A- Polinomi a coefficienti interi

Titolo nota 01/09/2018

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

$p(a) \in \mathbb{Z}$ per ogni $a \in \mathbb{Z}$.

(⚠ occhio: anche $\frac{x(x-1)}{2}$ assume valori interi per ogni x intero)

<u>Oss</u>: se $a(x) \in \mathbb{Z}[x]$, $b(x) \in \mathbb{Z}[x]$ <u>monico</u>

<u>allora</u> $q(x)$, $r(x)$ della divisione sono a coeffic. interi.

<u>Lemma</u>: se $p(x) \in \mathbb{Z}[x]$, allora, per ogni a, b interi

(*) $b-a \mid p(b)-p(a)$.

<u>Dim</u>: Lo faccio innanzitutto per $p(x) = x^n$

Se $p(x) = x$ (*) diventa $b-a \mid b-a$ ovvio

se $p(x) = x^2$ (*) $b-a \mid b^2-a^2$ $\quad b^2-a^2 = (b-a)\underbrace{(b+a)}_{\in \mathbb{Z}}$

$p(x) = x^3$ $\quad b^3-a^3 = (b-a)\underbrace{(a^2+ab+b^2)}_{\in \mathbb{Z}}$

$b-a \mid b^n-a^n$ perché $b^n-a^n = (b-a)(b^{n-1}+b^{n-2}a+\ldots+ba^{n-2}+a^{n-1})$

$$p(b)-p(a) = \sum_{n=0}^{d} p_n b^n - \sum_{n=0}^{d} p_n a^n =$$

$$= \sum_{n=0}^{d} \underbrace{p_n}_{\in \mathbb{Z}} \underbrace{(b^n-a^n)}_{\text{multipli di } b-a} \qquad \square$$

ES: Dato un polinomio $p(x) \in \mathbb{Z}[x]$,
se $p(0)$ e $p(1)$ sono dispari, allora $p(n)$ è dispari per ogni $n \in \mathbb{Z}$.

dim: n pari: $\quad 2 \mid n-0 \mid p(n)-p(0) \quad$ $p(n)-p(0)$ pari, $p(0)$ dispari

n dispari: $\quad 2 \mid n-1 \mid p(n)-p(1) \quad \Rightarrow p(n)$ dispari

(In particolare, $p(x)$ non ha radici intere)

Rational root theorem:
Se $\frac{m}{n} \in \mathbb{Q}$ (m,n primi tra loro) è radice $a(x) \in \mathbb{Z}[x]$
$= a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d$ $\quad a_d \neq 0$, allora
$m \mid a_0$, $n \mid a_d$.

Dim:
$$0 = \left(a_0 + a_1 \frac{m}{n} + a_2 \frac{m^2}{n^2} + \dots + a_d \frac{m^d}{n^d}\right) n^d =$$
$$= a_0 n^d + a_1 m n^{d-1} + a_2 m^2 n^{d-2} + \dots + a_d m^d.$$

Tutti gli altri termini multipli di $n \Rightarrow$ ultimo term. multiplo di n
$n \mid a_d m^d \Rightarrow n \mid a_d$
$m \mid a_0 n^d \Rightarrow m \mid a_0$. $\square$

ES: cerco radici di $p(x) = 3x^4 + 4x^3 + 2x^2 + x + 5$
Se ha radici razionali, allora numeratori $= 1, 5$
denominatori $= 1, 3$

$\pm 1, \pm 5, \pm \frac{1}{3}, \pm \frac{5}{3}$

(Occhio: questo teorema non dice nulla su eventuali radici non razionali; ad es. $p(x)=x^2-2$ $\sqrt{2}$)

Lemma (Lemma di Gauss):

Se $\underset{\in \mathbb{Z}[x]}{c(x)} = \underset{\in \mathbb{Q}[x]}{a(x)}\, \underset{\in \mathbb{Q}[x]}{b(x)}$,

allora $\exists\, q \in \mathbb{Q}$ t.c. $q a(x)$, $\frac{1}{q} b(x) \in \mathbb{Z}[x]$.

ES: $x^2-4 = (3x+6)\left(\frac{1}{3}x - \frac{2}{3}\right)$ ⚠
$= (x+2)(x-2)$

Dim: $c(x) = a(x)b(x) = \frac{1}{A}\alpha(x)\, \frac{1}{B}\beta(x)$

ES. $\frac{1}{3}x^2 + \frac{1}{5}x = \underbrace{\frac{1}{15}}_{A}\underbrace{(5x^2+3x)}_{\alpha(x)}$

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

$p \mid AB$ primo

Vogliamo dimostrare che $p \mid \mathrm{mcd}(\alpha_i)$ oppure $p \mid \mathrm{mcd}(\beta_i)$

Per assurdo: $p \mid \alpha_0, \alpha_1 \dots \alpha_{k-1}$ $p \nmid \alpha_k$

$p \mid \beta_0, \beta_1, \dots \beta_{h-1}$ $p \nmid \beta_h$

Allora i coeff. di $\alpha(x)\beta(x)$

$\alpha(x)\beta(x) = \alpha_0\beta_0$
$+ (\alpha_1\beta_0 + \alpha_0\beta_1)x$

$$+(\alpha_2\beta_0+\alpha_1\beta_1+\alpha_0\beta_2)x^2$$
$$+(\alpha_3\beta_0+\alpha_2\beta_1+\alpha_1\beta_2+\alpha_0\beta_3)x^3$$
$$\vdots$$
$$+(\underbrace{\alpha_{k+h}\beta_0+\dots}_{\text{mult. di } p}+\underbrace{\alpha_k\beta_h}_{\substack{\not{p} \\ \text{non mult. di } p}}+\underbrace{\dots+\alpha_0\beta_{k+h}}_{\text{mult. di } p})x^{k+h}$$

$\Rightarrow$ un coeff. di $\alpha(x)\beta(x)$ non è mult. di p

$= \underbrace{AB}_{p}c(x)$ Assurdo!

$$\underbrace{\frac{AB}{p}c(x)}_{\in\mathbb{Z}[x]} = \underbrace{\frac{\alpha(x)}{p}}_{\in\mathbb{Z}[x]}\underbrace{\beta(x)}_{\in\mathbb{Z}[x]}$$

Posso ripetere il ragionamento finché lo elimino tutti i fattori di AB

$$\underbrace{c(x)}_{\in\mathbb{Z}[x]}=\underbrace{\alpha'(x)}_{\in\mathbb{Z}[x]}\underbrace{\beta'(x)}_{\in\mathbb{Z}[x]}.$$