SENIOR 2011 - ALGEBRA 1 (Basic)

Titolo nota 06/09/2011

NUMERI COMPLESSI $\quad \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$$\mathbb{C} = \{ a+bi : a \in \mathbb{R}, b \in \mathbb{R} \} \qquad i^2 = -1$$

$z = a+bi \in \mathbb{C}$, allora $\quad a = Re(z) \quad b = Im(z)$

Piano di Gauss: normale piano dove identifico $z = a+bi$ con il p.to di coordinate (a,b)

$z \in \mathbb{R} \iff Im(z) = 0 \iff$ sta sull'asse x del piano di Gauss

Operazioni tra numeri complessi $\quad z = a+bi \qquad w = c+di$

$$z \pm w = (a+bi) \pm (c+di) = (a \pm c) + (b \pm d)\, i$$

$$z \cdot w = (a+bi)\cdot(c+di) = ac + adi + bci + db\boxed{i^2}^{=-1}$$
$$= (ac-db) + (ad+bc)i$$

$$\frac{w}{z} = \underbrace{\frac{c+di}{a+bi} \cdot \frac{a-bi}{a-bi}}_{\frac{a^2-(bi)^2}{a^2+b^2}} = \frac{ac - cbi + adi - dbi^2}{a^2+b^2} =$$

$$= \underbrace{\boxed{\frac{ac+bd}{a^2+b^2}}}_{Re\left(\frac{w}{z}\right)} + \underbrace{\boxed{\frac{ad-cb}{a^2+b^2}}}_{Im\left(\frac{w}{z}\right)}\, i$$

Oss. $\frac{w}{z}$ esiste sempre purché $z \neq 0 \quad (z = 0 + 0 \cdot i)$

Coniugato di z $\quad$ Se $z = a+bi$, allora $\bar{z} = a-bi$ (simmetrico di z rispetto all'asse x)

Modulo di z $\quad$ Se $z = a+bi$, allora $|z| = \sqrt{a^2+b^2}$

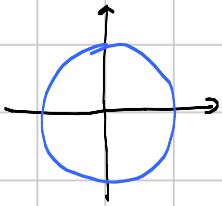
Esercizi $\quad z\cdot\bar{z} = (a+bi)(a-bi) = a^2+b^2 = |z|^2$

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2} \qquad \frac{1}{a+bi} = \frac{1}{a+bi}\,\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$$

$$\overline{z\pm w} = \bar{z}\pm\bar{w}, \quad \overline{z\cdot w} = \bar{z}\cdot\bar{w}, \quad \overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$$

Quali sono tutti i complessi z t.c. $\frac{1}{z} = \bar{z}$?

$\Leftrightarrow \ |z| = 1 \ \Leftrightarrow$



$$|z\cdot w| = |z|\cdot|w|$$

Dim. Faccio i quadrati $\quad |z\cdot w|^2 = |z|^2\cdot|w|^2 \qquad z = a+bi$

$w = c+di$

$$(ac-bd)^2 + (ad+bc)^2 \underset{\text{verifica}}{=} (a^2+b^2)(c^2+d^2)$$

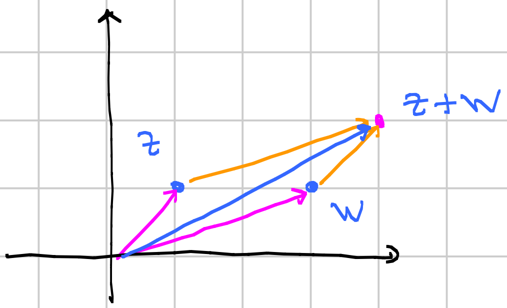
Corollario $\quad$ L'insieme degli interi del tipo a^2+b^2, con $a\in\mathbb{N}, b\in\mathbb{N}$ è chiuso rispetto alla moltiplicazione.

Esercizio $\quad$ L'insieme degli interi del tipo a^2+7b^2 con $a\in\mathbb{N}, b\in\mathbb{N}$ è chiuso rispetto alla moltiplicazione

Idea basic : $\quad (a^2+7b^2)\cdot(c^2+7d^2) = \dots = (\quad)^2 + 7(\quad)^2$

$$|a+\sqrt{7}bi|^2\cdot|c+\sqrt{7}di|^2 = |(ac-7bd)+\sqrt{7}(ad+bc)i|^2$$

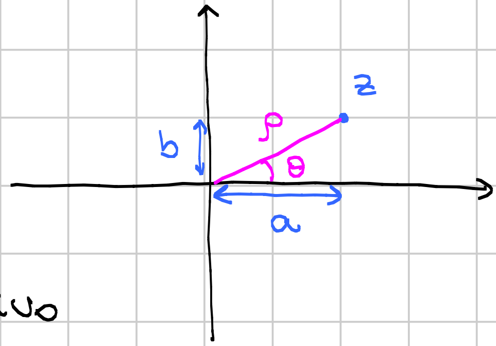
Nel piano di Gauss si vedono bene somma e diff. con la regola del parallelogramma



$$|z\pm w| \underset{\text{disuguaglianza triangolare}}{\leq} |z|+|w|$$

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}$$

Forma trigonometrica $\quad z = a + bi$



Per individuare z uso
- distanza ρ dall'origine $(\rho \geq 0)$
- angolo θ con il semiasse reale positivo

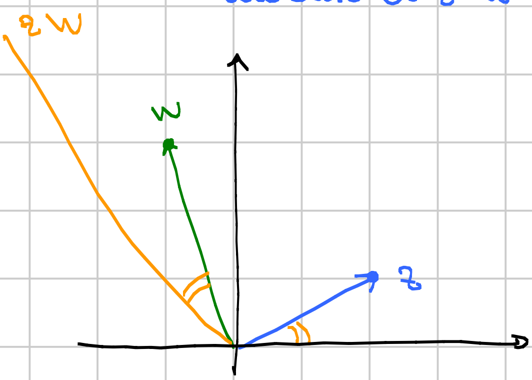
Relazioni ovvie: $\boxed{\rho = |z| = \sqrt{a^2+b^2}}$ $\qquad \boxed{a = \rho\cos\theta \qquad b = \rho\sin\theta}$

$$z = \rho\cos\theta + \rho\sin\theta\, i = \rho(\cos\theta + i\sin\theta)$$

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

$$z \cdot w = \rho r\left(\cos\theta\cos\varphi - \sin\theta\sin\varphi + i(\cos\theta\sin\varphi + \sin\theta\cos\varphi)\right)$$
$$= \boxed{\rho r}\left(\cos\boxed{(\theta+\varphi)} + i\sin\boxed{(\theta+\varphi)}\right)$$

modulo di $z \cdot w$ $\qquad$ angolo (o argomento) del prodotto



Analogamente

$$\frac{z}{w} = \frac{\rho}{r}\left(\cos(\theta-\varphi) + i\sin(\theta-\varphi)\right)$$

— o — o —

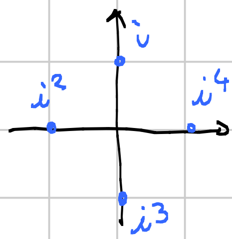
Potenza n-esima di un numero complesso

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

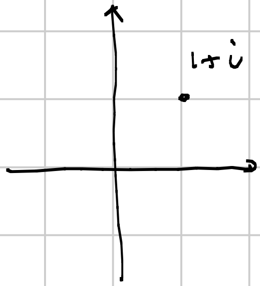
Dim.: induzione su n a partire dalla formula del prodotto.

Esercizio $\qquad (\cos\theta + i\sin\theta)^5 = \cos(5\theta) + i\sin(5\theta)$

sviluppare con il binomio di Newton



Esercizio Calcolare $(1+i)^{2011}$. Passo in forma trigonometrica



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

$$(1+i)^{2011} = \left(\sqrt{2}\right)^{2011}\left(\cos\frac{2011}{4}\pi + i\sin\frac{2011}{4}\pi\right)$$

$$= 2^{1005}\underbrace{\boxed{\sqrt{2}\left(\cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi\right)}}_{-1+i} = -2^{1005} + 2^{1005}\,i$$

— o — o —

Forma esponenziale: ρ e θ come nella trigonometrica

$$z = \boxed{\rho}\cdot e^{i\boxed{\theta}} \qquad w = r\cdot e^{i\varphi}$$

$$z\cdot w = \rho\cdot e^{i\theta}\cdot r\cdot e^{i\varphi} = (\rho\cdot r)\cdot e^{i(\theta+\varphi)}$$

$$\frac{1}{z} = \left(\rho\cdot e^{i\theta}\right)^{-1} = \rho^{-1}\cdot e^{-i\theta}$$

Occhio: scrivere -1 in forma esponenziale: $-1 = 1\cdot e^{i\pi}$

scrivere $-i$ in forma esponenziale: $-i = 1\cdot e^{\frac{3\pi}{2}i}$

— o — o —

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

— o — o —

Esercizio Trovare formula per $\cos x + \cos(2x) + \dots + \cos(nx) = C$

Considero anche $i\left(\sin x + \sin(2x) + \dots + \sin(nx)\right) = iS$

$$C + iS = (\cos x + i\sin x) + (\cos(2x) + i\sin(2x)) + \dots$$
$$= z + z^2 + z^3 + \dots + z^n = z\left(1 + z + z^2 + \dots + z^{n-1}\right)$$

Posto $z = \cos x + i\sin x$
$$= z\,\frac{z^n - 1}{z - 1}$$

$$C + iS = \boxed{(\cos x + i \sin x)\ \frac{\cos(nx) + i\sin(nx) - 1}{\cos x + i \sin x - 1}}$$

$$C = \text{Re}\ (\text{Mostro})$$

— o — o —

Radice n-esima di un numero complesso

Dato $a \in \mathbb{C}$, trovare tutti gli $z \in \mathbb{C}$ t.c. $z^n = a$ ($n \geq 2$ intero)

Banale: se $a = 0$, allora l'unica soluzione è $z = 0$.

Teorema Se $a \neq 0$, allora esistono esattamente n numeri complessi z t.c. $z^n = a$.
Inoltre nel piano di Gauss sono i vertici di un poligono regolare di n lati con centro nell'origine.

Dim. Pongo $a = \rho(\cos\theta + i \sin\theta)$ e cerco $z = r(\cos\varphi + i\sin\varphi)$
Impongo

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

Quindi

$$\begin{cases} r^n = \rho & \text{devono avere lo stesso modulo} \\ n\varphi = \theta + 2k\pi & k \in \mathbb{Z}, \text{ stesso angolo a meno di multipli di } 2\pi \end{cases}$$

$r = \sqrt[n]{\rho}$ ← radice n-esima di un numero reale ≥ 0
(che è un unico numero reale ≥ 0)

$\varphi = \frac{\theta}{n} + \frac{2k\pi}{n}$ ← ottengo n oggetti distinti se do a k i valori $k = 0, 1, 2, \dots, n-1$. Poi si ripete.

Esempio Calcolare le radici cubiche di $-8i$

Soluzione con la formula: $-8i$ ha $\rho = 8$ e $\theta = \frac{3\pi}{2}$

Quindi $r = \sqrt[3]{8} = 2$ $\qquad \theta = \left(\frac{3\pi}{2}\right)\frac{1}{3} + \frac{2k\pi}{3}$

$$= \frac{\pi}{2} + \frac{2k\pi}{3}$$

$k=0 \quad \frac{\pi}{2}$

$k=1 \quad \frac{7\pi}{6}$

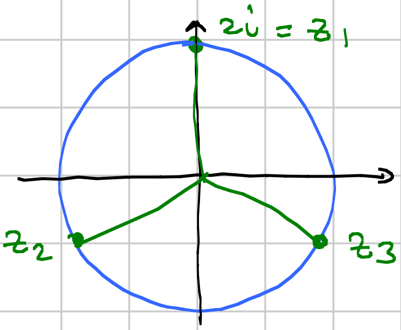
$k=2 \quad \frac{11\pi}{6}$

Quindi le 3 soluzioni sono $\quad z_1 = 2\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right) = 2i$

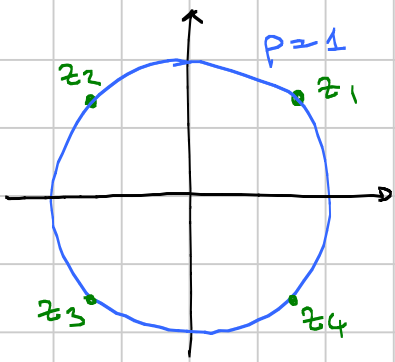
$$z_2 = 2\left(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}\right) = -\sqrt{3} - i$$

$$z_3 = 2\left(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}\right) = \sqrt{3} - i$$

Alternativa: $z^3 = -8i$. Una soluzione è $z = 2i$. Le altre due devono completare il triangolo equilatero



<u>Esercizio</u> $\quad z^4 = -1$



$$z_{1,2,3,4} = \frac{\sqrt{2}}{2}(\pm 1 \pm i)$$

$\boxed{\text{POLINOMI}}$ $\quad p(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$

a_i = coeff. del polinomio $(\in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$
Si intende che $a_k \neq 0$ e $k = \deg(p(x))$ è il grado del polinomio.

Funzione polinomiale: ad ogni x associo $p(x)$

<u>Principio di identità dei polinomi</u>. Se due polinomi coincidono per ogni valore di x, allora i due polinomi hanno gli stessi coefficienti.
(In realtà, per polinomi di grado $\leq k$, basta sapere che coincidono per $k+1$ valori di x).

<u>Possibilità di assegnare $(k+1)$ valori</u>.
Siano $x_0, x_1, \dots, x_k$ $(k+1)$ numeri reali distinti
Siano $a_0, a_1, \dots, a_k$ " " " qualunque.
Allora esiste un <u>unico</u> polinomio $p(x)$, a coeff. reali, di grado $\leq k$, tale che

$$p(x_i) = a_i \quad \text{per ogni } i = 0, 1, \dots, k.$$

$\boxed{\text{DIM 1}}$ Impongo le condizioni $\quad p(x) = b_0 + b_1 x + \dots + b_k x^k$.
Le incognite sono i coeff. $b_0, b_1, \dots, b_k$.

$$\begin{cases} b_0 + x_0 b_1 + \dots + x_0^k b_k = a_0 \\ b_0 + x_1 b_1 + \dots + x_1^k b_k = a_1 \\ \dots \\ b_0 + x_k b_1 + \dots + x_k^k b_k = a_k \end{cases}$$

Sistema lineare di $k+1$ equazioni in $k+1$ incognite

Non sarebbe obbligato ad avere soluzioni, ma in questo caso lo ha perché la tabella (matrice) dei coefficienti è

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^k \\ 1 & x_1 & x_1^2 & \cdots & x_1^k \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^k \end{pmatrix}$$

WANDERMONDE

$\boxed{\text{DIM 2}}$ "DIVIDE ET IMPERA". Risolvo il caso in cui tutti gli a_i sono 0, tranne uno che è uguale ad 1.

WLOG: $a_0 = 1$, $a_1 = \ldots = a_k = 0$

Sto chiedendo $\underbrace{p(x_1) = p(x_2) = \ldots = p(x_k) = 0}_{\alpha(x-x_1)(x-x_2)\cdot\ldots\cdot(x-x_k)}$ e $p(x_0) = 1$

↑ scelgo α in modo da sistemare $p(x_0) = 1$,

cioè $$\alpha = \frac{1}{(x_0-x_1)(x_0-x_2)\cdot\ldots\cdot(x_0-x_k)}$$

Come si risolve il caso generale? Considero

$p_0(x)$ la soluzione con $a_0 = 1$ e gli altri nulli

$\vdots$

$p_i(x)$ la soluzione con $a_i = 1$ e gli altri nulli.

Allora

$$a_0 p_0(x) + a_1 p_1(x) + \ldots + a_k p_k(x) = p(x)$$

Il polinomio $p(x)$ così costruito vale a_i in x_i per ogni $i = 0, 1, \ldots, k$ (ogni volta si annullano tutti gli addendi tranne 1)

— o — o —

<u>Oss.</u> La possibilità di assegnare $(k+1)$ valori vale su $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, ma <u>non</u> vale su $\mathbb{Z}$.

— o — o —

<u>Divisione di polinomi</u> Dati $A(x)$ e $B(x)$ esistono unici $Q(x)$ ed $R(x)$ t.c.

$$\boxed{A(x) = B(x) \cdot Q(x) + R(x)} \qquad \boxed{\deg(R(x)) < \deg(B(x))}$$

<u>Dim</u>: induzione sul grado di $A(x)$.

<u>Oss.</u> La divisione vale a coeff. in $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Vale su $\mathbb{Z}$ se $B(x)$ è MONICO (coeff. grado max = 1)

Oss. C'è un BEZOUT sui polinomi.

Teorema di RUFFINI Se divido un certo $A(x)$ per $B(x) = (x-\alpha)$, allora $R(x)$ ha grado 0, quindi $R(x)$ è un numero, e questo numero è $A(\alpha)$.

$$\boxed{A(x) = (x-\alpha)\,Q(x) + A(\alpha)}$$

Corollario Se $A(\alpha)=0$, cioè se α è una radice di $A(x)$, allora $A(x)$ è divisibile per $(x-\alpha)$, cioè resto $=0$.

Corollario Un polinomio di grado d può avere al max d radici.

Dim. Formalmente è induzione su d. Praticamente: se avesse $d+1$ radici avrebbe $d+1$ fattori ed il grado sarebbe superiore.

Sia $P(x)$ un polinomio, e sia α una radice, cioè $P(\alpha)=0$.
Si dice molteplicità di α il più grande esponente k t.c. $(x-\alpha)^k$ divide $P(x)$.

Detto bene: un pol. di grado d ha al più d radici, se contate con molteplicità.

Back to principio identità polinomi. Siano $P(x)$ e $Q(x)$ di grado $\leq k$. Supponiamo che coincidano in $x_0, x_1, \dots, x_k$ distinti. Allora $P(x)-Q(x)$ avrebbe $(k+1)$ radici, il che è impossibile a meno che non sia il polinomio nullo.

<u>Teorema fondamentale dell'algebra</u> Un polinomio di grado d a coeff. complessi ha esattamente d radici complesse, se contate con molteplicità.

<u>Oss.</u> Basta dimostrare che ne ha almeno una, poi è fatta.

<u>Corollario</u> Ogni polinomio a coeff. complessi si scrive come prodotto di fattori di 1° grado, eventualmente ripetuti

$$p(x) = \alpha\,(x-x_1)\cdot\ldots\cdot(x-x_d)$$

$x_1, \ldots, x_d$ sono le radici complesse, ripetute con molteplicità

—o—o—

<u>Polinomi a coeff. reali.</u> Un pol. a coeff. reali si può sempre scrivere come prodotto di pol. a coeff. reali di grado 1 o 2 (e i fattori di grado 2 hanno $\Delta < 0$, cioè non si scompongono)

<u>Corollario</u> Se il grado è dispari, almeno un fattore è di grado 1, quindi c'è almeno 1 radice reale.

<u>Idee della dim.</u> ① Scrivo sui complessi come prod. di fattori di grado 1. I fattori corrispondenti a radici reali vanno già bene.

② Se $\alpha \in \mathbb{C}$ è radice di $P(x)$ a coeff. reali, allora $\bar{\alpha}$ è anche lei radice con la stessa molteplicità. Infatti $P(\bar{\alpha}) = \overline{P(\alpha)}$.

③ Se tra i fattori c'è $\underbrace{x-a-bi}_{x-\alpha}$, ci sarà anche $\underbrace{x-a+bi}_{x-\bar{\alpha}}$

e $(x-a-bi)(x-a+bi) = x^2 - 2ax + (a^2+b^2)$ REALE !!!

—o—o—

<u>Oss.</u> Un polinomio a coeff. reali ha, per x grandi o molto negativi, lo stesso segno del termine di grado max.

POLINOMI A COEFF. INTERI

Esempio $p(x)$ a coeff. interi. So che $p(1)=3$, $p(3)=7$. Cosa posso dire di $p(9)$?

Se $p(1)=3$, allora $p(x)-3$ ha $x=1$ come radice, quindi

$$p(x)-3=(x-1)\,q(x)$$

cioè

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

Impongo $p(3)=7$:

$$7=3+2\,q(3) \Rightarrow q(3)=2$$

Ma allora, come prima, $q(x)=2+(x-3)\,r(x)$, quindi

$$\begin{aligned} p(x) &= 3+(x-1)\{2+(x-3)\,r(x)\} \\ &= 3+2(x-1)+(x-1)(x-3)\,r(x) \\ &= 1+2x+(x-1)(x-3)\,r(x) \end{aligned}$$

Mettendo $x=9$ trovo $p(9)=19+48\,\boxed{r(9)}$ (intero), quindi $p(9)\equiv 19 \pmod{48}$

Può essere qualunque cosa perché $r(9)$ può essere un qualunque intero.

— o — o —

Sapendo che $p(3)=2011$, cosa posso dire di $p(20)$?

$$p(x)=2011+(x-3)\,q(x) \Rightarrow p(20)=2011+17\,q(20)$$

$$\Rightarrow p(20)\equiv 2011 \pmod{17}$$

— o — o —

Fatto generale Se $P(x)$ ha coeff. interi, allora $(a-b)\mid(P(a)-P(b))$

Dim. Dato $P(a)$ ho che $P(x)=P(a)+(x-a)\,Q(x)$.
Sostituisco $x=b$ e ho che $P(b)=P(a)+(b-a)\,Q(b)$
Porto $P(a)$ dall'altra parte.

Esercizio $P(x)$ ha coeff. interi. $P(P(3)) = 3$, $P(0) = 2011$

Pongo $P(3) = a$, quindi $P(a) = 3$, quindi

$$P(x) = 3 + a - x + (x-3)(x-a)\,Q(x)$$

Metto $x = 0$

$$2011 = 3 + a + 3a\,Q(x)$$

$$2008 = a\,(1 + 3Q(x))$$

Quindi $a \mid 2008$, e $a \equiv 1 \pmod 3$

— o — o —

$P(1) = 1$, $P(2) = 8$, $P(3) = 27$

$$P(x) = x^3 + (x-1)(x-2)(x-3)\,Q(x)$$

— o — o —

$\boxed{\text{RELAZIONI RADICI - COEFFICIENTI}}$

$$P(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1 x + a_0$$

$P(x)$ ha k radici complesse $r_1, \dots, r_k$ contate con molteplicità.
Allora

$$-a_{k-1} = r_1 + r_2 + \dots + r_k = \sum_{1 \le i \le k} r_i$$

$$a_{k-2} = \sum_{1 \le i < j \le k} r_i r_j \quad \text{(somma dei prodotti a 2 a 2)}$$

$$-a_{k-3} = \sum_{1 \le i < j < l \le k} r_i r_j r_l \quad \text{(prodotti a 3 a 3)}$$

e così via fino a

$$(-1)^k a_0 = r_1 \cdot r_2 \cdot \ldots \cdot r_k$$

Se non è monico, basta dividere per il coeff. di x^k e diventa monico con le stesse radici.

Esempio 1 $x^3 - 3x^2 + 7x + 5$ a, b, c radici complesse

Allora

$$S = a+b+c = 3$$
$$Q = ab+bc+ca = 7$$
$$P = abc = -5$$

Quanto fa $a^2+b^2+c^2 = (a+b+c)^2 - 2(ab+bc+ca)$

$$= 3^2 - 2\cdot 7 = -5$$

$\Rightarrow$ le radici sono 1 reale e 2 complesse coniugate

Teorema funzioni simmetriche Ogni polinomio simmetrico nelle variabili a, b, c si scrive come polinomio nelle variabili S, Q, P. Stessa cosa vale in k variabili usando le k funzioni simmetriche elementari (cioè quelle coinvolte nelle relazioni radici-coefficienti).

Esempio $a^2b^2+b^2c^2+c^2a^2 = (ab+bc+ca)^2 - 2(a^2bc+ab^2c+abc^2)$

$$= Q^2 - 2SP.$$

— o —

Dim. relazioni: segue immediatamente dalla fattorizzazione

$$(x-r_1)(x-r_2)(x-r_3) = x^3 - x^2(r_1+r_2+r_3) + x(r_1r_2+r_2r_3+r_3r_1) - r_1r_2r_3$$

— o — o —

Fatti generali $P(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$

$$r_1^2 + r_2^2 + \dots + r_k^2 = [a_{k-1}]^2 - 2a_{k-2}$$

$$\frac{1}{r_1} + \frac{1}{r_2} + \dots + \frac{1}{r_k} = -\frac{a_1}{a_0}$$

$$P\left(\frac{1}{x}\right) = \frac{1}{x^k} + a_{k-1}\frac{1}{x^{k-1}} + \dots = \frac{1 + a_{k-1}x + a_{k-2}x^2 + \dots + a_1x^{k-1} + a_0x^k}{x^k}$$

Ora $\frac{1}{r_1}, \frac{1}{r_2}, \dots, \frac{1}{r_k}$ sono le radici del numeratore.

— o — o —

Radici razionali $P(x) = a_k x^k + \dots + a_0$ a coeff. interi

Se $P(x)$ ha una radice razionale del tipo $\boxed{\frac{m}{n}}$, allora $m \mid a_0$ e $n \mid a_k$

con $MCD(m,n)=1$

Corollario Se è monico allora le radici razionali sono per forza intere.

Dim. Brutale sostituzione

$$a_k \frac{m^k}{n^k} + a_{k-1} \frac{m^{k-1}}{n^{k-1}} + \dots + a_1 \frac{m}{n} + a_0 = 0$$

$$\frac{a_k m^k + a_{k-1} n m^{k-1} + \dots + a_1 n^{k-1} m + a_0 n^k}{n^k} = 0$$

Tutti i termini al num, tranne il 1°, sono multipli di n, quindi anche $a_k m^k$ deve esserlo, quindi $n \mid a_k$ (non potendo dividere m)
Idem per l'ultimo termine.

— o — o —

$\boxed{\text{IMO } 1988-4}$ Disequazione

$$\frac{1}{x-1} + \frac{2}{x-2} + \dots + \frac{70}{x-70} \geq \frac{5}{4}$$

L'insieme delle soluzioni è unione di intervalli di ampiezza complessiva pari a 1988.

Dim. $P(x) = (x-1) \cdot \ldots \cdot (x-70)$ $\qquad P_i(x) = \frac{P(x)}{x-i}$

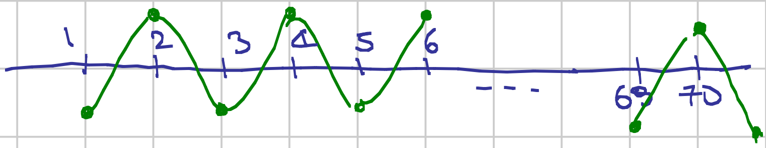
Disequazione $\Leftrightarrow$ $$\frac{4[P_1(x) + 2P_2(x) + \dots + 70 P_{70}(x)] - 5P(x)}{4P(x)} \geq 0$$

Il numeratore ha deg $= 70$ con termine di grado max $= -5x^{70}$, quindi è negativo per x molto grandi e molto negativi
Inoltre

Num $(1) = 4P_1(1) =$ neg.

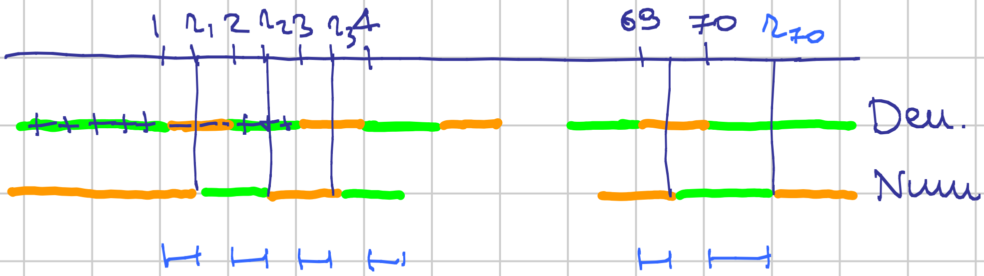
$Num(2) = 8 P_2(2) = $ pos.

$Num(3) = 12 P_3(3) = $ neg.



Quindi il numeratore ha 70 radici, tutte reali,

$r_1 < r_2 < \dots < r_{70}$ e $i < r_i < i+1$ per ogni $i = 1, \dots, 69$



La disequazione ha come soluzione l'unione dei 70 intervalli $[i, r_i]$

quindi la lunghezza totale è $L = \sum_{i=1}^{70} (r_i - i) =$

$$= \sum_{i=1}^{70} r_i - (1 + 2 + \dots + 70)$$

Per calcolare $\sum r_i$, mi servono i coeff. di x^{70} e x^{69} nel num.

$$Num = -5x^{70} + \underbrace{4x^{69}(1+2+\dots+70)}_{\text{viene fuori dai } P_i(x)} + \underbrace{5x^{69}(1+2+\dots+70)}_{\text{viene fuori da } P(x)}$$

$$\sum_{i=1}^{70} r_i = \frac{9}{5}(1+2+\dots+70)$$

$$L = \left(\frac{9}{5} - 1\right)(1+2+\dots+70) = \frac{4}{5} \cdot 71 \cdot 35 = 1988 \quad !!!$$

— o — o —

$\boxed{\text{IMO 1974-6}}$ $P(x)$ a coeff. interi di grado d.

Allora $[P(x)]^2 = 1$ ha al max $d+2$ soluzioni distinte intere

$P(x) = 1$ oppure $P(x) = -1$ Quindi le sol. sono al max $2d$

Quindi ok banalmente per $d = 1$ e per $d = 2$.

Lemma Se esistono 4 interi distinti tali che
$$P(a) = P(b) = P(c) = P(d) = 1$$
allora $P(x) = -1$ non ha soluzioni intere

Dim. Pongo $Q(x) = P(x) - 1$. Allora
$$P(x) - 1 = Q(x) = (x-a)(x-b)(x-c)(x-d)R(x)$$
Supponiamo che $P(e) = -1$. Allora ponendo $x = e$

$$-2 = \underbrace{(e-a)(e-b)}_{\text{potrebbero essere } \pm 1}(e-c)(e-d)\underbrace{R(e)}_{\text{potrebbe essere } 1}$$

-2 non può essere divisibile per il prodotto di 4 interi distinti

Dato il lemma si chiude il problema. Se $d \geq 4$ e avessi più di $d+2$ soluzioni, ne avrei almeno 7, quindi almeno 4 p.ti in cui vale $+1$ o vale -1. Quindi vale addirittura con d invece di $d+2$. Il caso $d = 3$ si fa a mano con la fattorizzazione.

— o — o —

Lemma $P(x)$ a coeff. interi. Considero
$$P^{(k)}(x) = P(P(P(\ldots))) \quad k \text{ volte}$$

Sia x intero. Allora $P^{(k)}(x) = x \Rightarrow P(P(x)) = x$.
(se si torna indietro in k passaggi, allora o si è stati fermi sempre, o si torna indietro ogni 2 passaggi).

Dim. Si usa ripetutamente $a-b \mid P(a) - P(b)$

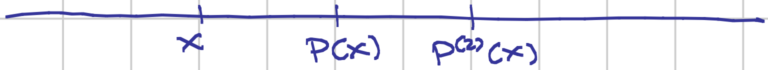
$$a-b \mid P(a) - P(b) \mid P(P(a)) - P(P(b)) \mid \ldots$$

La uso con $a = P(x)$ e $b = x$

$P(x) - x \mid P(P(x)) - P(x) \mid \dots \mid \underset{P(x)}{\underset{\shortparallel}{P^{(k+1)}(x)}} - \underset{x}{\underset{\shortparallel}{P^{(k)}(x)}}$

Quindi tutte le differenze sono uguali a meno del segno

$P^{(2)}(x)$ può essere x (e siamo a posto) o dall'altra parte.
Per assurdo sia dall'altra parte



Ogni volta faccio avanti o indietro della stessa quantità e dopo k passaggi torno in x

Se voglio tornare ad x devo fare un passo da $P(x)$ ad x. La regola di passaggio è sempre la stessa, quindi da $P(x)$ non si può andare una volta avanti e una indietro.

(From IMO 2006-5: Se $P(x)$ ha grado d, allora $P^{(k)}(x) = x$ ha al più d radici)
Sui complessi avrebbe d^k soluzioni, perchè $\deg(P^{(k)}) = d^k$
Grazie al lemma ci si riduce a d^2 soluzioni.

— o — o —