Кронекеров алгоритам

Према Гаусовој леми, полином са целим коефицијентима је растављив на производ два полинома степена барем један са рационалним коефицијентима ако и само ако је растављив на производ два полинома степена барем један са целим коефицијентима. Кронекеровим алгоритмом се утврђује да ли је дати полином са целим коефицијентима растављив на производ два полинома степена барем један са целим коефицијентима.

Нека је на улазу у алгоритам дат полином степена барем два. Најпре треба потражити његове рационалне корене, па га раставити на чиниоце степена барем један, при чему чиниоци степена барем два немају рационалних корена. Рецимо, ако је $\frac{p}{q}$ један од рационалних корена датог полинома степена барем један са целобројним коефицијентима, где је $p \in \mathbb{Z}$ и $q \in \mathbb{N}$, онда је дати полином дељив полиномом $qx - p$, при чему количник има целобројне коефицијенте. Тиме се проблем факторизације полинома са целим коефицијентима своди на случај полинома са целобројним коефицијентима.

Нека је $P(x) = a_k x^k + \cdots + a_0$ полином степена бар два са целобројним коефицијентима, где је $a_k \neq 0$. Нека су $Q(x) = b^m x^m + \cdots + b_0$ и $R(x) = c^n x^n + \cdots + c_0$ полиноми степена барем један са целобројним коефицијентима такви да је $b_m, c_n \neq 0$ и да је $P(x) = Q(x)R(x)$. Одатле је наравно $m + n = k$. На основу претходног, можемо још претпоставити да полином $P(x)$ нема целобројних нула. Такође, без умањења општости можемо узети да је $m \leq n$.

Изаберимо било које међусобно различите целе бројеве $x_0, \ldots, x_m$. Тада су $P(x_i) = y_i$, као и $Q(x_i) = u_i$ и $R(x_i) = v_i$ цели бројеви. Такође је $y_i \neq 0$ јер по претпоставци полином $P(x)$ нема целобројних корена. Међутим, пошто је $P(x) = Q(x)R(x)$ за свако x, стављајући x_i уместо x, добијамо да је $u_i v_i = y_i$. Али, пошто је y_i цео број различит од нуле, он има коначно много растављања на производ два цела броја. Нека су $r_1 s_1, \ldots, r_{n_i} s_{n_i}$ сва растављања броја y_i на производ два цела броја. Тада за неко $k_i \leq n_i$ важи $u_i = r_{k_i}$ и $v_i = s_{k_i}$. Другим речима, постоји функција f чији је домен скуп $\{0, \ldots, m\}$ и за коју је $f(i) \in \{1, \ldots, n_i\}$ и $Q(x_i) = r_{f(i)}$ и $R(x_i) = s_{f(i)}$ за све i из домена.

Дакле, када испитујемо дали дати полином $P(x)$ степена барем два са целобројним коефицијентима може да се прикаже као производ два полинома са целобројних степена, при чему је један од њих степена $m \geq 2$, а други степена не мањег од m, најпре бирамо различите целе бројеве $x_0, \ldots, x_m$, потом израчунавамо вредности $y_i = P(x_i)$, затим сваку од вредности y_i растављамо на производ два цела броја на све могуће начине $r_1 s_1, \ldots, r_{n_i} s_{n_i} = y_i$, а онда за сваку[1] функцију f чији је домен скуп $\{0, \ldots, m\}$ за коју је $f(i) \in \{1, \ldots, n_i\}$ за свако i из домена функције f израчунавамо интерполациони полином $Q(x)$ не већег степена од m који пролази кроз систем чворова $(x_i, r_{f(i)})$. Уколико тај полином има целе коефицијенте и дели полином $P(x)$, онда смо добили једно растављање полинома $P(x)$ на производ два полинома степена барем један са целобројнијм коефицијентима. Уколико то није случај нити за једну од коначно много функција f које долазе у обзир, онда се полином $P(x)$ не може приказати као производ два полинома са целобројним коефицијентима, при чему је један од њих степена m, а други степена на мањег од m.

Полином степена 1 је увек нерастављив. Полином степена 2 или 3 са целим коефицијентима је нерастављив над прстеном целих бројева ако и само ако нема рационалних корена. Полином степена $k \geq 4$ са целобројним коефицијентима је нерастављив над прстеном целих бројева ако и само ако нема рационалних корена и не може се приказати као производ два полинома од којих један има степен $2 \leq m \leq k - 2$, а други степен који није мањи од m.

Галоаова група полинома са рационалним коефицијентима је такође алгоритамски израчунљива (до на изоморфизам). Такође, постоји алгоритам који за дату алгебарску једначину степена барем један са рационалним коефицијентима налази у радикалима сва њена решења која се могу изразити у радикалима, као и за рачунање са алгебарским бројевима у апсолутној тачности.

[1] Таквих функција има $n_0 \cdots n_m$, то јест коначно много.