

Non vale il Teorema di divisione euclidea in $\mathbb{Z}[X]$.

Infatti, dati due polinomi $a(X), b(X) \in \mathbb{Z}[X]$, con $b(X) \neq 0$, il quoziente $q(X)$ ed il resto $r(X)$ della divisione euclidea di $a(X)$ per $b(X)$ in $\mathbb{Q}[X]$ possono non appartenere a $\mathbb{Z}[X]$. Data la loro unicità, non esisteranno in tal caso in $\mathbb{Z}[X]$ un quoziente ed un resto verificanti le condizioni (i) e (ii) del Teorema di divisione euclidea. Un esempio è il seguente:

$$a(X) = X, \quad b(X) = 2X + 1.$$

In questo caso, il quoziente è $q(X) = \frac{1}{2}$ e il resto è $-\frac{1}{2}$. Nessuno dei due è un polinomio a coefficienti interi.

Si può però provare che quoziente e resto appartengono certamente a $\mathbb{Z}[X]$ se il divisore $b(X)$ è monico. Se il dividendo $a(X)$ è nullo, l'affermazione è banale, essendo in tal caso quoziente e resto a loro volta nulli. Supponendo che $a(X)$ sia non nullo, la dimostrazione

procede per induzione su $d = \deg(a)$. Siano $a(X) = \sum_{i=0}^d a_i X^i$ e $b(X) = \sum_{i=0}^e b_i X^i$, con

$a_i, b_i \in \mathbb{Z}$, $b_e = 1$. Se $e > d$, allora il quoziente è il polinomio nullo e il resto è il polinomio $a(X)$ stesso. Supponiamo allora che sia $e \leq d$. Consideriamo il polinomio $a'(X) = a(X) - a_d X^{d-e} b(X) \in \mathbb{Z}[X]$. Allora $a'(X) = 0$, oppure $\deg(a') < d$. Quindi per $a'(X)$ vale la tesi, banalmente oppure in virtù dell'ipotesi induttiva. Siano $q'(X)$ e $r'(X)$ il quoziente e il resto della divisione di $a'(X)$ per $b(X)$, entrambi appartenenti a $\mathbb{Z}[X]$. Risulta allora che $r'(X) = 0$ oppure $r'(X) \neq 0$ e $\deg(r') < \deg(b)$. Inoltre si ha:

$$a(X) = a'(X) + a_d X^{d-e} b(X) = q'(X) b(X) + r'(X) + a_d X^{d-e} b(X) = (q'(X) + a_d X^{d-e}) b(X) + r'(X).$$

Quindi il quoziente e il resto della divisione di $a(X)$ per $b(X)$ sono $q(X) = q'(X) + a_d X^{d-e}$ e $r(X) = r'(X)$, entrambi appartenenti a $\mathbb{Z}[X]$.