SENIOR 2022 — A1 MEDIUM

Note Title 03/09/2022

POLINOMI

1. Ripasso del Basic
2. Fattorizzazione
3. Grandi classici
4. Esercizi da IMO e IMO-SL

1 Ripasso del basic

→ Divisione euclidea

→ Teo. RUFFINI

→ Principio di identità dei pol.

→ Congruenze tra polinomi

→ Possibilità di assegnare n+1 valori

Polinomio

$$P(x) = \underbrace{a_n}_{\uparrow} x^n + \underbrace{a_{n-1}}_{\uparrow} x^{n-1} + \dots + \underbrace{a_1}_{\uparrow} x + \underbrace{a_0}_{\uparrow}$$

coeff.

I coeff. ai a_i prendiamo

→ in un anello (un ambiente in cui hanno senso $+, -, \cdot$, ma non necessariamente la divisione) (esempio classico: $\mathbb{Z}$)

→ in un campo (come sopra, ma in aggiunta posso dividere) (esempi: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ = classi di resto mod p)

Polinomio MONICO: $a_n = 1$

Divisione euclidea: dati $A(x)$ e $B(x)$ polinomi, esistono unici $Q(x)$ e $R(x)$ tali che

$$\boxed{\begin{aligned} &A(x) = B(x)\,Q(x) + R(x) \\ &\deg(B(x)) < \deg(A(x)) \end{aligned}}$$

<u>Achtung!</u> La divisione si può fare

→ se i coeff. sono in un campo

→ " " anello, MA $B(x)$ è monico

(pensare al caso $A(x) = x^2+2$ $B(x) = 3x+5$)

$\boxed{\text{Dim}}$ Induzione sul grado di $A(x)$

$\boxed{\text{Teorema di RUFFINI}}$ Se $P(a) = 0$ per un certo $a \in$ ambiente dove stanno i coeff., allora

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

cioè $(x-a) \mid P(x)$

↑ divide

$\boxed{\text{Dim.}}$ Faccio la divisione ($x-a$ è monico)

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

↑ grado < 1 e quindi costante

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

↑ numero

Mettendo $x=a$ trovo $R = P(a) = 0$.

$\boxed{\text{Teorema di BEZOUT}}$ Siano $A(x)$ e $B(x)$ pol. a coeff. in un campo. Allora esistono $M(x)$ ed $N(x)$ a coeff. nello stesso campo t.c.

$$A(x)\,M(x) + B(x)\,N(x) = D(x)$$

↑ MCD di $A(x)$ e $B(x)$ = pol. di grado max che divide sia $A(x)$ sia $B(x)$.
(Definito a meno di una costante)

$\boxed{\text{Dim}}$ Induzione sul numero dei passi dell'algoritmo Euclideo

Il punto chiave della dim, come nel caso degli interi, è che

$$MCD(A(x), B(x)) = MCD(B(x), R(x))$$

Quindi MCD non cambia durante l'algoritmo.

$\boxed{\text{Oss.}}$ Bezout si estende a $\mathbb{Z}[x]$ pur di ammettere un numero a moltiplicare

(Faccio il conto in $\mathbb{Q}[x]$ e poi elimino i denominatori)

$\boxed{\text{Ricaduta aritmetica}}$ Siano $A(x)$ e $B(x)$ pol. in $\mathbb{Z}[x]$ senza fattori in comune, quindi $MCD(A(x), B(x)) = 1$.

Allora $\exists$ $M(x)$ ed $N(x)$ in $\mathbb{Z}[x]$ t.c.

$$A(x)\,M(x) + B(x)\,N(x) = c$$

↑ costante che elimina i denominatori

Ora per ogni $n \in \mathbb{Z}$ vale che $\underbrace{MCD(A(n), B(n))}_{\text{Numero}}$ divide c

$\boxed{\text{ASSEGNAZIONE DI N+1 valori}}$ Siano $x_1, \dots, x_{n+1}$ numeri distinti (elem. del campo)

Siano $y_1, \dots, y_{n+1}$ numeri qualunque (sempre del campo, anche NON distinti)

Allora esiste $P(x)$ a coeff. nel campo, con grado $(P(x)) \leq n$, tale che $P(x_i) = y_i$ per ogni $i = 1, 2, \dots, n+1$

Morale: $P(x)$ dipende da $n+1$ coeff. incogniti, e abbiamo $n+1$ equazioni

$\boxed{\text{DIM 1}}$ Scrivo bovinamente il sistemone nelle incognite $a_0, a_1, \dots, a_{n+1}$

$$\begin{cases} x_1^n \boxed{a_n} + x_1^{n-1} \boxed{a_{n-1}} + \dots + x_1 \boxed{a_1} + \boxed{a_0} = y_1 \\ x_2^n \; \dots \qquad = y_2 \\ \vdots \qquad \vdots \\ x_{n+1}^n \boxed{a_n} + x_{n+1}^{n-1} \boxed{a_{n-1}} + \dots + x_{n+1}^{a_1} + \boxed{a_0} = y_{n+1} \end{cases}$$

Si tratta di un sistema LINEARE in $a_0, a_1, \dots, a_n$.
Un sistema lineare $\boxed{r \times r}$ si risolve (in modo unico) se e solo se il Det della matrice dei coeff. è $\neq 0$

$$\operatorname{Det} \begin{pmatrix} x_1^n & x_1^{n-1} & \dots & x_1 & 1 \\ x_2^n & x_2^{n-1} & \dots & x_2 & 1 \\ \vdots & & & & \vdots \\ x_{n+1}^n & x_{n+1}^{n-1} & \dots & x_{n+1} & 1 \end{pmatrix} \neq 0$$

quando $x_1, \dots, x_{n+1}$ sono diversi

Det di Vandermonde

$\boxed{\text{DIM 2}}$ Risolvo il problema in un caso molto particolare, cioè quando gli y_i sono tutti nulli, tranne l'i-esimo che vale 1. In questo caso

$$P_i(x) = \frac{(x-x_1) \dots (x-x_{i-1})(x-x_{i+1}) \dots (x-x_{n+1})}{(x_i-x_1) \dots (x_i-x_{i-1})(x_i-x_{i+1}) \dots (x_i-x_{n+1})}$$

A quel p.to quello che voglio è

$$P(x) = y_1 P_1(x) + y_2 P_2(x) + \dots + y_{n+1} P_{n+1}(x) = \sum_{i=1}^{n+1} y_i P_i(x)$$

(provare per credere)

Achtung! In $\mathbb{Z}[x]$ non c'è un analogo di questa proprietà, anzi i polinomi in $\mathbb{Z}[x]$ sono molto rigidi

$\boxed{\text{Principio di identità dei polinomi}}$

Supponiamo che l'anello abbia ∞ elementi (bastano $n+1$)
Sia $A(x)$ e $B(x)$ due polinomi di grado $\leq n$
Supponiamo che $A(x) = B(x)$ per $n+1$ valori distinti di x.
Allora $A(x)$ e $B(x)$ hanno gli stessi coeff. (il viceversa è ovvio)

$\boxed{\text{Dim}}$ Ponendo $P(x) = A(x) - B(x)$ otteniamo che $\deg(P(x)) \leq n$ e $P(x)$ ha almeno $n+1$ radici distinte.
Siano $a_1, a_2, \dots, a_{n+1}$ queste radici. Allora per RUFFINI

$$P(x) = (x-a_1)\,Q_1(x) = (x-a_1)(x-a_2)\,Q_2(x)$$
$$= \dots = (x-a_1)(x-a_2)\cdot\ldots\cdot(x-a_{n+1})\,Q_{n+1}(x)$$

ma così il grado sarebbe troppo grosso.

Oss. Lo stesso conto ci dice che un pol. di grado n ha al massimo n radici distinte

Controesempio Il polinomio $x^p - x$ a coeff. in $\mathbb{F}_p$ si annulla per ogni valore di x, ma non è il polinomio nullo.

$\boxed{\text{Teorema fondamentale dell'algebra}}$

Un polinomio $P(x) \in \mathbb{C}[x]$ con $\deg(P(x)) = n$ ha esattamente n radici complesse, purché contate con molteplicità

Def. Si dice che a è radice di molt. m per $P(x)$ se

$$(x-a)^m \mid P(x) \qquad \text{ma} \qquad (x-a)^{m+1} \nmid P(x)$$

(La parte difficile è dimostrare che esiste almeno una radice)

② $\boxed{\text{FATTORIZZAZIONE}}$ → Radici razionali

→ Modulo p

→ EISENSTEIN

→ Eisenstein ∞

→ Lemma di Gauss

$\boxed{\text{Criterio radici razionali}}$ Sia $P(x) = a_n x^n + \dots + a_0$ un pol. a coeff. interi.

Supponiamo che $P(x)$ ammetta una radice razionale $\frac{p}{q}$ (frazione ridotta ai minimi termini).

Allora

$$p \mid a_0 \quad e \quad q \mid a_n$$

<u>Dim</u> sostituisco e faccio denom. comune:

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

Ora basta imporre che num $= 0$ e usare che p e q non hanno fattori in comune.

$\boxed{\text{EISENSTEIN}}$ $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$.

Supponiamo che esista p primo tale che

- $p \nmid a_n$
- $p \mid a_i$ per ogni $i = 0, \dots, n-1$
- $p^2 \nmid a_0$

Allora $P(x)$ è IRRIDUCIBILE in $\mathbb{Z}[x]$ (non si può scomporre come prodotto di polinomi non banali, cioè di grado ≥ 1)

$\boxed{\text{Dim}}$ Supponiamo $P(x) = B(x) \cdot C(x)$

$B(x) = b_0 + b_1 x + \dots + b_k x^k$

$C(x) = c_0 + c_1 x + \dots + c_\ell x^\ell$ con $k + \ell = n$

Andiamo a moltiplicare

$$a_0 = b_0 c_0$$

Esattamente uno tra b_0 e c_0 è multiplo di p. Supponiamo $p \mid b_0$

$$\underset{p}{\uparrow a_1} = \underset{p}{\uparrow b_0} c_1 + b_1 \underset{\text{NO } p}{\uparrow c_0} \quad \rightsquigarrow \quad p \mid b_1$$

$$\underset{p}{\uparrow a_2} = \underset{p}{\uparrow b_0} c_2 + \underset{p}{\uparrow b_1} c_1 + b_2 \underset{\text{NO } p}{\uparrow c_0} \quad \rightsquigarrow \quad p \mid b_2$$

Per induzione $p \mid b_i$ per ogni $i = 1, \dots, k$

Ma allora $p \mid a_n = b_k c_\ell$, contro l'ipotesi

— o — o —

$\boxed{\text{Eisenstein } \infty}$ $P(x)$ come prima. Supponiamo che

- $a_0 = p$ primo
- $|a_0| > |a_1| + |a_2| + \dots + |a_n|$

Allora $P(x)$ è irriducibile in $\mathbb{Z}[x]$

$\boxed{\text{Dim}}$ Supponiamo che si fattorizzi $P(x) = B(x) \cdot C(x)$

Come prima

$$p = a_0 = b_0 c_0 \quad \rightsquigarrow \quad \text{WLOG} \quad b_0 = \pm p \quad \text{e} \quad c_0 = \pm 1$$

Quindi $C(x)$ è un polinomio a coeff. interi con termine noto $= 1$.

Ora $\boxed{\dfrac{\text{termine noto}}{c_n}} = \pm$ prod. radici complesse contate con molteplicità di $C(x)$

↑ numero di modulo ≤ 1

Quindi $C(x)$ ha una radice $b \in \mathbb{C}$ tale che $|b| \leq 1$

Ora questo b è radice di $P(x)$, cioè

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

Sfruttando la seconda ipotesi

$$|a_0| = |a_n b^n + \dots + a_1 b| \leq |a_n| \cdot |b|^n + \dots + |a_1| \cdot |b|$$

proprietà modulo in $\mathbb{C}$

$$\leq |a_n| + \dots + |a_1| < |a_0|$$

e questo è assurdo!

$\boxed{\text{Modulo } p}$ Se $A(x) = B(x) \cdot C(x)$ in $\mathbb{Z}[x]$
allora riducendo i fattori modulo p ottengo una fattorizzazione in $\mathbb{F}_p(x)$

$\boxed{\text{Conseguenza pratica}}$ Per dim. che $A(x)$ è irriducibile in $\mathbb{Z}[x]$ basta essere fortunati e trovare un primo p tale che $A(x)$ è irriducibile in $\mathbb{F}_p[x]$.

$\boxed{\text{Dim}}$ Se fosse riducibile in $\mathbb{Z}$, lo sarebbe pure in $\mathbb{F}_p$.

Oss. Per fattorizzare in $\mathbb{F}_p$, alla peggio provo tutti i casi.

$\boxed{\text{Dim. Eisenstein 2}}$ Supponiamo $P(x) = B(x) \cdot C(x)$.
Allora riducendo mod p:

$$a_n x^n = \overline{P}(x) = \overline{B}(x) \cdot \overline{C}(x)$$

Ma allora

$$\overline{B}(x) = b_k x^k \quad \rightsquigarrow \quad B(x) = b_k x^k + p \cdot B_1(x)$$
$$\overline{C}(x) = c_\ell x^\ell \quad \rightsquigarrow \quad C(x) = c_\ell x^\ell + p \cdot C_1(x)$$

Ma allora i termini noti di $B(x)$ e $C(x)$ contengono p, quindi $p^2 \mid a_0$.
L'unico caso in cui non succede è se $k=0$ oppure $\ell = 0$

— o — o —

$\boxed{\text{LEMMA DI GAUSS}}$ Supponiamo che $P(x) \in \mathbb{Z}[x]$ si fattorizzi in $\mathbb{Q}[x]$.
Allora $P(x)$ si fattorizza anche in $\mathbb{Z}[x]$

Oss. Non è detto che la fattorizz. sia la stessa

$$x^2+x = \frac{1}{2}x\,(2x+2)$$

Def. Dato un polinomio $P(x)$, chiamiamo

$$MCDC\,(P(x)) = MCD \text{ dei coeff. di } P(x)$$

↑ ufficialmente si chiama "contenuto"

$\boxed{\text{Lemma}}$ Siano $A(x)$ e $B(x)$ in $\mathbb{Z}[x]$. Allora

$$MCDC\,(A(x)\cdot B(x)) = MCDC\,(A(x))\cdot MCDC\,(B(x))$$

$\boxed{\text{Lemma} \Rightarrow \text{Gauss}}$ Supponiamo $\boxed{MCDC\,(P(x)) = 1}$

Prendiamo una fattorizzazione in $\mathbb{Q}[x]$:

$$P(x) = A(x)\cdot B(x)$$

Sia m = mcm denominatori di a

n = mcm " " b.

Allora

$$mn\,P(x) = \bar{A}(x)\cdot\bar{B}(x)$$

Applico Lemma:

$$mn = MCDC\,(mnP(x)) = MCDC\,(\bar{A}(x))\cdot MCDC\,(\bar{B}(x))$$

$$P(x) = \frac{\bar{A}(x)\cdot\bar{B}(x)}{mn} = \frac{\bar{A}(x)\cdot\bar{B}(x)}{MCDC\,(\bar{A}(x))\cdot MCDC\,(\bar{B}(x))}$$

$$= \frac{\bar{A}(x)}{MCDC\,(\bar{A}(x))}\cdot\frac{\bar{B}(x)}{MCDC\,(\bar{B}(x))} = \text{fatt. in } \mathbb{Z}[x]$$

Se $MCDC(P(x)) \neq 1$ la dim. è analoga a partire da una fattorizzazione di
$$\frac{P(x)}{MCDC(P(x))}$$

Dim Lemma

→ RHS | LHS è ovvio

→ È facile che posso supporre WLOG
$$MCDC(A(x)) = MCDC(B(x)) = 1$$
In questo caso resta da dimostrare che
$$MCDC(A(x) \cdot B(x)) = 1.$$
Supponiamo che non lo sia, dunque esiste primo p che divide tutti i coeff. di $A(x) \cdot B(x)$.

Ora p non divide tutti i coeff. di $A(x)$ ... $a_k x^k$ è il primo
" " " " " " $B(x)$ ... $b_\ell x^\ell$ è il primo non diviso

Il coeff. di $x^{k+\ell}$ nel prodotto è

$$\underbrace{a_0 b_{k+\ell} + a_1 b_{k+\ell-1} + \dots}_{\text{qui c'è } p \text{ per colpa degli } a_i} + \underbrace{a_k b_\ell}_{\text{NON c'è } p} + \underbrace{a_{k+1} b_{\ell-1} + \dots + a_{k+\ell} b_0}_{\text{qui c'è } p \text{ per colpa dei } b_i}$$

[Nota: se $k+\ell > \deg B(x)$, possiamo far finta che i coeff. successivi siano 0]

— o — o —

I GRANDI CLASSICI

① Rigidità polinomi in $\mathbb{Z}[x]$. Sia $P(x) \in \mathbb{Z}[x]$ tale che

$$P(1) = 2022$$

Quali valori può assumere $P(4)$?

$P(x) - 2022$ ha $a = 1$ come radice, quindi

$$P(x) - 2022 = (x-1)\,Q(x)$$

$$P(x) = 2022 + (x-1)\,Q(x)$$

$$P(4) = 2022 + 3\,Q(4)$$

$$\Rightarrow P(4) \equiv 0 \pmod 3$$

Si vede che ogni valore di questo tipo è ok.

② Siano $P(x)$ e $Q(x)$ in $\mathbb{Z}[x]$.
Supponiamo che $P(n) \mid Q(n)$ per infiniti interi n.
Allora $P(x) \mid Q(x)$ come polinomi, e quindi $P(n) \mid Q(n)$ per ogni intero n.

$\boxed{\text{Dim}}$ Faccio la divisione $Q(x) = P(x)\,A(x) + R(x)$, quindi

grado più piccolo di $P(x)$

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

Ne segue che $\dfrac{R(x)}{P(x)}$ è intero per ∞ valori di n interi

Ora per n grande $\left|\dfrac{R(x)}{P(x)}\right| < 1$, quindi per forza $R(n) = 0$ per infiniti n,
quindi $R(x)$ è il polinomio nullo.

③ Sia $P(x,y)$ un polinomio in 2 variabili a coeff. interi.
Supponiamo che $P(n,n)=0$ per infiniti interi n.
Allora
$$P(x,y) = (y-x)\, Q(x,y)$$
per un certo $Q(x,y)$ a coeff. interi

$\boxed{\text{Dim}}$ $P(x,y)$ lo penso come un polinomio in y che ha come coeff. dei polinomi della x, che sono un anello.
In questo senso posso fare la divisione tra $P(x,y)$ e $y-x$ che è monico. Allora

$$P(x,y) = (y-x)\, Q(x,y) + R(x,y)$$

il suo grado in y è $<$ del grado in y di $y-x$
quindi è un pol. della sola x

$$= (y-x)\, Q(x,y) + R(x)$$

Ponendo $x=y=n$ otteniamo che $R(n)=0$ per infiniti n, quindi R è il polinomio nullo !!

④ Calcolare quanto vale al massimo
$$\mathrm{MCD}\left(n^2+100,\ (n+1)^2+100\right)$$
al variare di n tra gli interi

Considero i polinomi $x^2+2x+101 = P(x)$ e $x^2+100 = Q(x)$
Non hanno fattori in comune, quindi $\mathrm{MCD}(P(x),Q(x))=1$
quindi
$$P(x)\cdot M(x) + Q(x)\cdot N(x) = 1 \quad \text{vale in } \mathbb{Q}[x]$$

$$\mathrm{MCD}\left(x^2+2x+101,\ x^2+100\right) = \mathrm{MCD}\left(x^2+100,\ 2x+1\right)$$
$$4x^2+400 = (2x+1)(2x-1) + 401$$

$$
\begin{array}{l|l}
4x^2+400 & 2x+1 \\
\hline
-4x^2-2x & 2x-1 \\
\hline
-2x+400 & \\
2x\quad +1 & \\
\hline
401 &
\end{array}
$$

Conclusione $\quad MCD(4x^2+400,\ x^2+2x+101) = 401$

Quindi

$$(x^2+100)\,\underset{\uparrow}{M(x)} + (x^2+2x+101)\,\underset{\uparrow}{N(x)} = 401$$

a coeff. interi

Si possono trovare $M(x)$ ed $N(x)$ che verificano questa relazione

Quindi per ogni n sappiamo che $MCD(n^2+100,\ n^2+2n+101) \mid 401$

Se troviamo n per cui è esattamente 401, allora ok

Come lo trovo ?

$$n^2+100 \equiv 0 \quad (401)$$

$$(n+1)^2+100 \equiv 0 \quad (401)$$

$$\rightsquigarrow \quad n^2 \equiv (n+1)^2 \quad (401)$$

$\nearrow \quad n \equiv n+1 \quad (401)$ ☹

$\rightsquigarrow \quad -n = n+1 \quad (401)$

$2n+1 \equiv 0 \quad (401)$

Ad esempio $\quad n = 200$

$$200^2+100 = 100 \cdot 401 \quad ☺$$

$$201^2+100 \equiv (-200)^2+100 = 200^2+100 \equiv 0 \quad (401) \quad ☺$$

(5) Sia $P(x) \in \mathbb{Z}[x]$. Supponiamo che $P(n) =$ quadrato perfetto per infiniti interi n.

Allora $P(x) = [Q(x)]^2$ per un opportuno $Q(x) \in \mathbb{Z}[x]$.

Così è un po' esagerato $\quad \to P(x) = x$, oppure $P(x) = x^3$

$\to P(x) = 2x^2+1$ è un □ infinite volte

L'equazione di PELL $y^2 - 2x^2 = 1$ ha infinite sol. intere (x,y)

La cosa diventa vera se aggiungiamo 2 ipotesi
→ grado pari
→ MONICO

$\boxed{\text{Dim}}$ $P(x) = x^{2m} + a_{2m-1}x^{2m-1} + \dots + a_1 x + a_0$

$\boxed{\text{Step 1}}$ Posso trovare $Q(x)$ di grado $\leq m$ tale che

$$P(x) - Q(x)^2$$

ha grado $< m$.

$$Q(x) = x^m + b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots$$

Deve succedere che

$2b_{m-1} = a_{2m-1}$ ⇝ NO problem

$\underset{\text{NOTO}}{b_{m-1}^2} + 2b_{m-2} = \underset{\text{NOTO}}{a_{2m-2}}$ ⇝ NO problem

Così ogni volta trovo un coeff. nuovo

$\boxed{\text{Step 2}}$ Ora sappiamo che $P(x) = \underset{\text{grado } m}{Q(x)^2} + \underset{\text{grado} < m}{R(x)}$

Se $R(n) \neq 0$, allora per forza $R(n) \geq 2Q(n) + 1$

$R(n) \leq -2Q(n) + 1$

Quindi in ogni caso $\underset{\text{grado} < m}{|R(n)|} \geq 2\underset{\text{grado } m}{|Q(n)|} - 1$

quindi è impossibile

Quindi per forza $R(n) = 0$ per infiniti n, dunque $R(x) \equiv 0$.

$\boxed{\text{Step 3}}$ Serve un piccolo aggiustamento perché i coeff. di $Q(x)$ potrebbero essere razionali. Alla fine si usa una specie di Lemma di Gauss.

(6) $\boxed{\text{IMO 1993-1}}$ $x^n + 5x^{n-1} + 3$ irriducibile in $\mathbb{Z}[x]$.

$\boxed{\text{Ricicclo Eisenstein}}$ $x^n + 5x^{n-1} + 3 = B(x) \cdot C(x)$

$b_0 \cdot c_0 = 3 \quad \rightsquigarrow \quad$ wlog $\quad 3 \mid b_0$

$b_0 c_1 + c_0 b_1 = 0 \quad \rightsquigarrow \quad 3 \mid b_1$

$b_0 c_2 + b_1 c_1 + b_2 c_0 = 0 \quad \rightsquigarrow \quad 3 \mid b_2$

... e così via fino a $n-1$ ESCLUSO

Tutti i coeff. di $B(x)$ fino a b_{n-2} sono multipli di 3

$\Rightarrow$ $B(x)$ ha grado almeno $n-1$ (è monico...), anzi ha grado esattamente $n-1$. Ma allora $C(x) = x - a$ con a radice intera! Le uniche radici intere (anzi razionali) possibili sono ± 1 e ± 3, ma non vanno bene (avrei la somma di 3 dispari!)

(7) $P(x) \in \mathbb{Z}[x]$ $\qquad P^{(k)}(x) = P(x)$ composto con se stesso k volte

Se $P^{(k)}(x) = x$, allora $P(P(x)) = x$

$\boxed{\text{Lemma}}$ Se $P(x) \in \mathbb{Z}[x]$, allora
$$(b-a) \mid P(b) - P(a)$$
per ogni coppia di interi a e b.

$P(b) - P(a)$ è somma di roba del tipo $c_k(b^k - a^k)$
$= c_k (b-a) \cdot \text{roba}$

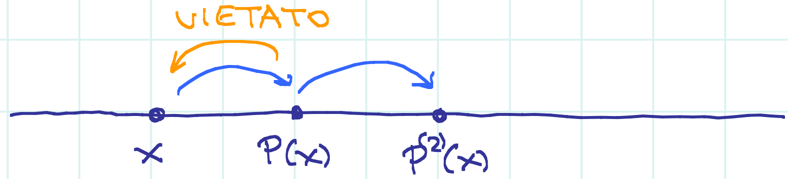
$\boxed{\text{Problema iniziale}}$

$$\underset{b}{\underset{\shortparallel}{P(x)}} - \underset{a}{\underset{\shortparallel}{x}} \mid P(P(x)) - P(x) \mid \ldots \mid P^{(k)}(x) - P^{(k-1)}(x)$$

$$x - P^{(k-1)}(x) \mid P(x) - x$$

Questo ci dice che sono = a meno del segno

$$|P(x)-x| = |P^{(2)}(x) - P(x)| = |P^{(3)}(x) - P^{(2)}(x)| = \dots$$



Dopo k passaggi bisogna tornare a x. Quindi prima o poi bisogna fare il passaggio da $P(x)$ indietro verso x

(8) Sia $P(x,y,z)$ a coeff. interi tale che

$$P(x,y,z) = P(x,y,xy-z) = P(x,zx-y,z) = P(yz-x,y,z)$$

per ogni x, y, z interi.
Allora

$$P(x,y,z) = Q(x^2+y^2+z^2-xyz)$$

$$(xy-z)^2 - xy(xy-z)$$

Il viceversa è ovvio

$\boxed{\text{Allenamento 1}}$ Se $P(x) = P(-x)$ per ogni $x \in \mathbb{Z}$, cosa possiamo dire?

Succede che $P(x) = Q(x^2)$, cioè ha solo le potenze pari

<u>Dim</u>
$$a_0 + a_1x + a_2x^2 + a_3x^3 + \dots = a_0 - a_1x + a_2x^2 - a_3x^3 + \dots$$
$$\rightsquigarrow a_1x + a_3x^3 + \dots = 0 \rightsquigarrow a_1 = a_3 = \dots = 0.$$

$\boxed{\text{Allenamento 2}}$ Se $P(x) = P(4-x)$ per ogni $z \in \mathbb{Z}$?

$P(x) = Q(x(4-x))$

<u>Dim</u> $A(t) = P(\underbrace{2+t}_{x}) \rightsquigarrow A(t) = A(-t) \rightsquigarrow A(t) = B(t^2)$

$$A(t) = B(t^2)$$

$$P(x) = A(x-2) = B((x-2)^2) = B(x^2-4x+4)$$
$$= C(x^2-4x)$$

$\boxed{\text{Esercizio iniziale}}$

$\boxed{\text{Step 1}}$ Se $P(x,y,z) = P(x,y,xy-z)$

Come prima $\leadsto$ $P(x,y,z) = Q(x,y,z(xy-z))$

Come sono fatti i termini di grado + alto ?

$$x^i y^j z^k (xy-z)^k$$

Quindi nei termini di grado + alto c'è $x^{i+k} y^{j+k} z^k$

Quindi nei termini di grado + alto gli esponenti di x e y sono $\geq$ dell'esponente di z.

Usando anche le altre 2 simmetrie scopriamo che nei termini di grado + alto in $P(x,y,z)$ gli esponenti sono tutti uguali !!!

Quindi

$$P(x,y,z) = \underset{\substack{\uparrow \\ \text{coeff.}}}{a} x^c y^c z^c + \text{roba di grado + basso}$$

$\boxed{\text{Step 2}}$ Considero $P(x,y,z) - a(xyz - x^2 - y^2 - z^2)^c$ e ottengo un polinomio di grado più basso che ha ancora le stesse simmetrie!

Ora basta andare per induzione!