetto all'asse x

Modulo: distanza dall'origine.



**Oss:** $|z+w| \leq |z|+|w|$

$$|z+w| = \overline{OB} \underset{\uparrow}{\leq} \overline{OA} + \overline{AB} = \overline{OA} + \overline{OC} = |z|+|w| .$$

disuguaglianza triangolare

**Proprietà:**

① $z\bar{z} = |z|^2$

$(a+ib)(a-ib) = a^2-(ib)^2 = a^2+b^2$

② $\dfrac{1}{z} = \dfrac{\bar{z}}{|z|^2}$

③ $\overline{z+w} = \bar{z}+\bar{w}$ $\qquad \overline{z\cdot w} = \bar{z}\cdot\bar{w}$ $\qquad \overline{\left(\dfrac{z}{w}\right)} = \dfrac{\bar{z}}{\bar{w}}$ .

④ $|z\cdot w| = |z|\cdot|w|$

$z = a+ib \qquad w = c+id$

$(a+ib)(c+id) = (ac-bd)+i(bc+ad)$

$|z\cdot w|^2 = |z|^2\,|w|^2$

$(ac-bd)^2+(bc-ad)^2 \underset{\uparrow (ex)}{=} (a^2+b^2)\cdot(c^2+d^2)$ .

**Oss:** possiamo generare terne pitagoriche

$a^2+b^2=c^2 \qquad d^2+e^2=f^2$

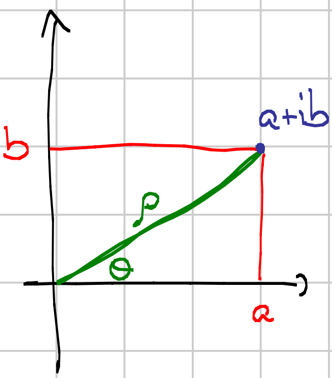
$(a^2+b^2)(d^2+e^2) = c^2f^2$

$(ac-bd)^2+(bc-ad)^2$

L'insieme dei numeri della forma $a^2+b^2$ $\quad a,b\in\mathbb{N}$ è chiuso rispetto al prodotto.

## Forma trigonometrica

Individuo $z$ mediante
- $\rho$ = distanza dall'origine
- $\theta$ = angolo col semiasse positivo delle ascisse.




Forma trigonometrica $\longleftrightarrow$ cartesiana

$$\begin{cases} a = \rho\cos\theta \\ b = \rho\sin\theta \end{cases} \qquad \begin{cases} \rho = \sqrt{a^2+b^2} \\ \theta \approx \operatorname{arctg}\dfrac{b}{a} \end{cases}$$

$$\boxed{z = \rho(\cos\theta + i\sin\theta)}$$

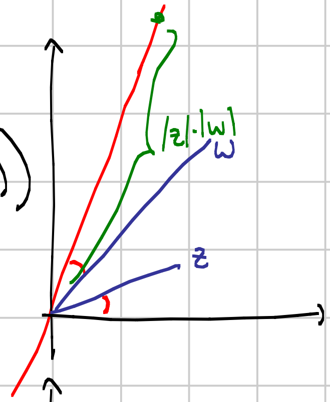
## Forma trigonometrica e prodotto

$z = \rho_1 (\cos\theta_1 + i \sin\theta_1)$

$w = \rho_2 (\cos\theta_2 + i \sin\theta_2)$

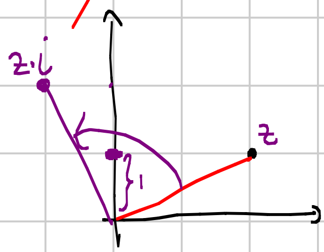
$z \cdot w = \rho_1 \rho_2 (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2 + i \sin\theta_1 \cos\theta_2 + i \sin\theta_2 \cos\theta_1)$

$\quad = \rho_1 \rho_2 ( \cos(\theta_1+\theta_2) + i \sin(\theta_1+\theta_2))$




Analogamente $\frac{z}{w} = \frac{\rho_1}{\rho_2} ( \cos(\theta_1-\theta_2) + i \sin(\theta_1-\theta_2))$

Es: cosa significa moltiplicare per $i$?
Ruotare di $90°$




Notazione: $\cos\theta + i \sin\theta = e^{i\theta}$

$e^{i\theta} \cdot e^{i\varphi} = e^{i(\theta+\varphi)}$

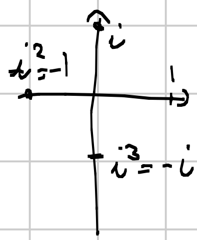
$(e^{i\theta})^{-1} = e^{-i\theta}$

Esempio: $-1 = e^{i\pi}$

Es: $[\rho(\cos\theta + i \sin\theta)]^2 = \rho^2 [\cos 2\theta + i \sin 2\theta]$

In generale

$$\boxed{[\rho(\cos\theta + i \sin\theta)]^n = \rho^n [\cos n\theta + i \sin n\theta]}$$




Es: $\cos 4\theta = \mathrm{Re}\,[\cos 4\theta + i \sin 4\theta]$

$= \mathrm{Re}\,[ (\cos\theta + i \sin\theta)^4 ]$

$= \mathrm{Re}\,[ \cos^4\theta + 4 i \sin\theta \cos^3\theta + 6 i^2 \sin^2\theta \cos^2\theta + 4 i^3 \sin^3\theta \cos\theta + i^4 \sin^4\theta ]$

$= \cos^4\theta - 6 \sin^2\theta \cos^2\theta + \sin^4\theta$

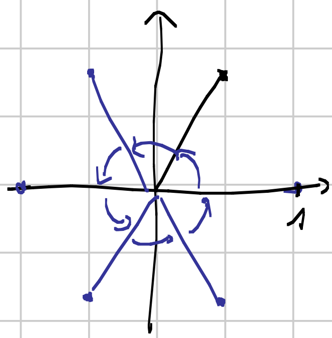
Es: $z = \frac{1}{2} + i \frac{\sqrt{3}}{2}$. Allora $z^6 = 1$

1° modo: svolgo la moltiplicazione.

2° modo: $|z| = 1$ $\quad \theta = \frac{\pi}{3}$

$z^6 = (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})^6 = \cos 2\pi + i \sin 2\pi = 1$

3° modo: graficamente




Es: $z = 1 + \sqrt{3}\, i$. $\quad z^{2012} = ?$

$z^{2012} = 2^{2012} (\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})^{2012}$

$= 2^{2012}\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)^{6\cdot 335+2}$

$= 2^{2012}\left[\left(\cos\pi/3 + i\sin\pi/3\right)^{6}\right]^{335} \cdot \left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)^{2}$

$= 2^{2012}\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$

$= 2^{2012}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$

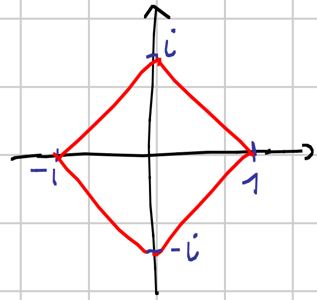
$= -2^{2011} + i\sqrt{3}\,2^{2011}$

## Radici di un numero complesso

Dato $a \in \mathbb{C}$, trovare $z \in \mathbb{C}$ $\quad z^n = a$.

Es: se $a = 0 \Rightarrow z = 0$

Es: $z^4 = 1 \qquad 1, -1, i, -i$ sono radici
$\qquad\qquad\qquad i^4 \quad i^2 \quad i \quad i^3$




$z^4 - 1 = (z-1)(z+1)(z-i)(z+i)$

Verifica: $(z-1)(z+1)(z-i)(z+i) = (z^2-1)(z^2+1) = z^4 - 1$.

**Teorema** se $a \neq 0$. Allora esistono $n$ numeri complessi t.c. $z^n = a$ e nel piano di Gauss sono i vertici di un poligono regolare con $n$ lati centrato nell'origine.

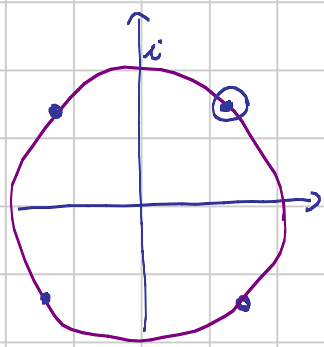
$a = \rho(\cos\theta + i\sin\theta) \qquad z = r(\cos\varphi + i\sin\varphi)$

Imponiamo $\rho(\cos\theta + i\sin\theta) = a = z^n = r^n(\cos n\varphi + i\sin n\varphi)$

Devono avere lo stesso modulo $\begin{cases} \rho = r^n \\ \theta = n\varphi + 2k\pi \quad k \in \mathbb{Z}. \end{cases}$
" " " " angolo
a meno di $2\pi$

$\begin{cases} r = \sqrt[n]{\rho} \\ \varphi = \dfrac{\theta - 2k\pi}{n} \end{cases}$ ($\sqrt{\ }$ dei numeri reali) $\quad k \in \mathbb{Z}$? basta prendere $k = 0, \dots, n-1$

**Esempio:** $z^4 = -1$




$n = 4 \quad \rho = 1 \quad \theta = \pi$

$+\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)$, $\quad \cos -\frac{\pi}{4} + i\sin -\frac{\pi}{4} = \cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi$

$\cos\left(-\frac{3}{4}\pi\right) + i\sin\left(-\frac{3}{4}\pi\right) = \cos\frac{5}{4}\pi + i\sin\frac{5}{4}\pi$

$\cos\left(-\frac{5}{4}\pi\right) + i\sin\left(-\frac{5}{4}\pi\right) = \cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi$

2° modo: $\frac{1+i}{\sqrt{2}}$ funziona.

# Polinomi

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$a_0, \dots, a_n \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono detti coefficienti.

$n = \deg(p(x))$ è il grado.

Diciamo che $p$ è monico se $a_n = 1$.

Possiamo sommare, moltiplicarli, fare la divisione col resto: dati $p(x), q(x)$ polinomi, esistono unici $a(x)$ e $r(x)$ t.c.

$$p(x) = a(x) \cdot q(x) + r(x) \quad \text{con} \quad \deg r(x) < \deg q(x)$$

Si dimostra per induzione su $\deg p$.

Esempio:

$$\begin{array}{rrrrr|l}
x^4 & -x^3 & +3x^2 & -2x & +1 & x^2+x+1 \\ \cline{6-6}
-x^4 & -x^3 & -x^2 & & & x^2-2x+4 \\ \cline{1-5}
 & -2x^3 & +2x^2 & -2x & +1 & \\
 & +2x^3 & +2x^2 & +2x & & \\ \cline{1-5}
 & & 4x^2 & +0 & +1 & \\
 & & -4x^2 & -4x & -4 & \\ \cline{1-5}
 & & & -4x & -3 &
\end{array}$$

$$x^4 - x^3 + 3x^2 - 2x + 1 = (x^2+x+1)(x^2-2x+4) - 4x - 3$$

Possiamo fare la divisione con $q(x) = x - a$

$$p(x) = q(x)(x-a) + r\cancel{(x)} \qquad \underset{\overset{\shortparallel}{0}}{\deg} r(x) < 1 \implies r(x) \text{ è costante}$$

Chi è $r$? Valuto il polinomio in $x = a$

$p(a) = r$.

Abbiamo ottenuto il

**Teorema di Ruffini**: $p(x) = q(x)(x-a) + p(a)$.

**Corollario**: se $a$ è una radice di $p(x)$ (ovvero $p(a) = 0$) allora $p(x) = q(x)(x-a)$.

**Corollario**: un polinomio di grado $n$ ha al più $n$ radici $x_1, \dots, x_n$.

Supponiamo per assurdo che ne abbia $n+1$: $x_1, \dots, x_{n+1}$

$p(x) = (x - x_1)\, q(x)$.

Valuto $x_i$ $\quad 0 = p(x_i) = (x_i - x_1)\, q(x_i) \Rightarrow q(x_i) = 0$

$\Rightarrow q(x) = (x - x_2)\, r(x) \ldots$

$p(x) = (x - x_1)\, q(x) = (x - x_1)(x - x_2)\, r(x) \ldots$

$= (x - x_1) \ldots (x - x_{n+1})\, s(x).$

Ma allora il RHS ha grado $\geq n+1$ oppure è $\equiv 0$, assurdo.

Possiamo pensare a un polinomio come $x \to p(x)$.
Chiamiamo funzione polinomiale.
È chiaro che se $p = q$ come polinomi, allora

$$p(x) = q(x) \quad \forall x$$

(cioè sono = come funzioni polinomiali).

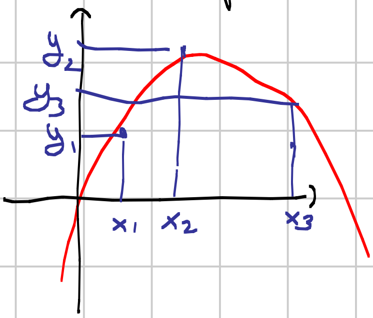
## Principio di identità dei polinomi

Se esistono $n+1$ ($\geq \deg p, q$) valori su cui $p(x)$ e $q(x)$ coincidono, allora $p = q$ come polinomi (ovvero hanno gli stessi coefficienti).

Siano $x_1, \ldots, x_{n+1}$ t.c. $p(x_i) = q(x_i)$.
Considero $p(x) - q(x)$. Ha $n+1$ radici (gli $x_i$).
$\Rightarrow$ per il corollario $p(x) - q(x)$ è il polinomio $\equiv 0$.

## Costruire un polinomio di grado $n$ assegnati $n+1$ valori

Date $n+1$ coppie $(x_i, y_i)$, esiste un unico polinomio $p(x)$ di grado $\leq n$ t.c. $p(x_i) = y_i \quad \forall i = 1, \ldots, n+1$.




Dim:
Unicità: segue dal principio di identità.
Esistenza: $p(x) = a_n x^n + \ldots + a_0$

$$\begin{cases} a_n x_1^n + \ldots + a_0 = y_1 \\ a_n x_2^n + \ldots + a_0 = y_2 \\ \vdots \end{cases}$$

$$\begin{pmatrix} x_1^n & x_1^{n-1} & \ldots & x_1 & 1 \\ x_2^n & x_2^{n-1} & \ldots & x_2 & 1 \\ \vdots & \vdots & & & \end{pmatrix}$$

È un sistema di $n+1$ equazioni lineari in $n+1$ incognite.
In questo caso il sistema ha sempre un'unica soluzione

(ma non è banale vederlo).

<u>Nuova strategia</u>:

- $y_1 = \dots = y_{n+1} = 0 \longrightarrow p(x) \equiv 0$
- $y_1 = \dots = y_n = 0 \qquad y_{n+1} = 1$

  $p(x)$ ha $n$ radici $x_1, \to x_n$

  $$p(x) = (x-x_1)(x-x_2)\dots(x-x_n)\cdot r$$

  è un numero perchè vogliamo $\deg p \le n$

  Scegliamo $r$ per verificare $p(x_{n+1}) = 1$:

  $$(x_{n+1}-x_1)(x_{n+1}-x_2)\dots(x_{n+1}-x_n)\cdot r = 1$$

  Scegliamo $r = \dfrac{1}{(x_{n+1}-x_1)\dots(x_{n+1}-x_n)}$.

  Chiamiamo $p_i(x) = \dfrac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)}$. $p_i(x)$ vale $1$ in $x_i$ e $0$ negli altri $x_j$, $j\neq i$.

- caso generale:

  $$p(x) = \sum_{i=1}^{n+1} y_i\, p_i(x)$$

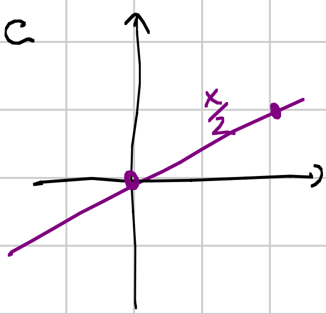
  Funziona!

  $$p(x_k) = y_1 p_1(x_k) + y_2 p_2(x_k) \dots + y_{n+1} p_{n+1}(x_k)$$
  $$= y_k p_k(x_k) = y_k.$$

<u>Oss</u>: la possibilità di assegnare $n+1$ valori vale in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, ma non in $\mathbb{Z}$.

Es: non esiste un poli di grado $\le 1$ con coeff in $\mathbb{Z}$ t.c

$p(0) = 0 \qquad p(2) = 1$



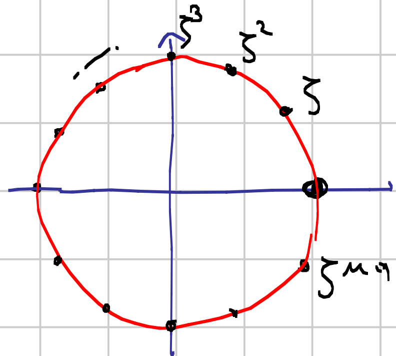
# Polinomi a coeff complessi

**Teorema (difficile):** $p(x)$ a coeff complessi, $\deg p(x) \geq 1$
$\Rightarrow$ $p(x)$ ha una (almeno!) radice in $\mathbb{C}$.

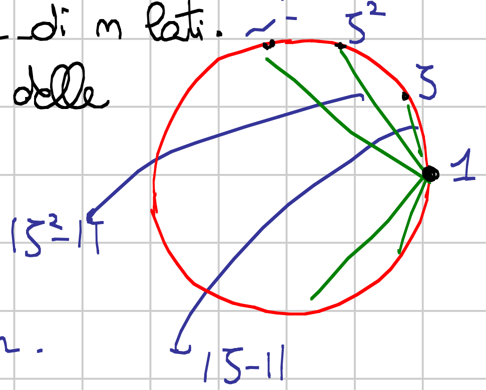
**Corollario (teorema fondamentale dell'algebra)**
$p(x)$ polinomio a coeff complessi
Allora esistono $\lambda_1, \dots, \lambda_n$ t.c.
$$p(x) = a_n (x-\lambda_1) \dots (x-\lambda_n).$$

Dim:
Per induzione su $n = \deg p$.
Se $p$ ha grado 1 ovvio.
$n \to n+1$. Per il teo precedente $p(x)$ (con $\deg p(x) = n+1$) ha una radice $\lambda_{n+1} \Rightarrow$
$$p(x) = (x-\lambda_{n+1})\, q(x). \quad (*)$$
$\Rightarrow$ $q$ ha grado $n$ e per hp induttiva
$$q(x) = a_n (x-\lambda_1) \dots (x-\lambda_n)$$
Sostituendo in $(*)$, ottengo
$$p(x) = a_n (x-\lambda_1) \dots (x-\lambda_n)(x-\lambda_{n+1}).$$

Es: $x^n - 1 = 1 \cdot (x-\zeta)(x-\zeta^2) \dots (x-\zeta^{n-1})(x-1)$
non c'è coeff perchè il polinomio è monico




Esercizio: consideriamo un poligono regolare di $n$ lati.
Vogliamo calcolare il prodotto dei lati e delle diagonali uscenti da un vertice fissato.




Vogliamo $\prod_{k=1}^{n-1} |\zeta^k - 1|$
$$= \left| \prod_{k=1}^{n-1} (\zeta^k - 1) \right| = |p(1)| = n.$$

Consideriamo $p(x) = \prod_{k=1}^{n-1} (x - \zeta^k) \overset{\text{esempio precedente}}{=} \dfrac{x^n - 1}{x-1} = x^{n-1} + x^{n-2} + \dots + x + 1$
$|p(1)| = n.$

# Polinomi a coefficienti reali

Un polinomio a coeff reali si scrive sempre come prodotto
- fattori di grado 1
- fattori di grado 2 con $\Delta < 0$.

Dim:
Nella fattorizzazione in $\mathbb{C}$ ci sono alcune radici reali e radici "veramente" complesse.

Oss: $\lambda \in \mathbb{C}$ è radice, ovvero $p(\lambda)=0 \Rightarrow \bar{\lambda}$ è radice.

$$a_n \lambda^n + a_{n-1}\lambda^{n-1} + \_\_ + a_0 = 0$$
$$\overline{a_n}\,\bar{\lambda}^n + \overline{a_{n-1}}\,\bar{\lambda}^{n-1} + \_\_ + \overline{a_0} = 0$$
$$a_n \bar{\lambda}^n + a_{n-1}\bar{\lambda}^{n-1} + \_\_ + a_0 = 0 \iff p(\bar{\lambda}) = 0.$$

Nella fattorizzazione in $\mathbb{C}$ c'è $(x-\lambda)(x-\bar{\lambda})$
È un poli di grado 2 a coeff reali
$$x^2 - \underbrace{(\lambda+\bar{\lambda})}_{\in \mathbb{R}} x + \underbrace{\lambda\bar{\lambda}}_{= |\lambda|^2 \in \mathbb{R}}$$

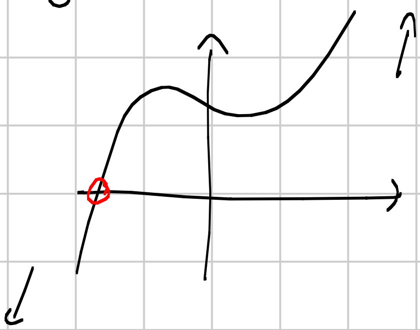
Oppure $\lambda = a+ib$
$$(x-a-ib)(x-a+ib) = (x-a)^2 + b^2$$

Oss: Un polinomio a coeff reali di grado dispari ha sempre una radice reale.
Idea: le radici complesse "vanno a coppie".

Oss: un polinomio ha lo stesso comportamento a $\pm\infty$ del suo termine di grado massimo

Es $x^{100} - 257x^{20} + x - 1$

Es $x^3 - 2x + 7$



Esercizio: Trovare tutti i poli a coeff reali $p(x)$ di grado dispari t.c.
$$p(x^2+1) = p(x)^2 + 1 \quad \forall x \in \mathbb{R}.$$

$p(x) = x$ funziona: $x^2+1 = x^2+1$
$p(x) = c$? $c = c^2+1 \iff c^2-c+1=0$ non ha sol reali.
Sappiamo che un poli di grado dispari si annulla sempre.
Supponiamo che esista $a \in \mathbb{R}$ t.c $p(a) = a$.
(esiste, perchè $p(x)-x$ ha grado dispari $\Rightarrow$ ha una radice).
Sostituendo $x=a$ $\quad p(a^2+1) = a^2+1$
Sostituendo $a^2+1$ $\quad p((a^2+1)^2+1) = (a^2+1)^2+1$. ....
$a < a^2+1 < (a^2+1)^2+1 < \dots$ risolvono

$$p(x) = x, \text{ ovvero } p(x)-x=0$$

Ma allora, visto che $p(x)-x$ ha un numero finito di radici oppure è nullo, $p(x)-x \equiv 0$.

## Polinomi a coefficienti interi

## Teorema delle radici razionali

$p(x)$ a coeff interi $\quad p(x) = a_n x^n + \dots + a_0$.
Allora se $q/r$ è una radice, $q \mid a_0$ e $r \mid a_n$
↳ ridotta ai min termini.

Sostituiamo

$$r^n \left(a_n \frac{q^n}{r^n} + a_{n-1} \frac{q^{n-1}}{r^{n-1}} + \dots + a_0\right) = 0$$

$$a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1} + a_0 r^n = 0$$

$q$ divide tutti i primi $n$ addendi $\Rightarrow q \mid a_0 r^n$.
Ma $(q, r) = 1$.
Lo stesso per $r$.

Es: $x^3+x+1$ è riducibile come poli a coeff in $\mathbb{Z}$?
No!
Se fosse riducibile, avrebbe un fattore di grado 1, cioè una radice.
Ma per il teo precedente le radici razionali possono essere solo $\pm 1$. Verificando, non funzionano.

**Esercizio:** $p(x)$ a coeff interi. $p(1)=1$ e $p(7)=7$

Mostrare che $p(4) \equiv 4 \ (9)$.

**1° modo:**

$$p(x) = \underbrace{(x-1)\, q(x) + 1}_{\text{Ruffini}} \qquad (\bullet)$$

$$7 = p(7) = 6\, q(7) + 1 \implies q(7) = 1$$

$$\implies q(x) = (x-7)\, r(x) + 1$$

Quindi da $(\bullet)$ $\quad p(x) = (x-1)\left[(x-7)\, r(x) + 1\right] + 1$

$$= (x-1)(x-7)\, r(x) + x$$

Valuto in $x=4$ $\quad p(4) = 3 \cdot (-3)\, r(4) + 4$

$$= -9\, r(x) + 4$$

**2° modo:** consideriamo $q(x) = p(x) - x$

$q(x)$ si annulla in $1$ e $7$ $\implies q(x) = (x-1)(x-7)\, r(x)$

...

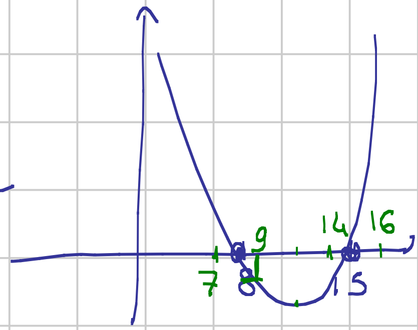
**Esercizio** esiste $p(x)$ a coeff interi t.c. $p(8)=8$ $\quad p(15)=15$

Trovare il min $a>0$ t.c. $p(x) = x + a$ ha una sol intera

$$p(x) - x = (x-8)(x-15)\, r(x) = a$$

vogliamo che esista una sol intera.

Mi conviene prendere $r(x) = \pm 1$




Vogliamo il pto a coordinate intere con ordinata + piccola che sta sulla parabola.

$$(7-8)(7-15)(\pm 1) = 8 = a$$

$$(9-8)(9-15)(\pm 1) = \boxed{6 = a}$$

$$(14-8)(14-15)(\pm 1) = 6 = a$$

$$(16-8)(16-15)(\pm 1) = 8 = a$$

Oss: $a-b \mid a^n - b^n$ (*) $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b + \_ + ab^{n-2}+b^{n-1})$

$a+b \mid a^n+b^n$ se $n$ è dispari.

Metto $-b$ nella precedente

$$a^n+b^n = (a+b)(a^{n-1} - a^{n-2}b + \_ \quad + b^{n-1})$$

uso $n$ dispari

Lemma: $p(x)$ a coeff interi.

$a-b \mid p(a)-p(b)$

[(*) si ottiene con $p(x)=x^n$]

Dim 1:

Per Ruffini: $p(x) = (x-a)\,q(x) + p(a)$.

Valuto in $b$: $p(b) = (b-a)\,q(b) + p(a)$.

Dim 2:

$p(x) = a_n x^n + \dots + a_0$

$p(b)-p(a) = a_n(b^n - a^n) + a_{n-1}(b^{n-1}-a^{n-1}) + \_ \quad + a_1(b-a)$

$a-b$ divide ogni addendo per l'oss.

Lemma [IMO 2006]

$p(x)$ a coeff interi. $\qquad p^{(k)}(x) = \underbrace{p(p \dots p(x)\dots))}_{k \text{ volte}}$

Supponiamo che $p^{(k)}(a) = a$ per un certo $a \in \mathbb{Z}$.

Allora $\qquad p^{(2)}(a) = a$.

Usiamo il lemma con $b = p(a)$

$p(a)-a \mid p(p(a)) - p(a) \mid p^{(3)}(a) - p^{(2)}(a) \mid \dots$

$\mid \_\_ \mid p^{(k)}(a) - p^{(k-1)}(a) \mid p^{(k+1)}(a) - p^{k}(a) = p(a)-a$

Sono tutti $=$ a meno del segno.

$\cancel{p(a)}-a = -p(p(a)) + \cancel{p(a)} \implies$ tesi.

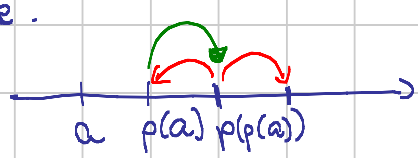
$p(a)-a = p(p(a)) - p(a)$

Vediamo che il 2° caso è impossibile.

Ci sono 2 casi:

$p^{(3)}(a) - \cancel{p^{(2)}(a)} = -\cancel{p^{(2)}(a)} + p(a)$ oppure

$p^{(3)}(a) - p^{(2)}(a) = p^{(2)}(a) - p(a) = p(a) - a$



Sappiamo che $p^{(k)}(a) = a$.
Per tornare ad $a$, la successione $p^{(i)}(a)$ deve andare su $p(a)$. Ma da $p(a)$ si va a $p(p(a))$, non ad $a$! Assurdo.

## Relazioni radici-coefficienti

$p(x) = x^n + a_{n-1}x^{n-1} + \_\_ + a_0$.
Siano $\lambda_1, \_\_, \lambda_n$ le radici $\in \mathbb{C}$ (eventualmente ripetute).
Allora:

$$-a_{n-1} = \lambda_1 + \_\_ + \lambda_n = \sum_{1\le i\le n} \lambda_i$$

$$a_{n-2} = \sum_{1\le i<j\le n} \lambda_i\lambda_j$$

$$-a_{n-3} = \sum_{1\le i<j<k\le n} \lambda_i\lambda_j\lambda_k$$

$$\vdots$$

$$(-1)^n a_0 = \lambda_1 \cdots \lambda_n.$$

$$p(x) = x^n + a_{n-1}x^{n-1} + \_\_ + a_0 = (x-\lambda_1)(x-\lambda_2)\_\_(x-\lambda_n)$$

$$\begin{aligned} &= x^n \\ &\quad - x^{n-1}(\lambda_1 + \_\_ + \lambda_n) \\ &\quad + x^{n-2}\left(\sum \lambda_i\lambda_j\right) \\ &\quad \vdots \\ &\quad + (-1)^n \lambda_1 \_\_ \lambda_n \end{aligned}$$

Esempio: $2x^3+6x+6$.
Non è monico. Considero $x^3+3x+3$

$\lambda_1+\lambda_2+\lambda_3 = 0$
$\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = 3$
$\lambda_1\lambda_2\lambda_3 = -3$

$$\lambda_1^2+\lambda_2^2+\lambda_3^2 = (\lambda_1+\lambda_2+\lambda_3)^2 - 2(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3)$$
$$= -6$$
$\Rightarrow$ il polinomio ha 2 radici complesse

<u>Oss</u>: $p(\lambda)=0 \Rightarrow \frac{1}{\lambda}$ è radice di $a_0x^n+a_1x^{n-1}+\ldots+a_n=0$

$$a_n\lambda^n+a_{n-1}\lambda^{n-1}+\ldots+a_0=0$$

Divido per $\lambda^n$ $\quad a_n+a_{n-1}\frac{1}{\lambda}+\ldots+a_0\frac{1}{\lambda^n}=0$

<u>Oss</u>: $\frac{1}{\lambda_1}+\frac{1}{\lambda_2}+\ldots+\frac{1}{\lambda_n} = -\frac{a_1}{a_0}$

<u>1° modo</u>: $\dfrac{\lambda_2\lambda_3\ldots\lambda_n+\lambda_1\lambda_3\ldots\lambda_n+\ldots}{\lambda_1\ldots\lambda_n}$

$$= \frac{(-1)^{n-1}a_1}{(-1)^n a_0} = -\frac{a_1}{a_0}$$

<u>2° modo</u>: $\frac{1}{\lambda_i}$ sono radici $\dfrac{a_0x^n+\ldots+a_n}{a_0}=0$

$\Rightarrow$ la somma delle radici è $-\frac{a_1}{a_0}$.

Torniamo a coeff in $\mathbb{Z}$.

<u>Criteri di irriducibilità</u>

<u>Criterio di Eisenstein</u>

$f(x)$ a coeff interi. $p$ primo

$$p\nmid a_n \qquad p\mid a_0,\ldots,a_{n-1} \qquad p^2\nmid a_0.$$

Allora $p(x)$ è irriducibile tra i poli a coeff interi.

Supponiamo per assurdo

$$a_nx^n+\ldots+a_0 = (b_kx^k+b_{k-1}x^{k-1}+\ldots+b_0)(c_\ell x^\ell+\ldots+c_0)$$

$p\mid a_0=b_0c_0$.

Esattamente uno tra $b_0$ e $c_0$ è divisibile per $p$.

Wlog, $p\mid b_0 \quad p\nmid c_0$.

$p \mid a_1 = b_0 c_1 + b_1 c_0 \implies p \mid b_1.$

$p \mid a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2 \implies p \mid b_2$

$\vdots \qquad \vdots$

$p \mid b_k$

$p \nmid a_m = b_k c_\ell$ ma questo è divisibile per $p$.

Esercizio: $x^{p-1} + x^{p-2} + \_\_ + x + 1$ è irriducibile in $\mathbb{Z}$.

È $\frac{x^p - 1}{x-1} =: P(x)$. $p(x)$ è irriducibile $\iff p(x+1)$ è irriducibile

Vediamo che $P(x+1)$ è irriducibile.

$$P(x+1) = \frac{(x+1)^p - 1}{x + \cancel{1} - \cancel{1}} = \frac{x^p + \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \ldots + px + \cancel{1} - \cancel{1}}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \_\_ + p$$

Siamo nelle hp di Eisenstein: $p \mid \binom{p}{i}$ $\forall i \neq 0, p$.

$$\boxed{4 \nmid \binom{4}{2} = 6}$$