

$\mathbb{Z}$ $\mathbb{R}[x]$ $\mathbb{N}$

$$n = mq + r$$

in $\mathbb{N}$: $r < m$ in $\mathbb{Z}$: $|r| < |m|$ in $\mathbb{R}[x]$: $\deg(r) < \deg(m)$ Dati $m, n \in \begin{matrix} \mathbb{N} \\ \mathbb{Z} \\ \mathbb{R}[x] \end{matrix}$

~~DEF~~ In $\mathbb{Z}$, in $\mathbb{R}[x]$ chiamo **elementi unitari** questi elementi che hanno inverso rispetto al prodotto.

Esempi: in $\mathbb{Z}$ 1 e -1
in $\mathbb{R}[x]$ ogni costante non nulla

DEF - Dico che m **divide** n , che m è un **divisore** di n , che n è un **multiplo** di m se $|n| \geq |m|$ e $\deg(n) \geq \deg(m)$ e il resto della divisione $n = mq + r$ è nullo: $r = 0$

PROP- Per ogni $n \neq 0$ esso ha divisori α e αn , dove α è un elemento unitario.

Esempio: 5 ha divisori $\pm 1, \pm 5$
 x " " " x

α α π

↑ ↗

cast to int $\neq$ 0

DEF - h , elemento non unitario, si dice ^{primo} irriducibile se i suoi unici divisori sono α e αh (α el. unitaria) cioè solo i divisori banali.

DEF - Un polinomio si dice **monico** se il coefficiente del termine di grado massimo è 1.

TEOR - Qualunque sia n , elemento non unitario, esiste esattamente un modo unico (a meno dell'ordine) di scrivere n come

$$n = \alpha \cdot m_1 \cdot \dots \cdot m_k$$

dove α è un elemento unitario e gli
 m_i sono interi primi positivi
polinomi irriducibili monici

DEF - Dati m ed n , un massimo comune
divisore di m ed n è:
1) un divisore d comune di m ed n , tale che
2) se d' è divisore comune di m ed n , allora
 d' è anche divisore di d .

OSS - Un massimo comune divisore è
definito a meno del prodotto con
un elemento unitario.

Per trovare un MCD potremmo usare il solito metodo che fa ricorso alla fattorizzazione in fattori primi irriducibili

Invece: metodo delle divisioni successive

Dati m, n , con $|n| \geq |m|$
 $q_1(n) \geq q_2(m)$

Se $r_1 \neq 0$

Se $r_2 \neq 0$

$$n = m q_1 + r_1$$

$$m = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$\vdots$

$$r_{k-2} = r_{k-1} q_k + r_k$$

$$r_{k-1} = r_k q_{k+1}$$

Allora $MCD(n, m) = d = r_k$

o algoritmo euclideo

$n = m q_1 + r_1$
 $m = r_1 q_2 + r_2$
 $r_1 = r_2 q_3 + r_3$
 $\vdots$
 $r_{k-2} = r_{k-1} q_k + r_k$
 $r_{k-1} = r_k q_{k+1} + r_{k+1}$

allora d è divisore comune di m ed n
 allora divide r_1 ed m
 allora divide r_1 ed r_2

$\uparrow$
 allora divide r_{k-1} ed r_{k-2}

$\uparrow$
 d divide r_k (se stessa) ed r_{k-1}

$n = m q_1 + r_1$ Sia d che divide m ed n
 allora divide $r_1 = n - m q_1$
 $m = r_1 q_2 + r_2$ ed r_1
 allora divide $r_2 = m - r_1 q_2$
 $r_1 = r_2 q_3 + r_3$ r_1 ed r_2
 allora divide $r_3 = r_1 - r_2 q_3$
 $\vdots$
 $r_{k-2} = r_{k-1} q_k + r_k$ r_{k-2} ed r_{k-1}
 allora divide $r_k = r_{k-2} - r_{k-1} q_k$

$$r_{k-1} = r_k q_{k+1}$$

allora
 divide r_{k-1} ed r_k
 r_k

$$\text{gcd}(286, 195) = 13$$

$$\begin{array}{r} 286 \\ 91 \end{array}$$

$$195$$

$$13$$

$$\begin{array}{r} 91 \\ 00 \end{array}$$

$$\begin{array}{r} 195 \\ 1 \end{array}$$

$$\begin{array}{r} 91 \\ 2 \end{array}$$

$$\begin{array}{r} 13 \\ 7 \end{array}$$

$$\begin{array}{r} x^5 + 2x^4 + 5x^3 + x^2 + 2x + 5 \\ -x^5 - 2x^4 - 3x^3 + 4x^2 + 10x \\ \hline \end{array}$$

$$\begin{array}{r} x^4 + 2x^3 + 3x^2 - 4x - 10 \\ \hline x \end{array}$$

$$\begin{array}{r} // \quad // \quad 2x^3 + 5x^2 + 12x + 5 \\ x^4 + 2x^3 + 3x^2 - 4x - 10 \\ -x^4 - \frac{5}{2}x^3 - 6x^2 - \frac{5}{2}x \\ \hline \end{array}$$

$$\begin{array}{r} 2x^3 + 5x^2 + 12x + 5 \\ \hline \frac{x}{2} - \frac{1}{4} \end{array}$$

Dovrei dividere per

$$\begin{array}{r} // \quad -\frac{1}{2}x^3 - 3x^2 - \frac{13}{2}x - 10 \\ +\frac{1}{2}x^3 + \frac{5}{4}x^2 + 3x + \frac{5}{4} \\ \hline \end{array}$$

Invece:

$$\begin{array}{r} 2x^3 + 5x^2 + 12x + 5 \\ -2x^3 - 4x^2 - 10x \\ \hline \end{array} \quad \begin{array}{r} x^2 + 2x + 5 \\ \hline 2x + 1 \end{array}$$

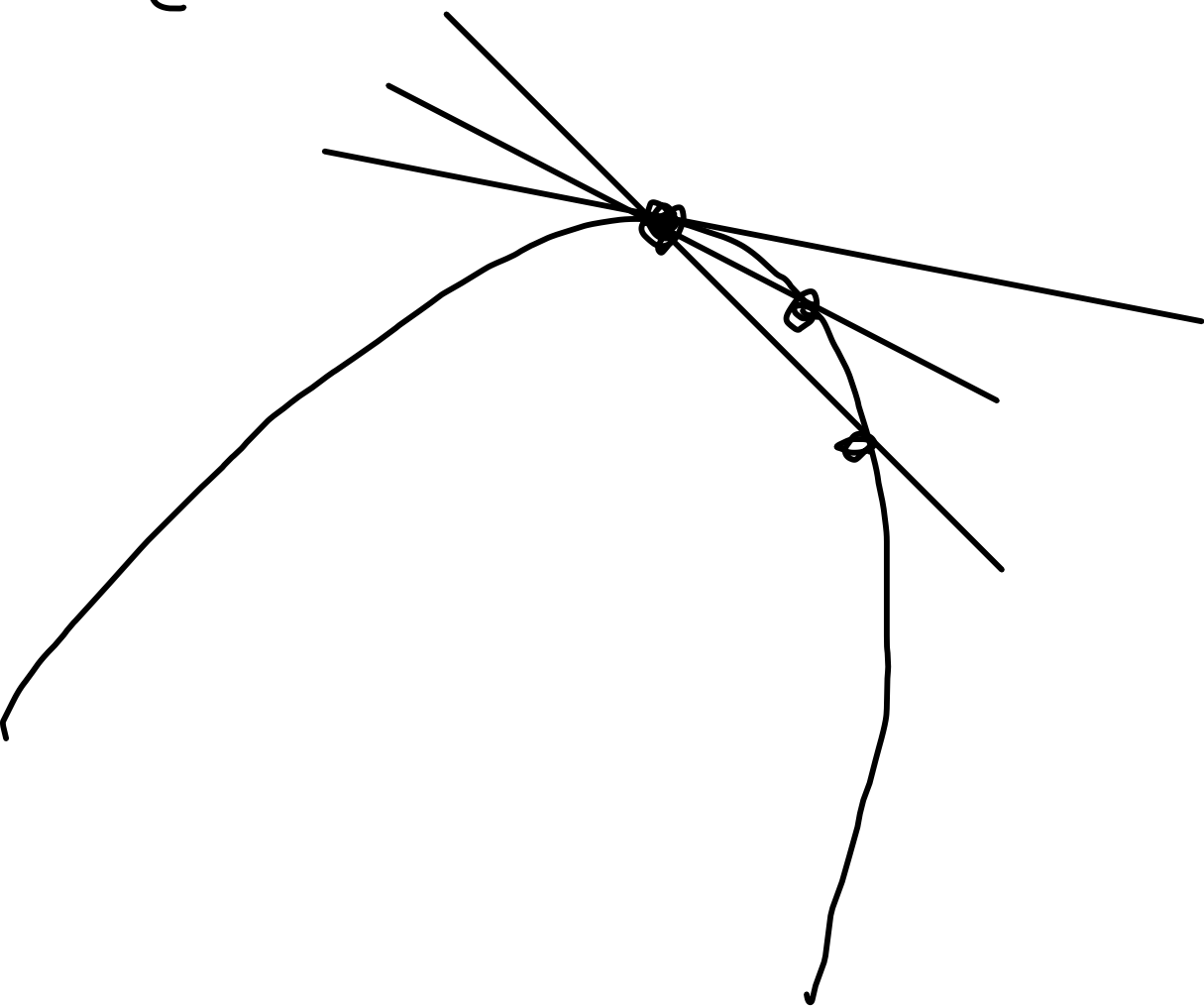
$$\begin{array}{r} // \quad x^2 + 2x + 5 \\ -x^2 - 2x - 5 \\ \hline 0 \end{array} = \text{MCD}$$

$$\begin{array}{r} // \quad -\frac{7}{4}x^2 - \frac{7}{2}x - \frac{35}{4} \\ -\frac{4}{7} \cdot (x^2 + 2x + 5) \\ \hline \end{array}$$

$$x - 3 = 0$$

$$x^2 - 6x + 9 = 0$$

$$(x - 3)^2$$



$$x^2 - 5.9x + 9.03 = 0$$

Discriminante di

$$f(x) = a_0 x^n + \dots$$

Basta fare il risultante di

$$f(x) = 0 \quad \text{ed} \quad f'(x) = 0$$

Scorciatoia, invece di $f(x)$ uso la comb. lin.

$$\begin{aligned} \varphi(x) &= n f(x) - x f'(x) = n \left(a_0 x^n + a_1 x^{n-1} + \dots \right) \\ &\quad - x \left(n a_0 x^{n-1} + (n-1) a_1 x^{n-2} \dots \right) \end{aligned}$$

$$= \underline{(n a_0 x^n - x \cdot n a_0 x^{n-1})}$$

$$f(x) = ax^2 + bx + c$$

$$a \neq 0$$

$$f'(x) = 2ax + b$$

$$q(x) = 2f - xf' = 2ax^2 + 2bx + 2c - 2ax^2 - bx$$

$$= // \quad bx + 2c$$

Usa Euler per

$q(x)$ ed $f'(x)$

$$\begin{vmatrix} b & 2c \\ 2a & b \end{vmatrix} = b^2 - 4ac$$