Сибирский математический журнал
Сентябрь—октябрь, 2026. Том 67, № 5

УДК 512.55

МАТРИЦЫ НАД ПОЛНЫМИ КОЛЬЦАМИ ДИСКРЕТНОГО НОРМИРОВАНИЯ

А. Н. Абызов

Аннотация. Для матриц над полными кольцами дискретного нормирования вводится и изучается матричный аналог понятия представителя Тейхмюллера, который тесно связан со свойствами p-адических пределов последовательностей следов p-примарных степеней целочисленных матриц, рассматриваемых в работе. Также получены обобщения матричных аналогов сравнений Эйлера и Гаусса на случай матриц над коммутативными кольцами.

DOI 10.33048/smzh.2026.67.501

Ключевые слова: кольцо дискретного нормирования, сравнение Гаусса, сравнение Эйлера, представитель Тейхмюллера.

1. Введение

В 1839 г. Шёнеманном в работе [1] было доказано сравнение

$$\alpha_1^p + \ldots + \alpha_m^p \equiv \alpha_1 + \ldots + \alpha_m \ (\mathrm{mod}\, p), \tag{1}$$

где $\alpha_1, \ldots, \alpha_m$ — все корни с учетом их кратностей унитарного многочлена $f \in \mathbb{Z}[x]$ и p — простое число. Это утверждение равносильно матричному аналогу малой теоремы Ферма, согласно которому для произвольной квадратной целочисленной матрицы A сравнение $\mathrm{tr}(A^p) \equiv \mathrm{tr}(A)(\mathrm{mod}\, p)$ имеет место для каждого простого числа p. Сравнение (1) впоследствии переоткрывалось в ряде работ, например, в работе С. О. Шатуновского [2]. Широким обобщением малой теоремы Ферма является сравнение

$$\sum_{d|n} \mu(d) a^{\frac{n}{d}} \equiv 0 (\mathrm{mod}\, n), \tag{2}$$

которое имеет место для произвольных $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и в литературе называется сравнением Гаусса. Частным случаем сравнения (2) является сравнение Эйлера, согласно которому сравнение

$$a^{p^n} \equiv a^{p^{n-1}} (\mathrm{mod}\, p^n) \tag{3}$$

имеет место для каждого простого числа p и всякого натурального числа n. Согласно Диксону [3, с. 84–86] сравнение (2) было впервые получено Гауссом в случае, когда a — простое число. В случае, когда a является степенью простого

Работа поддержана грантом Российского научного фонда (проект № 25-11-00348) и выполнена в рамках реализации программы развития Научно-образовательного математического центра Приволжского федерального округа (соглашение № 075-02-2026-1328/1).

числа сравнение Гаусса было доказано Шёнеманном в 1846 г. на основе того факта, что если p — простое число, то $\frac{\sum\limits_{d|n}\mu(d)(p^m)^{\frac{n}{d}}}{n}$ — количество неразложимых унитарных многочленов степени n над полем из p^m элементов. В общем случае сравнение Гаусса было доказано Серре в 1855 г. Обобщение сравнения Гаусса на случай кольца целых конечного расширения поля $\mathbb{Q}$ было получено согласно [3, с. 86] в 1902 г. Вестлундом. Этот результат также был переоткрыт в недавней работе [4]. Матричный аналог сравнения Гаусса, согласно которому для каждой квадратной целочисленной матрицы A сравнение

$$\sum_{d|n}\mu(d)\operatorname{tr}(A^{\frac{n}{d}})\equiv 0(\operatorname{mod} n) \tag{4}$$

имеет место для всякого натурального числа n, независимо был получен в 1921 г. Янихеном [5] и Шуром [6] в 1937 г. В частности, имеет место матричный аналог сравнения Эйлера, согласно которому для произвольной квадратной целочисленной матрицы A и простого числа p сравнение

$$\operatorname{tr}(A^{p^n})\equiv \operatorname{tr}(A^{p^{n-1}})(\operatorname{mod} p^n) \tag{5}$$

имеет место для каждого $n\in\mathbb{N}$. Матричные аналоги сравнений Эйлера и Гаусса и различные способы их доказательств изучены в работах [7–12].

Из сравнения (5) следует, что для произвольной квадратной целочисленной матрицы A последовательность $(\operatorname{tr}(A^{p^n}))_{n\in\mathbb{N}}$ сходится относительно p-адической нормы к некоторому p-адическому числу. Одной из целей настоящей работы является изучение свойств таких пределов на основе арифметических свойств матриц над полными кольцами дискретного нормирования. Также изучаются обобщения сравнений Эйлера и Гаусса на случай матриц над коммутативными кольцами. Второй раздел носит предварительный характер и в нем в случае коммутативного кольца R приводятся обобщения сравнений Эйлера и Гаусса по модулю максимальных идеалов M, у которых фактор-кольца R/M конечны. В третьем разделе показано, что каждая матрица $A\in M_n(R)$, где R — полное кольцо дискретного нормирования, у которого $R/J(R)\cong\mathbb{F}_q$ и $J(R)=\pi R$, однозначно представима в виде $A=E+N$, где $E^{q^s}=E$, $N^k\in M_n(J(R))$ для некоторых $s,k\in\mathbb{N}$ и $EN=NE$. При этом π-адический предел $\lim\limits_{t\to\infty}A^{q^{st}}$ равен E. Матрицу E можно рассматривать как естественный матричный аналог представителя Тейхмюллера для матрицы A. В четвертом разделе матричные аналоги сравнений Эйлера и Гаусса обобщаются на случай коммутативных колец. В качестве приложений получены аналогичные сравнения для следов целых алгебраических элементов из конечных расширений поля $\mathbb{Q}$. В пятом разделе с помощью матричного аналога представителя Тейхмюллера доказываются свойства p-адических пределов вида $\lim\limits_{k\to\infty}\operatorname{tr}(A^{p^k})$, где A — целочисленная матрица и p — простое число. В частности, показано, что такие пределы являются целыми над $\mathbb{Z}$, а группы Галуа полей разложения их минимальных многочленов над $\mathbb{Q}$ являются абелевыми. Также приведены примеры, иллюстрирующие доказанные утверждения.

Группу обратимых элементов кольца R и радикал Джекобсона R будем обозначать соответственно через $U(R)$ и $J(R)$. Если I — идеал кольца R, то для произвольных элементов $a,b\in R$ тот факт, что $a-b\in I$, будем обозначать через $a\equiv b(\operatorname{mod} I)$.

2. Предварительные результаты

Лемма 2.1. *Пусть R — коммутативное локальное кольцо, I — собственный идеал R и $R/J(R) \cong \mathbb{F}_q$, где $q = p^s$ и p — простое число. Если $\bigcap\limits_{k=1}^{\infty} I^k = 0$, R полно в I-адической топологии и $J(R)/I$ — ниль-идеал фактор-кольца R/I, то всякий элемент $a \in R$ однозначно представим в виде*

$$a = e + j,$$

где $e^q = e$, $j \in J(R)$. При этом I-адический предел $\lim\limits_{k\to\infty} a^{q^k}$ равен e.

Доказательство. Первый случай: I — ниль-идеал. Ясно, что согласно условию леммы первый случай равносилен тому факту, что $J(R)$ является ниль-идеалом. Рассмотрим естественный гомоморфизм $f : R \to R/J(R)$. Гомоморфизм f индуцирует сюръективный гомоморфизм $g = f_{|U(R)} : U(R) \to U(R/J(R))$. Покажем, что $\operatorname{Ker}(g) = \{1 + j \mid j \in J(R)\}$ является p-группой. Пусть $1 + j \in \operatorname{Ker}(g)$, где $j \in J(R)$. Так как $p1_R \in J(R)$, то $(p1_R)^{k_1} = j^{p^{k_2}} = 0$ для некоторых $k_1, k_2 \in \mathbb{N}$. Тогда для некоторого $t \in R$ имеют место равенства $(1 + j)^{p^{k_1+k_2}} = (1 + pt)^{p^{k_1}} = 1$. Так как $U(R)/\operatorname{Ker}(g)$ является циклической группой порядка $q - 1$ и $q - 1$ не делится на p, то стандартные рассуждения показывают, что для некоторой циклической подгруппы H группы $U(R)$ группа $U(R)$ является прямым произведением своих подгрупп $\operatorname{Ker}(g)$ и H. Очевидно, что H совпадает с множеством всех элементов r из R, для которых выполнено равенство $r^{q-1} = 1$. Следовательно, для каждого элемента r из R существует однозначно определенный q-потент e такой, что $r \equiv e (\operatorname{mod} J(R))$.

Второй случай: $I^k \neq 0$ для каждого $k \in \mathbb{N}$. Для каждого натурального числа k естественный гомоморфизм из R/I^{k+1} в R/I^k обозначим через π_k. Из условия леммы следует, что имеет место изоморфизм $R \cong \varprojlim R/I^k = \{(r_k)_{k\in\mathbb{N}} \mid \pi_k(r_{k+1}) = r_k\}$. Для произвольного элемента $(r_k)_{k\in\mathbb{N}} \in \varprojlim R/I^k$, где $r_k \in R/I^k$ для каждого k, согласно первому случаю имеет однозначное представление в виде $r_k = e_k + j_k$, где $e_k \in R/I^k$, $j_k \in J(R)/I^k$ и $e_k^q = e_k$. Тогда из однозначности следует, что для каждого $k \in \mathbb{N}$ имеют место равенства $\pi_k(e_{k+1}) = e_k$, $\pi_k(j_{k+1}) = j_k$. Таким образом, всякий элемент r из R однозначно представим в виде $r = e + j$, где $e^q = e$ и $j \in J(R)$.

Рассмотрим произвольный элемент $a \in R$. Согласно изложенному выше имеет место равенство $a = e + j$, где $e^q = e$, $j \in J(R)$. Покажем, что $e = \lim\limits_{k\to\infty} a^{q^k}$. Для некоторого t_0 имеем $p^{t_0}, j^{t_0} \in I$. Пусть n — произвольное натуральное число. Тогда для каждого натурального числа N такого, что $N > \frac{2t_0 n}{s}$, имеют место равенства

$$a^{q^N} = (e + j)^{q^N} = e + \sum_{1\le k\le sN} \binom{p^{sN}}{k} e^{p^{sN}-k} j^k + \sum_{sN<k} \binom{p^{sN}}{k} e^{p^{sN}-k} j^k$$

и поскольку $p^{sN-k+1} \mid \binom{p^{sN}}{k}$ для $1 \le k \le sN$, то $a^{q^N} - e \in I^n$. Таким образом, $e = \lim\limits_{k\to\infty} a^{q^k}$. $\square$

Отметим важный случай предыдущего утверждения. Пусть L — локальное поле, т. е. поле, полное относительно дискретного нормирования ν, у которого поле вычетов конечно. В этом случае хорошо известно, что для всякого элемента a из кольца нормирования для ν однозначно определен такой q-потент e, где

q — количество элементов из поля вычетов ν, что $\nu(a-e)<1$. Этот q-потент называется *представителем Тейхмюллера* для a.

Следствие 2.2. *Пусть кольцо R коммутативно и M — максимальный идеал. Если $R/M\cong\mathbb{F}_q$, где $q=p^s$ и p — простое число, то имеют место утверждения:*

(1) *для каждого $n\in\mathbb{N}$ всякий элемент $a\in R/M^n$ однозначно представим в виде*
$$a=e+\beta,$$
где $e^q=e$ и $\beta\in Nil(R/M^n)$;

(2) *для каждого $n\in\mathbb{N}$ и всякого элемента $a\in R/M^{s(n-1)+1}$ выполнено равенство $a^{q^n}=a^{q^{n-1}}$.*

Доказательство. Первый пункт следует из леммы 2.1. Докажем второй пункт. Так как при $n=1$ утверждение п. (2) очевидно, то без ограничения общности можно считать, что $n>1$. Пусть $a\in R/M^{s(n-1)+1}$. Согласно п. (1) для a имеет место равенство $a=e+\beta$, где $e^q=e$ и $\beta\in M/M^{s(n-1)+1}$. Так как $p^{s(n-1)-k+1}\mid\binom{p^{s(n-1)}}{k}$ для $1\leq k\leq s(n-1)$ и $p\in M$, то

$$a^{q^{n-1}}=(e+\beta)^{q^{n-1}}=e+\sum_{1\leq k\leq s(n-1)}\binom{p^{s(n-1)}}{k}e^{p^{s(n-1)}-k}\beta^k + \sum_{s(n-1)<k}\binom{p^{s(n-1)}}{k}e^{p^{s(n-1)}-k}\beta^k=e$$

и, следовательно, $a^{q^n}=(a^{q^{n-1}})^q=e^q=e=a^{q^{n-1}}$. $\square$

Следствие 2.3. *Пусть $P/\mathbb{Q}$ — конечное расширение и R — кольцо целых поля P. Если M — простой идеал кольца R, то для каждого $n\in\mathbb{N}$ и для всякого $a\in R$ имеет место сравнение*
$$a^{N(M)^n}\equiv a^{N(M)^{n-1}}(\mathrm{mod}\, M^{s(n-1)+1}),$$
где s — относительная степень идеала M над $M\cap\mathbb{Z}$. В частности, для каждого $a\in R$ имеет место сравнение
$$a^{N(M)^n}\equiv a^{N(M)^{n-1}}(\mathrm{mod}\, M^n).$$

Следствие 2.4. *Пусть R — коммутативное кольцо, $M_1,\ldots,M_k$ — различные максимальные идеалы кольца R и для каждого i имеет место изоморфизм $R/M_i\cong\mathbb{F}_{q_i}$, где $q_i=p_i^{s_i}$ и p_i — простое число. Тогда для каждого $a\in R$ и любого набора натуральных чисел $n_1,\ldots,n_k$ имеет место сравнение*
$$a^{q_1^{n_1}\cdots q_k^{n_k}}+\sum_{t=1}^{k}(-1)^t\sum_{1\leq i_1<\ldots<i_t\leq k}a^{\frac{q_1^{n_1}\cdots q_k^{n_k}}{q_{i_1}\cdots q_{i_t}}}\equiv 0\left(\mathrm{mod}\prod_{i=1}^{k}M_i^{s_i(n_i-1)+1}\right). \qquad (6)$$

Доказательство. Обозначим левую часть сравнения (6) через A. Для каждого $1\leq i\leq k$ и всякого натурального числа m согласно следствию 2.2 имеет место сравнение
$$a^{mq_i^{n_i}}\equiv a^{mq_i^{n_i-1}}\left(\mathrm{mod}\, M_i^{s_i(n_i-1)+1}\right).$$

Следовательно, $A \in M_i^{s_i(n_i-1)+1}$ для каждого $1 \leq i \leq k$. Так как семейство идеалов $M_1, \ldots, M_k$ комаксимально, то

$$\bigcap_{i=1}^{k} M_i^{s_i(n_i-1)+1} = \prod_{i=1}^{k} M_i^{s_i(n_i-1)+1}.$$

Таким образом, $A \in \prod\limits_{i=1}^{k} M_i^{s_i(n_i-1)+1}$. $\square$

Следуя [4], введем обобщение функции Мёбиуса на случай колец целых конечных расширений поля $\mathbb{Q}$. Пусть $K/\mathbb{Q}$ — конечное расширение поля $\mathbb{Q}$ и R — кольцо целых K. Для произвольного ненулевого собственного идеала I кольца R положим $\mu(I) = (-1)^n$, если I является произведением n различных простых идеалов R, и $\mu(I) = 0$, если I делится на квадрат некоторого простого идеала. Также положим $\mu(R) = 1$. Из следствия 2.4 непосредственно вытекает

Следствие 2.5. *Пусть $P/\mathbb{Q}$ — конечное расширение, R — кольцо целых поля P и $A = M_1^{n_1} \ldots M_k^{n_k}$, где $M_1, \ldots, M_k$ — различные простые идеалы кольца R и $n_1, \ldots, n_k \in \mathbb{N}$. Если $N(M_i) = p_i^{s_i}$ для каждого $1 \leq i \leq k$, где p_i — простое число, то для всякого $a \in R$ имеет место сравнение*

$$\sum_{I|A} \mu(I) a^{N(AI^{-1})} \equiv 0 \left(\mathrm{mod} \prod_{i=1}^{k} M_i^{s_i(n_i-1)+1} \right). \tag{7}$$

В частности, для каждого $a \in R$ имеет место сравнение

$$\sum_{I|A} \mu(I) a^{N(AI^{-1})} \equiv 0 (\mathrm{mod}\, A). \tag{8}$$

Следствие 2.6. *Пусть $P/\mathbb{Q}$ — конечное расширение и R — кольцо целых поля P. Если M — простой идеал кольца R и $N(M) = p^s$, где p — простое число, то имеют место утверждения*

(1) *для каждого $n \in \mathbb{N}$ всякий элемент $a \in R/M^n$ однозначно представим в виде*

$$a = e + \beta,$$

где $e^{p^s} = e$ и $\beta \in Nil(R/M^n)$;

(2) *сравнение*

$$a^{p^r} \equiv a^{p^{r-1}} (\mathrm{mod}\, M^r)$$

выполнено для каждых $a \in R$ и $r \in \mathbb{N}$ в точности тогда, когда $s = 1$.

3. Разложения матрицы над полными кольцами дискретного нормирования

Пусть A — алгебра над кольцом дискретного нормирования R и $J(R) = \pi R$. Линейную топологию на A, в которой степени идеала πA образуют фундаментальную систему окрестностей нуля, назовем *π-адической.*

Теорема 3.1. *Пусть R — полное кольцо дискретного нормирования, $J(R) = \pi R$ и $R/J(R) \cong \mathbb{F}_q$, где $q = p^r$ и p — простое число. Тогда для каждого $n \in \mathbb{N}$ всякая матрица $A \in M_n(R)$ однозначно представима в виде*

$$A = E + N,$$

где $E^{q^s} = E$, $N^k \in M_n(J(R))$ *для некоторых* $s, k \in \mathbb{N}$ *и* $EN = NE$. *При этом* π*-адический предел* $\lim\limits_{k\to\infty} A^{q^{sk}}$ *равен* E.

Доказательство. Пусть $A \in M_n(R)$. Так как R-алгебра $R[A]$ является алгеброй конечного типа, то из [13, теорема 10.1.4] следует, что для некоторого семейства ортогональных ненулевых идемпотентов $e_1, \ldots, e_m \in R[A]$ выполнены условия: $R[A]e_i$ — локальная алгебра для каждого i и $1 = e_1 + \ldots + e_m$. Фиксируем некоторое $1 \leq i \leq m$. Ясно, что алгебра $R[A]e_i$ является полной в π-адической топологии и как R-модуль конечно порождена и свободна. Покажем, что πe_i содержится в радикале Джекобсона $J(R[A]e_i)$ алгебры $R[A]e_i$. Предположим противное, тогда для некоторого $a \in R[A]e_i$ имеет место равенство $\pi a = e_i$ и, следовательно, $\pi R[A]e_i = R[A]e_i$. Получили противоречие с леммой Накаямы. Таким образом, $\pi R[A]e_i \subseteq J(R[A]e_i)$. Фактор-кольцо $R[A]e_i/\pi R[A]e_i$ имеет естественную структуру конечномерного векторного пространства над полем $R/\pi R$. Тогда $R[A]e_i/\pi R[A]e_i$ — конечное кольцо и, следовательно, $J(R[A]e_i)/\pi R[A]e_i$ является нильпотентным идеалом $R[A]e_i/\pi R[A]e_i$. Заметим, что $R[A]e_i/J(R[A]e_i)$ — конечное поле, порядок которого равен q^{s_i}, где s_i — некоторое натуральное число. Тогда из леммы 2.1 следует, что имеет место равенство $e_iA = E_i + N_i$, где $E_i^{q^{s_i}} = E_i \in R[A]e_i, N_i \in J(R[A]e_i)$ и $N_i^{k_i} \in \pi R[A]e_i$ для некоторого $k_i \in \mathbb{N}$. Таким образом, для матрицы A имеет место представление

$$A = E + N,$$

где

$$E = \sum_{i=1}^{m} E_i,\ N = \sum_{i=1}^{m} N_i,\ E^{q^{s_1\cdots s_m}} = E,\ N^{\max(k_1,\ldots,k_m)} \in \pi M_n(R),\ EN = NE.$$

Пусть $s = s_1 \ldots s_m$ и $k = \max(k_1, \ldots, k_m)$.

Покажем, что $E = \lim\limits_{k\to\infty} A^{q^{sk}}$. Пусть k_0 — такое натуральное число, что $p^{k_0} > k$. Тогда для некоторого $T \in M_n(R)$ имеет место равенство $A^{p^{k_0}} = (E+N)^{p^{k_0}} = E^{p^{k_0}} + pT + N^{p^{k_0}}$. Так как $p \in \pi R$ и $N^{p^{k_0}} \in \pi M_n(R)$, то $A^{p^{k_0}} = E^{p^{k_0}} + \pi T'$, где $T' \in M_n(R)$. Несложно заметить, что T' коммутирует с E. Тогда для каждого натурального числа $t > \frac{k_0}{rs}$ имеют место равенства

$$A^{q^{st}} = A^{p^{rst}} = (A^{p^{k_0}})^{p^{rst-k_0}} = (E^{p^{k_0}} + \pi T')^{p^{rst-k_0}}$$

$$= E + \sum_{1\leq i\leq rst-k_0} \binom{p^{rst-k_0}}{i} E^{p^{rst}-ip^{k_0}} \pi^i T'^i + \sum_{rst-k_0<i} \binom{p^{rst-k_0}}{i} E^{p^{rst}-ip^{k_0}} \pi^i T'^i.$$

Поскольку $p^{rst-k_0-i+1} \mid \binom{p^{rst-k_0}}{i}$ для $1 \leq i \leq rst-k_0$, то $A^{q^{st}} - E \in \pi^{rst-k_0} M_n(R)$. Таким образом, последовательность $(A^{q^{sk}})_{k\in\mathbb{N}}$ в π-адической топологии сходится к E.

Предположим, что для матрицы A имеет место также разложение

$$A = E' + N',$$

где $E'^{q^{s'}} = E'$, $N'^{k'} \in \pi M_n(R)$ и $E'N' = N'E'$. Тогда $E' = \lim\limits_{k\to\infty} A^{q^{s'k}}$ и, следовательно,

$$E' = \lim_{k\to\infty} A^{q^{s'k}} = \lim_{k\to\infty} A^{q^{s'sk}} = \lim_{k\to\infty} A^{q^{sk}} = E. \quad \square$$

Далее матрицу E из формулировки предыдущего утверждения будем называть *представителем Тейхмюллера* для матрицы A.

Лемма 3.2. *Пусть R — полное кольцо дискретного нормирования и $R/J(R) \cong \mathbb{F}_q$. Тогда*

(1) *если E_1, E_2 — представители Тейхмюллера соответственно для матриц $A, B \in M_n(R)$ и $AB = BA$, то E_1E_2 — представитель Тейхмюллера для матрицы AB;*

(2) *если матрица A обратима в $M_n(R)$ и E — ее представитель Тейхмюллера, то матрица E обратима в $M_n(R)$ и E^{-1} является представителем Тейхмюллера для A^{-1}.*

Доказательство. (1) Для некоторых $s_1, s_2 \in \mathbb{N}$ имеют место равенства

$$E_1 = \lim_{k\to\infty} A^{q^{s_1 k}}, \quad E_2 = \lim_{k\to\infty} B^{q^{s_2 k}}.$$

Тогда

$$E_1E_2 = \lim_{k\to\infty} A^{q^{s_1 s_2 k}} \lim_{k\to\infty} B^{q^{s_1 s_2 k}} = \lim_{k\to\infty} (AB)^{q^{s_1 s_2 k}}$$

и, следовательно, E_1E_2 — представитель Тейхмюллера для матрицы AB.

(2) Следует из первого пункта. □

Теорема 3.3. *Пусть R — коммутативное локальное кольцо, для которого имеет место изоморфизм $R/J(R) \cong \mathbb{F}_q$ и $\bigcap\limits_{k=1}^{\infty} J(R)^k = 0$. Если R полно в $J(R)$-адической топологии, то для каждого $n \in \mathbb{N}$ всякая матрица $A \in M_n(R)$ представима в виде*

$$A = E + N,$$

где $E^q = E$, $N^k \in M_n(J(R))$ для некоторого $k \in \mathbb{N}$.

Доказательство. Пусть $A \in M_n(R)$. Рассмотрим естественный гомоморфизм $f : R \to R/J(R)$. Через f также обозначим гомоморфизм из $M_n(R)$ в $M_n(R/J(R))$, индуцированный этим естественным гомоморфизмом. Обозначим поле $R/J(R)$ через P. Согласно [14, теорема 2] имеет место равенство $f(A) = E + N$, где $E, N \in M_n(P), E^q = E$ и $N^k = 0$ для некоторого $k \in \mathbb{N}$. Так как фактор-алгебра $P[x]/(x^q - x)$ изоморфна конечному прямому произведению поля P, то для некоторого семейства ортогональных идемпотентов $e_1, \ldots, e_m \in P[E]$ имеет место равенство $E = \sum\limits_{i=1}^{m} e_i f(\alpha_i)$, где $\alpha_i \in R$ для каждого i. Согласно [15, теорема 12.4, с. 43] для некоторого семейства ортогональных идемпотентов $E_1, \ldots, E_m \in M_n(R)$ равенство $f(E_i) = e_i$ выполнено для каждого i. Из леммы 2.1 следует, что для каждого i имеет место равенство $\alpha_i = \varepsilon_i + \beta_i$, где $\varepsilon_i, \beta_i \in R$, $\varepsilon_i^q = \varepsilon_i$ и $\beta_i \in J(R)$. Тогда $E' = \sum\limits_{i=1}^{m} E_i\varepsilon_i$ — q-потент и $f(E') = E$. Так как $f(A - E')^k = N^k = 0$, то $(A - E')^k \in J(M_n(R))$. □

Следующее утверждение можно рассматривать как матричный аналог первого пункта следствия 2.2.

Следствие 3.4. *Пусть кольцо R коммутативно и M — максимальный идеал. Если $R/M \cong \mathbb{F}_q$, то для каждых $m, n \in \mathbb{N}$ всякая матрица $A \in M_n(R/M^m)$ представима в виде*

$$A = E + N,$$

где $E^q = E$, $N^k = 0$ для некоторого $k \in \mathbb{N}$.

4. Сравнения для следов матриц над коммутативными кольцами

Следующее утверждение является обобщением матричного аналога малой теоремы Ферма, установленного в работе [1], на случай коммутативных колец.

Теорема 4.1 [14, следствие 2]. *Пусть R — коммутативное кольцо и M — максимальный идеал кольца R такой, что $R/M \cong \mathbb{F}_q$. Тогда для произвольного $n \in \mathbb{N}$ и каждой матрицы $A \in M_n(R)$ имеет место сравнение*

$$\operatorname{tr}(A^q) \equiv \operatorname{tr}(A) (\operatorname{mod} M). \tag{9}$$

Пусть R — область целостности, $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in R[x]$ — унитарный многочлен степени n и $\alpha_1, \ldots, \alpha_n$ — все его корни с учетом их кратностей из некоторого конечного расширения поля частных R. Через C_f будем обозначать сопровождающую матрицу к f, т. е. матрицу вида

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Хорошо известно, что характеристический многочлен матрицы C_f совпадает с f. Следовательно, для каждого натурального числа m имеет место равенство $\alpha_1^m + \ldots + \alpha_n^m = \operatorname{tr}\big(C_f^m\big)$. Таким образом, всякая последовательность $(\operatorname{tr}(A^{q^k}))_{k\in\mathbb{N}}$, где $A \in M_n(R)$ и $q \in \mathbb{N}$, совпадает с последовательностью вида $\big(\alpha_1^{q^k} + \ldots + \alpha_n^{q^k}\big)_{k\in\mathbb{N}}$, где $\alpha_1, \ldots, \alpha_n$ — все корни с учетом их кратностей некоторого унитарного многочлена $f \in R[x]$, и наоборот.

Следующее утверждение можно рассматривать как матричный аналог второго пункта следствия 2.2.

Теорема 4.2. *Пусть R — коммутативное кольцо и M — максимальный идеал кольца R такой, что $R/M \cong \mathbb{F}_q$, где $q = p^s$ и p — простое число. Тогда для произвольного неотрицательного целого числа m, каждого $n \in \mathbb{N}$ и всякой матрицы $A \in M_n(R)$ имеет место сравнение*

$$\operatorname{tr}(A^{q^{m+1}}) \equiv \operatorname{tr}(A^{q^m}) (\operatorname{mod} M^{sm+1}). \tag{10}$$

В частности, если $R/M \cong \mathbb{F}_p$, то $\operatorname{tr}(A^{p^{m+1}}) \equiv \operatorname{tr}(A^{p^m}) (\operatorname{mod} M^{m+1})$.

Доказательство. Предположим, что R — область целостности. Докажем с помощью индукции по k, что для произвольного $n \in \mathbb{N}$ и для каждой матрицы $X \in M_n(R)$ имеет место сравнение

$$\operatorname{tr}(X^{qp^k}) \equiv \operatorname{tr}(X^{p^k}) \ (\operatorname{mod} M^{k+1}). \tag{11}$$

При $k = 0$ утверждение следует из теоремы 4.1. Предположим, что для некоторого неотрицательного целого числа k сравнение (11) имеет место для всякой матрицы $X \in M_n(R)$. Пусть $A \in M_n(R)$ и $Q(R)$ — поле частных кольца R, $K/Q(R)$ — поле разложение характеристического многочлена $\chi_A(t)$ матрицы A и $\alpha_1, \ldots, \alpha_n \in K$ — все корни $\chi_A(t)$ с учетом их кратностей. Для каждого семейства неотрицательных целых чисел $k_1, \ldots, k_n$ через $A_{k_1,\ldots,k_n}$ обозначим

множество всех мономов из $R[x_1,\dots,x_n]$, получаемых из $x_1^{k_1}\dots x_n^{k_n}$ перестановками переменных. Сумму всех элементов из множества $A_{k_1,\dots,k_n}$ обозначим через $S_{k_1,\dots,k_n}(x_1,\dots,x_n)$. Несложно заметить, что если $f_1,\dots,f_N$ — все различные мономы из $A_{k_1,\dots,k_n}$, то $f_1(\alpha_1,\dots,\alpha_n),\dots,f_N(\alpha_1,\dots,\alpha_n)$ — все корни с учетом их кратностей некоторого унитарного многочлена из $R[x]$.

Из предположения индукции и замечаний, сделанных перед теоремой 4.2, следуют сравнения

$$\alpha_1^{qp^k}+\dots+\alpha_n^{qp^k}\equiv\alpha_1^{p^k}+\dots+\alpha_n^{p^k}(\operatorname{mod}M^{k+1}),\tag{12}$$

$$f_1(\alpha_1,\dots,\alpha_n)^{qp^k}+\dots+f_N(\alpha_1,\dots,\alpha_n)^{qp^k}\equiv f_1(\alpha_1,\dots,\alpha_n)^{p^k}+\dots+f_N(\alpha_1,\dots,\alpha_n)^{p^k}(\operatorname{mod}M^{k+1}).$$

При этом последнее сравнение можно записать в виде

$$S_{k_1,\dots,k_n}\big(\alpha_1^{qp^k},\dots,\alpha_n^{qp^k}\big)\equiv S_{k_1,\dots,k_n}\big(\alpha_1^{p^k},\dots,\alpha_n^{p^k}\big)(\operatorname{mod}M^{k+1}).\tag{13}$$

Имеют место равенства

$$\big(\alpha_1^{qp^k}+\dots+\alpha_n^{qp^k}\big)^p=\alpha_1^{qp^{k+1}}+\dots+\alpha_n^{qp^{k+1}}+\sum_{\substack{k_1+\dots+k_n=p,\\ p>k_1\geq k_2\geq\dots\geq k_n}}\binom{p}{k_1,\dots,k_n}S_{k_1,\dots,k_n}\big(\alpha_1^{qp^k},\dots,\alpha_n^{qp^k}\big),$$

$$\big(\alpha_1^{p^k}+\dots+\alpha_n^{p^k}\big)^p=\alpha_1^{p^{k+1}}+\dots+\alpha_n^{p^{k+1}}+\sum_{\substack{k_1+\dots+k_n=p,\\ p>k_1\geq k_2\geq\dots\geq k_n}}\binom{p}{k_1,\dots,k_n}S_{k_1,\dots,k_n}\big(\alpha_1^{p^k},\dots,\alpha_n^{p^k}\big).$$

Так как $p\in M$, из сравнений (12), (13) следует, что

$$\big(\alpha_1^{qp^k}+\dots+\alpha_n^{qp^k}\big)^p\equiv\big(\alpha_1^{p^k}+\dots+\alpha_n^{p^k}\big)^p(\operatorname{mod}M^{k+2}),$$

$$\sum_{\substack{k_1+\dots+k_n=p,\\ p>k_1\geq k_2\geq\dots\geq k_n}}\binom{p}{k_1,\dots,k_n}S_{k_1,\dots,k_n}\big(\alpha_1^{qp^k},\dots,\alpha_n^{qp^k}\big)\equiv\sum_{\substack{k_1+\dots+k_n=p,\\ p>k_1\geq k_2\geq\dots\geq k_n}}\binom{p}{k_1,\dots,k_n}S_{k_1,\dots,k_n}\big(\alpha_1^{p^k},\dots,\alpha_n^{p^k}\big)(\operatorname{mod}M^{k+2}).$$

Таким образом, имеет место сравнение $\operatorname{tr}(A^{qp^{k+1}})\equiv\operatorname{tr}(A^{p^{k+1}})(\operatorname{mod}M^{k+2})$.

Покажем, что для произвольной матрицы $A\in M_n(R)$ выполнено сравнение (10). Так как согласно доказанному выше для произвольного неотрицательного целого числа k имеет место сравнение $\operatorname{tr}(A^{qp^k})\equiv\operatorname{tr}(A^{p^k})(\operatorname{mod}M^{k+1})$, то для $k=sm$ имеем $\operatorname{tr}(A^{q^{m+1}})\equiv\operatorname{tr}(A^{q^m})(\operatorname{mod}M^{sm+1})$.

Предположим теперь, что R — произвольное коммутативное кольцо, для которого выполнены условия теоремы, и $A\in M_n(R)$. Несложно заметить, что для некоторой области целостности R' имеет место эпиморфизм колец $\psi:R'\to$

R. В качестве такого эпиморфизма можно рассмотреть, например, гомоморфизм, действующий из $\mathbb{Z}[\{x_r\}_{r\in R}]$ в R согласно правилу $x_r \mapsto r$ для каждого $r \in R$. Гомоморфизм ψ индуцирует кольцевой гомоморфизм $\psi' : M_n(R') \to M_n(R)$. Ясно, что $\psi^{-1}(M)$ — максимальный идеал кольца R' и $R'/\psi^{-1}(M) \cong \mathbb{F}_q$. Для некоторой матрицы $B \in M_n(R')$ имеет место равенство $\psi'(B) = A$. Тогда согласно доказанному выше имеет место сравнение

$$\operatorname{tr}(B^{q^{m+1}}) \equiv \operatorname{tr}(B^{q^m}) (\operatorname{mod} \psi^{-1}(M)^{sm+1}).$$

Таким образом, $\operatorname{tr}(A^{q^{m+1}}) \equiv \operatorname{tr}(A^{q^m}) (\operatorname{mod} M^{sm+1})$. $\square$

Замечание 4.3. Пусть M — максимальный идеал коммутативного кольца R, для которого выполнены условия: $R/M \cong \mathbb{F}_q$ и $\bigcap\limits_{i=1}^{\infty} M^i = 0$. Из предыдущей теоремы следует, что для каждого $n \in \mathbb{N}$ и всякой матрицы $A \in M_n(R)$ последовательность $(\operatorname{tr}(A^{q^k}))_{k\in\mathbb{N}}$ сходится к некоторому элементу из M-адического пополнения кольца R. Свойства таких пределов в случае, когда R — кольцо целых некоторого конечного расширения $P/\mathbb{Q}$, будут рассмотрены в следующем разделе.

Доказательство следующего утверждения аналогично доказательству следствия 2.4.

Следствие 4.4. *Пусть R — коммутативное кольцо, $M_1, \dots, M_k$ — различные максимальные идеалы R и для каждого i имеет место изоморфизм $R/M_i \cong \mathbb{F}_{q_i}$, где $q_i = p_i^{s_i}$ и p_i — простое число. Тогда для произвольного $n \in \mathbb{N}$, каждой матрицы $A \in M_n(R)$ и любого набора натуральных чисел $n_1, \dots, n_k$ имеет место сравнение*

$$\operatorname{tr}(A^{q_1^{n_1}\cdots q_k^{n_k}}) + \sum_{t=1}^{k}(-1)^t \sum_{1\le i_1<\ldots<i_t\le k} \operatorname{tr}(A^{\frac{q_1^{n_1}\cdots q_k^{n_k}}{q_{i_1}\cdots q_{i_t}}}) \equiv 0 \left(\operatorname{mod} \prod_{i=1}^{k} M_i^{s_i(n_i-1)+1}\right). \tag{14}$$

Матричным аналогом сравнения (8) является следующее утверждение.

Следствие 4.5. *Пусть $K/\mathbb{Q}$ — конечное расширение, R — кольцо целых поля K и I — ненулевой идеал R. Тогда для произвольного $n \in \mathbb{N}$ и каждой матрицы $A \in M_n(R)$ имеет место сравнение*

$$\sum_{J|I} \mu(J) \operatorname{tr}(A^{N(IJ^{-1})}) \equiv 0 (\operatorname{mod} I). \tag{15}$$

Теорема 4.6. *Пусть R — дедекиндово кольцо, P — поле частных R, K/P — конечное сепарабельное расширение P и R' — целое замыкание R в K. Если M — максимальный идеал R и $R/M \cong \mathbb{F}_{p^s}$, где p — простое число, то для каждого $\alpha \in R'$ и произвольного неотрицательного целого числа m выполнено сравнение*

$$\operatorname{tr}_{K/P}(\alpha^{q^{m+1}}) \equiv \operatorname{tr}_{K/P}(\alpha^{q^m}) (\operatorname{mod} M^{sm+1}),$$

где $q = p^s$. В частности, если $R/M \cong \mathbb{F}_p$, то

$$\operatorname{tr}_{K/P}(\alpha^{p^{m+1}}) \equiv \operatorname{tr}_{K/P}(\alpha^{p^m}) (\operatorname{mod} M^{m+1}).$$

Доказательство. Пусть $\alpha \in R'$. Из условия теоремы следует, что R' является конечно порожденным R-модулем. Пусть $S = R \setminus M$. Тогда R_S является

кольцом дискретного нормирования и, следовательно, R'_S — свободный конечно порожденный R_S-модуль. Пусть $e_1, \dots, e_n$ — базис R_S-модуля R'_S. Так как $\alpha \in R'_S$, то имеет место эндоморфизм $\widehat{\alpha}$ модуля ${}_{R_S}R'_S$, действующий согласно правилу $x \mapsto \alpha x$ для каждого $x \in R'_S$. Пусть A — матрица $\widehat{\alpha}$ относительно базиса $e_1, \dots, e_n$. Так как $R_S/M_S \cong R/M \cong \mathbb{F}_{p^s}$, то согласно теореме 4.2 для каждого неотрицательного целого числа m имеет место сравнение

$$\operatorname{tr}(A^{q^{m+1}}) \equiv \operatorname{tr}(A^{q^m}) \big(\bmod M_S^{sm+1}\big). \tag{16}$$

Поскольку $\operatorname{tr}(A^{q^m}) = \operatorname{tr}_{K/P}(\alpha^{q^m}) \in R$, то стандартные рассуждения показывают, что выполнено также сравнение

$$\operatorname{tr}_{K/P}(\alpha^{q^m}) \equiv \operatorname{tr}_{K/P}(\alpha^{q^{m+1}}) (\bmod M^{sm+1}). \quad \square \tag{17}$$

Следующее утверждение вытекает из следствия 2.6 и теоремы 4.6.

Следствие 4.7. *Пусть L/K — конечное расширение числового поля K, R — кольцо целых поля K, R' — целое замыкание R в L и M — простой идеал кольца R, содержащий простое число p. Тогда для каждого элемента $b \in R'$ и произвольного неотрицательного целого числа m выполнено сравнение*

$$\operatorname{tr}_{L/K}(b^{N(M)^{m+1}}) \equiv \operatorname{tr}_{L/K}(b^{N(M)^m}) (\bmod M^{sm+1}),$$

где $N(M) = p^s$. В частности, если $R/M \cong \mathbb{F}_p$, то

$$\operatorname{tr}_{L/K}(b^{p^{m+1}}) \equiv \operatorname{tr}_{L/K}(b^{p^m}) (\bmod M^{m+1}).$$

Следствие 4.8. *Пусть L/K — конечное расширение числового поля K, R — кольцо целых поля K, R' — целое замыкание R в L и I — ненулевой идеал кольца R. Тогда для каждого элемента $b \in R'$ выполнено сравнение*

$$\sum_{J|I} \mu(J) \operatorname{tr}_{L/K}(b^{N(IJ^{-1})}) \equiv 0 (\bmod I). \tag{18}$$

Следствие 4.9 [9, теорема 3]. *Пусть L/K — расширение Галуа числового поля K, R — кольцо целых поля K и R' — целое замыкание R в L, M — простой идеал кольца R, содержащий простое число p и такой, что свойство*

$$a^{p^r} \equiv a^{p^{r-1}} (\bmod M^r) \tag{19}$$

выполнено для всех $r \in \mathbb{N}$ и $a \in R$. Тогда для каждого элемента $b \in R'$ и произвольного $r \in \mathbb{N}$ выполнено сравнение

$$\operatorname{tr}_{L/K}(b^{p^r}) \equiv \operatorname{tr}_{L/K}(b^{p^{r-1}}) (\bmod M^r).$$

Замечание 4.10. А. В. Зарелуа в работе [9] на странице 89 отметил возможность освобождения от требования справедливости сравнения (19) для всех $r \in \mathbb{N}$ и $a \in R$ из предыдущего утверждения за счет замены показателей p^r в формулировке следствия 4.9 на показатели $N(M^r)$. Следствие 4.7 можно рассматривать как одно из возможных утверждений, которое удовлетворяет выше сформулированному требованию.

5. Приложения и примеры

Теорема 5.1. *Пусть $P/\mathbb{Q}$ — конечное расширение, R — кольцо целых поля P, M — максимальный идеал R и $R/M \cong \mathbb{F}_q$. Тогда имеют место утверждения:*

(1) *для каждой матрицы $A \in M_n(R)$ M-адический предел $\lim\limits_{k\to\infty} \mathrm{tr}(A^{q^k})$ является целым над $\mathbb{Z}$ и группа Галуа поля разложения его минимального многочлена над $\mathbb{Q}$ является абелевой;*

(2) *для произвольной обратимой матрицы A из $M_n(R)$ M-адические пределы $\lim\limits_{k\to\infty} \mathrm{tr}(A^{q^k})$ и $\lim\limits_{k\to\infty} \mathrm{tr}(A^{-q^k})$ сопряжены над $\mathbb{Q}$.*

Доказательство. Пусть $A \in M_n(R)$. Через P' обозначим пополнение P относительно M-нормы. Также через R' и M' обозначим замыкания относительно M-нормы соответственно R и M в поле P'. Так как $R'/M' \cong R/M \cong \mathbb{F}_q$, то согласно теореме 3.1 для некоторого $s_0 \in \mathbb{N}$ имеет место равенство $\lim\limits_{k\to\infty} A^{q^{s_0 k}} = E$, где $E = E^{q^{s_0}}$ — представитель Тейхмюллера матрицы A, принадлежащий кольцу $M_n(R')$. Согласно замечанию 4.3 последовательность $(\mathrm{tr}(A^{q^k}))_{k\in\mathbb{N}}$ сходится к некоторому элементу из M-адического пополнения кольца R. Следовательно,

$$\lim_{k\to\infty} \mathrm{tr}(A^{q^k}) = \lim_{k\to\infty} \mathrm{tr}(A^{q^{s_0 k}}) = \mathrm{tr}(E).$$

Так как $E^{q^{s_0}} = E$, то $\mathrm{tr}(E)$ — сумма корней $(q^{s_0}-1)$-степени из единицы, принадлежащих алгебраическому замыканию поля P'. Таким образом, $\lim\limits_{k\to\infty} \mathrm{tr}(A^{q^k})$ — корень некоторого целочисленного унитарного многочлена, у которого группа Галуа его поля разложения над $\mathbb{Q}$ является абелевой.

Предположим, что $\det(A)$ обратим в R. Из леммы 3.2 следует, что

$$\lim_{k\to\infty} \mathrm{tr}(A^{-q^k}) = \mathrm{tr}(E^{-1}).$$

Следовательно, для автоморфизма φ поля $\mathbb{Q}(\varepsilon_{q^{s_0}-1})$, для которого выполнено равенство $\varphi(\varepsilon_{q^{s_0}-1}) = \varepsilon_{q^{s_0}-1}^{-1}$, имеем

$$\varphi(\lim_{k\to\infty} \mathrm{tr}(A^{q^k})) = \lim_{k\to\infty} \mathrm{tr}(A^{-q^k}). \quad \square$$

Следствие 5.2. *Пусть $A \in M_n(\mathbb{Z})$ и p — простое число. Тогда имеют место следующие утверждения:*

(1) *p-адический предел $\lim\limits_{k\to\infty} \mathrm{tr}(A^{p^k})$ является целым над $\mathbb{Z}$ и группа Галуа поля разложения его минимального многочлена над $\mathbb{Q}$ является абелевой;*

(2) *если $|\det(A)| = 1$, то p-адические числа $\lim\limits_{k\to\infty} \mathrm{tr}(A^{p^k})$, $\lim\limits_{k\to\infty} \mathrm{tr}(A^{-p^k}) \in \mathbb{Q}_p$ сопряжены над полем $\mathbb{Q}$.*

Следствие 5.3. *Пусть $P/\mathbb{Q}$ — конечное расширение, R — кольцо целых поля P, M — максимальный идеал R и $R/M \cong \mathbb{F}_q$. Если $A \in M_n(R)$ и $x^n + \sum\limits_{i=1}^{n} (-1)^i a_i^{(k)} x^{n-i}$ — характеристический многочлен A^k для каждого $k \in \mathbb{N}$, то для всякого $1 \le i \le n$ существует M-адический предел $\lim\limits_{k\to\infty} a_i^{(q^k)}$, который является целым над $\mathbb{Z}$ и группа Галуа поля разложения его минимального многочлена над $\mathbb{Q}$ является абелевой. При этом если A — обратимая матрица в $M_n(R)$ и E — представитель Тейхмюллера матрицы A, то коэффициенты характеристических*

многочленов матриц E и E^{-1}, стоящие при одинаковых степенях, сопряжены над $\mathbb{Q}$.

Доказательство. Рассмотрим линейный операторa $\mathbf{A}$, действующий на векторном пространстве P^n и у которого матрица относительно некоторого базиса P^n равна A. Тогда хорошо известно, что для каждого $1 \leq i \leq n$ и всякого $k \in \mathbb{N}$ $a_i^{(k)}$ — след линейного оператора $\bigwedge^i \mathbf{A}^k$, который действует на $\bigwedge^i(P^n)$. Так как, очевидно, относительно некоторого базиса $\bigwedge^i(P^n)$ компоненты матрицы линейного оператора $\bigwedge^i \mathbf{A}$ принадлежат R, то утверждение следствия 5.3 непосредственно вытекает из теоремы 5.1. $\square$

Для каждого $n \in \mathbb{N}$ через $L_n(x)$ и $F_n(x)$ обозначим соответственно многочлены

$$\sum_{i=0}^{[\frac{n}{2}]}(-1)^i \frac{n}{n-i}\binom{n-i}{i}x^{n-2i} - x \text{ и } \sum_{i=0}^{[\frac{n}{2}]}\frac{n}{n-i}\binom{n-i}{i}x^{n-2i} - x.$$

Далее нам потребуется следующее тождество, которое в литературе называется тождеством Куммера и является частным случаем тождества Жирара — Варинга:

$$x^n + y^n = \sum_{i=0}^{[\frac{n}{2}]}(-1)^i \frac{n}{n-i}\binom{n-i}{i}(xy)^i(x+y)^{n-2i}. \tag{20}$$

Теорема 5.4. *Пусть $P/\mathbb{Q}$ — конечное расширение, R — кольцо целых поля P, M — максимальный идеал R и $R/M \cong \mathbb{F}_q$. Если $A \in M_2(R)$, то M-адический предел $\alpha = \lim\limits_{k\to\infty} \operatorname{tr}(A^{q^k})$ — корень многочлена $\sum\limits_{i=0}^{[\frac{q}{2}]}(-1)^i \frac{q}{q-i}\binom{q-i}{i}\beta^i x^{q-2i} - x$, где β — представитель Тейхмюллера $\det(A)$, принадлежащий пополнению поля P относительно M-нормы.*

Доказательство. Пусть α_1, α_2 — корни характеристического многочлена матрицы A из алгебраического замыкания поля P. Тогда $\operatorname{tr}(A^n) = \alpha_1^n + \alpha_2^n$ для каждого $n \in \mathbb{N}$. Подставим в тождество (20) вместо n, x и y соответственно q, $\alpha_1^{q^k}$ и $\alpha_2^{q^k}$. В результате получим равенства

$$\sum_{i=0}^{[\frac{q}{2}]}(-1)^i \frac{q}{q-i}\binom{q-i}{i}(\alpha_1\alpha_2)^{q^k i}\operatorname{tr}(A^{q^k})^{q-2i} = \operatorname{tr}(A^{q^{k+1}}),$$

$$\lim_{k\to\infty}\left(\sum_{i=0}^{[\frac{q}{2}]}(-1)^i \frac{q}{q-i}\binom{q-i}{i}(\alpha_1\alpha_2)^{q^k i}\operatorname{tr}(A^{q^k})^{q-2i}\right) = \lim_{k\to\infty}(\operatorname{tr}(A^{q^{k+1}})),$$

$$\sum_{i=0}^{[\frac{q}{2}]}(-1)^i \frac{q}{q-i}\binom{q-i}{i}\beta^i\alpha^{q-2i} = \alpha. \quad \square$$

Если p — простое число, то кольцо целых p-адических чисел будем обозначать через $\widehat{\mathbb{Z}}_p$.

Следствие 5.5. *Пусть p — простое число. Имеют место следующие утверждения:*

(1) *для каждой матрицы $A \in M_2(\mathbb{Z})$, у которой $\det(A) = 1$, p-адический предел $\alpha = \lim\limits_{k\to\infty} \operatorname{tr}(A^{p^k})$ — корень многочлена $L_p(x)$ и $\alpha \equiv \operatorname{tr}(A) (\operatorname{mod} p)$;*

(2) *для каждого* $0 \leq r \leq p-1$ *существует такой однозначно определенный корень* $\alpha_r \in \widehat{\mathbb{Z}}_p$ *многочлена* $L_p(x)$, *что* $\alpha_r \equiv r (\mathrm{mod}\, p)$;
(3) *корни многочлена* $L_p(x)$ *составляют полную систему представителей смежных классов фактор-кольца* $\widehat{\mathbb{Z}}_p/p\widehat{\mathbb{Z}}_p$ *и имеет место равенство*

$$L_p(x) = \prod_{r=0}^{p-1}(x - \alpha_r).$$

Доказательство. Пусть A — произвольная матрица из $M_2(\mathbb{Z})$ и $\alpha = \lim\limits_{k\to\infty} \mathrm{tr}(A^{p^k})$. Так как сравнение $\mathrm{tr}(A^{p^n}) \equiv \mathrm{tr}(A) (\mathrm{mod}\, p)$ имеет место для каждого $n \in \mathbb{N}$, то $\alpha \equiv \mathrm{tr}(A) (\mathrm{mod}\, p)$. Для каждого $k \in \mathbb{N}$ для матрицы $A_0 = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ имеют место равенства $\mathrm{tr}(A_0) = k$ и $|A_0| = 1$. Тогда для каждого $0 \leq r \leq p-1$ существует такая матрица $A \in M_2(\mathbb{Z})$, что $|A| = 1$ и $\alpha_r = \lim\limits_{k\to\infty} \mathrm{tr}(A^{p^k})$ сравнимо с r по модулю p. Из теоремы 5.4 следует, что $\alpha_0, \ldots, \alpha_{p-1}$ — различные корни многочлена $L_p(x)$ степени p. Таким образом, имеет место равенство $L_p(x) = \prod\limits_{r=0}^{p-1}(x - \alpha_r)$. $\square$

Доказательство следующего утверждения аналогично доказательству следствия 5.5.

Следствие 5.6. *Пусть* p — *нечетное простое число. Имеют место следующие утверждения:*
(1) *для каждой матрицы* $A \in M_2(\mathbb{Z})$, *у которой* $\det(A) = -1$, *p-адический предел* $\beta = \lim\limits_{k\to\infty} \mathrm{tr}(A^{p^k})$ — *корень многочлена* $F_p(x)$ *и* $\beta \equiv \mathrm{tr}(A) (\mathrm{mod}\, p)$;
(2) *для каждого* $0 \leq r \leq p-1$ *существует такой однозначно определенный корень* $\beta_r \in \widehat{\mathbb{Z}}_p$ *многочлена* $F_p(x)$, *что* $\beta_r \equiv r (\mathrm{mod}\, p)$;
(3) *корни многочлена* $F_p(x)$ *составляют полную систему представителей смежных классов фактор-кольца* $\widehat{\mathbb{Z}}_p/p\widehat{\mathbb{Z}}_p$ *и имеет место равенство*

$$F_p(x) = \prod_{r=0}^{p-1}(x - \beta_r).$$

Рассмотрим некоторые свойства введенных выше семейств многочленов $(L_n(x))_{n\in\mathbb{N}}$ и $(F_n(x))_{n\in\mathbb{N}}$, которые представляют определенный интерес ввиду приведенных выше утверждений.

Лемма 5.7. *Пусть* n — *нечетное число,* $n > 1$. *Тогда*
(1) *над полем* $\mathbb{R}$ *для многочлена* $L_n(x)$ *имеет место разложение*

$$L_n(x) = \prod_{k=0}^{\frac{n-1}{2}} \left(x - 2\cos\left(\frac{2\pi k}{n-1}\right)\right) \prod_{k=1}^{\frac{n-1}{2}} \left(x - 2\cos\left(\frac{2\pi k}{n+1}\right)\right); \qquad (21)$$

(2) *над полем* $\mathbb{R}$ *для многочлена* $F_n(x)$ *имеют место следующие разложения:*
(a) *если* $n \equiv 1 (\mathrm{mod}\, 4)$ *и* $n = 4m+1$, *то*

$$F_n(x) = \prod_{k=1}^{m} \left(x^2 + 4\sin^2\left(\frac{2\pi k}{n-1}\right)\right) \prod_{k=1}^{m} \left(x^2 + 4\sin^2\left(\frac{\pi(2k-1)}{n+1}\right)\right) x, \qquad (22)$$

(b) *если* $n \equiv 3(\mathrm{mod}\,4)$ *и* $n = 4m+3$, *то*

$$F_n(x) = \prod_{k=1}^{m}\left(x^2 + 4\sin^2\left(\frac{2\pi k}{n-1}\right)\right)\prod_{k=1}^{m+1}\left(x^2 + 4\sin^2\left(\frac{\pi(2k-1)}{n+1}\right)\right)x. \tag{23}$$

Доказательство. (1) Для каждого натурального n через ε_n будем обозначать комплексный примитивный корень n-й степени из единицы. Так как $\varepsilon_{n-1}^{kn} = \varepsilon_{n-1}^{k}$, то согласно тождеству (20) имеют место равенства

$$L_n\left(2\cos\left(\frac{2\pi k}{n-1}\right)\right) = L_n\big(\varepsilon_{n-1}^{k} + \varepsilon_{n-1}^{-k}\big) = 0,$$

$$L_n\left(2\cos\left(\frac{2\pi k}{n+1}\right)\right) = L_n\big(\varepsilon_{n+1}^{k} + \varepsilon_{n+1}^{-k}\big) = 0.$$

Несложно заметить, что множество

$$\left\{2\cos\left(\frac{2\pi k}{n-1}\right) \mid 0 \le k \le \frac{n-1}{2}\right\} \cup \left\{2\cos\left(\frac{2\pi k}{n+1}\right) \mid 1 \le k \le \frac{n-1}{2}\right\}$$

состоит из n чисел. Таким образом, имеет место равенство (21).

(2) Так как $\varepsilon_{n-1}^{kn} = \varepsilon_{n-1}^{k}$ и $\varepsilon_{2(n+1)}^{(2k-1)n} = -\varepsilon_{2(n+1)}^{-(2k-1)}$, то согласно тождеству (20) имеют место равенства

$$F_n\left(2\sin\left(\frac{2\pi k}{n-1}\right)i\right) = F_n\big(\varepsilon_{n-1}^{k} - \varepsilon_{n-1}^{-k}\big) = 0,$$

$$F_n\left(2\sin\left(\frac{\pi(2k-1)}{n+1}\right)i\right) = F_n\big(\varepsilon_{2(n+1)}^{2k-1} - \varepsilon_{2(n+1)}^{-(2k-1)}\big) = 0.$$

Несложно заметить, что множества

$$\{0\} \cup \left\{2\sin\left(\frac{2\pi k}{n-1}\right)i \mid -m \le k \le m\right\} \cup \left\{2\sin\left(\frac{\pi(2k-1)}{n+1}\right)i \mid -m \le k \le m\right\},$$

если $n \equiv 1\ (mod\ 4)$ и $n = 4m+1$, и

$$\{0\} \cup \left\{2\sin\left(\frac{2\pi k}{n-1}\right)i \mid -m \le k \le m\right\} \cup \left\{2\sin\left(\frac{\pi(2k-1)}{n+1}\right)i \mid -(m+1) \le k \le m+1\right\},$$

если $n \equiv 3(\mathrm{mod}\,4)$ и $n = 4m+3$, состоят из n чисел. Таким образом, имеют место равенства (22) и (23). □

Теорема 5.8. *Пусть* p *— нечетное простое число,* $n, m \in \mathbb{N}$ *и* $n \mid m$. *Тогда*
(1) $L_{p^n}(x) \mid L_{p^m}(x)$;
(2) $F_{p^n}(x) \mid F_{p^m}(x)$.

Доказательство. Пусть $m = nl$.

(1) Согласно доказательству п. (1) леммы 5.7

$$A = \big\{\varepsilon_{p^n-1}^{k} + \varepsilon_{p^n-1}^{-k}\big\}_{k\in\mathbb{Z}} \cup \big\{\varepsilon_{p^n+1}^{k} + \varepsilon_{p^n+1}^{-k}\big\}_{k\in\mathbb{Z}}$$

— множество всех решений уравнения $L_{p^n} = 0$ и

$$B = \big\{\varepsilon_{p^{nl}-1}^{k} + \varepsilon_{p^{nl}-1}^{-k}\big\}_{k\in\mathbb{Z}} \cup \big\{\varepsilon_{p^{nl}+1}^{k} + \varepsilon_{p^{nl}+1}^{-k}\big\}_{k\in\mathbb{Z}}$$

— множество всех решений уравнения $L_{p^{nl}} = 0$. Так как имеют место свойства
(a) $p^n - 1 \mid p^{nl} - 1$,
(b) $p^n + 1 \mid p^{nl} + 1$, если l нечетно,
(c) $p^n + 1 \mid p^{nl} - 1$, если l четно,
то $\langle \varepsilon_{p^n-1} \rangle \cup \langle \varepsilon_{p^n+1} \rangle \subseteq \langle \varepsilon_{p^{nl}-1} \rangle \cup \langle \varepsilon_{p^{nl}+1} \rangle$ и, следовательно, $A \subseteq B$.
(2) Согласно доказательству п. (2) леммы 5.7

$$A = \left\{ \varepsilon_{p^n-1}^k - \varepsilon_{p^n-1}^{-k} \right\}_{k\in\mathbb{Z}} \cup \left\{ \varepsilon_{2(p^n+1)}^{2k+1} - \varepsilon_{2(p^n+1)}^{-(2k+1)} \right\}_{k\in\mathbb{Z}}$$

— множество всех решений уравнения $F_{p^n} = 0$ и

$$B = \left\{ \varepsilon_{p^{nl}-1}^k - \varepsilon_{p^{nl}-1}^{-k} \right\}_{k\in\mathbb{Z}} \cup \left\{ \varepsilon_{2(p^{nl}+1)}^{2k+1} - \varepsilon_{2(p^{nl}+1)}^{-(2k+1)} \right\}_{k\in\mathbb{Z}}$$

— множество всех решений уравнения $F_{p^{nl}} = 0$. Так как имеют место свойства
(a) $p^n - 1 \mid p^{nl} - 1$,
(b) $p^n + 1 \mid p^{nl} + 1$ и $\frac{p^{nl}+1}{p^n+1}$ — нечетное натуральное число, если l нечетно,
(c) $p^n + 1 \mid p^{nl} - 1$ и $\frac{p^{nl}-1}{p^n+1}$ — четное натуральное число, если l четно,
то

$$\langle \varepsilon_{p^n-1} \rangle \cup \left\{ \varepsilon_{2(p^n+1)}^{2k+1} \right\}_{k\in\mathbb{Z}} \subseteq \langle \varepsilon_{p^{nl}-1} \rangle \cup \left\{ \varepsilon_{2(p^{nl}+1)}^{2k+1} \right\}_{k\in\mathbb{Z}}$$

и тем самым получаем $A \subseteq B$. $\square$

В качестве замечания отметим связь семейства многочленов $(F_n(x))_{n\in\mathbb{N}}$ с подходом к доказательству квадратичного закона взаимности, предложенным Эйзенштейном в работе [16]. Воспользуемся леммой Гаусса — Шеринга для доказательства квадратичного закона взаимности для символа Якоби, согласно которой для произвольных различных натуральных нечетных чисел n, m имеет место равенство

$$\prod_{k=1}^{\frac{n-1}{2}} \frac{\varepsilon_n^{mk} - \varepsilon_n^{-km}}{\varepsilon_n^k - \varepsilon_n^{-k}} = \left(\frac{m}{n}\right).$$

Замечание 5.9. Пусть n, m — различные нечетные натуральные числа > 1. Имеет место равенство

$$F_n(x) + x = xG_n(x^2),$$

где

$$G_n(x) = \sum_{i=0}^{[\frac{n}{2}]} \frac{n}{n-i} \binom{n-i}{i} x^{\frac{n-2i-1}{2}}.$$

Из тождества Куммера для каждого $1 \leq k \leq \frac{m-1}{2}$ следуют равенства

$$G_n\left(\left(\varepsilon_m^k - \varepsilon_m^{-k}\right)^2\right) = \frac{F_n\left(\varepsilon_m^k - \varepsilon_m^{-k}\right) + \varepsilon_m^k - \varepsilon_m^{-k}}{\varepsilon_m^k - \varepsilon_m^{-k}} = \frac{\varepsilon_m^{nk} - \varepsilon_m^{-kn}}{\varepsilon_m^k - \varepsilon_m^{-k}}.$$

Аналогично для каждого $1 \leq k \leq \frac{n-1}{2}$ имеет место равенство

$$G_n\left(\left(\varepsilon_n^k - \varepsilon_n^{-k}\right)^2\right) = 0.$$

Так как $\deg(G_n(x)) = \frac{n-1}{2}$ и $\left(\varepsilon_n - \varepsilon_n^{-1}\right)^2, \ldots, \left(\varepsilon_n^{\frac{n-1}{2}} - \varepsilon_n^{-\frac{n-1}{2}}\right)^2$ — попарно различные числа, то

$$G_n(x) = \prod_{k=1}^{\frac{n-1}{2}} \left(x - \left(\varepsilon_n^k - \varepsilon_n^{-k}\right)^2\right).$$

Тогда

$$\operatorname{Res}(G_m(x), G_n(x)) = \prod_{k=1}^{\frac{m-1}{2}} G_n\big(\big(\varepsilon_m^k - \varepsilon_m^{-k}\big)^2\big) = \prod_{k=1}^{\frac{m-1}{2}} \frac{\varepsilon_m^{nk} - \varepsilon_m^{-kn}}{\varepsilon_m^k - \varepsilon_m^{-k}} = \left(\frac{n}{m}\right).$$

Аналогично $\operatorname{Res}(G_n(x), G_m(x)) = \left(\frac{m}{n}\right)$. Так как

$$\operatorname{Res}(G_n(x), G_m(x)) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \operatorname{Res}(G_m(x), G_n(x)),$$

то

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \left(\frac{m}{n}\right).$$

Другой подход к доказательству квадратичного закона взаимности для символа Якоби, также основанному на лемме Гаусса — Шеринга, предложен в [17].

Пример 5.10. Пусть $A \in M_2(\mathbb{Z})$ и $\det(A) = 1$. Найдем значение 2-адического предела $\alpha = \lim\limits_{k\to\infty} \operatorname{tr}(A^{2^k})$. Пусть α_1, α_2 — корни характеристического многочлена A с учетом их кратностей. Так как

$$\operatorname{tr}(A^{2^{k+1}}) = \alpha_1^{2^{k+1}} + \alpha_2^{2^{k+1}} = \big(\alpha_1^{2^k} + \alpha_2^{2^k}\big)^2 - 2 = \operatorname{tr}(A^{2^k})^2 - 2,$$

то α — корень многочлена $x^2 - x - 2 = (x+1)(x-2)$. Покажем, что для каждого $k \in \mathbb{N}$ имеют место сравнения

(a) $\operatorname{tr}(A^{2^k}) \equiv -1 (\operatorname{mod} 2^{k+1})$, если след $\operatorname{tr}(A)$ нечетен;

(b) $\operatorname{tr}(A^{2^k}) \equiv 2 (\operatorname{mod} 2^{k+1})$, если след $\operatorname{tr}(A)$ четен.

Докажем по индукции п. (a). Если $k = 1$, то сравнение п. (a) проверяется непосредственно. Предположим, что сравнение п. (a) имеет место для некоторого k. Тогда $\operatorname{tr}(A^{2^k}) = -1 + 2^{k+1}t$, где $t \in \mathbb{Z}$. Следовательно,

$$\operatorname{tr}(A^{2^{k+1}}) = (-1 + 2^{k+1}t)^2 - 2 = -1 + 2^{k+2}(-t + t^2 2^k).$$

П. (b) доказывается аналогично.

Таким образом, $\lim\limits_{k\to\infty} \operatorname{tr}(A^{2^k}) = \begin{cases} -1, & \text{если след } \operatorname{tr}(A) \text{ нечетен,} \\ 2, & \text{если след } \operatorname{tr}(A) \text{ четен.} \end{cases}$

Пример 5.11. Пусть $A \in M_2(\mathbb{Z})$ и $\det(A) = 1$. Найдем значение 3-адического предела $\alpha = \lim\limits_{k\to\infty} \operatorname{tr}(A^{3^k})$. Пусть α_1, α_2 — корни характеристического многочлена A с учетом их кратностей. Так как

$$\operatorname{tr}(A^{3^{k+1}}) = \alpha_1^{3^{k+1}} + \alpha_2^{3^{k+1}} = \big(\alpha_1^{3^k} + \alpha_2^{3^k}\big)^3 - 3\big(\alpha_1^{3^k} + \alpha_2^{3^k}\big) = \operatorname{tr}(A^{3^k})^3 - 3\operatorname{tr}(A^{3^k}),$$

то α — корень многочлена $L_3(x) = x^3 - 4x$. Покажем, что для каждого $k \in \mathbb{N}$ имеют место сравнения

(a) $\operatorname{tr}(A^{3^k}) \equiv 2 (\operatorname{mod} 3^{2k+1})$, если $\operatorname{tr}(A) \equiv 2 (\operatorname{mod} 3)$;

(b) $\operatorname{tr}(A^{3^k}) \equiv -2 (\operatorname{mod} 3^{2k+1})$, если $\operatorname{tr}(A) \equiv 1 (\operatorname{mod} 3)$;

(c) $\operatorname{tr}(A^{3^k}) \equiv 0 (\operatorname{mod} 3^{k+1})$, если $\operatorname{tr}(A) \equiv 0 (\operatorname{mod} 3)$.

Докажем по индукции п. (a). Если $k = 1$, то сравнение п. (a) проверяется непосредственно. Предположим, что сравнение п. (a) имеет место для некоторого k. Тогда $\operatorname{tr}(A^{3^k}) = 2 + 3^{2k+1}t$, где $t \in \mathbb{Z}$. Следовательно, $\operatorname{tr}(A^{3^{k+1}}) = (2 + 3^{2k+1}t)^3 - 3(2 + 3^{2k+1}t) = 2 + t'3^{2k+3}$, где $t' \in \mathbb{Z}$.

Пп. (b) и (c) доказывается аналогично.

Таким образом,

$$\lim_{k\to\infty} \operatorname{tr}(A^{3^k}) = \begin{cases} 2, & \text{если } \operatorname{tr}(A) \equiv 2 (\operatorname{mod} 3), \\ -2, & \text{если } \operatorname{tr}(A) \equiv 1 (\operatorname{mod} 3), \\ 0, & \text{если } \operatorname{tr}(A) \equiv 0 (\operatorname{mod} 3). \end{cases}$$

Пример 5.12. *Числами Перрена* называется последовательность $\{P_n\}_{n\in\mathbb{N}}$, удовлетворяющая условиям

$$P_1 = 0,\ P_2 = 2,\ P_3 = 3 \text{ и } P_{n+3} = P_{n+1} + P_n \ (n \in \mathbb{N}).$$

Для любого $n \in \mathbb{N}$ имеет место равенство $P_n = \operatorname{tr}(C^n)$, где C — сопровождающая матрица к многочлену $x^3 - x - 1$. Доопределим последовательность Перрена на множество всех целых чисел согласно правилу $P_n = \operatorname{tr}(C^n)$, где $n \in \mathbb{Z}$.

Найдем значения 2-адических пределов $\alpha = \lim\limits_{k\to\infty} P_{2^k}$ и $\beta = \lim\limits_{k\to\infty} P_{-2^k}$. Пусть $\alpha_1, \alpha_2, \alpha_3$ — корни характеристического многочлена C. Заметим, что поскольку $\alpha_1\alpha_2\alpha_3 = 1$, то $\operatorname{tr}(C^{-n}) = \alpha_1^{-n} + \alpha_2^{-n} + \alpha_3^{-n} = (\alpha_1\alpha_2)^n + (\alpha_1\alpha_3)^n + (\alpha_2\alpha_3)^n$ для каждого $n \in \mathbb{N}$.

Имеют место равенства

$$\begin{aligned} &\operatorname{tr}(C^{2^{k+1}}) = \alpha_1^{2^{k+1}} + \alpha_2^{2^{k+1}} + \alpha_3^{2^{k+1}} \\ &= \big(\alpha_1^{2^k} + \alpha_2^{2^k} + \alpha_3^{2^k}\big)^2 - 2\big(\alpha_1^{2^k}\alpha_2^{2^k} + \alpha_1^{2^k}\alpha_3^{2^k} + \alpha_2^{2^k}\alpha_3^{2^k}\big) = \operatorname{tr}(C^{2^k})^2 - 2\operatorname{tr}(C^{-2^k}). \end{aligned}$$

Аналогично получаем равенство

$$\operatorname{tr}(C^{-2^{k+1}}) = \operatorname{tr}(C^{-2^k})^2 - 2\operatorname{tr}(C^{2^k}).$$

Тогда $\alpha = \alpha^2 - 2\beta$, $\beta = \beta^2 - 2\alpha$ и, следовательно, α, β являются корнями многочлена $x^4 - 2x^3 - x^2 - 6x = x(x-3)(x^2+x+2)$.

Покажем, что для каждого $k \in \mathbb{N}$ имеют место сравнения

(a) $P_{2^k}P_{-2^k} \equiv 2 (\operatorname{mod} 2^k)$;

(b) $P_{2^k} + P_{-2^k} + 1 \equiv 0 (\operatorname{mod} 2^k)$.

Докажем по индукции пп. (a) и (b). Если $k = 1$, то сравнения пунктов (a) и (b) проверяются непосредственно. Предположим, что сравнения пунктов (a) и (b) имеют место для некоторого k. Тогда $P_{2^k}P_{-2^k} = 2 + 2^k t$, $P_{2^k} + P_{-2^k} = -1 + 2^k t'$, где $t, t' \in \mathbb{Z}$. Справедливы равенства

$$\begin{aligned} P_{2^{k+1}}P_{-2^{k+1}} &= \big(P_{2^k}^2 - 2P_{-2^k}\big)\big(P_{-2^k}^2 - 2P_{2^k}\big) \\ &= \big(P_{2^k}P_{-2^k}\big)^2 - 2(P_{2^k} + P_{-2^k})((P_{2^k} + P_{-2^k})^2 - 3P_{2^k}P_{-2^k}) + 4P_{2^k}P_{-2^k} \\ &= (2 + 2^k t)^2 - 2(-1 + 2^k t')((-1 + 2^k t')^2 - 3(2 + 2^k t)) + 4(2 + 2^k t) = 2 + t'' 2^{k+1}, \end{aligned}$$

где $t'' \in \mathbb{Z}$. Аналогично доказывается сравнение $P_{2^{k+1}} + P_{-2^{k+1}} + 1 \equiv 0 (\operatorname{mod} 2^{k+1})$.

Таким образом, 2-адические числа α и β являются различными корнями многочлена $x^2 + x + 2$.

ЛИТЕРАТУРА

1. *Schönemann T.* Theorie der symmetrischen Functionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congruenzen nebst einigen Anwendungen derselben // J. Reine Angew. Math. 1839. N 19. P. 289–308.
2. *Шатуновский С. О.* Объ условіяхъ существованія n неравныхъ корней сравненія n-й степени по простому модулю. Казань: Типо-литографія Императорск. ун-та, 1903.
3. *Dickson L. E.* History of the theory of numbers. New York: Chelsea, 1971. V. 1.

4. *Gladki P., Pulikowski M.* Gauss congruences in algebraic number fields // Ann. Math. Silesianae. 2022. V. 36, N 1. P. 53–56.

5. *Jänichen W.* Über die Verallgemeinerung einer Gaussschen Formel aus der Theorie der höhern Kongruenzen // Sitzungsberichte der Berliner Mathematischen Gesellschaft. 1921. V. 20. P. 23–29.

6. *Schur I.* Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung // Compositio Mathematica. 1937. V. 4. P. 432–444.

7. *Арнольд В. И.* Матричная теорема Эйлера — Ферма // Изв. РАН. Сер. мат. 2004. Т. 68, № 6. С. 61–70.

8. *Зарелуа А. В.* О матричных аналогах малой теоремы Ферма // Мат. заметки. 2006. Т. 79, № 6. С. 838–853.

9. *Зарелуа А. В.* О сравнениях для следов степеней некоторых матриц // Тр. МИАН. 2008. Т. 263. С. 85–105.

10. *Винберг Э. Б.* Малая теорема Ферма и ее обобщения // Мат. просвещение. Сер. 3. 2008. Т. 12. С. 43–53.

11. *Smyth C. J.* A coloring proof of a generalization of Fermat's little theorem // Am. Math. Monthly. 1986. V. 93, N 6. P. 469–471.

12. *Jezierski J., Marzantowicz W.* Homotopy methods in topological fixed and periodic points theory. Dordrecht: Springer-Verl., 2006.

13. *Ford T. J.* Separable algebras. Providence, RI: Am. Math. Soc., 2017.

14. *Абызов А. Н., Мухаметгалиев И. И.* О некоторых матричных аналогах малой теоремы Ферма // Мат. заметки. 2017. Т. 101, № 2. С. 163–168.

15. *Фейт У.* Теория представлений конечных групп. М.: Наука, 1990.

16. *Eisenstein G.* Applications de l'Algèbre à l'Arithmétique transcendante // J. Reine Angew. Mathematik. 1845. V. 29. P. 177–184.

17. *Kuroki A., Katayama S.* A variation of Takagi's proof for quadratic reciprocity laws of Jacobi symbols // J. Math. Univ. Tokushima. 2009. V. 43. P. 9–23.

Поступила в редакцию 28 октября 2025 г.
После доработки 17 июня 2026 г.
Принята к публикации 22 июня 2026 г.

Абызов Адель Наилевич (ORCID 0000-0002-9809-2091)
Казанский (Приволжский) федеральный университет,
Институт математики и механики им. Н.И. Лобачевского,
ул. Кремлевская, 18, Казань 420000;
Петербургский государственный университет
путей сообщения Императора Александра I,
Московский пр., 9, Санкт-Петербург 190031
`Adel.Abyzov@kpfu.ru`