ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 21 МАТЕМАТИКИ Выпуск 2
2014

К. Д. Жуков (Москва, ТВП)**. Вычисление результанта многочленов над коммутативным кольцом с единицей и без делителей нуля.**

Пусть $a(x)=\sum_{i=0}^{n}a_ix^i$ и $b(x)=\sum_{i=0}^{m}b_ix^i$, $n\geqslant m$, — многочлены над коммутативным кольцом с единицей и без делителей нуля. Результантом многочленов и $a(x)$ и $b(x)$ называется определитель матрицы Сильвестра размером $(n+m)\times(n+m)$:

$$R(a,b)=\begin{vmatrix} a_n & \dots\dots & a_0 & \dots & 0 \\ & \ddots & & \ddots & \\ 0 & \dots & a_n & \dots\dots & a_0 \\ b_m & \dots\dots & b_0 & \dots & 0 \\ & \ddots & & \ddots & \\ 0 & \dots & b_m & \dots\dots & b_0 \end{vmatrix}. \tag{1}$$

Алгоритмы вычисления результантов имеют важное практическое значение. Они, например, дают общий метод решения систем полиномиальных уравнений от нескольких переменных.

Наиболее эффективный метод вычисления результантов носит название алгоритм Субрезультант (см. [1]). В основе данного алгоритма лежит следующая теорема.

Теорема (Габихт). *В последовательности полиномиальных остатков* $u_1(x)$, $u_2(x),\dots,$ *получаемых по правилам* (2)–(4), *все операции деления* (4) *корректны*:

$$u_1(x)=a(x),\quad u_2(x)=b(x), \tag{2}$$

$$u_j'(x)=g_{j-1}^{\delta_{j-2}+1}u_{j-2}(x)-u_{j-1}(x)\,q_{j-2}(x),\quad j=3,4,\dots, \tag{3}$$

$$u_j(x)=\frac{u_j'(x)}{g_{j-2}\,h_{j-2}^{\delta_{j-2}}},\quad j=3,4,\dots, \tag{4}$$

где равенство (4) *задается псевдоделением полиномов с остатком* (*см.* [1], *алгоритм* 3.1.2), $\delta_j=\deg(u_j)-\deg(u_{j+1})$ *для* $j=1,2,\dots$, $g_1=1$, $g_j=\mathrm{lc}(u_j)$ *— старший коэффициент* $u_j(x)$ *при* $j=2,3,\dots$, $h_1=1$, $h_j=h_{j-1}^{1-\delta_{j-1}}g_j^{\delta_{j-1}}$ *при* $j=2,3,\dots$

Ниже приводится схема доказательства теоремы с использованием Гауссова исключения для вычисления определителя (1). Алгоритм Субрезультант рассматривается как приведение матрицы к треугольному виду с помощью алгоритма Барейсса [3], адаптированного для матрицы специального вида. Такой подход дополняет схему доказательства, предложенную в [2].

С доказательством теоремы, не использующим Гауссово исключение для вычисления определителя (1), можно ознакомиться в [4] (метод Сильвестра–Габихта).

Для примера рассмотрим первые четыре члена последовательности полиномиальных остатков, а именно, многочлены $a(x)$, $b(x)$, $c(x)$ и $d(x)$, где $c(x)=b_m^{n-m+1}a(x)-$

$q(x)b(x) = \sum_{i=0}^{l} c_i x^i$ и $d(x) = c_l^{m-l+1} b(x) - p(x)c(x) = \sum_{i=0}^{k} d_i x^i$.

Приведем определитель (1) к верхнетреугольному виду. Для этого переставим строки в (1) так, чтобы вначале располагались $n-m+1$ строк из коэффициентов многочлена $b(x)$, вслед за этим $m-l+1$ строк из коэффициентов $a(x)$ и затем снова $(m-l-1)+(l-k+1)$ строк из коэффициентов $b(x)$:

$$\begin{vmatrix} b_m & \dots & b_0 & \dots & 0 \\ & \ddots & & \ddots & \\ 0 & \dots & b_m & \dots & b_0 \\ a_n & \dots & \dots & a_0 & \dots \\ & \ddots & & & \ddots \\ 0 & \dots & a_n & \dots & a_0 \end{vmatrix} = \begin{vmatrix} b_m & \dots & b_0 & \dots & 0 \\ & \ddots & & \ddots & \\ 0 & \dots & b_m & \dots & b_0 \\ 0 & \dots & c_l & \dots & c_0 \\ & & & \ddots & \ddots \\ 0 & \dots & \dots & c_l & c_0 \end{vmatrix} \Big/ b_m^{(n-m+1)(m-l+1)}.$$

Далее, сдвинем блок строк с коэффициентами $c(x)$ на $m-l-1$ позиций вниз, а на освободившееся место вставим $m-l-1$ строк с коэффициентами $b(x)$, взятых из нижнего блока.

Обозначим через M минор левой матрицы, стоящий в первых $n+m-2l+2$ строках, в первых $n+m-2l+1$ столбцах и столбце с номером $n+m-l-k+1$, и заметим, что он равен:

$$M = \begin{vmatrix} b_m & \dots & b_0 & \dots & 0 \\ & \ddots & & \ddots & \\ 0 & \dots & b_m & \dots & b_0 \\ 0 & \dots & c_l & \dots & c_0 \\ & & & \ddots & \\ 0 & \dots & \dots & c_l & c_{l-1} \\ 0 & \dots & \dots & \dots & d_k \end{vmatrix} \Big/ (b_m^{(n-m+1)(m-l+1)} c_l^{m-l+1}).$$

Учитывая, что определитель верхнетреугольной матрицы равен произведению диагональных элементов, получаем равенство

$$M = \frac{b_m^{n-l} c_l^{m-l+1} d_k}{b_m^{(n-m+1)(m-l+1)} c_l^{m-l+1}} = \frac{d_k}{b_m^{(m-l)(n-m)+1}},$$

и, значит, d_k делится на $b_m^{(m-l)(n-m)+1}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Cohen H.* A Course in Computational Algebraic Number Theory. Heidelberg etc.: Springer, 2000.
2. *Кнут Д. Э.* Искусство программирования. Т. 2. М.: Вильямс, 2001.
3. *Bareiss E. H.* Sylvester's identity and multistep integer-preserving Gaussian elimination. — Math. Comput., 1968, v. 22, с. 565–578.
4. *Акритас А.* Основы компьютерной алгебры с приложениями. М.: Мир, 1994.