К МОДУЛЯРНЫМ ВЫЧИСЛЕНИЯМ В КОЛЬЦАХ ПОЛИНОМОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

© В.Н. Казаков

Kazakov V.N. On modulus calculations in circles of polynomials from several variables.

В предыдущей работе [1] предложен способ организации модулярных вычислений, позволяющий повысить скорость вычислений за счет проведения предварительных подготовительных вычислений. Эти результаты могут применяться для модулярных вычислений в кольце целых чисел и в кольце полиномов.

В настоящей работе обсуждается поход к применению модулярных вычислений в кольце полиномов нескольких переменных $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ и в матрицах над ними.

Обозначим переменные $(x_1, x_2, \ldots, x_n) = X_n$ и введем некоторый порядок на этих переменных. Тогда любой полином $f(x_1, x_2, \ldots, x_n) = f(X_n)$ можно представить как полином от старшей переменной x_n с коэффициентами $\alpha_i(X_{n-1})$, зависящими от остальных переменных

$$f(X_n) = \alpha_1(X_{n-1})x_n^m + \alpha_2(X_{n-1})x_n^{m-1} + \cdots \alpha_{m-1}(X_{n-1})x_n + \alpha_m(X_{n-1}).$$

Определим норму полинома $\|f(X_n)\| = \sqrt{\sum_{i=0}^{k} \lambda_i^2}$,

где λ_i – числовые коэффициенты полинома f.

Тогда для матрицы полиномов A

$$\begin{pmatrix} \alpha_{11}(X_{n-1}) & \alpha_{12}(X_{n-1}) & \cdots & \alpha_{1m}(X_{n-1}) \\ \alpha_{21}(X_{n-1}) & \alpha_{22}(X_{n-1}) & \cdots & \alpha_{2m}(X_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1}(X_{n-1}) & \alpha_{m2}(X_{n-1}) & \cdots & \alpha_{mm}(X_{n-1}) \end{pmatrix}$$

можно оценить определитель, используя неравенство Адамара. Верхняя оценка для нормы определителя будет

$$\alpha = \sqrt{\prod_{i=0}^{n}\left(\sum_{j=0}^{n}\left(\|\alpha_{ij}(X_{n-1})\|\right)^2\right)}.$$

Отсюда следует неравенство для нахождения количества простых модулей p_i, которые требуются по китайской теореме об остатках для восстановления определителя матрицы:

$$2^*\alpha \le \prod_{i=0}^{n} p_i.$$

В остальном, случай многих переменных аналогичен случаю одной переменной. Поэтому можно использовать подход, который предложен в [1].

Стоит заметить, что указанная верхняя оценка достигается редко. Поэтому экспериментальным или теоретическим путем можно найти наиболее вероятное число простых модулей для восстановления результата вычислений. После восстановления с использованием этого числа простых модулей нужно делать проверку результата подстановкой. Если проверка показала, что решение не получено, то добавляется следующий простой модуль. Выполняется следующее восстановление и проверка, и так далее, пока не будет получено решение.

ЛИТЕРАТУРА

1. *Казаков В.Н.* Препроцессинг в модулярных алгоритмах // Вестн. Тамб. ун-та. Сер. Естеств. и техн. науки. Тамбов, 2006.Т. 11. № 4.
2. *Малашонок Г.И.* Матричные методы вычислений в коммутативных кольцах. Тамбов: Изд-во ТГУ им. Г. Р. Державина, 2002.

БЛАГОДАРНОСТИ: Работа частично поддержана грантом РФФИ 04-07-90268б.

Поступила в редакцию 19 октября 2006 г.