A1 Basic

Danilo

Note Title 9/3/2016

Polinomi e numeri complessi

NUMERI COMPLESSI STRIKE BACK

$$\mathbb{C} = \{ a+ib \mid a,b \in \mathbb{R},\ i^2 = -1 \}$$

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

Operazioni

- SOMMA
- PRODOTTO
- CONIUGIO
- MODULO

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

Abbiamo scoperto che $\frac{1}{w} = \frac{\bar{w}}{|w|^2}$ $\left(\Rightarrow w\bar{w} = |w|^2\right)$

PROPRIETÀ

- $\overline{wz} = \bar{w}\cdot\bar{z}$
- $\overline{w+z} = \bar{w}+\bar{z}$
- $|w\cdot z| = |w||z|$
- $|z+w| \leq |z|+|w|$

$$\left(\mathbb{R} = \{ a+ib \in \mathbb{C} \mid b=0 \} = \{ z \in \mathbb{C} \mid z = \bar{z} \} \right)$$

Formula di de Moivre

$$z^n = \left[\rho\left(\cos\theta + i\sin\theta\right)\right]^n = \rho^n\left(\cos(n\theta) + i\sin(n\theta)\right)$$

$$z^n = \left(\rho\, e^{i\theta}\right)^n = \rho^n\, e^{in\theta}$$

Perché questi complessi?

$x^2 + 2x + 1 = 0$

$x^2 + 1 = 0$

ha soluz $x = \pm i$

$x^2 - 1 = 0$

$x^2 + 2x + 3 = 0$

$-1 \pm \sqrt{-2}$

$\sqrt{-2} = 0 + i(\sqrt{2})$

Non è forse che $p(x)$ ha sempre radici in $\mathbb{C}$?

Polinomi

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

n — deg p

a_n — coefficiente direttore

a_1 — termine lineare

a_0 — termine noto

$a_n = 1$, p è monico

$a_n, a_{n-1}, a_{n-2}, \dots, a_1, a_0 \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \square, \dots$

Tra polinomi funziona la divisione con resto!
Cioè se ho due polinomi $a(x)$, $b(x)$, esistono altri due polinomi $q(x)$ e $r(x)$ t. c.

$$\boxed{a(x) = q(x)\,b(x) + r(x)}, \quad \deg r < \deg b$$

Def (MCD) Dati $a(x)$, $b(x)$, esiste $d(x)$ t.c.:

- $d(x) \mid a(x)$
- $d(x) \mid b(x)$
- se $e(x)$ t.c. $e(x) \mid a(x)$ e $e(x) \mid b(x)$ allora $e(x) \mid d(x)$

L'algoritmo di Euclide funziona (in particolare è vero che $(a(x), b(x)) = (b(x), r(x))$)

(Identità di) Bézout $a(x), b(x), d(x) = (a(x), b(x))$, esistono $h(x), k(x)$ t.c.

$$d(x) = a(x)h(x) + b(x)k(x)$$

Dim $a(x) = b(x)q(x) + r(x)$

$d(x) = (b(x), r(x))$ | Induzione su $\deg b$

supponiamo che Bézout valga per i polinomi di grado $\leq \deg a$

$$d(x) = b(x)h'(x) + r(x)k'(x)$$

$$r(x) = a(x) - b(x)q(x)$$

$$d(x) = b(x)h'(x) + \big(a(x) - b(x)q(x)\big)k'(x) =$$

$$= b(x)h'(x) + a(x)k'(x) - b(x)q(x)k'(x) =$$

$$= a(x)k'(x) + b(x)\underbrace{\big(h'(x) - q(x)k(x)\big)}_{\text{polinomio}}$$

□

Ruffini (Odi et amo)

$b(x) = x - \alpha$

$a(x) = (x-\alpha)q(x) + r(x)$ ← chi è?

$\deg b \geq \deg r \Rightarrow$ r è un polinomio di grado 0

calcoliamo tutto in $x = \alpha$

$$a(\alpha) = (\alpha - \alpha)\, q(\alpha) + r(\alpha)$$

$$\boxed{a(x) = (x-\alpha)\, q(x) + a(\alpha)}$$

Cor (Ruffini che conoscevate)

se $p(\alpha) = 0 \Rightarrow (x-\alpha) \mid p(x)$

Cor Un polinomio di grado n ha al più n radici

$\deg p = n$

$p(x) = (x-\alpha_1)\, q(x)$ ha $\deg n-1$

↳ ↳ ...

Criterio di identità dei polinomi Se $a(x)$ e $b(x)$ $\deg a, \deg b < n$, se $a(x_i) = b(x_i)$ $i = 1, \dots, n$

$\Rightarrow a(x) = b(x)$.

$p(x) = a(x) - b(x)$

$p(x_i) = a(x_i) - b(x_i) = 0$ per $i = 1, \dots, n$

$\Rightarrow p(x) \equiv 0 \Rightarrow a(x) = b(x)$

Fattorizzazione unica Un polinomio $a(x)$ ammette un'unica scrittura come

$$a(x) = f_1(x)^{\alpha_1} \cdot \dots \cdot f_n(x)^{\alpha_n}$$

dove f_i sono irriducibili (:= "non hanno divisori")

Interpolazione di Lagrange

(x_i, y_i) $i = 1, \dots, n$ voglio trovare un polinomio t.c. $p(x_i) = y_i$ $\forall i = 1 \dots n$. Esiste?
Sì, e lo costruiamo:

$$p_i(x) = \frac{(x-x_1)(x-x_2)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)(x_i-x_2)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)}$$

$p_i(x_i) = 1$ $\qquad$ $p_i(x_j) = 0$ per $j \neq i$

$$P(x) = \sum_{i=1}^{n} p_i(x)\, y_i$$ funziona!

$P(x)$ ha grado $n-1$.

Polinomi a coefficienti interi

Lemma (degli zeri razionali) $p(x) = a_n x^n + \dots + a_1 x + a_0$ a coefficienti interi, $\frac{q}{r}$, $q, r \in \mathbb{Z}$, $(q,r) = 1$.
se $p(\frac{q}{r}) = 0$ allora $q \mid a_0$, $r \mid a_n$

Dim $0 = p\left(\frac{q}{r}\right) = a_n\left(\frac{q}{r}\right)^n + a_{n-1}\left(\frac{q}{r}\right)^{n-1} + \dots + \left(\frac{q}{r}\right)a_1 + a_0 =$

$$= \underbrace{a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1}}_{\text{div. per } q} + \underbrace{a_0 r^n}_{\text{div per } r}$$

Siccome $(q,r) = 1$, $\Rightarrow$ a_n deve essere divisibile per r
allo stesso modo a_0 deve essere divisibile per q. □

Lemma $p(x)$ a coefficienti interi, $a, b \in \mathbb{Z}$, $a \neq b$
$\rightarrow$ $a - b \mid p(a) - p(b)$

Dim

$p(x) = (x-a)\,q(x) + \underbrace{r(x)}_{\text{è } p(a)}$ e calcolo in b

$p(b) = (b-a)\,q(x) + p(a) \Rightarrow p(a) - p(b) = (a-b)\,q(b)$ □

Polinomi a coefficienti razionali

Teorema di Gauss $p(x)$ monico a coefficienti razionali.
$p(x)$ è irriducibile su $\mathbb{Q} \iff p(x)$ è irriducibile su $\mathbb{Z}$.

Polinomi a coefficienti complessi

Teorema Ogni polinomio a coefficienti in $\mathbb{C}$ ammette radici in $\mathbb{C}$.

Teorema (fondamentale dell'algebra)
$p(x)$ è un polinomio a coefficienti complessi di grado n e $x_1, \dots x_n$ sono le sue radici posso scrivere

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

Polinomi a coefficienti reali

Teorema (bello) Ogni polinomio a coefficienti reali si spezza in fattori di grado 1 o 2.

Dim Lemma preliminare: se $p(\overset{\in \mathbb{C}}{z}) = 0$ allora $p(\bar{z}) = 0$

$$\begin{aligned} 0 &= a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = \\ &= \overline{a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0} = \\ &= a_n \bar{z}^n + a_{n-1} \bar{z}^{n-1} + \dots + a_1 \bar{z} + a_0 = p(\bar{z}) \end{aligned}$$ #

Per induzione sul grado (uso l'induzione forte: il teorema vale per ogni $q(z)$, $\deg q < n$)

- $p(z)$ ha una radice $\alpha \in \mathbb{R}$

allora $p(z) = \underbrace{q(z)}_{\text{ha grado } < n}(z-\alpha)$ ✓

- $p(z)$ ha una radice $\in \mathbb{C}\setminus\mathbb{R}$

$(z-\alpha) \mid p(z) \xrightarrow[\text{lemma}]{} (z-\bar{\alpha}) \mid p(z)$

$(z-\alpha)(z-\bar{\alpha}) \mid p(z)$

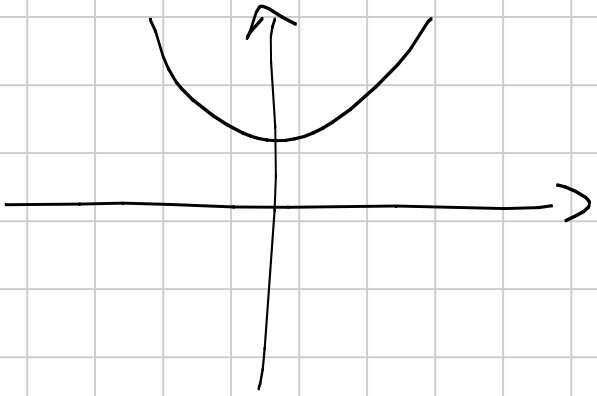
$\alpha+\bar{\alpha} = a+ib+(a-ib) = 2a = 2\,\mathrm{Re}\,\alpha$

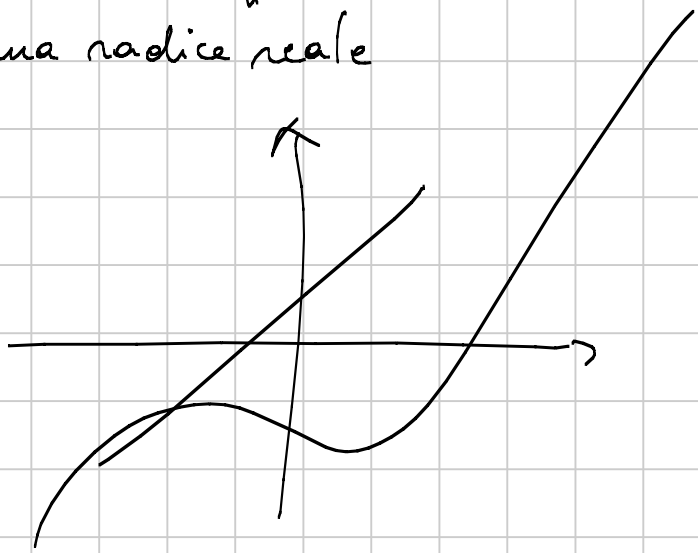
$z^2 - (\alpha+\bar{\alpha})z + \alpha\bar{\alpha} = z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2$

$z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2 \mid p(z)$

significa $p(z) = (z^2 - 2\,\mathrm{Re}\,\alpha\, z + |\alpha|^2)\,\underbrace{q(z)}_{\text{ha grado } n-2}$ □

Corollario Ogni polinomio a coefficienti reali di grado dispari ha una radice reale





Formule di Viète

$(x-\lambda_1)(x-\lambda_2) = x^2 - \overbrace{(\lambda_1+\lambda_2)}^{\swarrow} x + \overbrace{\lambda_1\lambda_2}^{\swarrow}$

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

$p(x)$ di grado n e monico

$$p(x) = 1\cdot(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) =$$

$$= x^n + (-\lambda_1-\lambda_2-\lambda_3-\cdots-\lambda_n)x^{n-1} + (\lambda_1\lambda_2+\lambda_1\lambda_3+\cdots)x^{n-2} +$$

$$\cdots + (-1)^{n-1}(\lambda_1\lambda_2\cdots\lambda_{n-1}+\cdots)x + (-1)^n\lambda_1\lambda_2\lambda_3\cdots\lambda_n$$

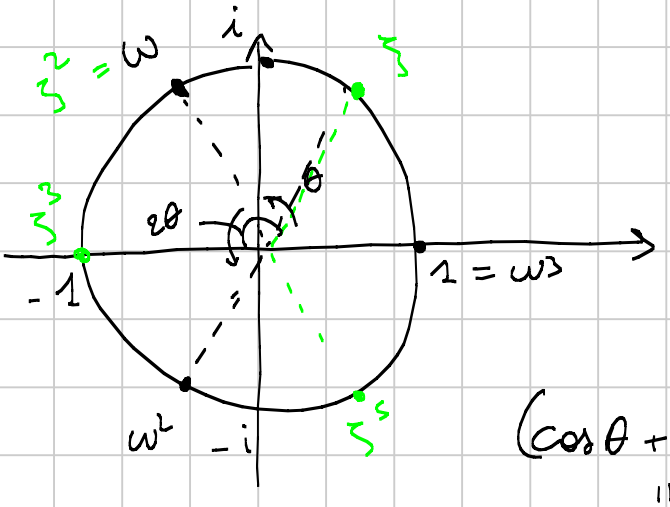
Tutti i coefficienti si scrivono in funzione di somme simmetriche nelle radici

$$S_k = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$$

Tutti i coefficienti si esprimono come somme e prodotti degli S_k.

Radici dell'unità

Sono quei numeri complessi per cui esiste $n \in \mathbb{N}\setminus\{0\}$, t.c. $z^n = 1$



ω è una radice terza

$\omega^3 = 1$

$$\omega = \underbrace{\rho}_{=1}(\cos\theta + i\sin\theta)$$

$$(\cos\theta + i\sin\theta)^3 = 1$$

$$\cos(3\theta) + i\sin(3\theta)$$

Quale angolo θ è t.c. $3\theta = \frac{2\pi}{3}$

$z^n = 1 \Rightarrow z^n - 1 = 0$ sono n radici

ξ radice sesta $\xi^6 = 1$. In particolare

$(\xi^2)^3 = 1 \Rightarrow \xi^2$ è una radice terza.

Una radice n-esima si dice primitiva se <u>non</u> è una radice d-esima per nessun $d|n$.

$\xi, \xi^2, \xi^{(3)}, \ldots \xi^{(n)} = 1$

se divide n

tutti gli esponenti coprimi con n mi danno radici primitive (attenzione: devo essere partito da una radice primitiva)

Domanda: come si fattorizza $x^n - 1$?

Pag 13 69, 70, 72, 75, 77

Pag 23 4, 5, 7, 8, 11.

(72) $p(2) = a \quad p(a) = a + 2$

$a - 2 \mid p(a) - p(2) = a + 2 - a = 2$

$a - 2 = \pm 1, \pm 2$

(75) $p(x) = \frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-a)(x-c)}{(b-c)(b-a)} = 1$

$p(x) - 1 = 0$ (deg 2) ha 3 radici (a, b, c).

(7) • Esiste un polinomio t.c. $p(n) = 2^n \ \forall 0 \le n \le k$?
• Ne esiste uno t.c. $p(n) = 2^n \ \forall n \in \mathbb{N}$?

1) Certo: Interpolazione di Lagrange

$(0,1)\ (1,2)\ (2,4), \dots\ (k, 2^k)$ ← $k+1$ valori

Con Lagrange so trovare il polinomio che cerco che avrà grado k.

2) $P(n) = 2^n$, $P(n+1) = 2^{n+1}$

~~$g(x) = P(x) - 2^x$~~

Costruisco $g(x) = P(x+1) - 2P(x)$.

$g(n) = 0 \ \forall n \in \mathbb{N}$, quindi $g \equiv 0$

$$P(x+1) = 2P(x)$$

$$a_n \underbrace{(x+1)^n}_{a_n x^n + (\dots)} + \dots = 2 a_n (x)^n + \dots \quad \Rightarrow a_n = 2a_n$$

$$\Rightarrow a_n = 0$$

ma non soddisfa le mie richieste.

(8) Polinomio $P(x)$, $P(0)=2$, $P(1)=4$, $P(2)=6$, $P(3)=56$

$p(x) = x\,q(x) + p(0)$ $\quad q(x) = x(x-1)(x-2)(x-3)$

Ho un polinomio di terzo grado (il resto!) di cui conosco 4 valori distinti.

⇒ Uso Lagrange per trovare il polinomio che passa per quei 4 valori.

(11) $p(z)$ di grado 2002

"Prendo" valori $a_1, a_2, \dots a_{2002}$

$$\begin{cases} P_1(z) = z - a_1 \\ P_{n+1}(z) = P_n(z)^2 - a_{n+1} \end{cases}$$

$$p(z) = \alpha (z-\lambda_1)(z-\lambda_2)\dots(z-\lambda_{2002})$$

$P(z) \mid P_{2002}(z)$ significa che $P_{2002}(\lambda_i) = 0$

$$0 = P_{2002}(\lambda_i) = \left[P_{2001}(\lambda_i)\right]^2 - a_{2002}$$

vuol dire che $P_{2001}(\lambda_i)$ deve essere una costante per tutti: λ_i.

Rinunciamo: Voglio ~~dopo~~ riuscire a trovare $a_1, \dots, a_{k+1}$ t.c. $P_k(\lambda_i) = \text{cost}$ per $i = 1 \dots k+1$

Procediamo per induzione:

- $\boxed{k=1}$ deve valere $P_1(z) = z - a_1$

$$(\lambda_1 - a_1)^2 = (\lambda_2 - a_1)^2$$

devono essere uno l'opposto dell'altro

$$a_1 = \frac{\lambda_1 + \lambda_2}{2}$$

- Passo induttivo $\boxed{k \Rightarrow k+1}$

Ho già scelto $a_1 \dots a_k$ che funzionano, cioè tali che $P_k(\lambda_i) = \text{cost}$ per $i = 1 \dots k$.

Devo controllare il $k+1$-esimo

$$P_{k+1}(\lambda_i) = P_k(\lambda_i)^2 - a_{k+1}$$

per $i = 1, \dots, k$ $P_k(\lambda_i) = \text{cost}$.

$$P_{k+1}(\lambda_{k+2})^2 = P_{k+1}(\lambda_1)^2$$

$$\left(P_k(\lambda_{k+2})^2 - a_{k+1}\right)^2 \stackrel{?}{=} \left(P_k(\lambda_1)^2 - a_{k+1}\right)^2$$

Di nuovo devono essere opposti:

$$P_k(\lambda_{k+2})^2 - a_{k+1} = a_{k+1} - P_k(\lambda_1)^2$$

$$\boxed{a_{k+1} = \frac{P_k(\lambda_{k+2})^2 + P_k(\lambda_1)^2}{2}}$$

□