Il metodo di Kronecker per fattorizzare polinomi a coefficienti interi

Dato un polinomio di $\mathbb{Q}[x]$ di grado positivo, vogliamo vedere un primo modo per ottenere la sua scomposizione in fattori irriducibili. Innanzitutto si può (moltiplicando opportunamente il polinomio f per un numero razionale) ottenere da esso un polinomio primitivo $f \in \mathbb{Z}[x]$ e si può quindi cercare la fattorizzazione di f in $\mathbb{Z}[x]$. Un'osservazione sugli eventuali fattori di f: sia f di grado n; se f non è irriducibile, si spezzerà in un prodotto di due polinomi g e h di gradi positivi e uno dei due polinomi dovrà avere grado minore o uguale a d, dove $d = \lfloor n/2 \rfloor$ (se tutti e due avessero grado maggiore di d, allora il loro prodotto avrebbe grado maggiore di n). Assumiamo che sia g il polinomio di grado minore o uguale a d. L'idea che si segue è la seguente: Se $f(x) = g(x) \cdot h(x)$, allora per ogni $n \in \mathbb{Z}$, $f(n)$ si fattorizza nel prodotto $g(n) \cdot h(n)$. I polinomi $g(x)$ e $h(x)$ non sono noti (una volta trovati, avremmo, almeno parzialmente, risolto il problema di fattorizzare f), però questa osservazione ci dice che, preso un qualunque $n \in \mathbb{Z}$, il polinomio g, valutato in n, deve essere un divisore di $f(n)$, quindi ha solo un numero finito di possibilità. Inoltre, se scriviamo $g = b_0 + b_1 x + \cdots + b_d x^d$ (dove $b_0, b_1, \ldots, b_d$ sono da determinare), $g(n) = b_0 + b_1 n + \cdots + b_d n^d$. Se dunque $D(n)$ è l'insieme di tutti i (finiti) divisori di $f(n)$, $g(n)$ dovrà essere uno di questi, chiamiamolo δ, pertanto i coefficienti $b_0, \ldots, b_n$ dovranno soddisfare all'equazione lineare $b_0 + b_1 n + \cdots + b_d n^d = \delta$. Questa è un'equazione lineare in $d+1$ incognite, quindi non può determinare del tutto i valori delle incognite, però possiamo ripetere il procedimento con più valori: se scegliamo $d+1$ interi distinti $n_0, n_1, \ldots, n_d$, calcoliamo gli insiemi $D(n_0), \ldots, D(n_d)$ di tutti i divisori di, rispettivamente, $f(n_0), \ldots, f(n_d)$ e prendiamo $\delta_i \in D(n_i)$ $(i = 0, \ldots, d)$ possiamo costruire il sistema lineare:

$$\begin{cases} b_0 + b_1 n_0 + \cdots + b_d n_0^d &= \delta_0 \\ b_0 + b_1 n_1 + \cdots + b_d n_1^d &= \delta_1 \\ \cdots & \\ b_0 + b_1 n_d + \cdots + b_d n_d^d &= \delta_d \end{cases}$$

che ha un'unica soluzione, la quale dà un polinomio g (di grado al più d). Facendo variare i divisori $\delta_0, \ldots, \delta_d$ in tutti i modi possibili, si ottiene un numero finito di polinomi $g_1, \ldots, g_k$. Se f si fattorizza (cioè se f è riducibile), un suo fattore deve essere tra i polinomi $g_1, \ldots, g_k$. Decidere quale è quello corretto può essere fatto facilmente, usando l'algoritmo di divisione. Naturalmente, se nessuno dei polinomi $g_1, \ldots, g_k$ divide f, significa che f è irriducibile. Il procedimento può essere iterato, trovando così la completa fattorizzazione di f in fattori irriducibili.

Questo metodo è detto metodo di Kronecker. Al lato pratico, è pressoché inutilizzabile, perché il numero di sistemi lineari da risolvere diventa spesso estremamente grande, però dal metodo di Kronecker un risultato teorico segue immediatamente:

Teorema. La scomposizione in fattori irriducibili di un polinomio di $\mathbb{Q}[x]$ (di $\mathbb{Z}[x]$) può essere trovata in un numero finito di passi.