Владикавказский математический журнал
2015, Том 17, Выпуск 2, С. 62–67

УДК **511.517**

О ЧИСЛЕ ПРИМИТИВНЫХ НЕАССОЦИИРОВАННЫХ МАТРИЦ ВТОРОГО ПОРЯДКА ОПРЕДЕЛИТЕЛЯ n, ДЕЛЯЩИХСЯ НА ЗАДАННУЮ МАТРИЦУ

У. М. Пачев

Посвящается 60-летию со дня рождения Владимира Амурхановича Койбаева

Получены формулы для числа примитивных неассоциированных матриц второго порядка заданного нечетного определителя, а также для числа таких матриц, делящихся справа (слева) на заданную матрицу, используемые в вопросах представимости целых чисел неопределенными тернарными квадратичными формами.

Ключевые слова: дискретный эргодический метод, целочисленная примитивная матрица, норма (определитель) матрицы, делимость матриц, неассоциированные справа (слева) матрицы.

В связи с применениями дискретного эргодического метода [1] к вопросу представления целых чисел неопределенными тернарными квадратичными формами возникает необходимость использования примитивных неассоциированных матриц $M \in M_2(Z)$ второго порядка, заданного определителя. Чтобы обеспечить конечность числа целых матриц заданной нормы накладывается условие их неассоциированности справа или слева. В [1–3] неассоциированные матрицы второго порядка, заданной нормы, используются в доказательстве асимптотической формулы для числа целых точек на гиперболоидах и леммы о делимости матриц большой нормы. Вопрос о делимости матриц на неассоциированные матрицы мы рассматриваем в общем виде, а именно, если $N(M) = q^n$ и $A \setminus M$ или M/A (делимость слева или справа) и $N(A)/q^n$, то $N(A)$ не обязательно равна q^k при $1 \leqslant k \leqslant n$ и составном q (здесь $N(A) = \det A$).

Для полноты изложения приведем необходимые сведения из арифметики матриц второго порядка (более полные сведения см. [2]). Мы рассматриваем кольцо целых матриц второго порядка $M_2(Z)$. Матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

называем *целой*, если $a_{ij} \in Z(i)$ $(i = 1, 2)$. Говорим, что целая матрица A *примитивна*, если $\text{НОД}(a_{11}, a_{12}, a_{21}, a_{22}) = 1$. Число

$$t = t(A) = \text{НОД}(a_{11}, a_{12}, a_{21}, a_{22})$$

называется *числовым делителем матрицы* A.

Если для некоторого целого числа $g > 0$ числовой делитель $t(A)$ взаимно прост с g, то матрица A называется *примитивной по модулю* g. Целая матрица U называется *обратимой* (или *единицей* в широком смысле), если $U^{-1} \in M_2(Z)$. В кольце $M_2(Z)$ любая обратимая матрица U имеет норму $N(U) = \pm 1$.

Определим в кольце $M_2(Z)$ ассоциированность матриц слева и справа.

Матрицу A_1 называем *ассоциированной слева* с матрицей A, если найдется такая целая матрица U с нормой $N(U) = 1$, для которой $A_1 = UA$. Аналогично говорим, что A_1 *ассоциирована справа* с A, если найдется $V \in M_2(Z)$, что $N(V) = 1$ и $A_1 = AV$.

Отношение ассоциированности разбивает $M_2(Z)$ на классы ассоциированных матриц. В классе ассоциированных справа матриц можно выбрать единственным образом каноническую треугольную матрицу.

Лемма 1 (о каноническом виде матриц)**.** *Для всякой невырожденной матрицы* $A \in M_2(Z)$ *найдется ассоциированная ей справа матрица вида*

$$T = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}, \quad 0 \leqslant c < a, \;\; b < 0.$$

При этом, если матрицы T *и*

$$T' = \begin{pmatrix} a' & c' \\ 0 & b' \end{pmatrix}, \quad 0 \leqslant c' < a', \;\; b' > 0,$$

ассоциированы справа, то $T' = T$.

Это есть частный случай общего утверждения для квадратных целочисленных матриц любого порядка (см. [4, гл. II]). Эту лемму можно доказать с помощью алгоритма Евклида и элементарных преобразований матриц второго порядка.

Говорим, что в кольце $M_2(Z)$ матрица A делится на матрицу B справа и пишем A/B, если найдется матрица Q, для которой $A = QB$. Если B невырождена, то делимость A/B равносильна условию $AB^{-1} \in M_2(Z)$.

Говорим, что матрица A делится на B слева и пишем $B \setminus A$, если найдется матрица $Q \in M_2(Z)$ с условием $A = BQ$ (о теории делимости матриц второго порядка см. [2]).

Следующее утверждение является аналогом основной теоремы арифметики о единственности разложения на простые множители.

Лемма 2 (матричный аналог основной теоремы арифметики)**.**

1) *Пусть* A *— целая невырожденная матрица второго порядка, причем* $N(A) = b \cdot c$, *где* $b, c \in Z$. *Тогда найдутся такие матрицы* B, C, *что*

$$A = BC, \quad N(B) = b, \quad N(C) = c. \tag{$*$}$$

2) *Если при этом матрица* A *примитивна* $(\mathrm{mod}\, c)$, *то представление* $(*)$ *единственно с точностью до ассоциированности, т. е. если*

$$A = BC = B_1C_1,$$

$$N(C_1) = N(C) = c,$$

то найдется матрица E, $N(E) = 1$, *для которой* $C_1 = EC$, $B_1 = BE^{-1}$.

Доказательство см. в [2, § 2].

Опираясь на леммы 1 и 2, получим результаты о неассоциированных матрицах из $M_2(Z)$ заданного определителя n (см. также [5], где дается только набросок доказательства; здесь мы даем развернутое изложение).

Теорема 1. *Пусть n — нечетное число и $\sigma_0(n)$ — число примитивных неассоциированных справа (слева) целочисленных матриц второго порядка определителя n. Тогда*

$$\sigma_0(n) = n\prod_{p/b}\left(1+\frac{1}{p}\right), \tag{1}$$

где произведение берется по всем простым делителям числа n.

$\lhd 1^0$. Будем проводить доказательство только для случая неассоциированных справа матриц. Сначала рассмотрим случай когда n есть степень нечетного простого числа p, т. е. $n = p^a$. В силу леммы 1 примитивными неассоциированными справа матрицами второго порядка определителя p^a будут матрицы вида

$$\begin{pmatrix} p^k & \xi \\ 0 & p^m \end{pmatrix}, \tag{2}$$

где

$$k+m=a, \quad \text{НОД}(\xi, p) = 1, \quad 0 \leqslant \xi \leqslant p^k - 1 \tag{3}$$

при всевозможных значениях $0 \leqslant k, m \leqslant a$.

Действительно, умножая матрицу

$$\begin{pmatrix} p^k & \xi \\ 0 & p^m \end{pmatrix}$$

справа на целочисленную унимодулярную матрицу

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

получим

$$\begin{pmatrix} p^k & \xi \\ 0 & p^m \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} p^k\alpha + \xi\gamma & p^k\beta + \xi\delta \\ p^m\gamma & p^m\delta \end{pmatrix} = \begin{pmatrix} p^s & \eta \\ 0 & p^t \end{pmatrix},$$

где $0 \leqslant \eta \leqslant p^s - 1$, $s + t = a$.

Отсюда следует, что $\gamma = 0$. Тогда

$$\begin{pmatrix} p^k\alpha & p^k\beta + \xi\delta \\ 0 & p^m\delta \end{pmatrix} = \begin{pmatrix} p^s & \eta \\ 0 & p^t \end{pmatrix}.$$

Переходя к определителям, будем иметь $p^{k+m}\alpha\delta = p^{s+t}$, т. е. $p^a\alpha\delta = p^a$, откуда $\alpha\delta = 1$. Так как α, δ — целые числа и $\alpha, \delta > 0$, то $\alpha = \delta = 1$. В таком случае получаем

$$\begin{pmatrix} p^k & p^k\beta + \xi\delta \\ 0 & p^m \end{pmatrix} = \begin{pmatrix} p^s & \eta \\ 0 & p^t \end{pmatrix},$$

откуда $s = k$, $t = m$ и $\eta = p^k\beta + \xi$.

Так как по условию $0 \leqslant \eta \leqslant p^s - 1$, то теперь, учитывая, что $s = k$, получаем $0 \leqslant p^k\beta + \xi \leqslant p^k - 1$, откуда $\beta = 0$.

Значит,

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

и поэтому различные матрицы вида (2) с условиями (3) попарно неассоциированы справа.

Найдем теперь $\sigma_0(p^a)$. При фиксированном $1 \leqslant k \leqslant a-1$ число матриц вида (2) с условиями (3) будет равно $\varphi(p^k) = p^k - p^{k-1}$. При $k = 0$ получаем только одну матрицу вида

$$\begin{pmatrix} 1 & \xi \\ 0 & p^k \end{pmatrix}$$

при $\xi = 0$, а при $k = a$ получаем матрицы вида

$$\begin{pmatrix} p^a & \xi \\ 0 & 1 \end{pmatrix},$$

где $\xi = 0, 1, \ldots, p^a - 1$, в этом случае получим p^a таких матриц. Тогда

$$\sigma_0(p^a) = 1 + p^a + \sum_{k=1}^{a-1} \left(p^k - p^{k-1}\right) = p^a \left(1 + \frac{1}{p}\right). \tag{4}$$

Итак, формула (1) в случае $n = p^a$ доказана.

2^0. Докажем теперь мультпликативность функции $\sigma_0(n)$, т. е. что

$$\sigma_0(b \cdot c) = \sigma_0(b) \cdot \sigma_0(c) \quad \text{при} \quad (b, c) = 1. \tag{5}$$

Пусть $B_1, B_2, \ldots, B_{\sigma_0(b)}$ — полный набор примитивных неассоциированных справа матриц определителя b, а $C_1, C_2, \ldots, C_{\sigma_0(c)}$ — все примитивные попарно неассоциированные слева матрицы определителя c, причем НОД$(b, c) = 1$.

Тогда по лемме 2 имеем, что матрицы $B_i C_j$ примитивны и неассоциированы справа. Действительно, предположим, что матрицы $B_i C_j$ и $B_{i'} C_{j'}$ $(i' \neq i,\ j' \neq j)$ ассоциированы справа, т. е.

$$B_{i'} C_{j'} = B_i C_j U, \tag{6}$$

где U — целочисленная унимодулярная матрица. Тогда по лемме 2 будем иметь равенства

$$B_{i'} = B_i E, \quad C_{j'} = E^{-1} C_j U, \tag{7}$$

где E — целочисленная унимодулярная матрица. Для того, чтобы имелись представления указанных видов (7) в силу леммы 2 нужно, чтобы матрица $A = BC$ была примитивной по модулю $c = \det C$.

Покажем, что последнее условие выполняется для нашего случая. Действительно, пусть

$$B = \begin{pmatrix} b_1 & \xi \\ 0 & b_2 \end{pmatrix}, \quad C = \begin{pmatrix} c_1 & \xi \\ 0 & c_2 \end{pmatrix},$$

где $0 \leqslant \xi \leqslant b_1 - 1$, $0 \leqslant \eta \leqslant c_1 - 1$ и НОД $= (b_1 b_2, c_1 c_2) = 1$, и пусть при этом t — числовой делитель матрицы $A = BC$. Надо показать, что НОД $= (t, c) = 1$. Имеем

$$A = BC = \begin{pmatrix} b_1 & \xi \\ 0 & b_2 \end{pmatrix} \begin{pmatrix} c_1 & \xi \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} b_1 c_1 & b_1 \eta + c_2 \xi \\ 0 & b_2 c_2 \end{pmatrix}. \tag{8}$$

Тогда $t | b_1 c_1$, $t | b_2 c_2$. Так как НОД$(b, c) = 1$, то $t | b$ или $t | c$.

Рассмотрим случай

$$t | b, \quad t / c_1. \tag{9}$$

Тогда из (8) следует, что $t | c_2 \xi$. Возможны два случая: а) $t | c_2$, б) t / ξ.

В случае а) из (8), учитывая (9), имеем, что t / b и t / c поскольку t / c_2.

Но так как НОД$(b,c)=1$, то $t=1$. В случае б) аналогично получаем, что $t=1$. Следовательно, НОД$(t,n)=1$. Итак, в наших условиях выполняются равенства (7). Но это противоречит тому, что матрицы B_i, $B_{i'}$ неассоциированы. Значит, наше допущение, что матрицы B_iC_j ассоциированы справа приводит к противоречию. Следовательно, матрицы B_iC_j $(i=1,\dots,\sigma(b),\ j=1,\dots,\sigma(c))$ попарно неассоциированы справа.

Попутно было установлено, что матрицы B_iC_j примитивны. Тем самым мультипликативность функции $\sigma_0(n)$ доказана. Из (4) и (5) уже следует теорема 1, т. е. формула (1). $\triangleright$

Замечание. Доказательство примитивности матриц B_iC_j можно было провести и следующим образом. Так как матрицы B_iC_j примитивны по условию, то они примитивны по любому модулю $g>0$. Так как

$$\text{НОД}(\det B_i, \det B_j)=1,$$

то в силу следствия 2 предложения 2.7 статьи [2] имеем, что B_iC_j примитивны по любому модулю g. Отсюда следует, что $t(B_i,C_j)=1$, т. е. матрица B_iC_j примитивна.

Перейдем теперь к вопросу о числе примитивных неассоциированных матриц $M\in M_2(Z)$ определителя n, делящихся на матрицу $A\in M_2(Z)$.

Обозначим через $\sigma_0(n,A)$ число примитивных неассоциированных матриц $M\in M_2(Z)$ определителя n, делящихся на матрицу $A\in M_2(Z)$.

Опираясь на теорему 1, получаем следующий результат.

Теорема 2. *Для числа $\sigma_0(n,A)$ справедливо соотношение*

$$\sigma_0(n,A)=\frac{n}{\det A}\prod_{p\,\left|\,\frac{n}{|\det A|}\right.}\left(p+\frac{1}{p}\right),$$

где произведение берется по всем простым делителям числа $\frac{n}{|\det A|}$.

$\triangleleft$ Пусть $M_1,M_2,\dots,M_r$ — набор всех неассоциированных справа примитивных матриц второго порядка определителя n, делящихся слева на матрицу $A\in M_2(Z)$, где $r=\sigma_0(n,A)$, при этом случай неассоциированности слева и соответственно делимости справа рассматривается аналогично.

В силу делимости матриц $M_1,M_2,\dots,M_r$ слева на матрицу A имеем

$$M_1=A\widetilde{M}_1,\ M_2=A\widetilde{M}_2,\ \dots,\ M_r=A\widetilde{M}_r,$$

где $\widetilde{M}_1,\widetilde{M}_2,\dots,\widetilde{M}_r\in M_2(Z)$.

Покажем, что $\widetilde{M}_i$ $(i=1,\dots,r)$ неассоциированы справа. Допустим, что это не так. Тогда $\widetilde{M}_i=\widetilde{M}_jE$ — целочисленная унимодулярная матрица, $i\neq j$. В таком случае $M_i=A\widetilde{M}_i=(A\widetilde{M}_j)E=M_jE$, а это противоречит неассоциированности матриц M_i и M_j справа при $i\neq j$. Покажем еще примитивность матриц $\widetilde{M}_i$ $(i=1,\dots,r)$. Допустим, что $\widetilde{M}_i$ не является примитивной. Тогда $\widetilde{M}_i=t\widetilde{M}_i'$, где $t>0$, $\widetilde{M}_i'\in M_2(Z)$. Подставляя это в матрицу $\widetilde{M}_i$ будем иметь $M_i=A\cdot t\widetilde{M}_i'=tA\cdot\widetilde{M}_i'$, где $t>1$, но это противоречит условию примитивности матрицы M_i. Таким образом, матрицы $\widetilde{M}_1,\widetilde{M}_2,\dots,\widetilde{M}_r$ — неассоциированы справа и примитивны. Но тогда в силу того, что $\det\widetilde{M}_i=\frac{n}{\det A}$, по теореме 1 получаем формулу для $\sigma_0(n,A)$. $\triangleright$

Замечание. Если рассматриваемые матрицы $M\in M_2(Z)$ лежат в некоторой области Ω на детерминантной поверхности $\det M=n$, то вместо точных формул могут быть получены только асимптотические формулы при $n\to\infty$ (см. [1]).

Литература

1. *Линник Ю. В.* Эргодические свойства алгебраических полей.—Изд-во ЛГУ, 1967.
2. *Малышев А. В., Пачев У. М.* Об арифметике матриц второго порядка // Записки научных семинаров ЛОМИ.—1980.—Т. 93.—С. 41–86.
3. *Пачев У. М.* Представление целых чисел изотропными тернарными квадратными формами // Изв. РАН. Сер. мат.—2006.—Т. 70, № 3.—С. 167–184.
4. *Newman M.* Integral matrices.—N. Y. L.: AP, 1972.—224 p.
5. *Пачев У. М.* О числе приведенных целочисленных бинарных квадратичных форм с условием делимости первых коэффициентов // Чебышевский сб.—2003.—Т. 4, вып. 3 (7).—С. 92–105.

Статья поступила 21 апреля 2015 г.

Пачев Урусби Мухамедович
Кабардино-Балкарский государственный
университет им. Х. М. Бербекова, *профессор*
РОССИЯ, 360004, Нальчик, ул. Чернышевского, 173
E-mail:urusbi@rambler.ru

ABOUT THE NUMBER OF PRIMITIVE NON-ASSOCIATED SECOND ORDER MATRICES OF DETERMINANT n DIVISIBLE BY A GIVEN MATRIX

Pachev U. M.

We obtained formulae for the number of primitive non-associated second order matrices of given odd determinant, as well as for the number of such matrices divisible on the right (left) by the given matrix used in questions of representability of integers by indefinite ternary quadratic forms.

Key words: discrete ergidic method, primitive matrix of integers, norm (determinant) of a matrix, divisibility of matrices, non-associated matrices on the right (left).