НЕКОТОРЫЕ ЗАДАЧИ В МОДУЛЯХ НАД КОММУТАТИВНЫМИ КОЛЬЦАМИ

© Г.И. Малашонок

Аннотация

G.I.Malaschonok. Some problems in the modules over commutative rings. There is stated a theorem about the solutions of the linear equations systems over a commutative domain that are obtained in the domain and in the field of fractions. Two algorithms are described for rings of principal ideals with zero devisors: an algorithm for computing the characteristic polynomials and an algorithm for computing adjoint matrices. Both algorithms have complexity $O(n^3)$ ring operations. There are discussed the using of modular method for solving problems in Euclidean domain.

О РЕШЕНИИ ЛИНЕЙНЫХ СИСТЕМ В КОММУТАТИВНЫХ ОБЛАСТЯХ

Известен уже не один алгоритм решения линейных систем в поле частных коммутативной области (см. обзор в [1] и [2]). Однако нет алгоритма, позволяющего находить решения линейной системы в любой коммутативной области.

В работе [3] описан метод решения линейных систем для случая коммутативного кольца главных идеалов. Сложность этого метода – $O(n^\beta)$ кольцевых мультипликативных операций (такая же, как и сложность матричного умножения). Этод метод позволяет построить наиболее быстрый из известных методов решения систем линейных диофантовых уравнений со сложностью $O(n^3)$ бит операций для квазиквадратных систем и $O(mn^{\beta+1})$ для прямоугольных $n \times m$ систем. Оценки приведены с точностью до логарифмического множителя.

Следующая теорема позволяет свести задачу решения систем линейных уравнений в коммутативной области к задаче вычисления обратимой матрицы, такой, что при умножении ее на заданную матрицу будет получена верхняя треугольная матрица.

В общем случае неизвестно, как строить такую обратимую матрицу. Но для колец главных идеалов в [3] описан метод построения такой обратимой матрицы. Он требует $O(n^\beta)$ операций в кольце.

Теорема 1 *Пусть* $Ax = b$ *– неоднородная система линейных уравнений над коммутативной областью* R,$A \in R^{n\times m}$, $e = (1, 0, \ldots, 0) \in R^{m+1}$, $A^* = (b, A)$, $\tilde{A} = (A^{*T}, e^T)$,

$$U\tilde{A}P = T,$$

где $U = \begin{pmatrix} U_0 & U_1 \\ x_0 & x_1 \\ W_0 & W_1 \end{pmatrix}$, $T = \begin{pmatrix} T_1 \\ t \\ 0 \end{pmatrix}$, U *– обратимая матрица,* T *– верхняя треугольная матрица,* T_1 *– верхний треугольный блок, диагональные элементы которого не равны нулю,* t *– последняя ненулевая строка матрицы* T, (x_0, x_1) *– строка матрицы* U *с тем же номером, что и строка* t, x_0 *– первый элемент этой строки,* $P = \mathrm{diag}(P_1, 1)$, P_1 *– матрица перестановок. Тогда*

(1) Система $Ax = b$ *совместна в поле частных кольца* R *в том и только в том случае, когда в строке* t *отличен от нуля только один последний элемент.*

(2) Если система $Ax = b$ *совместна в поле частных, то* $x = -{x_0}^{-1}x_1^T$ *– ее решение, а строки матрицы* W_1 *образуют базис пространства всех решений однородной системы* $Ax = 0$.

(3) Система $Ax = b$ *совместна в кольце* R *в том и только в том случае, когда* x_0 *– обратимый элемент* R. *При этом* $x = -{x_0}^{-1}x_1^T$ *– решение системы в кольце* R, *а строки матрицы* W_1 *образуют базис модуля всех решений однородной системы* $Ax = 0$.

Доказательство.

Пусть в строке t найдется ненулевой элемент, стоящий не в последнем столбце, тогда ранг матрицы T не уменьшится после вычеркивания последнего столбца. Так как U и P обратимы, то значит и ранг $\tilde{A}$ не уменьшается при вычеркивании последнего столбца. Но система с расширенной матрицей $\tilde{A}^T$, очевидно, несовместна. Следовательно несовместна система с расширенной матрицей A^*.

Пусть теперь в строке t только последний элемент не равен нулю. Имеем

$$\begin{pmatrix} x_0 & x_1 \\ W_0 & W_1 \end{pmatrix} \cdot \begin{pmatrix} b^T \\ A^T \end{pmatrix} = 0.$$

Очевидно, что первый столбец матрицы U совпадает с последним в матрице T, поэтому $x_0 \neq 0$ и $W_0 = 0$. Получим $Ax_1^T = -x_0 b$ и $AW_1^T = 0$. Строки матрицы W_1 линейно независимы, так как U обратима и $W_0 = 0$. Число строк в матрице T_1 равно $\operatorname{rank}(A)$, поэтому число строк в матрице W_1 будет $m - \operatorname{rank}(A)$. Следовательно строки матрицы W_1 образуют базис пространства всех решений однородной системы $Ax = 0$, и $x = -{x_0}^{-1} x_1^T$ – решение системы $Ax = b$ в поле частных.

Если x_0 обратимый элемент кольца R, то решение $x = -{x_0}^{-1} x_1^T$ лежит в кольце R. Предположим теперь, что x_0 необратим в R и докажем, что система $Ax = b$ несовместна в R.

Пусть y – некоторое решение системы $Ax = b$ в поле частных. Тогда найдется такой вектор g в поле частных, что $y^T = -{x_0}^{-1} x_1 + gW_1$. Запишем вектор g в виде $g = g_0^{-1} g_1$, где $g_0 \in R$, $g_1 \in R^m$, g_0 необратим или равен 1, когда $g \in R^m$. Получим

$$y^T = -{x_0}^{-1} x_1 + g_0^{-1} g_1 W_1.$$

Предполагая, что $y \in R^m$, получим вектор $-g_0 x_1 + x_0 g_1 W_1 = x_0 g_0 y^T$, все компоненты которого являются кратными $x_0 g_0$.

Если строку (x_0, x_1) матрицы U заменить на линейную комбинацию $g_0(x_0, x_1) - x_0 g_1 (W_0, W_1)$, то определитель матрицы U умножится на g_0. Но все компоненты новой строки кратны $x_0 g_0$. Следовательно определитель должен делиться на $x_0 g_0$. Запишем $g_0 \det(U) = k x_0 g_0$, отсюда $g_0(\det(U) - k x_0) = 0$, $k \in \mathbf{R}$. Но в $\mathbf{R}$ нет делителей нуля, и $\det(U)$ обратим, поэтому $\det(U)^{-1} k x_0 = 1$. Следовательно и x_0 обратим. Мы пришли к противоречию.

Осталось доказать, что когда x_0 обратим в $\mathbf{R}$, то строки матрицы W_1 образуют базис модуля всех решений однородной системы $Ax = 0$ над кольцом R.

Строки матрицы W_1 образуют базис пространства всех решений однородной системы $Ax = 0$ в поле частных, поэтому всякое решение однородной системы y имеет вид $y^T = gW_1$.

Запишем вектор g в виде $g = g_0^{-1} g_1$, где $g_0 \in R$, $g_1 \in R^m$, получим $g_0 y^T = g_1 W_1$.

Пусть строки матрицы W_1 не образуют базис модуля и y – решение системы, которое не может быть получено как линейная комбинация строк W_1 с коэффициентами из R. Следовательно, хоть одна из компонент вектора g_1 не делится на g_0. Пусть это будет компонента g_r.

Если соответствующую компоненте g_r строку матрицы W_1 заменить на $g_1 W_1$, то определитель матрицы U умножится на g_r. Однако $g_1 W_1 = g_0 y^T$, поэтому этот определитель должен делиться на g_0: $g_r \det(U) = k g_0$, $k \in R$. Мы пришли к противоречию, так как $det(U)$ – обратим в $\mathbf{R}$, а g_r не делится на g_0.

Пример. Пусть $3x + 4y = -2$ – диофантовое уравнение. $A = (3, 4)$, $b = (-2)$. Матричное уравнение $U\tilde{A} = T$ имеет вид

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & -1 \\ 0 & 4 & -3 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3 & 0 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Так как элемент в первой строке $W[2,1] = 1$, то $-(W[2,2], W[2,3]) = (-2, 1)$ – диофантово решение $(W[3,2], W[3,3]) = (4, -3)$ – решение уравнения $3x + 4y = 0$.

ВЫЧИСЛЕНИЕ ХАРАКТЕРИСТИЧЕСКОГО МНОГОЧЛЕНА НАД КОЛЬЦОМ ГЛАВНЫХ ИДЕАЛОВ

Вычисление характеристического многочлена для матрицы над полем имеет асимптотическую оценку сложности такую же, как и матричное умножение – $O(n^\beta)$. Для матриц над произвольным коммутативным кольцом лучшая сегодня оценка сложности – $O(n^{1+\beta} \log n)$, для коммутативных областей – $O(n^3)$ [4].

Рассмотрим случай коммутативного кольца главных идеалов $\mathbf{R}$, которое может не являться областью и содержать делители нуля. Приведем алгоритм вычисления характеристического многочлена для этого случая со сложностью $O(n^3)$.

Элементы матрицы, стоящие сразу под элементами главной диагонали, образуют поддиагональ. Квазитреугольной матрицей называют матрицу, у которой все элементы расположенные ниже поддиагонали нулевые. Ее характеристический многочлен вычисляется непосредственно разложением определителя $\det(\lambda I - A)$ по правому столбцу. Асимптотическая оценка числа умножений в кольце R при таком вычислении определителя составляет $n^3/6$ [4].

Приведем алгоритм, основанный на вычислении подобной квазитреугольной матрицы.

Диофантовы матрицы. Пусть $\mathbf{R}$ кольцо главных идеалов, в котором существует алгоритм вычисления генератора g идеала (p, q), $p, q \in \mathbf{R}$. Будем называть его GI алгоритм:

$$\{g, a, b\} = GI(p, q),$$

$$(g) = (p, q), \quad ap + bq = g.$$

Для ненулевой пары $\alpha = (p, q)$ диофантовой матрицей будем называть матрицу

$$E_\alpha = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \text{ где } c = -\frac{q}{g}, \quad d = \frac{1+bc}{a}.$$

Два главных свойства диофантовой матрицы – это унимодулярность $\det(E_\alpha) = 1$ и обращение первого элемента пары в ноль $\alpha E_\alpha = (0, g)$, $g \neq 0$. Если g не делитель нуля, то диофантова матрица определена однозначно. В этом случае $d = \frac{p}{g}$. Если g – делитель нуля, то c и d определяются неоднозначно. Число c определяется с точностью до аннулятора g, а число d – с точностью до аннулятора a. Если в кольце ввести порядок и выбирать c и d как минимальные из множеств $c + Ann(g)$ и $d + Ann(a)$, то диофантова матрица будет определена однозначно.

Для нулевой пары диофантовой матрицей будем называть единичную. Заметим, что для евклидовых колец GI алгоритм - это алгоритм Евклида.

Алгоритм вычисления подобной квазитреугольной матрицы. Пусть $A = (a_{i,j})$ – матрица порядка n над $\mathbf{R}$. $[k, s]$ – обозначение для квадратной подматрицы, стоящей на пересечении строк и столбцов с номерами $k, k+1, \ldots, s$. D_{ij} – диофантова матрица для пары $(a_{i,j}, a_{i,j+1})$, E_{ij} обозначает матрицу, полученную из единичной матрицы порядка n заменой блока $[j, j+1]$ на D_{ij}, $\det(E_{ij}) = 1$. Тогда в матрице AE_{ij} элемент (ij) равен нулю.

В дальнейшем будем считать, что матрица A, из которой берутся элементы для построения матриц $E_{i,j}$, не является фиксированной, элементы $(a_{i,j}, a_{i,j+1})$ всегда берутся из той матрицы, на которую умножается матрица $E_{i,j}$. Тогда в матрице $AE_{k,1}E_{k,2}\cdots E_{k,k-2}$ будут нулевыми элементы $1, 2, \ldots, k-2$ строки k, $(k = 3, 4, \cdots, n)$.

Обозначим $E_k = E_{k,1}E_{k,2}\cdots E_{k,k-2}$, $k = n, n-1, \ldots, 3$ и для обратных матриц $E_k^{-1} = E_{k,k-2}^{-1}E_{k,k-3}^{-1}\cdots E_{k,1}^{-1}$, $(k = 3, 4, \cdots, n)$.

Матрица $E_k^{-1}AE_k$ будет подобна матрице A, и у нее будут нулевыми элементы $1, 2, \ldots, k-2$ строки k. Действительно, матрица E_k^{-1} отличается от единичной только блоком $[1, k-1]$, и если она умножается слева на матрицу, то в результате не меняются последние строки, начиная со строки k.

Кроме того, если элементы первых $k-1$ столбцов матрицы A были нулевые во всех строках, начиная с $k+1$, то они останутся нулевые в матрице $E_k^{-1}AE_k$, так как E_k отличается от единичной только блоком $[1, k-1]$ и при умножении справа переводит каждый из первых $k-1$ столбцов в некоторую их линейную комбинацию.

Следовательно, последовательно умножая на матрицы $E_n, E_{n-1}, \ldots, E_3$ справа и, соответственно, на обратные к ним слева, получим матрицу $U^{-1}AU$, имеющую квазитреугольный вид и подобную матрице A, $U = E_n\cdots E_4E_3$, $U^{-1} = E_3^{-1}\cdots E_{n-1}^{-1}E_n^{-1}$.

Оценка сложности. С каждым нулевым элементом связано вычисление диофантовой матрицы. Следовательно, необходимо $n^2/2$ раз вычислять диофантовы матрицы. Для умножения на матрицу $E_{i,j}^{-1}$ достаточно $4n$ операций умножения. При умножении на матрицу $E_{i,j}$ достаточно $4i$ операций умножения, так как элементы ниже строки i нулевые. Поэтому всего получим $\sum_{i=3}^{n}(i-2)(4i+4n)$.

Следовательно, общая асимптотическая оценка сложности вычисления квазитреугольной матрицы будет $\frac{8}{3}n^3$.

ВЫЧИСЛЕНИЕ ПРИСОЕДИНЕННОЙ МАТРИЦЫ В КОЛЬЦЕ ГЛАВНЫХ ИДЕАЛОВ

Вычисление присоединенной матрицы для матрицы над полем, а так же для матрицы над произвольной коммутативной областью, имеет асимптотическую оценку сложности такую же, как и матричное умножение – $O(n^\beta)$ [2].

Рассмотрим случай коммутативного кольца главных идеалов $\mathbf{R}$, которое может не являться областью и содержать делители нуля. Приведем алгоритм вычисления характеристического многочлена, который имеет сложность $O(n^3)$.

Присоединенную матрицу A^* для невырожденной матрицы A над кольцом R определим уравнением

$$A^*A = AA^* = \det(A)\, I.$$

Если $\mathbf{R}$ не является областью, то присоединенная матрица может быть определена неоднозначно. Будем называть задачей вычисления присоединенной матрицы задачу вычисления какой-нибудь одной присоединенной матрицы.

Воспользуемся результатом из работы [3]. Для заданной невырожденной матрицы A порядка n вычисление унимодулярной матрицы Q и верхней треугольной матрицы U, таких, что $QA = U$, можно выполнить за $O(n^\beta)$ операций.

Для вычисления определителя матрицы A достаточно перемножить элементы на главной диагонали матрицы U. Обозначим его $d =$

$\det(A)$. Легко видеть, что i-тый столбец присоединенной матрицы – это решение системы линейных уравнений $Ax = d_i$, где $d_i = (0, \ldots, 0, d, 0, \ldots, 0)^T$ – нулевой столбец, у которого i-тый элемент заменен на d, $(i = 1, 2, \ldots, n)$. Следовательно, достаточно решить n систем $Ux = Qd_i$. Так как матрица U – верхняя треугольная, то для вычисления одного решения каждой из этих систем достаточно $O(n^2)$ операций. Всего для n систем достаточно $O(n^3)$ операций.

ВЫЧИСЛЕНИЯ В МОДУЛЯХ НАД ЕВКЛИДОВЫМИ КОЛЬЦАМИ

Рассмотрим следующие задачи: вычисление определителя, решение системы линейных уравнений (определенной или неопределенной), вычисление присоединенной матрицы, вычисление характеристического многочлена.

Известно, что эти задачи могут быть решены за $O(n^\beta)$ мультипликативных операций, если они решаются для матриц над некоторым полем F.

В этом параграфе мы обсудим применение китайской теоремы об остатках и p-адического подъема для решения этих задач в евклидовых областях Z и $F[x]$.

Согласно китайской теореме об остатках, если $m_1, \ldots, m_n$ – взаимно простые элементы кольца R, $(m_i, m_j) = 1$ для всех $i \neq j$, и $r_1, \ldots, r_n$ – произвольные элементы из $\mathbf{R}$, то существует единственный элемент r, $r \leq m$, $m = \prod_{i=1}^n m_i$, такой, что $r_i = r \mod m_i$ для всех i, $(i = 1, \ldots, n)$.

Пусть $m_1, \ldots, m_n$ – простые элементы коммутативной области R, тогда каждый фактор $F_i = R/m_i$ является полем. Решение в поле F_i каждой из рассматриваемых задач имеет сложность $O(n^\beta)$ мультитликативных операций.

Вычисление определителя. Пусть $A = (a_{i,j})$ – матрица порядка n.

Если $\mathbf{R} = \mathbb{Z}$, то можно воспользоваться неравенством Адамара $\det(A)^2 \leq \prod_{i=1}^n \sum_{j=1}^n a_{i,j}^2$ и получить оценку для определителя матрицы $|\det(A)| \leq n^{n/2} a^n$, где $a = |\max(a_{i,j})|$.

Пусть $m_1, \ldots, m_n$ – простые числа, такие что $\prod_{i=1}^n m_i > 2|\det(A)|$, тогда достаточно вычислить $\det(A)$ в каждом поле R/m_i. После этого $\det(A)$ можно будет однозначно наити в $\mathbb{Z}$. Для восстановления одного числа p по остаткам $r_1, r_2, \ldots, r_n$ достаточно $O(n^2)$ операций над целыми числами порядка $O(a\sqrt{n})$,

$$p_j = r_1 + (r_2 - \tilde{r}_1)e_2 m_1 + (r_3 - \tilde{r}_2)e_3 m_1 m_2 + \ldots$$
$$+ (r_j - \tilde{r}_{j-1})e_j m_1 m_2 \cdots m_{j-1},$$

где $e_j = (m_1 m_2 \cdots m_{j-1})^{-1} \mod m_j$, $\tilde{r}_i = p_i \mod m_{i+1}$. В итоге получим $p = p_n$.

Таким образом, можно вычислить определитель за $O(n^{\beta+1})$ операций над целыми числами порядка $O(a\sqrt{n})$. Если используется стандартное умножение целых чисел, то получим всего $O(n^{\beta+1}(\log(n) + log(a))^2)$ бит операций.

Если $\mathbf{R} = F[x]$, то можно воспользоваться оценкой $\deg(\det A) \leq \sum_{i=1}^n \max_{j=1}^n \deg a_{i,j} \leq n \deg a$, где a – элемент матрицы A имеющий наибольшую степень. Если выбрать, например, $n \deg a$ модулей первой степени, то всего потребуется $O(n^{\beta+1} \deg a)$ операций в поле F.

Будем считать a константой и пренебрегать логарифмом n. Тогда оценка сложности вычисления определителя в обоих случаях равна $O(n^{\beta+1})$.

Решение определенной системы линейных уравнений. Если определитель $\delta = \det A$ матрицы коэффициентов определенной системы линейных уравнений $Ax = b$ уже найден, то можно умножить его на столбец свободных членов. В результате получим систему $Ax = \delta b$, решение которой лежит в кольце R и каждая компонента не превосходит по абсолютной величине наибольшего минора матрицы (A, b). Следовательно оценку можно получить также, как для определителя матрицы, только теперь a - наибольший по соответствующей эвклидовой мере элемент расширенной матрицы (A, b).

Для решения системы в поле F_i достаточно $O(n^\beta)$ операций, а количество полей пропорционально n, как в предыдущем случае. Поэтому общая оценка снова будет $O(n^{\beta+1})$.

Однако p-адический метод [9] имеет лучшую оценку. Нет необходимости вычислять предворительно $\det A$, достаточно выбрать границу для модуля $m = p^s > 2(d)^2$, где d – оценка для максимального минора матрицы (A, b). Всякой дроби, у которой числитель и знаменатель не превосходят по модулю d и знаменатель не кратен p, ставится в соответствие единственный элемент в кольце $\mathbf{R}/m\mathbf{R}$. Поэтому достаточно решить систему по модулю m и затем найти соответстующий этому решению вектор в поле частных кольца R.

Будем последовательно искать коэффициенты (p-ичные цифры) в разложении вектора

$$x = \sum_{i=0}^{s} x_i p^i$$

по степеням p. Пусть A_p^{-1} – матрица, обратная к A_p в поле $\mathbf{R}/p\mathbf{R}$ и $b_0 = b$, тогда

	Вычисление определителя	Решение систем линейных уравнений		Вычисление присоединенной матрицы	Вычисление характеристического многочлена
		Определенной $n \times n$	Неопределенной $n \times m$		
$\frac{R}{F}$	n^{β}	n^{β}	$\frac{*}{mn^{\beta-1}}$	n^{β}	n^{3}
R'	n^{β}	n^{β}	$mn^{\beta-1}$	n^{3}	n^{3}
$\frac{R''}{F''}$	$n^{\beta+1}$	n^{3}	$\frac{(m-n+1)n^{\beta+1}}{(m-n+1)n^{3}}$	n^{4}	$n^{\beta+1}$

$x_0 = A_p^{-1}b \mod p$, $b_i = (b_{i-1} - Ax_{i-1})/p$, $x_i = A_p^{-1}b_i \mod p$, $i = 1, 2, \ldots, s-1$.

Если p порядка $O(a\sqrt{n})$, то $s = 2n$. Вычисление A_p^{-1} можно выполнить за $O(n^{\beta})$ операций, умножение матрицы на вектор требует n^2 операций и это нужно выполнять $4n$ раз. Восстановление одной дроби имеет сложность порядка $O(n^2)$, а количество компонент вектора x равно n. Следовательно общее число операций имеет порядок $O(n^3)$. Если переходить к бит операциям, то получим $O(n^3(\log a + \log n)^2)$.

Вычисление присоединенной матрицы. Если определитель уже известен, то присоединенную матрицу можно вычислить, решая n определенных систем, как и в параграфе 3. Если применять р-адический метод, то потребуется $O(n^4)$.

Решение неопределенной системы линейных уравнений. Пусть $Ax = b$ неопределенная система линейных уравнений, $A = (A_0, A_1) \in \mathbf{R}^{n\times m}$, A_0 – квадратный блок и $\det(A_0) \neq 0$. Решая системы $A_{0i} = b_i$, где b_i – столбцы матрицы (A_1, b), очевидно, получим базисное множество решений системы $Ax = b$. Если применять p-адический метод, то число операций будет $O(n^3(m - n + 1))$.

Вычисление характеристического многочлена. Коэффициенты характеристического многочлена – это суммы диагональных миноров матрицы. Поэтому количество модулей и в этом случае пропорционально размерам матрицы. Поэтому, как и при решении определенной системы, получим общую сложность $O(n^{\beta+1})$.

ЗАКЛЮЧЕНИЕ

В заключение сведем оценки сложности описанных алгоритмов в одну таблицу. Сюда же добавим оценки сложности алгоритмов для коммутативных областей (см. [2], [4], [6]) и алгоритмов решения систем линейных уравнений и вычисления определителя для колец главных идеалов [7], [3].

В таблице введены следующие обозначения. R – коммутативная область, F – поле частных области R, R' – кольцо главных идеалов, в котором могут быть делители нуля, R'' – евклидова область ($\mathbb{Z}$ или $F[x]$), F'' – поле частных R''.

Все оценки приведены с точностью до логарифмических множителей. Для R'' оценки даны в числе бит операций в случае $R'' = \mathbb{Z}$ (операций в поле F при $R'' = F[x]$). В средней колонке для областей в числителе стоит сложность решения системы в области [7], а в знаменателе – сложность решения системы в поле частных.

Следует отметить, что библиография, приведенная в этой статье, очень не полная. Возможно историки установят авторство для алгоритмов в евклидовых областях. Например, модулярный способ вычисления определителя известен очень давно (см. например [8]), он остается лучшим и сегодня. Нужно отметить, что в работе [10] приводится алгоритм, у которого ожидаемая сложность уменьшена в $\log n$ раз, хотя в наихудшем случае оценка остается такая же. Основная идея состоит в том, что решается несколько раз система линейных уравнений со случайными столбцами свободных членов с помощью р-адического метода. Находится общий знаменатель решений, который является делителем искомого определителя, а затем продолжается стандартный модулярный метод.

ЛИТЕРАТУРА

1. *Малашонок Г.И.* Решение систем линейных уравнений в коммутативных областях // Вестник Тамбов. ун-та. Сер. Естеств. и технич. науки. Тамбов, 2000. Т.5, Вып.1. P. 147-154.

2. *Malaschonok G.I.* Effective Matrix Methods in Commutative Domains // Formal Power

Series and Algebraic Combinatorics. Springer, 2000. P. 506–517.

3. *Малашонок Г.И.* Решение систем линейных диофантовых уравнений // Вестник Тамбов. ун-та. Сер. Естеств. и технич. науки. Тамбов, 2000. Т.5, Вып.5. С. 620-627.

4. *Abdeljaoued,J., Malaschonok G.I.* Efficient Algorithms for Computing the Characteristic Polynomial in a Domain // J. of Pure and Applied Algebra, V. 156, I. 2-3, 2001. P. 127-145.

5. *Chistov A.L.* Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic // Proc. FCT '85. Springer, LNCS V. 199, 1985. P. 147–150.

6. *Malaschonok,G.I.* Recursive Method for the Solution of Systems of Linear Equations // Computational Math. V.I. Wiss. & Tech., Berlin 1997. P. 475-480.

7. *Malaschonok G.I.* Solution of Systems of Linear Diophantine Equations // Computer Algebra in Scientific Computing, CASC'01. Springer, Berlin, 2001. P. 101–115.

8. *Кнут Д.Е.* Исскуство программирования для ЭВМ // Т.2. Получисленные алгоритмы. Москва, МИР, 1977.

9. *Dixon J.* Exact solution of linear equations using p-adic expansions // Numer. Math., V. 40, 1982. P. 137–141.

10. *Abbott,J. Bronstein,M., Mulders,T.* Fast Deterministic Computation of Determinants of Dense Matrices // Proc. of ISSAC'99. Vancouver, ACM Press, 1999. P. 197–204.

Поступила в редакцию 1 июня 2001 г.