A1 Medium Tess

Note Title 9/3/2016

Polinomi

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

Ci servono 2 proprietà sui coefficienti

ho le operazioni di $+$ e $\cdot$

un Anello è insieme con queste operazioni

la x non è un elemento dell'anello dei coefficienti
semplicemente distingue i coefficienti grado per grado

La valutazione è una funzione $p : A \to A$

$$a \mapsto p(a)$$

es. di Anelli : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; $\mathbb{F}_p$ = gli interi mod p

field

Se A è un anello, $A[x] := \{$ polinomi a coeff. in $A \}$
è ancora un anello

(se ho 2 polinomi posso sommarli e moltiplicarli)

Es: $\mathbb{Z}[x]$ è l'anello dei polinomi a coeff. interi

$\mathbb{Z}[x][y] =: \mathbb{Z}[x,y]$ sono i polinomi in 2 variabili (a coeff. interi)

Se in A posso fare la divisione (inverso moltiplicativo)

chiamerò A un campo

es di campi: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

non è vero che se K è un campo anche $K[x]$ lo è

Con i polinomi a coeff. in un campo avete

la DIVISIONE EUCLIDEA

(le operazioni usate sono solo $+, \cdot,$ e si usa l'inverso del coefficiente di testa del divisore)

es: x^2+x+1 diviso $3x+1$ (in $\mathbb{Q}[x]$)

$$Q = \frac{x}{3} + c \ , \quad R = \frac{1}{9} + \frac{1}{3} + 1$$

l'inverso

Thm di Ruffini: $p(x) \in K[x]$ e $a \in K$

t.c. $p(a) = 0 \Rightarrow p(x) = (x-a)q(x)$

Dim: potete fare la divisione tra $p(x)$ e $x-a$

$$p(x) = (x-a)q(x) + r(x)$$

deg < 1

$\Rightarrow$ valutando in a viene $p(a) = r = 0$

Allora un polinomio non nullo di grado n ha al massimo n radici

Dim: per induzione il passo base è che $p(x)$ non ha radici

il passo induttivo
- Ruffini
- legge di ann. del prodotto

$$p(x) = (x-a)q(x)$$ (ruffini)

ha grado 1 in meno di $p(x)$

una radice di p è radice di $x-a$ oppure di $q(x)$
(legge ann. prod.)

Principio di identità dei polinomi

Supponete di avere $p(x)$ di grado $\leq n$ con $n+1$ radici, allora $p(x)$ è nullo

Dim: conseguenza dell'enunciato precedente

Variante se non sapete nulla sul grado di $p(x)$?

Mi bastano infinite radici.

Es: esiste un polinomio a coeff. in $\mathbb{Q}$ t.c.

$$p(n) = 2^n \quad \forall\, n \in \mathbb{N} \,?$$

No! $\quad q(x) = p(x) - 2p(x-1)$ è un polinomio

è chiaro che $q(x)$ si annulla su $\mathbb{N}$

$\Rightarrow q(x) = 0$ (come uguaglianza sui polinomi)

$\Rightarrow p(x) = 2p(x-1)$

guardo il coeff. direttivo (= il coeff. di grado + alto)

sarà a_n:

$a_n = 2a_n \Rightarrow$ assurdo se $p(x)$ non è nullo

Altre conseguenze di Ruffini

$$a - b \mid a^n - b^n$$

considero $\quad p(a) = a^n - b^n \in \mathbb{Z}[b][a]$

$\quad d(a) = a - b \in \mathbb{Z}[b][a]$

è monico $\Rightarrow$ posso fare la DIV EUCL

$\Rightarrow$ " Ruffini

Ma $p(b)=0 \Rightarrow p(a)=(a-b)\underbrace{q(a)}_{\in \mathbb{Z}[b][a]}$

$\underbrace{a-b}_{d(a)} \mid \underbrace{p(a)-p(b)}_{f(a)}$ (divisibilità tra interi se $p \in \mathbb{Z}[x]$)

(ma anche come polinomi a coeff. in $\mathbb{Z}[b]$)

$f(b)=0 \Rightarrow d(a) \mid f(a)$ per Ruffini

$\underbrace{a+b+c}_{d(a) \in \mathbb{Z}[b,c]} \mid \underbrace{a^3+b^3+c^3-3abc}_{p(a) \in \mathbb{Z}[b,c][a]}$

è monico!

Posso applicare Ruffini: infatti $p(-b-c)=0$

$$p(a)=a^3-(3bc)a+(b^3+c^3)$$

Es: IMO SL 2006 A6

$$|ab(a^2-b^2)+bc(b^2-c^2)+ca(c^2-a^2)| \leq M(a^2+b^2+c^2)^2$$

determinare la migliore M che renda vera la dis.

$\forall\, a,b,c \in \mathbb{R}$

Oss 1 è che il termine in $|\cdot|$ si fattorizza!

Sia $p(a) \in \mathbb{Z}[b, c]$ il polinomio in $|\cdot|$

vale che $p(b) = 0$ (infatti $0 + bc(b^2 - c^2) + cb(c^2 - b^2) = 0$)

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

Ma allora $p(a, b, c)$ è multiplo di $(a-b), (b-c), (c-a)$

il quoziente $\dfrac{p(a,b,c)}{(a-b)(b-c)(c-a)}$ è ciclico in a, b, c

è di 1° grado $\Rightarrow ka + kb + kc$ per $k \in \mathbb{Z}$

viene $k = 1$

IMO 2004 - 2

Determinare tutti i polinomi $p(x) \in \mathbb{R}[x]$

tali che

$p(a-b) + p(b-c) + p(c-a) = 2p(a+b+c)$

$\forall\ a, b, c \in \mathbb{R}$ t.c. $ab + bc + ca = 0$

Oss. banale $p(0) = 0$ (ponendo $a = b = c = 0$)

Ponendo solo $a = b = 0$

$p(0) + p(-c) + p(c) = 2p(c)$

$\Rightarrow \quad p(-c) = p(c) \qquad \forall c \in \mathbb{R}$

$\Rightarrow \quad p(-x) = p(x)$ come polinomi (principio di identità dei polinomi)

Guardando i coeff. di grado dispari

$\Rightarrow -a_{2n+1} = a_{2n+1}$ $\Rightarrow$ il polinomio ha solo termini di grado pari

Poniamo $a = 6\lambda$, $b = 3\lambda$, $c = -2\lambda$

$$p(3\lambda) + p(5\lambda) + p(8\lambda) = 2p(7\lambda) \quad \forall \lambda \in \mathbb{R}$$

$\Rightarrow$ vale l'uguaglianza dei coeff.

Guardo il termine di testa se $[x^n]\,p(x) = a_n$

$$3^n a_n + 5^n a_n + 8^n a_n = 2 \cdot 7^n a_n$$

$$3^n + 5^n + 8^n = 2 \cdot 7^n$$

$\Rightarrow$ ora so che non può essere n troppo grande

(se per esempio $8^n > 2 \cdot 7^n$ non è vera l'$=$)

(mi pare che si abbia $n < 6$)

Ora so che $p(x) = ax^4 + bx^2$

(in realtà questa è soluzione $\forall a, b \in \mathbb{R}$)

Supponiamo che $p(x), q(x) \in \mathbb{Z}[x]$ sono tali che

$p(n) \mid q(n) \quad \forall\, n \in \mathbb{Z}$ (mi bastano ∞ $n \in \mathbb{Z}$)

e che $p(x)$ sia monico

Allora $p(x) \mid q(x)$ (esiste $r \in \mathbb{Z}[x]$ t.c. $q(x) = p(x)r(x)$)

$\Rightarrow$ DIV EUCL.

$$m\, q(x) = p(x)r(x) + s(x) \qquad \text{con } \deg(s) < \deg(p), \quad r, s \in \mathbb{Z}[x]$$

vedi fondo pagina

Valuto x in n $\forall\, n \in \mathbb{Z}$

$$q(n) = p(n)r(n) + s(n)$$

$$\underset{\text{hyp.}}{\mathbb{Z} \ni} \frac{q(n)}{p(n)} = \underset{\mathbb{Z}}{\underset{\cap}{r(n)}} + \frac{s(n)}{p(n)} \qquad \text{quindi } \frac{s(n)}{p(n)} \in \mathbb{Z}$$

per $n \gg 0$ (n abbastanza grande)

deve essere $|p(n)| > |s(n)|$ (convincersene per esercizio)

(basta farlo quando $p(x) = x^m$)

$$\Rightarrow \left|\frac{s(n)}{p(n)}\right| < 1 \Rightarrow \frac{s(n)}{p(n)} = 0$$

$$\Rightarrow s(n) = 0 \quad (\text{ma è vero per } \infty\ n)$$

(Si può dire qualcosa anche se p non è monico, anche in tal caso vale la div)

Sia $p(x,y) \in \mathbb{C}[x,y]$ t.c.

$$p(t^3,t) = 0 \quad \text{per } \infty \ t \in \mathbb{C}$$

Allora $x - y^3 \mid p(x,y)$

DIV EUCL. $x-y^3 \in \mathbb{C}[y][x]$ è monico!

$$p(x,y) = (x-y^3)\underset{\mathbb{C}[\cancel{x}][x]}{\underset{\cap}{q(x,y)}} + \underset{\mathbb{C}[y][x]}{\underset{\cap}{r(x,y)}}$$

La tesi è $r(x,y) = 0$

sapete già che $\mathrm{Deg}_x(r(x,y)) < \mathrm{Deg}_x(x-y^3)$

quindi $r(x,y) = r(y)$

valutando $x = t^3$, $y = t$ $\forall t$ dell'ipotesi

$$0 = p(t^3,t) = r(t)$$

$\Rightarrow$ r è il polinomio nullo! (principio d'identità polinomi)

$p(x,y) \in \mathbb{C}[x,y]$ t.c.

$$p(\sin\theta, \cos\theta) = 0 \quad \forall \theta \in \mathbb{R}$$

Allora $x^2+y^2-1 \mid p(x,y)$

DIV EUCL rispetto a x (x^2+y^2-1 è monico in x)

$$p(x,y) = (x^2+y^2-1)\,q(x,y) + r(x,y)$$

ora però $\mathrm{Deg}_x(r(x,y)) < 2$

$$\Rightarrow r(x,y) = a_0(y) + x\,a_1(y)$$

l'ipotesi dice che $0 = a_0(\sin\theta) + \cos\theta\, a_1(\sin\theta)$

quindi: vorrei scrivere $0 = a_0(t) + \sqrt{1-t^2}\, a_1(t)$ e dire che è un polinomio

$$a_0^2(\sin\theta) = \cos^2\theta\, a_1^2(\sin\theta) = (1-\sin^2\theta)\, a_1(\sin\theta)$$

ora il polinomio $a_0^2(x) - (1-x^2)\,a_1^2(x) = 0$

$$a_0^2(x) = \underset{\substack{\Uparrow \\ (1-x)(1+x)}}{(1-x^2)}\, a_1^2(x)$$

conto il # di radici "1" a dx e a sx

$\equiv 1 \pmod 2$ $\equiv 0 \pmod 2$

se a_0, a_1 sono non nulli

$$\Rightarrow a_0(y) = a_1(y) = 0$$

Es. per casa:

$a^n - b^n \mid a^m - b^m$ (come polinomi $\mathbb{Z}[a,b]$, $\mathbb{C}[a,b]$

oppure per $b \in \mathbb{Z}$ come polinomi in $\mathbb{Z}[a]$ o $\mathbb{C}[a]$

$$\Downarrow$$

$$n \mid m$$

oppure come divisibilità in $\mathbb{Z}$ (se $a, b \in \mathbb{Z}$))

Sia $p_k(a,b,c) \in \mathbb{Z}[a,b,c]$

$$p_k(a,b,c) = a^k + b^k + c^k \quad \forall k \in \mathbb{N},\ k > 0$$

trovare tutte le coppie (n,m) t.c.

$$p_n \mid p_m$$

Sia $p(x,y,z) \in \mathbb{C}[x,y,z]$ t.c.

$p(\cos\alpha, \cos\beta, \cos\gamma) = 0 \quad \forall\, \alpha, \beta, \gamma$ angoli di un triangolo

[vale $\cos^2\alpha + \cos^2\beta + \cos^2\gamma + 2\cos\alpha\cos\beta\cos\gamma = 1$]

allora $x^2+y^2+z^2+2xyz-1 \mid p(x,y,z)$

Oss. sparse:

con i polinomi a coeff. in un campo potete fare il thm di Bezout ($(p,q)=1 \Rightarrow \exists\, a,b \in K[x]$ t.c. $ap+bq=1$)

avete le congruenze tra polinomi

es. dovete ottenere il resto della divisione di $x^{2016}+x^{1008}+x+1$ per x^2+x+1

vale che $x^2 \equiv -x-1 \pmod{x^2+x+1}$

$x^3 \equiv 1 \pmod{x^2+x+1}$

$x^{2016} \equiv x^{3(\dots)} \equiv 1$

$x^{1008} \equiv 1$

$\Rightarrow$ il resto è $x+3$

Potete anche fare thm cinese su $x^2+x+1=(x-\xi)(x-\xi^2)$

con ξ 3-primita dell'unità

$p(x) \equiv a+b\xi \quad (x-\xi)$

$p(x) \equiv a'+b'\xi \quad (x-\xi^2)$

Interpolazioni

avete dei punti (x_0, y_0) con $x_i, y_i \in K$

$\vdots$

(x_n, y_n)

$\boxed{\text{gli } x_i \text{ sono tutti diversi}}$

volete trovare un polinomio $p(x) \in K[x]$ t.c.

$p(x_i) = y_i$

Siano p_1, p_2 polinomi di grado $\leq n$

allora $p_1 = p_2$

infatti $p_1(x) - p_2(x)$ ha grado $\leq n$

con $x_0, \dots, x_n$ come radici (distinte)

$\Rightarrow$ è il polinomio nullo

Se avete un polinomio p che soddisfa, allora ce ne sono ∞

$p(x) + (x - x_0) \cdot \ldots \cdot (x - x_n) q(x)$

soddisfa $\forall q \in K[x]$

Se voglio trovare p che soddisfa induzione su n

per $n=0$ voglio $p(x_0)=y_0$ ho $p(x)=y_0$

$n \Rightarrow n+1$ se p soddisfa per $x_0, \dots, x_n$

voglio p' che soddisfa per $x_0, \dots, x_{n+1}$

sarà $p'(x) = p(x) + (x-x_0) \cdot \ldots \cdot (x-x_n)\, q(x)$

basta imporre $q(x) = C$ con C t.c.

$$y_{n+1} = p(x_{n+1}) + \underbrace{(x_{n+1}-x_0) \cdot \ldots \cdot (x_{n+1}-x_n)}_{\neq 0}\, C$$

Un altro modo è usare la linearità

osservo che se riesco a risolvere il problema

con $(x_0, 1), (x_1, 0), \dots, (x_n, 0)$

e $(x_0, 0), (x_1, 1), \dots, (x_n, 0)$

e $\vdots$

e $(x_0, 0), (x_1, 0), \dots, (x_n, 1)$

allora so risolvere il problema anche per

$(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n)$

Siano $L_0(x), \dots, L_n(x)$ [Si chiama metodo di Lagrange] i polinomi che soddisfano gli $n+1$ problemi di cui sopra

allora $y_0 L_0 + y_1 L_1 + \dots + y_n L_n$ soddisfa il problema originale.

(basta valutare in $x = x_i \quad \forall i$)

ad esempio

$L_0(x) = C\,(x - x_1) \cdot \ldots (x - x_n)$

con C t.c. $\quad 1 = L_0(x_0) = C\,\underbrace{(x_0 - x_1) \cdot \ldots \cdot (x_0 - x_n)}_{\neq 0}$

Es: voglio $p(x)$ t.c. $p(n) = 2^n$ per $n = 0, 1, \dots, k$

$$p(x) = \sum_{n=0}^{k} \binom{x}{n} \qquad \binom{x}{n} := \frac{x(x-1) \cdot \ldots \cdot (x-n+1)}{n!}$$

(sto usando $\sum_n \binom{k}{n} = 2^n = (1+1)^n$)

Es bis: voglio $p(n) = \alpha^n \quad \alpha \in \mathbb{R}$ (per $n = 0, \dots, k$)

Uso $(1 + (\alpha - 1))^n = \sum_{i=0}^{n} (\alpha - 1)^i \binom{n}{i}$

Funzionerà $p(x) = \sum_{i=0}^{k} (\alpha - 1)^i \binom{x}{i}$

Se voglio interpolare un polinomio a coeff. in $\mathbb{F}_p = \mathbb{Z}/_p$

ottengo che qualsiasi funzione $f: \mathbb{Z}/p \to \mathbb{Z}/p$

è polinomiale di grado $\leq p-1$

(Sto risolvendo un problema di interpolazione sui punti:

$x_i = i$ per $i = 0, \dots, p-1$)
$y_i = f(i)$

Polinomi simmetrici

sono $p \in \mathbb{Z}[x_1, \dots, x_n]$

tali che $p = \tau p$ con $\tau = (i\,j)$ ← trasposizione

cioè $p(x_0, \dots, x_{i-1}, x_j, x_{i+1}, \dots x_{j-1}, x_i, \dots)$

cioè scambio 2 variabili senza cambiare il polinomio

Es: se $n=1$, tutti

$n=2$ $\quad a+b,\ a^2+b^2,\ ab$

$n=3$ $\quad a+b+c,\ ab+bc+ca,\ abc$

Thm: fondamentale sui polinomi simmetrici in 3 variabili:

se $p \in \mathbb{Z}[a,b,c]$ simmetrico

$\Rightarrow \exists\, q \in \mathbb{Z}[x,y,z]$ t.c.

$$q(a+b+c,\ ab+bc+ca,\ abc) = p(a,b,c)$$

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

quindi $q(x,y,z) = x^3 - 3xy + 3z$

Def: i coefficienti di

$(x+x_1)(x+x_2)\cdot\ldots\cdot(x+x_n) \in \mathbb{Z}[x_1,\ldots,x_n][x]$

sono detti polinomi simmetrici elementari, $e_1,\ldots,e_n$

$e_1 = x_1+\ldots+x_n$

Thm (fondamentale sui polinomi simmetrici)

Se $p \in \mathbb{Z}[x_1,\ldots,x_n]$ è simmetrico

$\Rightarrow \exists\, q \in \mathbb{Z}[y_1,\ldots,y_n]$ t.c.

$$p(x_1,\ldots,x_n) = q(e_1,\ldots,e_n)$$

Dim: induzione su n

$n=1$ (tutti i polinomi sono simmetrici) banale

$n \Rightarrow n+1$ So che tutti i polinomi in n variabili si scrivono ... come in tesi

voglio fare altrettanto per $n+1$ "

Posso fare così:

$p \in \mathbb{Z}[x_1, \dots, x_{n+1}]$

Oss: allora $p(x_1, \dots, x_n, 0)$ è simmetrico

$p(x_1, \dots, x_n, 0) = q(e_1, \dots, e_n)$ ← in n var.

Oss: e_i in $n+1$ variabili, se ne valuto una in 0 ottengo e_i in n variabili (o 0 se $i = n+1$)
(segue facilmente dalla definizione degli e_i)

$r(\underline{x}) = p(x_1, \dots, x_n, x_{n+1}) - q(e_1, \dots, e_n)$ ← in $n+1$ var.

per Ruffini: $(x_{n+1} - 0) \mid r(\underline{x})$

ma $r(\underline{x})$ è simmetrico in $n+1$ var. perché somma di simmetrici

quindi: $x_i \mid r(\underline{x}) \quad \forall i$

$\Rightarrow \quad e_{n+1} \mid r(\underline{x})$

$\Rightarrow$ Concludo con induzione sul grado di p

ora $\dfrac{r(\underline{x})}{e_{n+1}}$ è simmetrico in $n+1$ variabili ma il grado è $< p$

Naturalmente il P.B. è facile:

se fosse $Deg(p(\underline{x})) < n+1$ allora ho già ottenuto

$$p(\underline{x}) = q(e_1, \dots, e_n)$$ $\square$

Es: esprimere $a^2+b^2+c^2$ in funzione delle simmetriche elementari

Sol: pongo $c=0$

$$a^2+b^2 = e_1^2 - 2e_2 = q(e_1, e_2)$$

$$q(x,y) = x^2 - 2y$$

$$a^2+b^2+c^2 = e_1^2 - 2e_2$$

Es per casa

Mostrare che se $q(y_1, \dots, y_n) \in \mathbb{Z}[y_1, \dots, y_n]$

tale che $q(e_1, \dots, e_n) = 0$

allora $q = 0$

(significa che $e_1, \dots, e_n$ sono indipendenti, cioè non si può esprimere qualsiasi polinomio simmetrico usando solo alcune delle simmetriche elementari)

$e_1^2 = e_2$ non si verificano

(qui $q(x,y) = x^2 - y$)

Sia $p(x_1, \dots, x_n) = \prod_{i<j} (x_i - x_j)^2$

mostrare che è simmetrico

e che se $q(e_1, \dots, e_n) = p(\underline{x})$, allora

$q(Y_1, \dots, Y_n)$ è irriducibile

(vuol dire $\nexists$ q_1, q_2 t.c. $q = q_1 \cdot q_2$ e q_1, q_2 non costanti)

Irriducibilità

Se $p(x) \in A[x]$ è irriducibile se

$\nexists$ $p_1(x), p_2(x)$ non costanti t.c.

$p(x) = p_1(x) p_2(x)$

Dipende moltissimo da A

Caso $A = \mathbb{C}$, ci sono solo polinomi di grado 1

(teorema fondamentale dell'algebra)

Caso $A = \mathbb{R}$, ci sono solo grado 1 e

grado 2 con $\Delta < 0$

(conseguenza del caso $A = \mathbb{C}$)

Casi $A=\mathbb{Q}$ e $A=\mathbb{Z}$

è vero che irriduc. su $\mathbb{Q}$ $\Rightarrow$ irriduc. su $\mathbb{Z}$

l'altra freccia è vera e si chiama lemma di Gauss

In $A=\mathbb{Z}$ ci sono alcuni criteri di irr.

ridurre mod p (ridurre i coeff.)

$q \in \mathbb{Z}[x]$ irr. di $\overline{q}$ in $\mathbb{Z}/_p[x] \Rightarrow$ irr di q su $\mathbb{Z}[x]$

es: x^2+x+1 mod 2 è irr.

Controllare le radici razionali

se $p(x) \in \mathbb{Z}[x]$ e r è una radice $\in \mathbb{Q}$

$r=\frac{n}{m}$ $(n,m)=1 \Rightarrow n \mid p_0$, $m \mid p_{deg(p)}$

$$p(x) = \sum_{i=0}^{\deg p} p_i x^i$$

Criterio di Eisenstein

se $p(x) \in \mathbb{Z}[x]$ ed esiste q primo t.c.

$q \mid$ tutti i coeff. di p, tranne il coeff. direttivo

e $q^2 \nmid$ il termine noto $\Rightarrow p(x)$ è irriducibile.

es: $p(x) = x^{2016} - 3$ è irr. per Eisentein con $q=3$.