A1 MEDIUM Pol

Titolo nota 07/09/2010

$$\sum_{n=0}^{d} a_n X^n$$

$\uparrow$

$R \subset \mathbb{Z} \quad (\mathbb{N}) \quad \mathbb{Z}/n\mathbb{Z}$

p primo $\qquad f(x) = x^p$

$\updownarrow$

$g(x) = x$

Principio di identità dei polinomi

f, g polinomi di grado $\leq n$

Se $f(x) = g(x)$ per $n+1$ valori di x,

allora $f = g$ (come polinomi)

$X^2 + 1$

$$[f - g](x) = (X - X_0)(x - X_1) \cdots (X - X_n)\, q(x)$$

$\wedge$ n

grado $n+1$

$\not\exists$

---

a_0, a_1, a_2, a_3, a_4 $\quad p(1)=5$ $\quad p(2)=7$

$$\begin{cases} a_0+a_1+a_2+a_3+a_4 = 5 \\ a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \dots = 7 \end{cases}$$

$a+bi$ $\qquad$ $r \cdot e^{i\vartheta}$

↑ facili somme $\qquad$ ↑ facile prodotti

Es $\quad p(2)=p(4)=5 \qquad p(3)=7$

$$p(x)-5 = (x-2)(x-4)q(x)$$

$$p(0)-5 = (-2)\cdot(-4)\cdot \underbrace{q(x)}_{\text{intero}}$$

$$\Rightarrow p(0) \equiv 5 \pmod 8$$

Interpolazione

Trovare un polinomio dati i suoi valori

$p(1)=5$

$\begin{cases} p(2)=6 \\ p(3)=9 \end{cases}$

Dati $n+1$ punti, $\exists!$ polinomio di grado $\leq n$ che ci passa

$(x_0, y_0), \dots (x_n, y_n)$

dim

1) Mi basta fare il caso $y_i = 0$ per tutti gli i tranne uno:

Sia $\boxed{L_j(x)} = \begin{cases} 0 & \text{in } x_i \ i \neq j \\ 1 & \text{in } x_j \end{cases}$

$$p(x) = \sum_{j=0}^{n} L_j(x)\, y_j$$

$$L_j = \frac{\prod_{i \neq j} (x - x_i)}{\prod_{i \neq j} (x_i - x_j)}$$

$$p(x_1) = \sum L_j(x_1) y_j = L_1(x_1)\, y_1 = y_1$$

ESISTENZA

UNICITÀ: grado $\leq n$, coincidono su $n+1$ punti $\Rightarrow$ uguali

Quelli di grado più alto sono

$$p(x) + (x-x_0)(x-x_1)\cdots(x-x_n)\, q(x)$$

$$\begin{cases} a_0 + a_1 x_1 + a_2 x_1^2 + \dots + a_n x_1^n = y_1 \\ \vdots \\ a_0 + a_1 \end{cases}$$

$$V = \begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & & & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{bmatrix}$$

Vandermonde

$$\det(V) = \prod_{i<j} (x_i - x_j)$$

Fatto

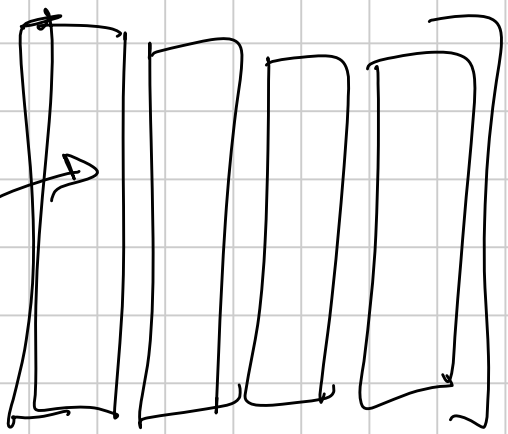
Chi è V^{-1}

$$V \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}$$

$$V^{-1} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix}$$

$$p(x) = \sum_{j=0}^{n} L_j(x)\, y_j \qquad a_0 = L_j(0)\, y_j$$

coefficienti di L_j



$$L_j = \sum_i c_i^{(j)} x^i$$

$$\begin{matrix} c_0^{(0)} \\ c_1^{(0)} \\ c_2^{(0)} \\ \vdots \\ 1 \end{matrix} \qquad \begin{matrix} c_0^{(1)} \\ c_1^{(1)} \\ c_2^{(1)} \\ \vdots \\ 1 \end{matrix}$$

---

parallelismo tra interi e polinomi:

MCD $\longleftrightarrow$ MCD

$a = q \cdot b + r$ $\qquad$ $a(x) = q(x) b(x) + r(x)$

$|r| < |b|$ $\qquad$ $\deg(r) < \deg(b)$

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

$b(x) = x - \alpha$

pongo $x = \alpha$, $a(\alpha) = r$

Bézout: a, b

Thm: dati a, b polinomi con m.c.d 1 esistono p, q polinomi t.c.

$$a \cdot p + b \cdot q = 1$$

In più, $\deg p < \deg b$

$\deg q < \deg a$

Esiste una e una sola scelta di p, q tali che

Fatto: altre soluzioni: [tutte]

$$\begin{cases} p + r(x) b \\ q - r(x) a \end{cases}$$

Teorema cinese $\Leftrightarrow$ interpolazione

$$\begin{cases} x \equiv y_0 & (x_0) \\ \vdots \\ x \equiv y_n & (x_n) \end{cases}$$

$$\begin{cases} p(x) \equiv y_0 & x - x_0 \\ \vdots \\ p(x) \equiv y_n & x - x_n \end{cases}$$

$$p(x) = y_n + (x - x_n) \cdot q(x)$$

congruenze tra polinomi

$p(x) \equiv r(x) \mod q(x)$

$p(x) - r(x)$ multiplo di $q(x)$

$\mathbb{Z}/n\mathbb{Z}$

$x^5 + x^4 - x + 1 \mod x^3 + 1$

$-(x^5 + x^2)$

$-(x^4 + x)$

$-x^2 - 2x + 1$

Fatto

Se il poly. rispetto al quale fate congruenza è irriducibile, lo spazio quoziente è un campo

$$\frac{\mathbb{R}[x]}{(x^3+1)}$$

$x \pm a \mid x^n \pm a^n$

Faccio congruenze mod $x-a$

$$x \equiv a$$

$$x^n \equiv a^n \qquad x^n - a^n \equiv 0$$

$$\Downarrow$$

$$x-a \mid x^n - a^n$$

$$\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}$$

$$ax+b + cx+d$$

$$(a+c)x + (b+d)$$

$$(ax+b)(cx+d) =$$

$$= acx^2 + bcx + adx + bd \equiv$$

$$\equiv (-ac+bd)$$

$$x^2 \equiv -1$$

$$\underbrace{(x-\alpha)(x-\bar{\alpha})}_{1}\,\underbrace{(x-\beta)(x-\bar{\beta})}_{2} \cdots (x-\lambda)(x-\mu)$$

$$\frac{\mathbb{Q}[x]}{(x^3-x+2)}$$

"Rational root theorem"

Se $\sum a_n x^n = p(x)$ ha radice p/q razionale, e $a_n \in \mathbb{Z}$, allora

$q \mid a_n$

$p \mid a_0$

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

moltiplico per q^n,

tutti multipli di q tranne lui

$$p(x)\,a(x) + (x^3 - x + 2)\,b(x) = 1$$

$$p(x)\cdot a(x) \equiv 1 \pmod{x^3 - x + 2}$$

È come dire: faccio i conti con $\mathbb{Q}$ e un "simbolo aggiuntivo" x (come con i complessi)

$$x^3 \longmapsto x - 2$$

$\mathbb{Z}/n\mathbb{Z}[x]$

$\frac{\mathbb{Z}/5\mathbb{Z}}{(p(x))}$

(E) $\frac{\mathbb{Z}/5\mathbb{Z}}{(x^3-x+2)}$ è un campo

ax^2+bx+c ↦ $\in \mathbb{Z}/5\mathbb{Z}$, $\in \mathbb{Z}/5\mathbb{Z}$, $\in \mathbb{Z}/5\mathbb{Z}$

Fatto: $\forall p$, $\forall n$, $\exists$ un polinomio irriducibile mod p di grado n

$\Downarrow$

$\forall p, \forall n$ $\exists$ un campo con p^n elementi $\frac{\mathbb{Z}/p\mathbb{Z}[x]}{(p(x))}$

Fatto: questi sono tutti i campi finiti

$\frac{\mathbb{Z}/5\mathbb{Z}}{x^2-2}$

chiamo j una soluzione

$a+bj$ $\quad j^2 \to 2$

$\mathbb{Z}/5$ $\mathbb{Z}/5$

$F_0 = 0$
$F_1 = 1$ mod 7 $\quad \frac{1+\sqrt{5}}{2} + \dots$

$\sqrt{5} = j \qquad x^2 = 5$

occhio che $x^p \equiv x$ è vero $\mathbb{Z}/7\mathbb{Z}$

$(a+bj)^7 = \dots$

$x^3 - x + 2$

Quando lavorate con radici, complessi

$\left[(\sqrt{2}+1)^{2010} \right]$ Qual è il resto modulo 5 di

$G_{2010} = (\sqrt{2}+1)^{2010} + \underbrace{(-\sqrt{2}+1)^{2010}}_{\text{modulo} < 1} =$

$(\sqrt{2}+1)^{2010} + (1-\sqrt{2})^{2010}$

$x^2 - ax + b$ $\qquad (1+\sqrt{2})(1-\sqrt{2}) = 1-2 = -1$

$2 \quad -1$

$x^2 - 2x - 1$

$\Rightarrow$ È la soluzione di

$$\begin{cases} G_0 = 2 \\ G_1 = 2 \\ G_{n+1} = 2G_n + G_{n-1} \end{cases}$$

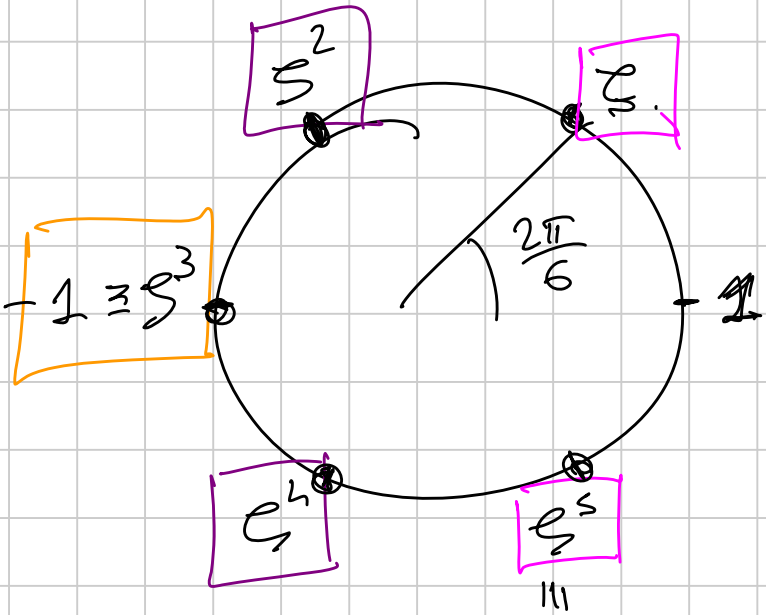
G_0 2
G_1 2
G_2 6
G_3 -1
G_4 -1
G_5 2
3
3
-1

$\vdots$

$G_{2010} \equiv \square$

A1 MEDIUM PARTE 2

Titolo nota 07/09/2010



potenze

#						
→	ζ_1	ζ_2	ζ_3	ζ_4	ζ_5	1
→	ζ_2	ζ_4	1	ζ_2	ζ_4	1
$-1 \equiv$	ζ_3	1	-1	1	-1	
→	ζ_4	ζ_2	1	ζ_4	ζ_2	1
	ζ_5					

Radici primitive = generatori

$$(X-\zeta_1)(X-\zeta_2)(X-\zeta_3)(X-\zeta_4)(X-\zeta_5)(X-1)$$

$$= X^6 - 1$$

$$\frac{X^6-1}{X-1} = X^5 + X^4 + X^3 + X^2 + X + 1$$

$$X^3 - 1 = (X - \varepsilon_2)(X - \varepsilon_4)(X - 1)$$

$$\Rightarrow (X - \varepsilon_2)(X - \varepsilon_4) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$

$X^{18} - 1$ radici 18-esime di 1

1 ε^9 periodo 2

2 $\varepsilon^6, \varepsilon^{12}$ periodo 3

2 $\varepsilon^3 \cdot \varepsilon^{15}$ 6

9 In $\mathbb{Z}_{18}$, quante classi di resto sono tali che

$6x \equiv 0$

$3x \not\equiv 0$

$2x \not\equiv 0$

$3 \mid x$

$6 \nmid x$

$9 \nmid x$

$0 \dots 17$

$3 \quad 15$

$0 \dots 18$

multipli di 3

$\updownarrow$

$3 \times (0 \dots 5)$

minori di 6 e primi con 6

$\varphi(6)$

Radici n-esime dell'unità di periodo $d \mid n$

$$\begin{cases} x^d = 1 \\ x^n = 1 \end{cases} \qquad x^{\mathrm{mcd}(d,n)} = x^{a\cdot d + b\cdot n} =$$

$$= (x^d)^a \cdot (x^n)^b = 1$$

$$x^d = 1 \qquad k = 1, 2, 3 \dots n$$

- $\zeta^{k\cdot d} = 1 \qquad n \mid k\cdot d$
- il periodo è <u>davvero</u> d, non qualcosa di più piccolo, cioè, per ogni $b \mid d$

$$\zeta^{k\cdot b} \neq 1 \qquad n \nmid k\cdot b$$

d divisore di n

$$k\cdot d \equiv 0 \pmod{n}$$

$$k \equiv 0 \pmod{\frac{n}{d}}$$

$K = [0, \dots, n]$

d

$\forall\ b \mid d$

$n \nmid k \cdot b \qquad k \cdot b \neq 0 \ (n)$

$\zeta^{(n/d)\cdot k} \qquad \zeta^{k \cdot n/d}$

$k \in 0, \dots d$

Se k non ha fattori comuni con d, $(d \mid n)$

$\left(k \cdot \frac{n}{d}\right)$ → periodo d

Se k ha fattori comuni con d,

$\mathrm{mcd}\left(k \cdot \frac{n}{d}, n\right)$

$\mathrm{mcd}\left(q \cdot k' \cdot \frac{n}{q \cdot d'}, n\right)$

Questo dovrebbe provare che: le radici n-esime dell'unità di periodo d sono:

- $\phi(d)$ se $d \mid n$
- 0 altrimenti

$$(X-\zeta^0)(X-\zeta^1)\cdots(X-\zeta^{n-1})$$

$n=18$

→ $\Phi_1 = (X-1)$ periodo 1

→ $\Phi_2 = (X+1)$ periodo 2 $\varphi(2)$

→ $\Phi_3 = (X-\zeta^6)(X-\zeta^{12})$ periodo 3 $\varphi(3)$

→ $(X-\zeta^3)(X-\zeta^{15})$ Φ_6 periodo 6 $\varphi(6)$

→ $(X-\zeta^2)(X-\zeta^4)(X-\zeta^8)$ Φ_9 periodo 9 $\varphi(9)$

10 14 16

tutte le altre Φ_{18} $\varphi(18)$

$$\Phi_N \overset{\circ}{=} \prod_{\substack{z \text{ di} \\ \text{periodo } N \\ z \in \mathbb{C}}} (X-z)$$

[o anche $z \in$ radici dell'unità]

Dim che hanno coeff. razionali: INDUZIONE

Φ_{18} è a coeff. razionali:

$$\frac{X^{18}-1}{\Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_6(x)\,\Phi_9(x)} =$$

$$= \Phi_{18}(x)$$

→ è un polinomio

→ ha coefficienti interi, perché lo ottengo da fratte divisioni fra polinomi, e i divisori sono monici

MENO BANALE: $\Phi(x)$ irriducibili

$\sqrt{2}$ $-\sqrt{2}$

$\zeta \mapsto \zeta^p$ p primo con n

dim: non fatta

Corollario

$$\phi(18)+\phi(9)+\phi(6)+\phi(3)+\phi(2)+\phi(1)=18$$

$$n = \sum_{d} \phi(d)$$

d|h

$$x^4+x^3+x^2+x+1=0$$

$$\cos\left(\frac{2\pi}{5}\right)+i\sin\left(\frac{2\pi}{5}\right)$$

1) divido per x^2

$$\left(\frac{1}{x^2}+x^2\right)+\left(\frac{1}{x}+x\right)+1=0$$

$$y:=\frac{1}{x}+x$$

$$y^2=\frac{1}{x^2}+x^2+2$$

$$y^2-2+y+1=0$$

$$y^2+y-1=0$$

$$ax^n+bx^{n-1}+cx^{n-2}+\dots+cx^2+bx+a$$

$$x \longleftrightarrow \frac{1}{x}$$

Se $a_n x^n+a_{n-1}x^{n-1}+\dots+a_0=0$

ha radici $\{x_i\}$

$a_n+a_{n-1}x+\dots+a_0x^n=0$

ha radici $\left\{\frac{1}{x_i}\right\}$ $\quad ax^2 + a = 0$

$\frac{1}{x_1} \longleftrightarrow x_1$

$\frac{1}{x_2} \longleftrightarrow x_2$

Lemma di Gauss

$a(x) = \sum a_n x^n$

contenuto di $a(x)$ è M.C.D(coefficienti)

Lemma

$$c(a \cdot b) = c(a)\, c(b)$$

dim: mi basta farlo quando $c(a) = c(b) = 1$

$$\left(\sum p_n x^n\right) = \left(\sum a_n x^n\right)\left(\sum b_n x^n\right)$$

$$(\quad) = \boxed{a}\left(\sum \alpha_n x^n\right)(\quad)$$

Devo dimostrare che $\nexists\, p$ t.c.
$p \mid$ tutti i coefficienti di $a(x)b(x)$
con a, b di contenuto 1

Vedo tutto mod p:
Se esistesse tale p,

$$0 = (\quad)(\quad)$$

cose che non sono zero

$$a(x) = \sum a_n x^n$$

prendo il coeff di grado più alto k di a t.c. $p \nmid a_k$

e poi di grado più alto h di b t.c. $p \nmid b_h$

$$a_k x^k \cdot b_h x^h$$

che non si annulla con niente

Allora contenuto è moltiplicativo ☐

Se un polinomio $p(x) \in \mathbb{Z}[x]$

$$p(x) = a(x)\, b(x)$$

con $a(x), b(x) \in \mathbb{Q}[x]$,

allora si spezza anche a coeff interi

$$\tilde{a}(x)\, \tilde{b}(x) = p(x) \qquad \tilde{a}, \tilde{b} \in \mathbb{Z}[x]$$

ES

$$p(x) = \left(\frac{x+2}{3}\right) \cdot (3x+6) = x^2+4x+4$$

$(x+2)\ (x+2) = \checkmark$

dim:

$$p(x) = a(x)\cdot b(x) =$$

$$p(x) = \frac{\bar{a}(x)}{m}\cdot\frac{\bar{b}(x)}{n}$$

↑ supponiamo inoltre $c[p]=1$

$$m\cdot n\cdot p(x) = \bar{a}(x)\,\bar{b}(x)$$

$c(\ ) = m\cdot n$ $\qquad$ $m\cdot n = c(\bar{a})\cdot c(\bar{b})$

↑ qui uso moltiplicatività

$$p(x) = \frac{\bar{a}(x)\bar{b}(x)}{mn} = \boxed{\frac{\bar{a}(x)}{c(a)}\,\frac{\bar{b}(x)}{c(b)}}$$

$\tilde{a}(x)\ \ \tilde{b}(x)$.

sono a coeff' interi. □

Idee buone

1) proiettare i coefficienti modulo n

(IE) se un polinomio è irriducibile in $\mathbb{Z}/p\mathbb{Z}[x]$

2) prendere i pezzi di grado massimo

$$(xy^2 + x^3 + 37y^3 + 2x^2y) =$$

$$\overset{*}{=} (xy + y + x)\left(y^2 + \;\cdots x \cdots\right)$$

polinomi omogenei hanno fattori omogenei

polinomi simmetrici hanno fattori simmetrici

$$a^3+b^3+c^3-3abc = (a+b+c)(\text{roba})$$

$*$ $a^3+b^3+x^3-3abx$ è un multiplo di $a+b+x$?

cioè:

è $\equiv 0 \mod (a+b+x)$

$$x \equiv -a-b$$

$$* \equiv a^3+b^3+\left(-a^3-b^3-3ab(a+b)\right)-3abx \equiv$$

($x \equiv -a-b$)

$$\equiv 0$$

$$\frac{a^3+b^3+x^3-3abx}{a+b+x}$$ è un polinomio in x

$$\frac{1}{a+b}x + \cdots$$

$$a^3+b^3+c^3-3abc=(a+b+c)(\text{roba})$$

omogeneo
simmetrico

$$\alpha(a^2+b^2+c^2)$$
$$\beta(ab+bc+ca)$$

guarda i coefficienti di a^3: $\boxed{\alpha=1}$

$$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca)$$

Teo ogni polinomio simmetrico è un polinomio nelle funzioni simm. elementari

---

$$S_k=\sum_{i=1}^{n} x_i^k$$

x_i radici di $\sum_{i=0}^{n} a_k x^k$

$$\sum a_k S_{t+k}=0$$

$$x_i^t\left(a_0 + a_1 x_i^1 + \dots + a_n x_i^n\right) = 0$$

$$D\left[\sum a_n x^n\right] := \sum a_n \cdot n x^{n-1}$$

Es $D\left[3x^3 + 2x + 37\right] = 3 \cdot 3x^2 + 2$

Proprietà

1) $D[f+g] = Df + Dg$

2) $D[af] = aDf$ (a costante)

3) $D[fg] = D[f] \cdot g + f \cdot D[g]$

$f_1, f_2 \longrightarrow f_1 + f_2$

$$D[(f_1+f_2)g] = D[f_1 g + f_2 g] =$$

$$D[f_1 g] + D[f_2 g] = D[f_1] g + f_1 \cdot Dg +$$

$$+ D[f_2]\, g + f_2 \cdot Dg =$$

$$= D[f_1 + f_2]\, g + (f_1 + f_2)\, Dg$$

Mi riconduco a f, g monomi con questo trucco

$$D[ax^m \cdot bx^n] \stackrel{?}{=} D[ax^m]bx^n + ax^m D[bx^n]$$

$$ab(m+n)x^{m+n-1} \stackrel{\checkmark}{=} abmx^{m-1}x^n + abx^m nx^{n-1}$$

CRITERIO DELLA DERIVATA

Un polinomio $f(x)$ ha radici multiple se e solo se

$$\mathrm{mcd}\left(f(x), Df(x)\right) \neq 1$$

dim: $\Rightarrow$

$$\mathrm{mcd}\left((X-a)^m q(x),\ m(x-a)^{m-1}q(x) + (x-a)^m q(x)\right)$$

entrambi i fattori contengono $(x-a)^{m-1}$

$\Leftarrow$

controllo tutti i fattori di $f(x)$

$(x-a)$: devo verificare che

$$x-a \nmid Df[x]$$

$$f(x) = (x-a)\boxed{q(x)} \rightarrow q(a) \neq 0$$

$$D[f] = (x-a)q'(x) + 1 \cdot q(x)$$

Valuto in a e vedo se fa 0:

$$D[f](a) = q(a) \neq 0$$

Fattorizzazione unica dei polinomi:

Se l'anello A è a fatt. unica,

$A[x]$ è a fatt. unica

IN PRATICA: SEMPRE

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

$$x^2-5 \qquad \mathbb{Z}/7\mathbb{Z}$$

$$(x^2-5)^2$$

se "chiamo" j una radice del polinomio $aj+b$

$$(x^3-x+2)^2, \quad (x^3-x+2)(18x+37)$$

"tutte le radici coniugate vanno insieme"

Se $p(x),\ q(x) \in \mathbb{Q}[x]$

$p(\sqrt{2}) = q(\sqrt{2}) = 0 \qquad (x-\sqrt{2})$

$p(-\sqrt{2}) = q(-\sqrt{2}) = 0 \qquad (x+\sqrt{2})$

$$\begin{cases} x+y+z+t=1 \\ x^2+y^2+z^2+t^2=2 \\ x^3+y^3+z^3+t^3=3 \\ x^4+y^4+z^4+t^4=4 \end{cases}$$

$x^2+y^2+z^2+t^2 = (x+y+z+t)^2 - 2(xy+\dots)$

$2 = 1^2$

$S = x+y+z+t$

$P = xyzt$

$Q = xy+yz+\dots$

$\lambda^4 - \lambda^3 - \frac{1}{2}\lambda^2 + \square\lambda + \square$

$S_3 + A_3 S_2 + A_2 S_1 + 3A_1 = 0$

$a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x = -a_0$

$a_4 x^3 + a_3 x^2 + a_2 x + a_1 = -\frac{a_0}{x}$

$$a_4 \sum x^3 + a_3 \sum x^2 + a_2 \sum x + n a_1 = -\frac{a_0}{x}$$

$$+ a_0 \cdot \frac{a_1}{a_0}$$

$$a_4 x^2 + a_3 x + a_2 + \boxed{\frac{a_1}{x} + \frac{a_0}{x^2}} = 2a_2$$