A17 - S23

Sam

Note Title 03/09/2023

Fattorizzare su $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ i polinomi

$$x^4+1 \qquad x^4+x^2+1$$

Sol: Mi basta capire la fatt. su $\mathbb{C}$, poi quelle su $\mathbb{R}$ e su $\mathbb{Q}$ si fanno "mettendo assieme" fattori

su $\mathbb{C}$:

$$x^4+1+2x^2-2x^2 = (x^2+1)^2-2x^2 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$$

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

su $\mathbb{R}$

$$(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) \longrightarrow \Delta = 2-4=-2 < 0$$

$$(x^2+x+1)(x^2-x+1) \longrightarrow \Delta = 1-4=-3 < 0$$

$$\to \left(x-\frac{-\sqrt{2}+i\sqrt{2}}{2}\right)\left(x-\frac{-\sqrt{2}-i\sqrt{2}}{2}\right)\left(x-\frac{\sqrt{2}+i\sqrt{2}}{2}\right)\left(x-\frac{\sqrt{2}-i\sqrt{2}}{2}\right)$$

$$\to \left(x-\frac{-1+i\sqrt{3}}{2}\right)\left(x-\frac{-1-i\sqrt{3}}{2}\right)\left(x-\frac{1+i\sqrt{3}}{2}\right)\left(x-\frac{1-i\sqrt{3}}{2}\right)$$

su $\mathbb{C}$

Oss: $(x-\lambda)(x-\bar{\lambda}) \in \mathbb{R}[x] \quad \forall \lambda \in \mathbb{C}$

Poiché non hanno radici razionali, l'unica possibile fatt. su $\mathbb{Q}$ è in 2 polinomi di grado 2, ma allora deve coincidere con quella su $\mathbb{R}$

$\Rightarrow$ x^4+1 è irriducibile su $\mathbb{Q}$

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

— o —

Polinomi

$A, +, \cdot$ si dice ANELLO se valgono le "solite" regole di $+, \cdot$
se ogni elemento ha un (unico) opposto
se esiste lo 0.

Se per ogni $a \in A$, $a \neq 0$ esiste l'inverso, allora A si dice CAMPO

Es: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/_{m}\mathbb{Z}$ sono anelli

$\mathbb{Z}[x]$ è un anello

In generale: se A è un anello, $A[x]$ è un anello.

$$A[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_n, \dots, a_0 \in A \}$$

Oss: $A[x,y] = A[x][y]$

Oss: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/_{p}\mathbb{Z}$ p primo sono campi

Es: $p(x) = x^3 - 4$ è irriducibile su $\mathbb{Q}$
perché lo è mod 7 (cioè lo è in $\mathbb{Z}/_{7\mathbb{Z}}[x]$)

Divisione Euclidea: Se $\mathbb{K}$ è un campo, dati $a(x), b(x) \in \mathbb{K}[x]$
allora esistono $q(x), r(x) \in \mathbb{K}[x]$ tali che
1) $a(x) = b(x) \cdot q(x) + r(x)$
2) $\deg r(x) < \deg b(x)$

Oss: Sempre possibile (a coeff in A) se $b(x)$ è monico.
Controesempio in $\mathbb{Z}$: $x^2 : 2x = ??$

Es: $P(x,y) \in \mathbb{R}[x,y]$ t.c. $P(\cos\theta, \sin\theta) = 0 \quad \forall \theta \in [0, \pi]$

Sol: Tutti i $P(x,y)$ multipli di x^2+y^2-1.
Penso $P(x,y)$ come polinomio in x a coeff. polinomi in y.
e allo stesso modo per x^2+y^2-1, che è monico.
$\Rightarrow$ posso fare la divisione euclidea

$$P(x,y) = (x^2+y^2-1)\, Q(x,y) + R(x,y)$$
dove $R(x,y) = x \cdot A(y) + B(y)$ $\quad (\deg_x R(x,y) < \deg_x (x^2+y^2-1))$

$$0 = P(\cos\theta, \sin\theta) = \cos\theta \cdot A(\sin\theta) + B(\sin\theta) \qquad \forall \theta \in [0, \pi]$$

$$0 = P(\cos(\pi-\theta), \sin(\pi-\theta)) = -\cos\theta \cdot A(\sin\theta) + B(\sin\theta)$$

$$\Rightarrow \forall \theta \in [0, \tfrac{\pi}{2}) \quad \begin{cases} A(\sin\theta) = 0 \\ B(\sin\theta) = 0 \end{cases} \Rightarrow \begin{array}{l} A(x) = 0 \\ B(x) = 0 \end{array} \quad \forall x \in [0,1)$$

$\Rightarrow A, B$ sono il polinomio nullo. $\Rightarrow P(x,y) = (x^2+y^2-1)\,Q(x,y)$ $\square$

Es x casa: $P(n, n^2) = 0 \ \forall n \in \mathbb{N} \Rightarrow y - x^2 \mid P(x,y)$

Cor: $x - y \mid \underbrace{P(x) - P(y)}_{\in \mathbb{A}[x,y] = \mathbb{A}[y][x]}$ $\leftarrow$ il suo t.n. è $P(0) - P(y)$

Teo di Ruffini: $P(x) \in \mathbb{A}[x]$, $a \in \mathbb{A}$ allora il resto della divisione di $p(x)$ per $x - a$ è $p(a)$.

dim: $x - a$ è monico $\Rightarrow$ (div. euc.) $p(x) = (x-a)\,q(x) + r(x)$ con $\deg r(x) < \deg x-a \Rightarrow r(x)$ è costante

$p(x) = (x-a)\,q(x) + r$. Sostituendo $x = a$ ho la tesi. $\square$

Oss: Il resto della div. di $p(x) - p(y)$ per $x - y$ è $p(y) - p(y) \equiv 0$.
$\Rightarrow x - y \mid p(x) - p(y)$.

Cor: $p(x)$ di grado n ha al più n radici.

Controesempio: $x^2 - 1$ in $\mathbb{Z}/8\mathbb{Z}[x]$ ha 4 radici

$(x-2)(x-3)$ in $\mathbb{Z}/6\mathbb{Z}[x]$

Cor vero: Se in $\mathbb{A}$ vale la legge di annullamento del prodotto (cioè se $ab = 0$ implica $a = 0$ oppure $b = 0$) allora un pol di grado n ha al più n radici.

dim: siano $a_1, \dots, a_{n+1}$ radici distinte
allora per Ruffini, posso scrivere

$p(x) = \alpha(x - a_1) \cdots (x - a_n)$ ma sostituendo $x = a_{n+1}$ dovrei avere 0.

$\square$

Divisione Euclidea $\Longrightarrow$ ⊙ MCD

⊙ Bezout (dati $a(x), b(x) \in \mathbb{K}[x]$, esistono $m(x), n(x) \in \mathbb{K}[x]$ tali che $MCD(a(x), b(x)) = m(x) \cdot a(x) + n(x) \cdot b(x)$)

⊙ Congruenze

ES: $a+b+c \mid a^3+b^3+c^3-3abc$

Sol: Guardo mod $a+b+c$ $\Rightarrow$ sostituisco $a=-b-c$

e faccio il conto $-(b+c)^3+b^3+c^3+3b^2c+3bc^2=0$

Interpolazione di Lagrange

Dati $b_1, \dots, b_{n+1}$, $c_1, \dots, c_{n+1} \in \mathbb{R}$ Voglio $p(x) \in \mathbb{R}[x]$ con $\deg p(x) \le n$ tale che $p(b_j) = c_j \quad \forall j = 1, \dots, n+1$

TCR: Voglio $p(x) \equiv c_j \mod (x-b_j) \quad j = 1, \dots, n+1$.

Per costruire una sol, trovo le sol. "fondamentali"

$$\begin{cases} q_j(x) \equiv 0 \mod x-b_k & k \neq j \\ q_j(x) \equiv 1 \mod x-b_j \end{cases} \longrightarrow q_j(x) = A_j \prod_{k \neq j} (x-b_k) \longrightarrow A_j = \frac{1}{\prod_{k\neq j}(b_j-b_k)}$$

$$p(x) = \sum_{j=1}^{n+1} c_j q_j(x)$$

$$\Rightarrow p(x) = \sum_{j=1}^{n+1} c_j \prod_{k \neq j} \frac{(x-b_k)}{(b_j-b_k)}$$

2 Fattorizzazione

Teo Fond dell'Algebra: $p(x) \in \mathbb{C}[x]$ di grado >0 ha almeno una radice $a \in \mathbb{C}$.

Fattori irriducibili

- in $\mathbb{C}$ sono della forma $x-a$ con $a \in \mathbb{C}$.
- in $\mathbb{R}$ sono della forma $x-a$ con $a \in \mathbb{R}$

  oppure $x^2+\alpha x+\beta$ con $\alpha^2-4\beta<0$
- in $\mathbb{Q}$ è un macello.

- in $\mathbb{Z}$ è "uguale" a $\mathbb{Q}$

Lemma di Gauss: Se $c(x) \in \mathbb{Z}[x]$ ed esistono $a(x), b(x) \in \mathbb{Q}[x]$ tali che $c(x) = a(x) \cdot b(x)$ allora $\exists\, q \in \mathbb{Q}$ t.c. $q\, a(x),\ \frac{1}{q} b(x) \in \mathbb{Z}[x]$.

Lemma del Lemma di Gauss: Se $p(x), q(x), r(x) \in \mathbb{Z}[x]$ tali che $p(x) = q(x) \cdot r(x)$ e se t è un numero primo che divide tutti i coeff. di $p(x)$ allora o t divide tutti i coeff di $q(x)$ o t divide tutti i coeff di $r(x)$.

dim: Considero i polinomi in $\mathbb{Z}/t\mathbb{Z}[x]$

$\boxed{\text{OCCHIO: } t \text{ è primo} \Rightarrow \mathbb{Z}/t\mathbb{Z} \text{ è un campo} \Rightarrow \text{vale l'annullamento del prodotto in } \mathbb{Z}/t\mathbb{Z}[x]}$

allora $p(x)$ è il pol. nullo

$\Rightarrow$ o $q(x)$ o $r(x)$ sono il pol nullo x l'annullamento del prodotto. □

Scrivo $a(x) = \frac{1}{A} \alpha(x)$ con $\alpha(x) \in \mathbb{Z}[x]$ $\quad A, B \in \mathbb{Z}$

$b(x) = \frac{1}{B} \beta(x)$ con $\beta(x) \in \mathbb{Z}[x]$

$\Rightarrow AB\, c(x) = \alpha(x)\beta(x)$

Se p è un primo con $p \mid AB$ allora p divide tutti i coeff di $\alpha(x)$ oppure tutti i coeff di $\beta(x)$.

$$\Rightarrow \frac{AB}{p} c(x) = \frac{\alpha(x)}{p} \beta(x) \quad \text{oppure} \quad \frac{AB}{p} c(x) = \alpha(x) \frac{\beta(x)}{p}$$

è ancora un'uguaglianza in $\mathbb{Z}[x]$.

Ripeto ottenendo $c(x) = \frac{\alpha(x)}{m} \cdot \frac{\beta(x)}{n}$ con $m \cdot n = AB$ e $\frac{\alpha}{m}(x), \frac{\beta(x)}{n} \in \mathbb{Z}[x]$

□.

Criterio di EISENSTEIN

$a(x) \in \mathbb{Z}[x]$ $\quad \deg p(x) = d \quad a_0 + a_1 x + \ldots + a_d x^d$

Se esiste p primo tale che $p \nmid a_d$, $p \mid a_1, \dots, p \mid a_{d-1}$, $p \mid a_0$, $p^2 \nmid a_0$ allora $a(x)$ è irriducibile in $\mathbb{Z}[x]$.

dim: Guardo $a(x)$ modulo p, cioè in $\mathbb{Z}/p\mathbb{Z}[x]$

$\Rightarrow a(x) = a_d x^d$ in $\mathbb{Z}/p\mathbb{Z}[x]$ $\Rightarrow$ se $a(x) = b(x) \cdot c(x)$ in $\mathbb{Z}[x]$ allora $b(x) = b_k x^k$, $c(x) = c_h x^h$ in $\mathbb{Z}/p\mathbb{Z}[x]$ con $k+h=d$

Allora in $\mathbb{Z}$: $a(x) = b(x) \cdot c(x) \to a_0 = b_0 \cdot c_0 \Rightarrow p^2 \mid a_0$ assurdo. $\square$

Es x casa: $p \mid a_i$ per $0 \le i < k$, $p \nmid a_k$, $p^2 \nmid a_0$

$\Rightarrow a(x)$ ha un fattore irriducibile di grado $\geq k$..

Es: $x^n + 5x^{n-1} + 3$ irriducibile in $\mathbb{Z}[x]$

Sol: Applico Eisenstein generalizzato con $k = n-1$ e $p=3$

$\Rightarrow$ c'è un fattore irrid. di grado $\geq n-1$.

se $x^n + 5x^{n-1} + 3 = A(x) \cdot (x-a)$ allora $a \in \{\pm 3, \pm 1\}$

ma non può avere radici dispari $\Rightarrow$ impossibile $\Rightarrow$ irriducibile. $\square$

$\boxed{\text{Eisenstein } \infty}$ $a(x) \in \mathbb{Z}[x]$ se

1) $a_0 = p$
2) $|a_0| > |a_1| + \dots + |a_n|$

allora $a(x)$ è irriducibile in $\mathbb{Z}[x]$.

dim: $a(x) = b(x) \cdot c(x) \Rightarrow a_0 = b_0 \cdot c_0 \Rightarrow$ wlog $b_0 = \pm p$, $c_0 = \pm 1$

Guardiamo $c(x)$. Il prodotto delle sue radici complesse fa $\frac{c_0}{c_k}(-1)^k$ ovvero fa $\pm \frac{1}{c_k}$, $c_k \in \mathbb{Z}$

$\Rightarrow c(x)$ ha almeno una radice $\gamma \in \mathbb{C}$ con $|\gamma| \leq 1$.

$\Rightarrow \gamma$ è anche radice di $a(x)$

$0 = a(\gamma) = a_n \gamma^n + a_{n-1}\gamma^{n-1} + \dots + a_1\gamma + a_0$

$\Rightarrow \ -a_0 = a_n\gamma^n + a_{n-1}\gamma^{n-1} + \dots + a_1\gamma$

$\Rightarrow \ |a_0| \leq |a_n|\cdot|\gamma|^n + |a_{n-1}||\gamma|^{n-1} + \dots + |a_1|\cdot|\gamma| \leq |a_n| + |a_{n-1}| + \dots + |a_1|$ assurdo. $\square$

<u>Criterio di Perron</u>: $a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ con $a_0 \neq 0$ tale che

$$|a_{n-1}| > 1 + |a_{n-2}| + \dots + |a_1| + |a_0|$$

$\Rightarrow a(x)$ irriducibile

<u>Dim</u>: <u>Sottolemma</u>: esattamente una radice in $\mathbb{C}$ di $a(x)$ soddisfa $|\alpha| > 1$ mentre le altre $n-1$ soddisfano $|\beta| < 1$.

Dimostriamo il criterio assumendo il Sottolemma.
Se per assurdo $a(x) = b(x)\cdot c(x)$, uno dei due, wlog $b(x)$, avrà tutte le radici di modulo < 1.

$\Rightarrow |b(0)| < 1 \Rightarrow b(0) = 0. \Rightarrow a(0) = a_0 = 0$ assurdo! $\square$

<u>dim Sottolemma</u>: Sia $\alpha \in \mathbb{C}$ con $|\alpha| = 1$ radice di $a(x)$.

$\Rightarrow -a_{n-1}\alpha^{n-1} = \alpha^n + a_{n-2}\alpha^{n-2} + \dots + a_1\alpha + a_0$

$|a_{n-1}| = |-a_{n-1}\alpha^{n-1}| = |\alpha^n + \dots + a_0| \leq 1 + |a_{n-2}| + \dots + |a_1| + |a_0|$ assurdo.

Siano $\alpha_1 \dots \alpha_n$ radici di $a(x)$ in $\mathbb{C}$. So che $\pm\alpha_1 \dots \alpha_n = a_0 \in \mathbb{Z}\setminus\{0\}$

$\Rightarrow$ almeno una radice ha modulo > 1, wlog α_1.

Ora voglio dim che $\alpha_2, \dots, \alpha_n$ hanno modulo < 1.

$b(x) = (x-\alpha_2)\dots(x-\alpha_n) = x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1 x + b_0$

$a(x) = (x-\alpha_1)\cdot b(x) = x^n + (b_{n-2} - \alpha_1)x^{n-1} + (b_{n-3} - \alpha_1 b_{n-2})x^{n-2} + \dots + (b_0 - b_1\alpha_1)x - \alpha_1 b_0$

$|b_{n-2}| + |\alpha_1| \geq |b_{n-2} - \alpha_1| > 1 + |b_{n-3} - \alpha_1 b_{n-2}| + \dots + |b_0 - b_1\alpha_1| + |b_0\alpha_1| \geq$

$\geq 1 - |b_{n-3}| + |\alpha_1 b_{n-2}| \dots - |b_0| + |b_1\alpha_1| + |b_0\alpha_1| =$

$= 1 + |b_{n-2}| + (|\alpha_1| - 1)\left(|b_{n-2}| + |b_{n-3}| + \dots + |b_1| + |b_0|\right)$

$|\alpha_L| > 1 + (|\alpha_L| - 1)\cdot x$

$\Rightarrow |b_{n-2}| + \dots + |b_0| < 1$

Sia $\alpha \in \mathbb{C}$ con $|\alpha| > 1$, allora

$$|Q(\alpha)| = |\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \dots + b_1\alpha + b_0| \geq$$

$$\geq |\alpha^{n-1}| - |b_{n-2}||\alpha|^{n-2} - \dots - |b_0| \geq$$

$$\geq |\alpha^{n-1}| - |\alpha|^{n-2}(|b_{n-2}| + \dots + |b_0|) \geq$$

$$\geq |\alpha|^{n-1}(1 - |b_{n-2}| - \dots - |b_0|) > 0.$$

$\Rightarrow Q$ ha tutte le radici di modulo < 1. $\square$

Ex buffo: p numero primo, $b \geq 2$ intero.

$\overline{p_n p_{n-1} \dots p_0}$ rappr. in base b di p. con $0 \leq p_i < b \ \forall i$

allora $p_n x^n + p_{n-1} x^{n-1} + \dots + p_0$ è irriducibile.

[Criterio di Cohn]

Teo Fatt. unica: in $K[x]$ vale la fatt unica per i polinomi!

$\boxed{\text{Ogni polinomio si scrive in modo unico come prodotto di irriducibili.}}$

③ Cose a caso

Claimione: $P(x), Q(x) \in \mathbb{Z}[x]$ se $P(n) \mid Q(n)$ in $\mathbb{Z}$ per infiniti valori di n allora $P(x) \mid Q(x)$ in $\mathbb{Z}[x]$.

dim: D.E.: scrivo $Q(x) = P(x)\cdot A(x) + R(x)$ con $\deg R < \deg P$

$$\frac{Q(x)}{P(x)} = A(x) + \frac{R(x)}{P(x)}.$$

$$\mathbb{Z} \ni \frac{Q(n)}{P(n)} = \underset{\substack{\cap \\ \mathbb{Z}}}{A(n)} + \frac{R(n)}{P(n)} \Rightarrow \frac{R(n)}{P(n)} \in \mathbb{Z}$$

per n abb grande $\left|\frac{R(n)}{P(n)}\right| < 1 \Rightarrow$ è zero.

$\Rightarrow R(n) = 0$ per infiniti valori di $n \Rightarrow R(x) = 0$ come polinomio. $\square$

Olimpicone n. 2:

Sia $P(x) \in \mathbb{Z}[x]$, monico, di grado pari. Se $P(n)$ è un quadrato per ogni $n \in \mathbb{N}$ allora $P(x) = Q(x)^2$

Sol: Idea "tipo divisione euclidea": voglio scrivere $P(x) = Q(x)^2 + R(x)$ con $\deg R$ controllato.

Ora so che $\quad P(n) = Q(n)^2 + R(n)$

Come dimostro che posso trovare Q e R? $\boxed{\text{x Induzione}}$

Se $\deg P = 2k$, $\deg Q = k$ Se so che $\deg R < k$

come prima $\left|\frac{R(n)}{Q(n)}\right| < 1$ da un certo punto in poi, ma se $R(n)$ è la differenza tra due quadrati, deve essere $\geq 2Q(n) + 1$.

Impossibile $\Rightarrow R(n) = 0$ per ∞ valori di $n \Rightarrow P(x) = Q(x)^2$.

Olimpicone n°3: Quali sono tutti i polinomi $p(x) \in \mathbb{Q}[x]$ tali che $p(n) \in \mathbb{Z}$ $\forall n \in \mathbb{Z}$?

Oss: tutti i $p(x) \in \mathbb{Z}[x]$ vanno bene, ma ce ne sono altri, ad esempio

$$p(x) = \binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

Si dimostra che le combinazioni a coeff interi di questi polinomi esauriscono tutte le possibilità.

Es: Determinare $p(x)$ di grado n t.c. $p(j) = 2^j$ $j = 0, \dots, n$

Sol: $p(x) = \sum_{k=0}^{n} \binom{x}{k}$

Derivate

$$p(x) \longrightarrow p'(x)$$
$$\cap \qquad\qquad \cap$$
$$A[x] \qquad A[x]$$

1) $(p(x)+q(x))' = p'(x) + q'(x)$
2) $(p(x)\cdot q(x))' = p'(x)\cdot q(x) + p(x)\cdot q'(x)$
3) $(\lambda)' = 0 \qquad \lambda \in A$
4) $(x)' = 1$

$\longrightarrow$ $p(x) = a_n x^n + \dots + a_1 x + a_0$

$$\Downarrow$$

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

Oss: Se $p(x) = (x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}$

allora $p'(x) = m_1(x-\alpha_1)^{m_1-1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_k)^{m_k} + m_2(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2-1}\cdots(x-\alpha_k)^{m_k} + \dots + m_k(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_k)^{m_k-1}$

Criterio della derivata: Le radici multiple di $p(x)$ sono anche radici di $p'(x)$.

Es: $p(x)$ pol. non nullo allora il num. delle radici distinte di $p(x)\cdot(p(x)+1)$ è almeno $\deg p(x) + 1$.

Sol: $\mathrm{MCD}(p(x), p(x)+1) = 1 \Rightarrow$ non hanno radici comuni

$p(x) = C(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k} \qquad p(x)+1 = D(x-\beta_1)^{n_1}\cdots(x-\beta_h)^{n_h}$

Oss: $p'(x) = (p(x)+1)'$

$\Rightarrow (x-\alpha_j)^{m_j-1} \mid p'(x) \quad \forall j = 1\dots k$

$ (x-\beta_j)^{n_j-1} \mid p'(x) \quad \forall j = 1\dots h$

$\Rightarrow (x-\alpha_1)^{m_1-1}\cdots(x-\alpha_k)^{m_k-1}(x-\beta_1)^{n_1-1}\cdots(x-\beta_h)^{n_h} \mid p'(x)$

$\Rightarrow (m_1-1)+\dots+(m_k-1)+(n_1-1)+\dots+(n_h-1) \le \deg p(x) - 1$

$$\sum_{j=1}^{k} m_j - k + \sum_{j=1}^{h} n_j - h \le \deg p(x) - 1$$

$$\Rightarrow \sum m_j + \sum n_j - \deg p(x) + 1 \leq k+h$$

$$\sum n_j = \deg p(x) + 1 \leq k+h = \#\text{ radici distinte}$$

<u>Es</u> (RMM 18) Dire se esistono $p(x), q(x) \in \mathbb{R}[x]$ non <u>costanti</u> t.c.

$$p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20}$$

"<u>Sol</u>": $p(x)^9 (p(x)+1) = q(x)^{20}(q(x)+1)$

faccio le derivate $9p(x)^8 p'(x)(p(x)+1) + p(x)^9 p'(x) = 20 q(x)^{19} q'(x)(q(x)+1) + q(x)^{20} q'(x)$

combino queste due + conto di gradi + assurdo.

<u>Es x casa</u>: # radici distinte di $p(x)(p(x)+1)\cdots(p(x)+k)$

$p(x)\cdot a(x) + q(x)\cdot b(x) = 1$

<u>Es</u>: Dire se esistono $p(x), q(x) \in \mathbb{R}[x]$ non costanti t.c. $\underline{p(x)^3 - q(x)^2} = 1$

$\Downarrow$

$\mathrm{MCD}(p,q) = 1$

$\deg p(x) = 2d$
$\deg q(x) = 3d$

<u>derivo</u>: $3p^2p' - 2qq' = 0$

$$3p(x)^2 p'(x) = 2q(x)q'(x)$$

se $r(x)$ irrid. divide $p(x)$ allora divide $q'(x)$ con molteplicità doppia.

$\Rightarrow p(x)^2 \mid q'(x)$. $\Rightarrow \deg p(x)^2 \leq \deg q'(x) = \deg q(x) - 1$

$\Rightarrow 4d \leq 3d - 1$ impossibile.

<u>Teorema ABC</u> (MASON-STOTHERS)

$a, b, c \in A[x]$ coprimi tali che $a(x) + b(x) = c(x)$
allora il numero di radici distinte di abc è $\geq \max\{\deg a(x), \deg b(x), \deg c(x)\} + 1$

<u>dim</u>: $W = ac' - ca'$ se $r^k \| a \Rightarrow r^{k-1} \mid W$
se $r^k \| c \Rightarrow r^{k-1} \mid W$

$a = -b + c \Rightarrow W = (-b+c)c' - c(-b'+c') = b'c - bc'$

se $r^k \| b \Rightarrow r^{k-1} \mid W$

poiché a, b, c sono coprimi, se $2^k \| abc$ allora $2^{k-1} \mid W$

+ Conto dei gradi come con $p(x), p(x)+1$ e si conclude. $\square$