Polinomio <u>monico</u>: il coefficiente del grado massimo è 1.

In un anello si chiamano <u>unitari</u> gli elementi invertibili rispetto al prodotto.

in $\mathbb{Z}$: $-1, 1$

in $\mathbb{R}[x]$: tutte le costanti non nulle

in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$: tutti tranne 0

n, m interi / polinomi

Divisione con resto: dati n, m con $|n| \geq |m|$ / $\operatorname{gr} n \geq \operatorname{gr} m$

$\exists\, q, r$ con $|r| < |m|$ / $\operatorname{gr} r < \operatorname{gr} m$ tali che

quoziente (q), resto (r)

$n = m \cdot q + r$

Se $r = 0$, allora diciamo che m __divide__ n, che m è __un divisore__ di n, che n è un __multiplo__ di m.

TEOR - Ogni intero / polinomio è divisibile per ogni elemento unitario e per se stesso moltiplicato per un elemento unitario. Questi sono detti i suoi <u>divisori banali</u>

$\mathbb{Z}$ $\quad 5$ è divisibile per $1, -1, 5, -5$

$\mathbb{R}[x]$ $\quad x^2-3$ è divisibile per $\alpha \neq 0$ e per

$$\underset{\neq 0}{\alpha} \cdot (x^2-3)$$

$$x^2 - 3 = 5 \cdot \left(\frac{1}{5}x^2 - \frac{3}{5}\right)$$

$$\parallel$$

$$\frac{1}{5}\left(x^2 - 3\right)$$

$$7 = 1 \cdot 7$$

$$= (-1)(-7)$$

Un intero / polinomio diverso da 0 e da 1 si dice primo / irriducibile se ha solo i divisori banali

---

TEOR - Dato un qualunque intero / polinomio $n \neq 0, 1$,

$\exists!$ α unitario, $p_1, \dots, p_k$ primi >0 / irriducibili monici per cui

$$n = \alpha \cdot p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

Esempi:

$$-6 = (-1)\cdot 2\cdot 3$$

$$6x^2 - 3 = 6\cdot\left(x+\frac{1}{\sqrt{2}}\right)\left(x-\frac{1}{\sqrt{2}}\right)$$

Dati n, m interi polinomi chiamo MCD massimo comun divisore un intero polinomio d tale che:

1) d sia divisore di n e di m
2) se d' è un divisore di n e di m, allora d' è divisore di d.

Metodo delle divisioni successive

Trovo $n = m \cdot q_1 + r_1$

$m = r_1 \cdot q_2 + r_2$

$r_1 = r_2 \cdot q_3 + r_3$

$\vdots$

$r_k = r_{k+1} \cdot q_{k+2} + r_{k+2}$

$r_{k+1} = r_{k+2} \cdot q_{k+3}$

$\rightarrow$ MCD è (a meno di elementi unitari) $d = r_{k+2}$

$d = q_{k+2}$

$$n = m \cdot q_1 + r_1$$

divide m e divide n

$$m = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

e così via divide

perciò anche r_1

$\vdots$

$$r_k = r_{k+1} \cdot q_{k+2} + r_{k+2}$$

$$r_{k+1} = r_{k+2} \cdot q_{k+3}$$

divide allora divide perciò anche

Sia d' divisore comune di m e di n. Allora

$$n = m \cdot q_1 + r_1 \qquad\qquad n - m q_1 = r_1$$

divide anche

$$m = r_1 \cdot q_2 + r_2 \qquad\qquad m - r_1 q_2 = r_2$$

divide anche

$$r_1 = r_2 \cdot q_3 + r_3$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$r_k = r_{k+1} \cdot q_{k+2} + r_{k+2} \qquad\qquad r_k - r_{k+1} q_{k+2} = r_{k+2}$$

anche

$$r_{k+1} = r_{k+2} \cdot q_{k+3}$$

Buono a sapersi:

TEOR - Polinomio $a_0 + a_1 x + \dots + a_n x^n$ a coefficienti interi. $a_0 \neq 0$, $a_n \neq 0$ SE ci sono radici razionali, esse sono della forma $\frac{p}{q}$, dove p è divisore di a_0 e q è divisore di a_n

$5x^3-4x^2+11x-2=0$

SE ci sono radici razionali, esse sono nella lista $\pm 1, \pm \frac{1}{5}, \pm 2, \pm \frac{2}{5}$

Estensione a coefficienti razionali

$7x^3-\frac{1}{2}x^2+\frac{3}{4}x-1=0$

Le soluzioni sono le stesse di

$28x^3-2x^2+3x-4=0$ SE ci sono sol. razionali, sono nella lista $\pm 1, \pm 2, \pm 4, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{7}, \pm \frac{1}{28}, \pm \frac{1}{14}$