*Владикавказский математический журнал*
*2008, Том 10, Выпуск 1, С. 75–78*

*УДК* **511.512**

# ОБ АРИФМЕТИКЕ КОЛЬЦА ЦЕЛЫХ МАТРИЦ $n$-ГО ПОРЯДКА

**У. М. Пачев**

Арифметика кольца $M_2(Z)$ целых матриц второго порядка переносится на целые матрицы $n$-го порядка. В частности, получены формулы для числа неассоциированных примитивных матриц заданной нормы и для числа классов вычетов в кольце $M_n(Z)$ по матричному модулю.

**Ключевые слова:** матрица $n$-го прядка, целая матрица, вектор-матрица, норма матрицы, ассоциированность матриц, число неассоциированных матриц, сравнимость матриц.

1. Целью предлагаемой заметки является краткое изложение основ теории делимости в кольце $M_n(Z)$ целых матриц $n$-го порядка, которая может быть использована при применении дискретного эргодического метода Ю. В. Линника [1, 2] к вопросу распределения классов идеалов алгебраических полей $n$-ой степени. Арифметика матриц второго порядка, в частности, теория делимости изложена в [3]. Эту вводную часть завершим изложением кратких сведений из алгебры $M_n(Q)$ рациональных матриц $n$-го порядка, необходимых для дальнейшего.

Пусть $M_n(Q)$ — алгебра матриц $n$-го порядка

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}$$

над полем рациональных чисел, $\alpha_{ij} \in Q$ $(i, j = 1, \dots, n)$

Матрица $E = (\delta_{ij}) \in M_n(Q)$, где $\delta_{ij}$ — символ Кронекера, является единицей этой алгебры. Матрицу $\alpha E$ называем скалярной и ее отождествляем с числом $\alpha \in Q$. В статье [3] определялось понятие вектор-матрицы второго порядка как матрицы $L \in M_2(Q)$ с нулевым следом, т. е. $\operatorname{Sp} L = 0$. При рассмотрении матриц $n$-го порядка, по-видимому, целесообразнее не прямое обобщение $(\operatorname{Sp} L = 0)$, а обобщение свойства вектор-матриц второго порядка удовлетворяющих уравнению $L^2 = -m$. Тогда аналогами вектор-матриц $L$ порядка $n$ следует считать [1] решение уравнения

$$L^n + a_1 L^{n+1} + \dots + a_n = 0,$$

где $a_1, \dots, a_n \in Q$ (вектор-матрица $L$ типа $(a_1, \dots, a_n)$). При изучении эргодических свойств алгебраических полей коэффициенты уравнения (1) могут считаться целочисленными функциями параметра $D \to \infty$, т. е. $a_i = a_i(D)$. Если для матрицы $A \in M_n(Q)$ ее сопряженную (присоединенную) обозначим через $\overline{A}$, то

$$A\overline{A} = \overline{A}A = (\delta_{ij} \det A)_{1 \leqslant i,j \leqslant n},$$

где $\delta_{ij} = \begin{cases} 1 \text{ при } i = j \\ 0 \text{ при } i \neq j \end{cases}$ — символ Кронекера, и, чтобы сохранить аналогию с алгеброй эрмитионов [3], условимся называть число $N(A) = \det A$ нормой матрицы $A$.

2. Перейдем теперь к теории делимости в кольце $M_n(Z)$ целых матриц $n$-го порядка. Матрицу $A = (a_{ij}) \in M_n(Q)$ называем целой (или целочисленной), если все ее элементы являются целыми числами, т. е. $a_{ij} \in Z$. Невырожденная матрица $E \in M_n(Z)$ называется обратимой, если $E^{-1} \in M_n(Z)$. Ясно, что обратимыми будут те и только те матрицы $E \in M_n(Z)$, для которых $N(E) = \pm 1$.

Матрицы $A, A' \in M_n(Z)$ называются ассоциированными справа, если найдется обратимая матрица $E \in M_n(Z)$, для которой $A' = AE$. Ассоциированность матриц справа — отношение эквивалентности, разбивающее кольцо $M_n(Z)$ на классы ассоциированных справа матриц. В каждом классе ассоциированных справа матриц $n$-го порядка можно выбрать единственную каноническую треугольную матрицу, а именно имеет место следующее

**Предложение 1.** *Для всякой невырожденной матрицы $A \in M_n(Z)$ найдется единственная ассоциированная ей справа матрица $T \in M_n(Z)$ вида*

$$T = \begin{pmatrix} d_1 & c_{12} & \dots & c_{1n} \\ 0 & d_2 & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{pmatrix}, \tag{1}$$

*где $d_1, \dots, d_n > 0$, $0 \leqslant c_{ik} < d_i$, $i + 1 \leqslant k \leqslant n$.*

Доказательство этого предложения можно найти в [4, гл. II]

Пользуясь каноническим видом (1), можно получить следующее

**Предложение 2.** *Число $\sigma(n, N)$ неассоциированных справа матриц порядка нормы $N > 0$ равно*

$$\sigma(n, N) = \sum_{N = d_1 \cdot \dots \cdot d_n} d_2 d_3^2 \cdot d_n^{n-1}, \tag{2}$$

*где суммирование проводится по всем натуральным числам $d_1, \dots, d_n$, для которых $N = d_1 d_2 \cdot \dots \cdot d_n$.*

Следующее предложение [5] используется в теории поворотов матриц $n$-го порядка, а также в вопросах разрешимости диофантовых систем линейных уравнений.

**Предложение 3.** *Для любой матрицы $A \in M_n(Z)$ найдутся такие обратимые матрицы $E_1, E_2 \in M_n(Z)$, что матрица $A' = E_1 A E_2$ имеет вид*

$$A' = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{pmatrix},$$

*где $d_k > 0$, $d_{k-1} | d_k$, $d_0 = 1$ $(k = 1, \dots, n)$.*

Доказательство проводится индукцией по порядку рассматриваемых матриц. Получающиеся числа $d_k$ называются инвариантными множителями целой матрицы $A$ и совпадают с наибольшими общими делителями всех миноров порядка $k$ матрицы $A$.

Введем еще понятие числового делителя матрицы. Число $t = t(A) =$ НОД $(a_{11}, a_{12}, \dots, a_{nn})$ называется числовым делителем матрицы $A = (a_{ij}) \in M_n(Z)$. Если $t(A) = 1$, то матрицу $A$ называем примитивной. Всякую матрицу $A \in M_n(Z)$ можно представить в виде $A = tA_0$, где $t = t(A)$, а $A_0$ — примитивная матрица. Следующая

теорема дает обобщение результата о числе неассоциированных справа матриц второго порядка заданной нормы из статьи [3] на случай матриц $n$-го порядка.

**Теорема 1.** *Число неассоциированных справа примитивных матриц $n$-го порядка нормы $N \neq 0$ равно*

$$\sigma_0(n, N) = \sum_{d^n|N} \mu(d)\sigma\left(n, \frac{N}{d^n}\right), \tag{3}$$

*где $\mu(d)$ — функция Мебиуса.*

$\lhd$ Имеем

$$\sigma_0(n, N) = \sum_{d^n|N} \sigma_0\left(n, \frac{N}{d^n}\right).$$

Представим число $N$ в следующем виде

$$N = N_0^n N_1,$$

где $N_1$ свободно от $n$-х степеней. Тогда

$$\sigma_0(n, N) = \sum_{d^n|N} \sigma_0\left(n, \frac{N_0^n N_1}{d^n}\right).$$

Отсюда по формуле обращения Мебиуса получаем

$$\sigma_0(n, N) = \sum_{d^n|N_0^n N_1} \mu(d)\sigma\left(n, \frac{N_0^n N_1}{d^n}\right) = \sum_{d^n|N} \mu(d)\sigma\left(n, \frac{N}{d^n}\right). \rhd$$

Из (3) в частном случае при $N = p$, где $p$ — простое число, получаем, что

$$\sigma_0(n, p) = \frac{p^n - 1}{p - 1}.$$

Рассмотрим теперь отношения делимости и сравнимости в кольце $M_n(Z)$. Говорим, что матрица $A$ делится на матрицу $B$ справа, $A|B$, если найдется матрица $Q \in M_n(Z)$, что $A = QB$. Если при этом $B$ невырождена, то делимость $A|B$ равносильна $AB^{-1} \in M_n(Z)$. Делимость справа матриц из $M_n(Z)$ обладает теми же свойствами, как и в случае матриц второго порядка [3].

Аналогично определяется делимость слева матриц из $M_n(Z)$. Говорим, что $A$ делится на $B$ слева, $B|A$, если найдется матрица $Q \in M_n(Z)$ с условием $A = BQ$.

Делимость слева матриц обладает свойствами, вполне аналогичными свойствам делимости справа. Это следует из того, что $B|A$ равносильна делимости $\overline{A}|\overline{B}$.

3. Пусть $M$ — невырожденная целая матрица $n$-го порядка. Говорим, что матрицы $A, B \in M_n(Z)$ сравнимы по модулю $M$ справа и пишем

$$A \equiv B(\mathrm{mod}_r\, M), \tag{4}$$

если $(A - B)|M$.

Сравнение (4) равносильно принадлежности $A - B \in M_n(Z)M$.

Говорим, что матрицы $A, B \in M_n(Z)$ сравнимы по модулю $M$ слева и пишем

$$A \equiv B(\mathrm{mod}_l\, M), \tag{5}$$

если $M|(A - B)$.

Если $M = mE$, где $E$ — единичная матрица, и $m \in Z$, то сравнения (4) и (5) равносильны, и мы пишем

$$A \equiv B(\mathrm{mod}\, m), \tag{6}$$

т. е. получаем сравнимость матриц по числовому модулю.

Сравнение (6) равносильно системе числовых сравнений

$$a_{ij} \equiv b_{ij}(\mathrm{mod}\, m) \quad (i, j = 1, n), \quad A = (a_{ij}), \quad B = (b_{ij}).$$

Поэтому из китайской теоремы об остатках, относящейся к целым числам, получаем следующую «матричную теорему об остатках».

**Предложение 4.** *Пусть $m_1, \ldots, m_k$ — попарно взаимно простые числа, $A_1, \ldots, A_k \in M_n(Z)$. Тогда найдется матрица $X \in M_n(Z)$, единственная по модулю $m_1 \cdot \ldots \cdot m_k$, что*

$$\begin{gathered} X \equiv A_1(\mathrm{mod}\, m_1), \\ \ldots\ldots\ldots\ldots\ldots \\ X \equiv A_k(\mathrm{mod}\, m_k). \end{gathered}$$

Отношение сравнимости $A \equiv B(\mathrm{mod}_r\, M)$ разбивает кольцо $M_n(Z)$ на классы вычетов $[A](\mathrm{mod}\, M)$ (аналогично и для сравнимости слева). Пусть $C_r(M)$ — число классов вычетов по модулю $M$ справа. Так как сравнение (4) равносильно $A - B \in M_n(Z)M$, то число $C_r(M)$ можно интерпретировать как индекс $(M_n(Z) : M_n(Z)M)$, который и есть абсолютная величина определителя $n^2$-мерного линейного преобразования $Y = XM$, равный $|\det M|^n$, где $X, Y \in M_n(Z)$. То же верно для $C_l(M)$ — числа классов вычетов по модулю $M$ слева. Тем самым доказали следующее утверждение.

**Теорема 2.** *Если $M \in M_n(Z)$ — невырожденная матрица, то*

$$C_r(M) = C_l(M) = |N(M)|^n.$$

## Литература


1. *Линник Ю. В.* Эргодические свойства алгебраических полей.—Л.: Изд-во Ленингр. ун-та, 1967.—208 с.
2. *Фаддеев Д. К.* О представлении алгебраических чисел матрицами // Записки научных семинаров ЛОМИ.—1974.—Т. 46.—С. 89–91.
3. *Малышев А. В., Пачев У. М.* Об арифметике матриц второго порядка // Записки научных семинаров ЛОМИ.—1980.—Т. 93.—С. 41–86.
4. *Newman M.* Integral matrices.—N.Y.L.: AP, 1972.—224 p.
5. *Толстиков А. В.* О поворотах целых матриц (замечание к одной теореме Ю. В. Линника) //Записки семинаров ЛОМИ.—1983.—Т. 121.—С. 169–170.


*Статья поступила 6 февраля 2008 г.*

Пачев Урусби Мухамедович
Кабардино-Балкарский госуниверситет
Нальчик, 360004, РОССИЯ
E-mail: urusbi@rambler.ru