$[a,b]$ $\{a,b\}$ $\{[a,b]\}$

WIMS ← CORRETTO

Algoritmo di divisione

$a,b \in \mathbb{Z}$ # in generale $q \in \mathbb{Z}$ $a = bq$ $\exists q \in \mathbb{Q} \supseteq \mathbb{Z}$

Approssimare "al meglio" a meno di multipli di b

ossia bq $q \in \mathbb{Z}$ tale che $|a - bq|$ minima possibile

$a = 347$ $b = 17$ Knuth Seminumerical Algorithms

$A = \mathbb{Z}, K[x]$

Sia $A = K[x]$ K campo A anello commutativo

Def Sia $a(x) = \sum_{i=0}^{n} a_i x^i$ Se $a \neq 0_A$ $a_n \neq 0_K$ ma $a_m = 0$ $m > n$

$n = \deg a$

$LT(a) = a_n x^n$ termine direttivo

$L((a) = a_n$ coefficiente n

Teorema (Algoritmo di Divisione Lunga)

Sia $a, b \in A = K[x]$ $b \neq 0_A$

1) $\exists q, r \in A$ $a = bq + r$ $(q := 0_A, r := a)$

2) $\deg r < \deg b$ (eventualmente $r = 0_A$ $\deg 0_A = -\infty < n$ $\forall n \in \mathbb{N}$)

Inoltre q, r sono unici. Pertanto QUOZIENTE, RESTO

Dim: $a_n = LC(a)$ $b_m = LC(b)$. Se $n < m$ $q = 0_A$ $r = a$

1. $a = b \cdot 0_A + a$ 2. $\deg r = \deg a = n <$ $\deg b = m$

Altrimenti: $n \geq m$ $a_n x^n + a_{n-1} x^{n-1} + \dots$ $b_m x^m + \dots$

$d = a_n b_m^{-1} x^{n-m} \in A$ $a - bd$ ha grado

n $m + n - m$

$a_n - b_m a_n b_m^{-1} = 0_K$ $LC(fg) = LC(f) LC(g)$

Per induzione sul grado di a $\quad \deg a = 0$ $\quad a = \begin{cases} bq \\ b\cdot 0_A + \underset{\| r}{a} \end{cases}$ $\quad \deg b = 0$ $\quad b \neq 0$ $\quad q = ab^{-1} = \frac{a}{b}$

$\deg b > 0$

$$\boxed{a - bd = b\tilde{q} + \tilde{r}} \qquad \deg \tilde{r} < \deg b \qquad q := d + \tilde{q} \qquad r := \tilde{r}$$

$$a = b(d + \tilde{q}) + \tilde{r}$$

□

Esempio: $a = \underset{\sqcup}{x}^4 + 3x^3 - 2x + 1 \qquad b = \underset{\sqcup}{x}^2 - 3x + 2$

$d_1 = x^2 \qquad a \longrightarrow a - bd = 0\cdot x^4 + (3+3)x^3 + (0-2)x^2 - 2x + 1$

$$= \underset{\sqcup}{6}x^3 - 2x^2 - 2x + 1 =: a_2$$

$-bd = -x^4 + 3x^3 - 2x^2$

$d_2 = 6x \qquad -bd_2 = -6x^3 + 18x^2 - 12x \qquad a_3 = a_2 - bd_2 = \underset{\sqcup}{16}x^2 - 14x + 1$

$d_3 = 16 \qquad -bd_3 = -16x^2 + 48x - 32 \qquad a_4 = a_3 - bd_3 = 34x - 31 = r$

$q = d + d_2 + d_3 = x^2 + 6x + 16 \qquad a = bq + r$

Unicità $\quad a = bq + r \qquad a = bq_1 + r_1 \qquad \deg r, r_1 < \deg b =: m$

$$b(q - q_1) + r - r_1 = 0_A \qquad b(q - q_1) = r_1 - r$$

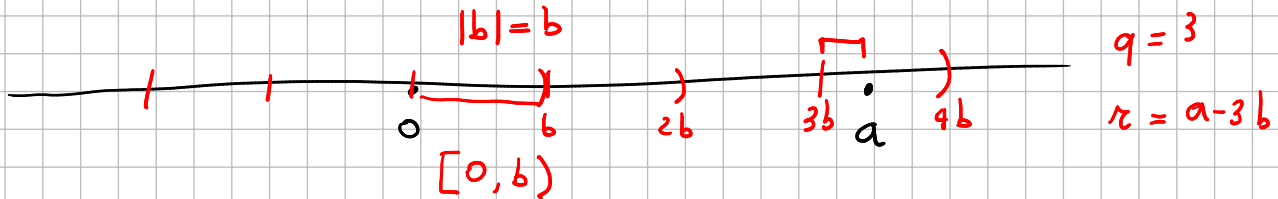
$\deg$ ↑ $< m$

$\deg b + \deg(q - q_1)$

m ↑ $\mathbb{N}$? No

$q - q_1 = 0_A \qquad q = q_1 \Longrightarrow r = r_1$

$A = \mathbb{Z}$ Pascal $\quad \mathbb{Z} \ni a, b \neq 0 \quad |a - bq|$ piccolo



$[0, b)$

Teorema (Algoritmo Divisione) Dati $a, b \in \mathbb{Z} \quad b \neq 0$

1) $\exists\, q, r \in \mathbb{Z} \qquad a = bq + r$

2) $0 \leq r < |b|$

Dim: Posso supporre che $b > 0 \qquad a = bq + r = (-b)(-q) + r$

$b > 0$. $\quad R = \{ a - bq : q \in \mathbb{Z} \} \cap \mathbb{N} \neq \emptyset \qquad \min R = r$

$r = a - bq$ $\quad a = bq + r$ $\quad 0 \le r$ $\quad$ Devo mostrare $r < b$

Se non fosse vero $\quad r \ge b \quad r - b \ge 0 \quad a = b(q+1) + r - b$

inoltre $r - b \ge 0$ e $\in \mathbb{R}$ essendo r è minimo $\quad r < b \quad \square$

In generale $\quad q = \left\lfloor \frac{a}{b} \right\rfloor$ parte intera

Def $\quad \alpha \in \mathbb{R} \quad \lfloor \alpha \rfloor = \max \{ k \in \mathbb{Z} : k \le \alpha \}$

$\lceil \alpha \rceil = \min \{ k \in \mathbb{Z} : k \ge \alpha \}$

Unicità $\quad \boxed{b(q - q_1) = r_1 - r} \quad 0 \le r \le r_1 < |b| \Rightarrow 0 \le r_1 - r < |b|$

$|$ $\quad$ $|$ $\quad$ $\wedge$

$|$ $\quad$ $|$ $\quad$ $|b|$

$\swarrow$ $|$

$|b|$

tranne $q - q_1 = 0 \quad q = q_1 \Rightarrow r_1 = r$

Algoritmi polinomiali, esponenziali, ibridi = subesponenziali

$n \qquad T = (\log_2 n)^k \qquad n^k = \exp(\log(n))^k \qquad \exp(\sqrt{\log n})$

M $\qquad$ $\downarrow$ costante

$n \in \mathbb{N}$

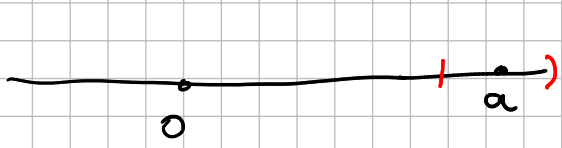
Problema: Quanto costa Alg. div. sui polinomi

dopo quanti passi otteniamo $\deg r < \deg b$?

$\deg b > \deg r \qquad a \quad a_2 \qquad\qquad n - m + 1$

$n \quad n-1$

Problema: $\quad a, b \in \mathbb{Z}$



$\boxed{q = \left\lfloor \frac{a}{b} \right\rfloor \approx a}$

esponenziale

Algoritmo Elementare è polinomiale $\sim T, M \approx \lceil \log_{10} a \rceil$

$10 \le \sqrt{\underset{\underset{n}{\shortparallel}}{191}} < 100$ è un numero decimale con 2 cifre $\quad ab.cd\ldots$

$(10a + b)^2 = n$

$100a^2 + 20ab + b^2 \qquad 100a^2 \approx n$