Algebra

Polinomi
- espressioni formali, somma di monomi
- funzioni

formale
- Monomio $\quad c\,❀^4 \qquad c\,❀^4$
- coeff. reali $\quad \mathbb{R}[❀] \qquad \mathbb{R}[x]$
- somma $\quad \mathbb{Q}[❀] \quad \mathbb{Z}[❀] \quad \mathbb{C}[❀]$
- prodotto $\quad \mathbb{N}[❀]$

funzione $\quad p(❀) \in \mathbb{Q}[❀] \rightsquigarrow$ funzione polinomiale

Funzione polinomiale $\quad p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$

$$\mathbb{Q} \longrightarrow \mathbb{Q}$$

$$a \longmapsto p(a) = c_n \cdot a^n + c_{n-1} \cdot a^{n-1} + \cdots + c_1 \cdot a + c_0$$

Grado se $p(x) \neq 0$

grado = il più grande esponente dei monomi con coefficienti diversi da 0

$\deg(p(x))$

$\deg(p \cdot q) = \deg p + \deg q$

$$\deg(p+q) \begin{cases} a & a > b \\ \leq a & a = b \end{cases} \qquad \begin{matrix} \deg p = a \\ \deg q = b \end{matrix} \qquad a \geq b$$

Radici di un polinomio

$p(x) \in \mathbb{Z}[x] \rightsquigarrow$ funzione $\mathbb{Z} \to \mathbb{Z}$

$A[x] \qquad A \to A$

a è radice di p se $p(a) = 0$

$p(x) \in \mathbb{Z}[x] \quad 3x+2$

non ha radici $\rightsquigarrow p(x) \in \mathbb{Q}[x]$

ha radice $-\frac{2}{3}$

Divisione con resto tra polinomi

$p \quad q \in A[x]$ quoziente a resto r

se 1) $p = a \cdot q + r$

2) $\deg(r) < \deg q$ oppure $r = 0$

$$\begin{array}{l|l} \boxed{a_n x^n} + a_{n-1} x^{n-1} + \dots + a_0 & \boxed{b_k x^k} + \dots + b_0 \\ \hline & \frac{a_n}{b_k} x^{n-k} \end{array}$$

$\mathbb{Z}$ va sempre bene se $b_k = 1$ (o -1)
(polinomio monico)

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ok
$\mathbb{Z}, \mathbb{N}$ ahi

Se $r=0$ allora q divide p
allora le radici di q sono anche radici di p!

$$p(\odot) = a(\odot)\cdot q(\odot) \quad e \quad q(b)=0$$

$$p(b) = a(b)\cdot q(b) = a(b)\cdot 0 = 0$$

Oss. b è radice di $\odot - b$

Teorema di Ruffini (legame tra pol. simbolico / pol. funzione)

Se $\boxed{p(b)=0}$ $\boxed{\odot - b \text{ divide } p(\odot)}$

(e viceversa)

Ma allora sulle radici non abbiamo veramente detto tutto...

b radice $\doteq p(b)=0$

$p(b)=0 \Leftrightarrow \odot - b$ divide $p(\odot)$

Ma se $(\odot - b)^2$ divide $p(\odot)$ che succede?

① se $(\odot - b)^2$ divide $p(\odot)$ e $p(\odot) = (\odot - b)q(\odot)$
ora $(\odot - b)$ deve dividere pure $q(\odot)$

[perché la fattorizzazione nei polinomi è unica.]

cioè $q(b)=0$

② Criterio della derivata

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

Derivata di p Dp o p' è

$$n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 .$$

Se $p(b)=0$ e $(x-b)^2$ divide $p(x)$ allora

anche $p'(b)=0$ (e viceversa)

$\mathbb{R}[x]$

$p(x) = 3x^4 - x^2 - x - 1$ 1 è radice

$x-1$ divide $p(x)$

$(x-1)^2$ " " ?

$12x^3 - 2x - 1$ 1 non è radice di p'

quindi $(x-1)^2$ non divide $p(x)$

Se $(x-b)^k$ divide $p(x)$ ma $(x-b)^{k+1}$ non divide $p(x)$

si dice che b è una radice di $p(x)$ di

$\boxed{\text{molteplicità } k}$

Composizione Quando 0 è radice?

se $a_0=0$ E che molteplicità ha 0?

il grado del monomio non nullo più piccolo

E se $p(b)=0$? Se calcolo $p(x+b)=\tilde{p}(x)$

se $\tilde{p}(0)=0$ (0 è radice di $\tilde{p}$)

allora $p(0+b)=0$ (b è radice di p)

E la molteplicità di b come radice di p è la stessa della molteplicità di 0 come radice di $\tilde{p}$.

Coefficienti in $\mathbb{Z}$

C'è un legame con la divisibilità dei numeri interi.

$p(x)\in\mathbb{Z}[x]$ $\quad n\in\mathbb{Z}$ $\quad p(n)=0$ $\quad$ n è una radice

$x-n$ divide $p(x)$ $\qquad p(x)=(x-n)\cdot q(x)$

<u>quindi</u> $\qquad q(x)\in\mathbb{Z}[x]$

$m-n$ divide $p(m)$ $\qquad p(m)=(m-n)\cdot q(m)$

$$3x^4-x^2-x-1=(x-1)(3x^3+3x^2+2x+1)$$

$$3\cdot10^4-10^2-10-1=(10-1)(3\cdot10^3+3\cdot10^2+2\cdot10+1)$$

$$29889=9\cdot(3321)$$

$$\underbrace{3\cdot17^4-17^2-17-1}_{\pentagon}=\underbrace{(17-1)}_{16}\underbrace{(3\cdot17^3+3\cdot17^2+2\cdot17+1)}_{\text{dispari}}$$

Qual è la massima potenza di 2 che divide $\pentagon$?

$16 \quad 2^4$

$p(x)$ coeff. interi $\quad p(3)=0 \quad p(1000)=0$

$x-3$ divide $p(x)$

$x-1000$ " "

$$p(x)=(x-3)(x-1000)\,q(x)$$

∃ un numero $n\in\mathbb{Z}$ t.c. $p(n)=2019$?

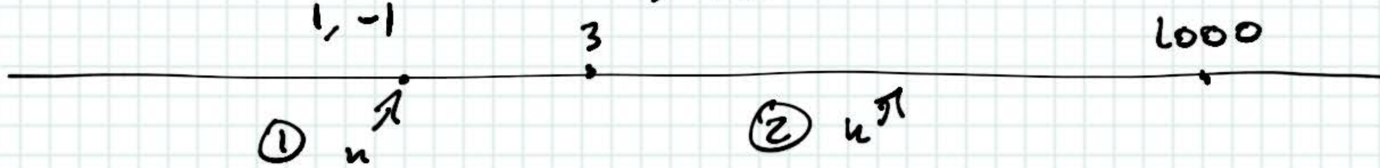
$2019=673\cdot 3$ Se $p(n)=2019$

$2019=(n-3)(n-1000)\,q(n)$ $q(x)\in\mathbb{Z}[x]$

↑ intero

3, 673, −3, −673 2019, −2019

1, −1



① $n-1000>997$ → −2019 −1019 ✗

② $|n-3|=3$ o $|n-1000|=3$

↓ $2019>|n-1000|>673$ $2019>|n-3|>673$

$q(n)$ mult. di 3

⇒ $|n-3|$ e $|n-1000|$ hanno poss. solo 1, −1, 673, −673 imposs.

③ analogo a ①

~~E se sappiamo "tutte"~~ le radici

E se sappiamo fattorizzare il polinomio completamente in fattori di primo grado?

Se siamo in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ tutti i fattori possono essere trasformati in $x-b_i$ $n=\deg p$.

$$p(x)=c\,(x-b_1)(x-b_2)\cdots(x-b_n)$$

$(c=1) \quad p(z) = z^n + a_{n-1} z^{n-1} + a_{n-2} z^{n-2} + \dots + a_1 z + a_0$

$a_0 = (-1)^n \, b_1 \cdot b_2 \cdot \dots \cdot b_n$

$a_{n-1} = -(b_1 + b_2 + \dots \; b_n)$

a_i = somma dei prodotti dei b_i a gruppi di $n-k$

$a_{n-2} = b_1 b_2 + b_1 b_3 + b_2 b_3 + b_1 b_4 \dots$

Esercizi

① $q(x) = x^4 + x^3 + x^2 + x + 1 \qquad p(x) = q(x^5)$

Qual è il resto della divisione di $p(x)$ per $q(x)$?

$$p(x) = x^{20} + x^{15} + x^{10} + x^5 + 1 \qquad p(x) = a(x)\cdot q(x) + r(x)$$

$$q(x) = \frac{(x^5 - 1)}{(x-1)} \qquad x^5 = (x-1)\,q(x) + 1$$

$$p(x) = ((x-1)q(x)+1)^4 + ((x-1)q(x)+1)^3 + ((x-1)q(x)+1)^2 +$$
$$+ ((x-1)q(x)+1) + 1 =$$

$$= [(x-1)q(x)]^4 + 4[(x-1)q(x)]^3\cdot 1 + 6[(x-1)q(x)]^2\cdot 1^2 +$$
$$+ 4[(x-1)q(x)]^1\cdot 1^3 + 1^4 + \dots =$$

$$= a_1(x)\,q(x) + 1 + a_2(x)\,q(x) + 1 + a_3(x)\,q(x) + 1 + a_4(x)\,q(x) + 1 + 1 =$$

$$= \left(\sum_{i=1}^{4} a_i(x)\right)\cdot q(x) + \boxed{5}$$

② $x^3 + ax^2 + bx + c = p(x) \qquad p(x) = 0$ per $x=2, x=4, x=-6$

$p(0)$? $\qquad p(x) = (x-2)(x-4)(x+6)$

$$p(0) = a_0 = c = (-1)^3\cdot 2\cdot 4\cdot(-6) = 48$$

$$p(0) = (0-2)(0-4)(0+6) = $$
$$= 48$$

③ $p(n) = n^5 + n^4 + 1$

Per quali n intero $p(n)$ è primo?

Si fattorizzerà $p(x)$?

Criterio della radice razionale: $p(x) \in \mathbb{Z}[x]$

$$p = a_n x^n + \cdots + a_0$$

Allora le radici razionali $\frac{p}{q}$ (ridotta ai minimi termini) soddisfa che p divide a_0 e q divide a_n.

infatti se $a_n\left(\frac{p}{q}\right)^n + \cdots + a_1 \frac{p}{q} + a_0 = 0$

allora molt. per q^n

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

mult. di q (sopra $a_{n-1} p^{n-1} q + \cdots + a_0 q^n$)

mult. di p (sotto $a_n p^n + \cdots + a_1 p q^{n-1}$)

mult. di q $\Rightarrow$ a_n mult. di q

quindi anche $a_0 q^n$ è mult. di p $\Rightarrow$ a_0 è mult. di p, perché p e q^n sono primi fra loro

In $p(x)$, se $\frac{m}{n}$ è radice, m divide 1
n divide 1

Ma $p(1) \neq 0$ $p(-1) \neq 0$

$$x^5 + x^4 + 1 = (x^3 + \cdots)(x^2 + \cdots)$$

4

$$= (x^2 + x + 1)(x^3 - x + 1)$$

Ah, ma allora se $p(n)$ è primo

$n^2 + n + 1 = 1$ o -1 (1)

$n^3 - n + 1 = 1$ o -1 (2)

1) $n^2+n+1=1$ $\quad n=0 \circ n=-1$ $\quad p(n)=1 \circ -1$ $\boxed{no}$

$n^2+n+1=-1$ $\quad n^2+n+2=0$ $\quad$ n viene irrazionale $\boxed{no}$

$n^3-n+1=1$ $\quad n=0 \quad n=1 \quad n=-1$ $\quad n=1 \quad p(n)=3$

$n^3-n+1=-1$ $\quad n^2+n+1=p$ $\quad n=1$

$n^3-n+2=0$

$-np = n^3-n+2-np = n^3-n+2-n(n^2+n+1) = -n^2-2n+2$

... $\boxed{no}$