А. В. Заварницин, В. Д. Мазуров, О порядках элементов в накрытиях простых групп $L_n(q)$ и $U_n(q)$, *Тр. ИММ УрО РАН*, 2007, том 13, номер 1, 89–98

ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 13 № 1 2007

УДК 512.542

О ПОРЯДКАХ ЭЛЕМЕНТОВ В НАКРЫТИЯХ ПРОСТЫХ ГРУПП $L_n(q)$ И $U_n(q)$[1]

А. В. Заварницин, В. Д. Мазуров

Мы доказываем, что если конечная простая линейная или унитарная группа, определенная над полем характеристики p и имеющая достаточно большую размерность по сравнению с p, действует на конечномерном векторном пространстве над некоторым полем той же характеристики p, то соответствующее полупрямое произведение содержит элемент, порядок которого отличен от всех порядков элементов исходной простой группы.

Введение

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Поведение спектра при расширениях групп является популярным предметом изучения. Так, в классической работе Холла и Хигмена [1] рассматриваются порядки p-элементов в накрытии G некоторой p-разрешимой группы $H = G/N$ в случае, когда N — элементарная абелева p-группа и H действует точно на N при сопряжении в G. В последние годы широко изучается проблема распознаваемости групп по спектру. Напомним, что конечная группа G называется *распознаваемой* (по спектру), если для любой конечной группы H равенство $\omega(G) = \omega(H)$ влечет за собой изоморфизм $G \cong H$. Очевидно, что любая распознаваемая группа G должна удовлетворять следующему свойству

$$(*) \qquad \omega(H) \neq \omega(G) \text{ для любого собственного накрытия } H \text{ группы } G,$$

где под собственным накрытием G мы понимаем группу H с такой нетривиальной нормальной подгруппой N, что $H/N \cong G$. Хотя свойство $(*)$ слабее распознаваемости, его проверка для некоторых групп может быть очень трудоемкой. В работе [3] было показано, что все конечные неразрешимые симметрические и знакопеременные группы удовлетворяют свойству $(*)$. Достаточно проверять свойство $(*)$ в случае, когда H — расщепляемое расширение элементарной абелевой p-группы N с помощью G, причем G действует неприводимо на N. Для группы G, изоморфной простой группе $\mathrm{PSL}_3(q)$, в единственном известном доказательстве [4] свойства $(*)$ используется явное описание неприводимых эквихарактеристических модулей для G. В этой работе мы рассматриваем аналогичную проблему для групп $L_n^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$ и $L_n^+(q) = \mathrm{PSL}_n(q)$, $L_n^-(q) = \mathrm{PSU}_n(q)$. Группы из следующего списка будем называть исключительными:

$$\begin{gathered} L_5^\varepsilon(2^m), L_6^\varepsilon(3^m), L_7^\varepsilon(3^m), L_{10}^\varepsilon(3^m), L_{11}^\varepsilon(5^m), L_{18}^\varepsilon(5^m), \text{ где } \varepsilon \in \{+,-\}, m \geqslant 1; \\ U_6(2), U_7(2), U_9(2), U_{10}(2), U_{11}(2), U_{18}(2), U_5(3), U_8(3), U_{11}(3). \end{gathered} \tag{1}$$

Теорема 1. *Пусть $\varepsilon \in \{+,-\}$ и $L = L_n^\varepsilon(q)$ — простая группа, где $q = p^m$. Предположим, что $n \geqslant p$, $n \neq p+1$ и L не является исключительной. Если L действует на векторном пространстве W над полем характеристики p, то $\omega(WL) \neq \omega(L)$, где WL — естественное полупрямое произведение W на L.*

[1]Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00797) и Сибирского отделения Российской академии наук (грант 29 для молодых ученых и интеграционный проект 2006.1.2).

Из этой теоремы вместе с результатами из [5] следует, что группы $L_n^+(q)$, где $q = p^m$, удовлетворяют $(*)$, если n достаточно велико по сравнению с p. Отметим, что вопрос о справедливости свойства $(*)$ для всех групп $L_n(q)$ при $n \geqslant 3$ включен в "Коуровскую тетрадь" [10, Проблема 14.60]. Другим следствием нашего результата является подтверждение следующей гипотезы из [9].

Следствие 1. *Проективные специальные линейные группы $L_n(2)$ распознаваемы по спектру для всех $n \geqslant 3$.*

Доказательство. Допустим противное: для некоторой группы $G = L_n(2)$, где $n \geqslant 3$, найдется группа H наименьшего порядка такая, что $\omega(H) = \omega(G)$, но $H \ncong G$. Тогда из предложения 1 в [9] следует, что пара (G, H) — контрпример к свойству $(*)$, причем $H \cong NG$, где N — элементарная абелева 2-группа. Из теоремы 1 вытекает, что $n = 3$ или 5. Однако группы $L_3(2)$ и $L_5(2)$ распознаваемы по спектру [7, 8]. Противоречие. $\square$

1. Предварительные результаты

На протяжении работы $\mathbb{Z}_m$ будет обозначать циклическую группу порядка m и $\mathbb{F}_q$ — конечное поле из q элементов. Если $\alpha \in \mathbb{F}_{q^2}$, то положим $\overline{\alpha} = \alpha^q$. Если V — невырожденное унитарное векторное пространство, то ортогональное разложение $V = V_1 \oplus V_2$ называется *невырожденным*, если V_1 и V_2 — невырожденные подпространства в V. Обозначим $\mathrm{SL}_n^-(q) = \mathrm{SU}_n(q)$ и $\mathrm{SL}_n^+(q) = \mathrm{SL}_n(q)$. Аналогичное соглашение касается проективных групп $L_n^\varepsilon(q) = \mathrm{PSL}_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$. Если $\varepsilon = +$, то пусть V — векторное пространство над $F = \mathbb{F}_q$, а если $\varepsilon = -$, то пусть V — невырожденное унитарное векторное пространство над $F = \mathbb{F}_{q^2}$. Предположим, что $n = \dim V > 1$, и пусть $\{e_1, \dots, e_n\}$ — (ортонормированный) базис пространства V. Если $V = V_1 \oplus V_2$ — (невырожденное ортогональное) разложение, то мы обозначим через $\mathrm{SL}^\varepsilon(V_1, V_2)$ подгруппу в $\mathrm{SL}^\varepsilon(V)$, которая стабилизирует V_1 и централизует V_2.

Лемма 1. *Пусть V — естественный n-мерный FH-модуль для группы $H = \mathrm{SL}_n^\varepsilon(q)$, где $q = p^m$. Предположим, что $V = V_1 \oplus V_2$ — (невырожденное ортогональное) разложение и K — циклическая подгруппа в $\mathrm{SL}^\varepsilon(V_1, V_2)$ порядка, взаимно простого с p. Если $\dim V_2 \geqslant (n-1)/2$, то K оставляет неподвижным некоторый ненулевой вектор в любом RH-модуле, где R — поле характеристики p.*

Доказательство. См. [15]. $\square$

Если $1 \leqslant i \neq j \leqslant n$, то пусть $W_{ij} = \langle e_i, e_j \rangle_F$, а W'_{ij} — подпространство, порожденное всеми e_k при $k \neq i, j$. Обозначим $S_{ij} = \mathrm{SL}^\varepsilon(W_{ij}, W'_{ij}) \cong \mathrm{SL}_2^\varepsilon(q)$. Аналогично определим $S_{123} \cong \mathrm{SL}_3^\varepsilon(q)$, если $n \geqslant 3$.

Лемма 2. *Группа $\mathrm{SL}^\varepsilon(V)$ порождается своими подгруппами S_{12}, S_{23}, ..., $S_{n-1,n}$ за исключением случая $(\varepsilon, q) = (-, 2)$ и $n > 2$, в котором $\mathrm{SL}^-(V)$ порождается подгруппами S_{123}, S_{34}, S_{45}, ..., $S_{n-1,n}$.*

Доказательство. Если $\varepsilon = +$, то хорошо известно, что $\mathrm{SL}^+(V)$ порождается трансвекциями $t_{ij}(a)$ при $1 \leqslant i \neq j \leqslant n$ и $a \in F$ (это можно доказать, используя метод Гаусса). Из формулы $[t_{ij}(a), t_{jk}(b)] = t_{ik}(ab)$ при различных i, j, k следует, что $\mathrm{SL}^+(V)$ на самом деле порождается с помощью $t_{i,i+1}(a)$ и $t_{i+1,i}(a)$ при $1 \leqslant i < n$ и $a \in F$. Поскольку $S_{i,i+1} = \langle t_{i,i+1}(a), t_{i+1,i}(a) \mid a \in F \rangle$, то получаем требуемое.

Унитарный аналог этого факта не столь хорошо известен. Некоторая растянутость следующего рассуждения компенсируется тем, что мы реально описываем алгоритм разложения элемента из $\mathrm{SL}^-(V)$ в произведение элементов порождающих подгрупп $S_{i,i+1}$ и, возможно,

S_{123}. Пусть $\varepsilon = -$. Можно считать, что $n > 2$. Обозначим $S = \mathrm{SL}^{-}(V)$. Заметим, что любой элемент $s \in S_{ij}$ в базисе $\{e_i, e_j\}$ имеет матрицу

$$\begin{pmatrix} \chi & -\overline{\eta} \\ \eta & \overline{\chi} \end{pmatrix} \tag{2}$$

для некоторых $\chi, \eta \in F$, удовлетворяющих условию $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Достаточно показать, что S порождается подгруппами S_{ij} при $i \neq j$ (и дополнительно подгруппой S_{123} при $q = 2$). В самом деле, если $j > i+1$, то $S_{ij}^{u_{i,i+1}} = S_{i+1,j}$, где матрица элемента $u_{kl} \in S_{kl}$ в базисе $\{e_k, e_l\}$ равна

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

Поэтому $S_{ij} \leqslant \langle S_{i,i+1}, \ldots, S_{j-1,j} \rangle$.

Выберем $a \in S$. Достаточно показать, что умножением a справа на подходящий элемент из S_{ij} (из S_{123} при $q = 2$) можно получить элемент b, централизующий e_1. В самом деле, в таком случае b будет стабилизировать $\langle e_1 \rangle^{\perp}$, и мы сможем применить индукцию по размерности при $q > 2$. Если же $q = 2$, то, сопрягая b с помощью $u_{1,n}$, получим элемент, централизующий e_n, и также применим индукцию.

Пусть (a_{ij}) — матрица элемента a в базисе $\{e_1, \ldots, e_n\}$. Пусть r — число ненулевых элементов в первой строке $[a_{11}, \ldots, a_{1n}]$ матрицы (a_{ij}). Тогда $1 \leqslant r \leqslant n$. Дальше применяем индукцию по r. Можно считать (умножая, если необходимо, на подходящий элемент $u_{ij} \in S_{ij}$, определенный выше), что $a_{11}, \ldots, a_{1r}$ отличны от нуля и $a_{1,r+1} = \ldots = a_{1n} = 0$. Если $r = 1$, то $a_{11}\overline{a_{11}} = 1$ и, умножая a на элемент $s \in S_{12}$, матрица которого в базисе $\{e_1, e_2\}$ равна

$$\begin{pmatrix} a_{11}^{-1} & 0 \\ 0 & (\overline{a_{11}})^{-1} \end{pmatrix}, \tag{4}$$

мы приведем a к требуемому виду. Предположим, что $r \geqslant 2$. Если для некоторого j, $1 < j \leqslant r$, имеет место $a_{11}\overline{a_{11}} + a_{1j}\overline{a_{1j}} = c \neq 0$, то существует такое $\sigma \in F\backslash\{0\}$, что $\sigma\overline{\sigma} = c$, и мы положим $\chi = \overline{a_{11}}/\sigma$, $\eta = \overline{a_{1j}}/\sigma$. Тогда $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Пусть s — элемент из S_{1j}, имеющий матрицу (2) в базисе $\{e_1, e_j\}$. Тогда для матрицы элемента $b = as$ имеем $b_{11} = a_{11}\chi + a_{1j}\eta \neq 0$, $b_{1j} = -a_{11}\overline{\eta} + a_{1j}\overline{\chi} = 0$, и индукцией по r получаем требуемое.

Следовательно, можно считать, что $a_{1j}\overline{a_{1j}} = -a_{11}\overline{a_{11}} = \nu$ при $1 < j \leqslant r$. Заметим, что это влечет за собой $r \geqslant 3$, поскольку в случае $r = 2$ получилось бы $a_{11}\overline{a_{11}} + a_{12}\overline{a_{12}} = 1$ ввиду унитарности a, противоречие. Если мы найдем такое $s \in S_{23}$, что элемент b_{12} матрицы $b = as$ удовлетворяет неравенству $b_{12}\overline{b_{12}} \neq \nu$, то по предыдущему рассуждению мы сможем уменьшить r и использовать индукцию.

Если $q > 2$, то существуют такие ненулевые $\chi, \eta \in F$, что $\chi\overline{\chi} + \eta\overline{\eta} = 1$. Положим $\tau = a_{12}/a_{13}$. Если соотношение

$$\tau\chi\overline{\eta} + \overline{\tau\chi}\eta \neq 0 \tag{5}$$

не выполнено, то мы заменим χ на $\chi\mu$, где $\mu \in F$ удовлетворяет соотношениям $\mu\overline{\mu} = 1$ и $\mu \neq \pm 1$ (такое μ всегда найдется). Тогда $\chi\overline{\chi} + \eta\overline{\eta} = 1$ и выполнено (5), поскольку в противном случае мы получили бы $\mu = \overline{\mu}$, то есть $\mu^2 = 1$, противоречие. Теперь пусть $s \in S_{23}$ имеет матрицу (2) в базисе $\{e_1, e_j\}$. Тогда

$$b_{12}\overline{b_{12}} = (a_{12}\chi + a_{13}\eta)(\overline{a_{12}\chi} + \overline{a_{13}\eta}) = \nu + a_{12}\overline{a_{13}}\chi\overline{\eta} + \overline{a_{12}}a_{13}\overline{\chi}\eta \neq \nu$$

ввиду (5), что и требовалось.

Пусть, наконец, $q = 2$. Тогда рассматриваемый выше элемент s не всегда существует в S_{23}. В этом случае найдется элемент $s \in S_{123}$, который аннулирует элементы a_{12} и a_{13}. Из унитарности a имеем $1 = a_{11}\overline{a_{11}} + \ldots + a_{1r}\overline{a_{1r}} = r\nu$, откуда следует, что r нечетно и $\nu = 1$. В частности, норма элемента $v = a_{11}e_1 + a_{12}e_2 + a_{13}e_3$ равна 1. Поскольку S_{123} действует транзитивно на векторах из $\langle e_1, e_2, e_3\rangle$ с нормой 1 (см. лемму 2.10.5 в [11]), то существует такое $s \in S_{123}$, что $vs = e_1$. Лемма доказана. $\square$

Отметим, что при $\varepsilon = -$, $q = 2$ и $n > 2$ группы S_{ij} мономиальны в базисе $\{e_1, \ldots, e_n\}$ и порождают (собственную) мономиальную подгруппу в $\mathrm{SL}^-(V)$.

Лемма 3. *Пусть $V = U \oplus C$ — такое (невырожденное ортогональное) разложение пространства V, определенного выше, что $\dim C > \dim U$. Если $(\varepsilon, q, \dim V, \dim U) \neq (-, 2, 3, 1)$, то*

$$\mathrm{SL}^\varepsilon(V) = \big\langle\, \mathrm{SL}^\varepsilon(U_0, C_0) \;\mid\; U_0 > U,\ C_0 < C,\ \dim U_0 = \dim C,\ V = U_0 \oplus C_0 \big\rangle, \tag{6}$$

где разложение $V = U_0 \oplus C_0$ предполагается невырожденным и ортогональным в случае $\varepsilon = -$.

Д о к а з а т е л ь с т в о. Пусть $u = \dim U$, $c = \dim C$. Можем считать, что $u \geqslant 1$. Тогда $c \geqslant 2$. Выберем (ортонормированные) базисы $\{e_1, \ldots, e_u\}$ для U и $\{e_{u+1}, \ldots, e_n\}$ для C. Обозначим через S правую часть равенства (6). Сначала покажем, что $S_{i,i+1} \leqslant S$ при $1 \leqslant i < n$, где S_{ij} определены так же, как перед леммой 2 по отношению к (ортонормированному) базису $\{e_1, \ldots, e_n\}$ пространства V. Заметим, что $S_{1j} \leqslant S$ для любого $j > 1$. В самом деле, поскольку $u \leqslant c - 1$, то можно положить $U_0 = \langle e_1, \ldots, e_c\rangle_F$, если $j \leqslant c$, и $U_0 = \langle e_1, \ldots, e_{c-1}, e_j\rangle_F$, если $j > c$. Тогда, обозначив $C_0 = \langle e_k \,|\, e_k \notin U_0\rangle_F$, получим $S_{1j} \leqslant \mathrm{SL}^\varepsilon(U_0, C_0)$. Из леммы 2 следует, что $S_{i,i+1} \leqslant \langle S_{1i}, S_{1,i+1}\rangle \cong \mathrm{SL}_3^\varepsilon(q)$, тогда $S_{i,i+1} \leqslant S$. Если либо $q > 2$, либо $(\varepsilon, q) = (+, 2)$, то требуемое следует из леммы 2. Если $(\varepsilon, q) = (-, 2)$, то также необходимо показать, что $S_{123} \leqslant S$. Предыдущее рассуждение проходит и тогда, когда либо $u \geqslant 2$, либо $u = 1$ и $c \geqslant 3$. А именно, в этих случаях можно положить $U_0 = \langle e_1, \ldots, e_c\rangle_F$ и $C_0 = \langle e_k \,|\, e_k \notin U_0\rangle_F$. Тогда $S_{123} \leqslant \mathrm{SL}^\varepsilon(U_0, C_0) \leqslant S$. $\square$

Если $\mathrm{SL}^\varepsilon(V) \cong \mathrm{SU}_3(2)$ и $\dim U = 1$, то равенство (6) не имеет места; можно показать, что в этом случае его правая часть является собственной подгруппой в $\mathrm{SU}_3(2)$ порядка 54.

Лемма 4. *Пусть $V = U \oplus C$ — такое (невырожденное ортогональное) разложение определенного выше пространства V, что $\dim C > \dim U$, и $a \in \mathrm{SL}^\varepsilon(U, C)$. Предположим, что $(\varepsilon, q, \dim V, \dim U) \neq (-, 2, 3, 1)$ и группа $\mathrm{SL}^\varepsilon(V)$ так действует на конечной группе или конечномерном пространстве G, что $\mathrm{SL}^\varepsilon(V)$ не централизует $C_G(a)$. Тогда $\mathrm{SL}^\varepsilon(C, U)$ также не централизует $C_G(a)$.*

Д о к а з а т е л ь с т в о. Рассуждаем от противного. Пусть сначала G — конечная группа. Имеем $C_G(a) \leqslant C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)$. Поскольку элемент a сопряжен в $\mathrm{SL}^\varepsilon(V)$ с элементом $\mathrm{SL}^\varepsilon(C, U)$, то мы получаем $\big|C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)\big| = |C_G(a)|$, и поэтому $C_G\big(\mathrm{SL}^\varepsilon(C, U)\big) = C_G(a)$.

Пусть $U_0 \leqslant V$ — (невырожденное) подпространство размерности $\dim C$ и $U_0 \geqslant U$. Можно выбрать $C_0 \leqslant C$ так, что $V = U_0 \oplus C_0$ — (невырожденное ортогональное) разложение пространства V. Тогда $a \in \mathrm{SL}^\varepsilon(U_0, C_0)$ и $\big|C_G\big(\mathrm{SL}^\varepsilon(U_0, C_0)\big)\big| = \big|C_G\big(\mathrm{SL}^\varepsilon(C, U)\big)\big| = |C_G(a)|$. Следовательно, $C_G\big(\mathrm{SL}^\varepsilon(U_0, C_0)\big) = C_G(a)$. Теперь из леммы 3 следует, что $\mathrm{SL}^\varepsilon(V)$ порождена всевозможными такими подгруппами $\mathrm{SL}^\varepsilon(U_0, C_0)$ и, следовательно, централизует $C_G(a)$, противоречие.

Если G — векторное пространство, то можно применить то же рассуждение с заменой порядка подгруппы из G на размерность подпространства из G. $\square$

Пусть $t > 1$ и n — натуральные числа, а $\varepsilon \in \{+, -\}$. Если существует простое число, делящее $t^n - (\varepsilon 1)^n$ и не делящее $t^i - (\varepsilon 1)^i$ при $1 \leqslant i < n$, то мы обозначим его через $t_{[\varepsilon n]}$ и назовем *примитивным делителем* числа $t^n - (\varepsilon 1)^n$. Примитивный делитель может не существовать или быть не единственным. Следующая лемма обобщает известную теорему Жигмонди [12].

Лемма 5. *Пусть $t, n > 1$ — натуральные числа. Тогда для любого $\varepsilon \in \{+, -\}$ существует примитивный делитель $t_{[\varepsilon n]}$ числа $t^n - (\varepsilon 1)^n$, за исключением следующих случаев.*

(i) $\varepsilon = +$, $n = 6$, $t = 2$;

(ii) $\varepsilon = +$, $n = 2$, $t = 2^l - 1$ *для некоторого* $l \geqslant 2$;
(iii) $\varepsilon = -$, $n = 3$, $t = 2$;
(iv) $\varepsilon = -$, $n = 2$, $t = 2^l + 1$ *для некоторого* $l \geqslant 0$.

Доказательство. Пункты (i) и (ii) составляют утверждение теоремы Жигмонди. Предположим, что $\varepsilon = -$. Будем рассуждать от противного. Если n нечетно, то можно считать, что $n > 1$ и $(n, t) \neq (3, 2)$. Можно взять в качестве $t_{[-n]}$ делитель $t_{[2n]}$ (примитивный делитель $t_{[2n]}$, очевидно, существует).

Если $i < n$ четно, то $t_{[-n]} \nmid t^i - (-1)^i$ по определению. Предположим, что $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$. Тогда $t_{[2n]} = t_{[-n]} \mid t^{2i} - 1$ и $2i < 2n$, противоречие. Отсюда следует пункт (iii).

Следовательно, $n = 2m$ четно. Если m четно, то можно взять в качестве $t_{[-n]}$ делитель $t_{[n]}$, который всегда существует. Тогда $t_{[-n]} \nmid t^i - (-1)^i$ для четных $i < n$ по определению. Предположим, что $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$. Тогда $t_{[n]} = t_{[-n]} \mid t^{2i} - 1$. С другой стороны $t_{[n]} \mid t^n - 1$. Следовательно, $t_{[n]} \mid t^{(n,2i)} - 1$. Поскольку $(n, 2i) \leqslant n$, то $(n, 2i) = n$ по определению $t_{[n]}$. Но тогда $m \mid i$, что невозможно ввиду четности m и нечетности i.

Если m нечетно и $m > 1$, то можно взять в качестве $t_{[-n]}$ делитель $t_{[m]}$. Если $t_{[-n]} \mid t^i - 1$ для некоторого положительного четного $i < n$, то $n > 2$, $i = 2j$ для некоторого $j < m$, и $t_{[m]} \mid t^{(m,i)} - 1$. Однако $(m, i) = (m, j) \leqslant j < m$, что противоречит определению $t_{[m]}$.

Если $t_{[-n]} \mid t^i + 1$ для некоторого нечетного $i < n$, то $t_{[m]} \mid t^{(m,2i)} - 1$. Однако $(m, 2i) = (m, i) \leqslant m$ и, значит, $(m, i) = m$ ввиду выбора $t_{[m]}$. Поэтому $m \mid i$. Поскольку $n = 2m > i$, то $m = i$ и число $t_{[m]}$ делит как $t^m + 1$, так и $t^m - 1$. Значит, $t_{[m]} = 2$ и t нечетно. Но тогда $m = 1$, поскольку $t_{[m]}$ нечетно при $m > 1$, противоречие.

Пусть, наконец, $n = 2$. Тогда любой нечетный простой делитель числа $t - 1$ может быть примитивным делителем $t_{[-2]}$ числа $t^2 - 1$. Однако, если $t - 1$ есть степень двойки, то $t^2 - 1$, очевидно, не имеет примитивных делителей вида $t_{[-2]}$, откуда следует пункт (iv). □

В следующей лемме мы обобщаем пункт (1) леммы 5 из [13] и исправляем небольшую неточность в приведенном там доказательстве.

Лемма 6. *Пусть n и q такие натуральные числа, что $L_n^\varepsilon(q)$ — простая группа и существует примитивный простой делитель $r = q_{[\varepsilon n]}$ числа $q^n - (\varepsilon 1)^n$. Тогда $L_n^\varepsilon(q)$ содержит подгруппу Фробениуса с ядром порядка r и циклическим дополнением порядка n. Более того, если n нечетно или q четно, то такая подгруппа Фробениуса существует уже в $\mathrm{SL}_n^\varepsilon(q)$.*

Доказательство. Заметим, что r нечетно, поскольку $n > 1$. Пусть $G = \mathrm{SL}(\overline{F})$, где $F = \mathbb{F}_q$ и $\overline{F}$ — алгебраическое замыкание поля F. Определим эндоморфизм Фробениуса σ группы G следующим образом: $\sigma = \big[(a_{ij}) \mapsto (a_{ij}^q)\big]$, если $\varepsilon = +$, и $\sigma = \big[(a_{ij}) \mapsto (a_{ij}^q)^{-T}\big]$, если $\varepsilon = -$. Тогда $C_G(\sigma) \cong \mathrm{SL}_n^\varepsilon(q)$. Обозначим через D диагональную подгруппу в G. Определим

$$w = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \dots \\ 0 & 0 & 0 & \dots & 1 \\ (-1)^{n-1} & 0 & 0 & \dots & 0 \end{pmatrix} \in G$$

и заметим, что $w^\sigma = w$ и элемент $w_0 = w^n$ равен $(-1)^{n-1}e$, где e — единичный элемент из G. Определим также $\sigma_w = \sigma \circ c_w^{-1}$, где c_w — сопряжение группы G с помощью w. Заметим, что $T = C_D(\sigma_w)$ — циклическая группа порядка $\dfrac{q^n - (\varepsilon 1)^n}{q - \varepsilon 1}$.

Пусть $t \in T$ — элемент порядка r. Поскольку $t^w = t^\sigma = t^{\varepsilon q}$, циклическая группа $\langle t \rangle$ является w-инвариантной. Обозначим $F = \langle t, w \rangle$ и заметим, что $F \cap Z = \langle w_0 \rangle$, где $Z = Z(G)$. Допустим, что $t^{w^l} \in \langle w_0 \rangle$ для некоторого $l \in \mathbb{N}$. Тогда элемент $t^{(\varepsilon q)^l - 1}$ имеет порядок, делящий 2, и, значит, r делит $2(q^l - (\varepsilon 1)^l)$. Поскольку r нечетно, имеем $r \mid \left(q^l - (\varepsilon 1)^l, q^n - (\varepsilon 1)^n\right) = q^{(l,n)} - (\varepsilon 1)^{(l,n)}$. Поэтому $(l,n) = n$, $l \mid n$, и $w^l \in \langle w_0 \rangle$. Значит, факторгруппа FZ/Z — группа Фробениуса с ядром порядка r и циклическим дополнением порядка n. Так как группа $\langle w_0 \rangle$ тривиальна тогда и только тогда, когда либо n нечетно, либо q четно, то мы получим оба утверждения леммы, если покажем, что F сопряжена в G с некоторой подгруппой из $C_G(\sigma)$.

По теореме Ленга — Стейнберга существует такой элемент $g \in G$, что $w = g^{-1}g^{\sigma}$. Поэтому

$$({}^g t)^{\sigma} = {}^{gw}(t^{\sigma}) = {}^g(t^{\sigma w}) = {}^g t, \qquad ({}^g w)^{\sigma} = {}^{gw}(w^{\sigma}) = {}^{gw}w = {}^g w.$$

Следовательно, ${}^g F \leqslant C_G(\sigma)$. □

Лемма 7. (i) *Если $x \geqslant 36$ — вещественное число, то отрезок $[2x/3, x-7]$ содержит по меньшей мере одно простое число.*

(ii) *Любое непростое натуральное число $f \neq 1,4,6$ является суммой попарно различных простых чисел.*

Д о к а з а т е л ь с т в о. (i) Если $x < 99$, то утверждение можно проверить непосредственно. Предположим, что $x \geqslant 99$. Существует такое число $a \in [0,3)$, что $2x/3 + a = 3s$ для некоторого натурального числа s. Отрезок $[3s, 4s]$ содержит простое число (см. [14]). Достаточно показать, что $4s \leqslant x - 7$. Имеем $4s = 8x/9 + 4a/3 < 8x/9 + 4 = x - 7 + (11 - x/9) \leqslant x - 7$.

(ii) Докажем утверждение индукцией по f. При $f < 36$ требуемое проверяется вручную. Предположим, что $f \geqslant 36$. По пункту (i) отрезок $[2f/3, f-7]$ содержит простое число p. Поскольку $f - p \geqslant 7$, то по индукции получаем $f - p = p_1 + \ldots + p_k$, где $k \geqslant 1$ и все p_i попарно различные простые числа. Заметим, что p отлично от всех p_i, поскольку $p_i \leqslant f - p < p$. Отсюда следует требуемое. □

Лемма 8. *Пусть натуральное число n и простое число p удовлетворяют соотношениям $n \geqslant p$ и $n \neq p+1$. Если $(p,n) \notin \{(2,5),(3,6),(3,7),(3,10),(5,11),(5,18)\}$, то существуют $t \geqslant 1$, $k \geqslant 0$ и такие попарно взаимно простые натуральные числа $b_1, \ldots, b_k$, бóльшие единицы, что*

$$\begin{gathered} n = p^t + b_1 + \ldots + b_k, \\ b_i < (n - b_1 - b_2 - \ldots - b_{i-1})/2 \quad \forall\ i = 1, \ldots, k. \end{gathered} \tag{7}$$

При этом для всех $i = 1, \ldots, k$ можно взять $b_i > 3$, если $p = 2$, $n \neq 5,6,7,9,10,11,18$, и $b_i > 2$, если $p = 3$, $n \neq 5,6,7,8,10,11$.

Д о к а з а т е л ь с т в о. Пусть n и p такие, как в формулировке. Будем рассуждать индукцией по n при фиксированном p. Если $n < 36$, то требуемое разложение может быть найдено вручную[2]. Предположим, что $n \geqslant 36$.

Допустим сначала, что $n < 2p$. Тогда $p \geqslant 7$. Если $n - p \neq 4,6$, то по пункту (ii) леммы 7 получаем нужное разложение $n - p = b_1 + \ldots + b_k$, где b_i — попарно различные простые числа. В самом деле, в этом случае выполнено $b_i \leqslant n - p < p$, тогда $b_i < (p + b_i)/2 = (n - b_1 - \ldots - b_{i-1} - b_{i+1} - \ldots - b_k)/2 \leqslant (n - b_1 - \ldots - b_{i-1})/2$. Если же $n = p + 4$ или $n = p + 6$, то это и есть требуемое разложение (7), поскольку $p \geqslant 7$.

Значит, можно считать, что $n \geqslant 2p$. Выберем простое b_1 из отрезка $[n/3, n/2 - 7]$, существующее по лемме 7 (i). Пусть $n_0 = n - b_1$. Тогда $n_0 - p \geqslant n - (n/2 - 7) - p = (n/2 - p) + 7 > 1$ и $n_0 \geqslant n/2 + 7 > 18$. Поэтому пара (n_0, p) не является исключительной, и по индукции получаем

$$n_0 = p^t + b_2 + \ldots + b_k \tag{8}$$

для некоторых $t \geqslant 1$ и $k \geqslant 0$, где числа b_i $(i = 2, \ldots, k)$ попарно взаимно просты, и $1 < b_i < (n_0 - b_2 - \ldots - b_{i-1})/2$. Значит, $b_i < (n - b_1)/2 \leqslant b_1$, все $b_2, \ldots, b_k$ отличны от простого числа

[2] Это разложение было вычислено для всех допустимых пар (p,n) при $n < 36$ (см. сводную таблицу в приложении).

b_1 и поэтому взаимно просты с ним. Следовательно, равенство (8) дает требуемое разложение $n = p^t + b_1 + b_2 + \ldots + b_k$. □

Пусть q — степень простого числа и $\varepsilon \in \{+,-\}$. Для натурального числа b определим

$$q^*_{[\varepsilon b]} = \begin{cases} q_{[\varepsilon b]}, & \text{если} \ \ q_{[\varepsilon b]} \ \text{существует}, \\ 9, & \text{если} \ \ (\varepsilon, b, q) = (+, 6, 2), \\ 2^l, & \text{если} \ \ (\varepsilon, b, q) = (+, 2, 2^l - 1) \ \text{при} \ l \geqslant 2, \\ 2^l, & \text{если} \ \ (\varepsilon, b, q) = (-, 2, 2^l + 1) \ \text{при} \ l \geqslant 2. \end{cases}$$

Отметим, что $q^*_{[\varepsilon b]}$ не определено только при $(\varepsilon, b, q) \in \{(-,2,2), (-,2,3), (-,3,2)\}$ и что

$$q^*_{[\varepsilon b]} \bigm| \bigl(q^s - (\varepsilon 1)^s\bigr) \iff b \mid s, \tag{9}$$

если $q^*_{[\varepsilon b]}$ определено, и в этом случае группа $\mathrm{SL}^\varepsilon_b(q)$ содержит неприводимый элемент порядка $q^*_{[\varepsilon b]}$ при дополнительном условии, что $b > 1$.

Лемма 9. *Пусть q — степень простого числа p и $\varepsilon \in \{+,-\}$. Пусть $n = p^t + b_1 + \ldots + b_k$, где $t \geqslant 0$, $k \geqslant 0$, а все числа $b_i > 1$ и попарно взаимно просты. Если $(\varepsilon, q) = (-,2)$, то пусть также $b_i \neq 2, 3$ для всех i. Если же $(\varepsilon, q) = (-,3)$, то пусть $b_i \neq 2$ для всех i. Положим $r_i = q^*_{[\varepsilon b_i]}$. Тогда $p^{t+1} r_1 \cdot \ldots \cdot r_k \notin \omega(\mathrm{SL}^\varepsilon_n(q))$.*

Д о к а з а т е л ь с т в о. Сначала заметим, что ввиду (9) все r_i попарно взаимно просты и не делятся на p. Предположим, что существует $a \in \mathrm{SL}^\varepsilon_n(q)$ порядка $p^{t+1} r_1 \cdot \ldots \cdot r_k$. Пусть $\zeta_1, \ldots, \zeta_n$ — характеристические корни элемента a. Поскольку жорданова форма элемента a содержит блок размера не менее $p^t + 1$, то среди корней ζ_i есть по крайней мере $p^t + 1$ одинаковых. Элемент $a^{p^{t+1}}$ полупрост, имеет порядок $r_1 \cdot \ldots \cdot r_k$ и характеристические корни $\mu_i = \zeta_i^{p^{t+1}}$, $i = 1, \ldots, n$. Отметим, что $r_1 \cdot \ldots \cdot r_k$ — наименьшее общее кратное чисел $|\mu_1|, \ldots, |\mu_n|$. Положим $R_i = \{\mu_j \mid r_i \,\text{делит}\, |\mu_j|\}$ при $i = 1, \ldots, k$. Все множества R_i непусты, но, возможно, пересекаются. Кроме того множество $\{\mu_1, \ldots, \mu_n\}$ является объединением непересекающихся орбит O_i относительно действия отображения Фробениуса $\mu \mapsto \mu^{\varepsilon q}$. Корни в одной орбите попарно различны, каждая орбита O_i содержится в некотором множестве $R_{i'}$, и длина орбиты каждого корня μ_j из любого множества R_j делится на b_j в силу (9). Ввиду взаимной простоты чисел b_i длина объединения $R = \cup_j R_j$ не менее $b_1 + \ldots + b_k$. Кроме того, среди корней μ_i есть как минимум $p^t + 1$ одинаковых, которые должны принадлежать разным орбитам. Если какой-то из этих корней лежит в некотором множестве R_j, то все равные ему тоже лежат в R_j, и $|R| \geqslant b_1 + \ldots + (p^t+1) b_j + \ldots + b_k > n$. В противном случае общее число элементов μ_j не менее $b_1 + \ldots + b_k + (p^t + 1) > n$. В обоих случаях получаем противоречие. □

Лемма 10. *Если группа Фробениуса KC с ядром K и циклическим дополнением $C = \langle c \rangle$ порядка n действует точно на векторном пространстве V над полем ненулевой характеристики p, взаимно простой с порядком ядра K, то минимальный многочлен элемента c на V равен $x^n - 1$. В частности, полупрямое произведение VC содержит элемент порядка $p \cdot n$ и* $\dim C_V(c) > 0$.

Д о к а з а т е л ь с т в о. См. лемму 1 в [6]. □

Лемма 11. *Пусть $\varepsilon \in \{+,-\}$ и $L = L^\varepsilon_n(q)$ — простая группа, где $q = p^m$. Если $G \cong \mathbb{Z}_p \times L$, то $\omega(G) \not\subseteq \omega(L)$.*

Д о к а з а т е л ь с т в о. При $n = 2$ утверждение хорошо известно. Пусть $n > 2$. Если $r = q^*_{[\varepsilon(n-1)]}$ определено, то L содержит элемент порядка r и $pr \notin \omega(\mathrm{SL}^\varepsilon_n(q))$ по лемме 9, откуда следует требуемое. В противном случае тройка (ε, n, q) совпадает с $(-,3,3)$ или с $(-,4,2)$, и тогда $3 \cdot 7 \in \omega\bigl(\mathbb{Z}_3 \times U_3(3)\bigr) \setminus \omega\bigl(U_3(3)\bigr)$ и $2 \cdot 5 \in \omega\bigl(\mathbb{Z}_2 \times U_4(2)\bigr) \setminus \omega\bigl(U_4(2)\bigr)$. □

2. Доказательство теоремы

Следующая теорема является переформулировкой нашего главного результата (теорема 1), представленного во введении.

Теорема 2. *Пусть $\varepsilon \in \{+,-\}$ и $L = L_n^\varepsilon(q)$ $(q = p^m)$ — простая группа, действующая на векторном пространстве W над полем характеристики p. Предположим, что $n \geqslant p$, $n \neq p+1$ и $(p,n) \notin \{(2,5),(3,6),(3,7),(3,10),(5,11),(5,18)\}$. Пусть, кроме того, $n \neq 6,7,9,10,11,18$ при $(\varepsilon,q) = (-,2)$ и $n \neq 5,8,11$ при $(\varepsilon,q) = (-,3)$. Тогда $\omega(WL) \neq \omega(L)$.*

Д о к а з а т е л ь с т в о. По лемме 11 можно считать, что L действует точно на W. Мы можем поднять представление группы L на W до (нетривиального) представления группы $S = \mathrm{SL}_n^\varepsilon(q)$.

Пусть $n = p^t + b_1 + \ldots + b_k$ — разложение числа n, существование которого утверждается в лемме 8. Если $(\varepsilon,q) = (-,2)$, то мы предполагаем, что $b_i > 3$, а если $(\varepsilon,q) = (-,3)$, то $b_i > 2$ для всех i. Пусть $r_i = q^*_{[\varepsilon b_i]}$ (по предположению это число определено для всех i).

Достаточно показать, что для любого нетривиального S-модуля W над полем характеристики p существует такой элемент $a \in WS$ порядка $c = p^{t+1} r_1 \cdot \ldots \cdot r_k$, что циклическая группа $\langle a \rangle$ тривиально пересекается с центром $Z(S)$. В самом деле, если это выполнено, то по лемме 9 получим $c \in \omega(WL) \setminus \omega(L)$ ввиду включения $\omega(L) \subseteq \omega(S)$.

Применим индукцию по k. Если $k = 0$, то $n = p^t$ и по лемме 6 группа S содержит подгруппу Фробениуса R с ядром порядка $q_{[\varepsilon n]}$ (этот примитивный делитель, очевидно, существует) и циклическим дополнением порядка p^t (лемма 6 может быть применена, поскольку либо $n = p^t$ нечетно, либо $q = p^m$ четно). Так как R действует точно на W, то из леммы 10 следует, что $p^{t+1} \in \omega(WS)$, и очевидно также, что циклическая подгруппа в WS порядка p^{t+1} тривиально пересекается с центром $Z(S)$.

Предположим, что $k > 0$. Пусть V — естественный n-мерный FS-модуль с (ортонормированным) базисом $\{e_1, \ldots, e_n\}$, где $F = \mathbb{F}_q$. Положим $U = \langle e_1, \ldots, e_{b_1} \rangle_F$ и $U' = \langle e_{b_1+1}, \ldots, e_n \rangle_F$. Пусть h_1 — неприводимый элемент из $\mathrm{SL}^\varepsilon(U,U')$ порядка r_1. Так как $1 < b_1 < n/2$, то $W_1 = C_W(h_1) \neq 0$ по лемме 1, и группа $S_1 = \mathrm{SL}^\varepsilon(U',U) \cong \mathrm{SL}^\varepsilon_{n_1}(q)$ действует нетривиально на W_1 по лемме 4, где $n_1 = p^t + b_2 + \ldots + b_n$. По индукции существует $a_1 \in W_1 S_1$ порядка $c_1 = p^{t+1} r_2 \cdot \ldots \cdot r_k$. Положим $a = h_1 a_1$. Так как $[h_1, a_1] = 1$ и r_1 взаимно просто с c_1, то $|a| = c$, и по построению ясно, что $a^{p^{t+1}} \in S$ централизует в V подпространство размерности p^t, откуда получаем $\langle a \rangle \cap Z(S) = 1$. □

3. Приложение

В таблице приведено разложение чисел $n < 36$ в виде $n = p^t + b_1 + \ldots + b_k$ для всех допустимых пар (n,p), существование которого утверждается в лемме 8. Если $p = 2$ и $n \neq 6,7,9,10,11,18$, то $b_i \neq 2,3$. Если $p = 3$ и $n \neq 5,8,11$, то $b_i \neq 2$.

(n,p)	$n = p^t + b_1 + \ldots + b_k$	(n,p)	$n = p^t + b_1 + \ldots + b_k$	(n,p)	$n = p^t + b_1 + \ldots + b_k$
$(2,2)$	$2 = 2$	$(20,7)$	$20 = 7+9+4$	$(29,2)$	$29 = 8+9+7+5$
$(3,3)$	$3 = 3$	$(20,11)$	$20 = 11+9$	$(29,3)$	$29 = 9+13+7$
$(4,2)$	$4 = 4$	$(20,13)$	$20 = 13+7$	$(29,5)$	$29 = 5+13+7+4$
$(5,3)$	$5 = 3+2$	$(20,17)$	$20 = 17+3$	$(29,7)$	$29 = 7+14+5+3$
$(5,5)$	$5 = 5$	$(21,2)$	$21 = 8+9+4$	$(29,11)$	$29 = 11+13+5$
$(6,2)$	$6 = 4+2$	$(21,3)$	$21 = 9+7+5$	$(29,13)$	$29 = 13+13+3$
$(7,2)$	$7 = 4+3$	$(21,5)$	$21 = 5+9+5+2$	$(29,17)$	$29 = 17+12$
$(7,5)$	$7 = 5+2$	$(21,7)$	$21 = 7+9+5$	$(29,19)$	$29 = 19+10$
$(7,7)$	$7 = 7$	$(21,11)$	$21 = 11+10$	$(29,23)$	$29 = 23+6$
$(8,2)$	$8 = 8$	$(21,13)$	$21 = 13+8$	$(29,29)$	$29 = 29$
$(8,3)$	$8 = 3+3+2$	$(21,17)$	$21 = 17+4$	$(30,2)$	$30 = 8+13+5+4$
$(8,5)$	$8 = 5+3$	$(21,19)$	$21 = 19+2$	$(30,3)$	$30 = 9+13+8$
$(9,2)$	$9 = 4+3+2$	$(22,2)$	$22 = 8+9+5$	$(30,5)$	$30 = 5+13+7+3+2$
$(9,3)$	$9 = 9$	$(22,3)$	$22 = 9+10+3$	$(30,7)$	$30 = 7+13+7+3$
$(9,5)$	$9 = 5+4$	$(22,5)$	$22 = 5+7+5+3+2$	$(30,11)$	$30 = 11+14+5$
$(9,7)$	$9 = 7+2$	$(22,7)$	$22 = 7+7+5+3$	$(30,13)$	$30 = 13+14+3$
$(10,2)$	$10 = 8+2$	$(22,11)$	$22 = 11+9+2$	$(30,17)$	$30 = 17+13$
$(10,5)$	$10 = 5+3+2$	$(22,13)$	$22 = 13+9$	$(30,19)$	$30 = 19+11$

$(10,7)$	$10=7+3$	$(22,17)$	$22=17+5$	$(30,23)$	$30=23+7$
$(11,2)$	$11=4+5+2$	$(22,19)$	$22=19+3$	$(31,2)$	$31=8+11+7+5$
$(11,3)$	$11=9+2$	$(23,2)$	$23=8+11+4$	$(31,3)$	$31=9+15+7$
$(11,7)$	$11=7+4$	$(23,3)$	$23=9+11+3$	$(31,5)$	$31=5+15+7+4$
$(11,11)$	$11=11$	$(23,5)$	$23=5+11+5+2$	$(31,7)$	$31=7+15+7+2$
$(12,2)$	$12=8+4$	$(23,7)$	$23=7+11+5$	$(31,11)$	$31=11+13+7$
$(12,3)$	$12=9+3$	$(23,11)$	$23=11+7+5$	$(31,13)$	$31=13+13+5$
$(12,5)$	$12=5+5+2$	$(23,13)$	$23=13+10$	$(31,17)$	$31=17+14$
$(12,7)$	$12=7+5$	$(23,17)$	$23=17+6$	$(31,19)$	$31=19+12$
$(13,2)$	$13=8+5$	$(23,19)$	$23=19+4$	$(31,23)$	$31=23+8$
$(13,3)$	$13=9+4$	$(23,23)$	$23=23$	$(31,29)$	$31=29+2$
$(13,5)$	$13=5+5+3$	$(24,2)$	$24=8+11+5$	$(31,31)$	$31=31$
$(13,7)$	$13=7+6$	$(24,3)$	$24=9+11+4$	$(32,2)$	$32=8+13+7+4$
$(13,11)$	$13=11+2$	$(24,5)$	$24=5+11+5+3$	$(32,3)$	$32=9+15+8$
$(13,13)$	$13=13$	$(24,7)$	$24=7+11+6$	$(32,5)$	$32=5+13+7+5+2$
$(14,2)$	$14=8+6$	$(24,11)$	$24=11+11+2$	$(32,7)$	$32=7+13+7+5$
$(14,3)$	$14=9+5$	$(24,13)$	$24=13+11$	$(32,11)$	$32=11+13+8$
$(14,5)$	$14=5+5+4$	$(24,17)$	$24=17+7$	$(32,13)$	$32=13+15+4$
$(14,7)$	$14=7+5+2$	$(24,19)$	$24=19+5$	$(32,17)$	$32=17+15$
$(14,11)$	$14=11+3$	$(25,2)$	$25=8+12+5$	$(32,19)$	$32=19+13$
$(15,2)$	$15=8+7$	$(25,3)$	$25=9+11+5$	$(32,23)$	$32=23+9$
$(15,3)$	$15=9+6$	$(25,5)$	$25=5+11+5+4$	$(32,29)$	$32=29+3$
$(15,5)$	$15=5+7+3$	$(25,7)$	$25=7+11+5+2$	$(33,2)$	$33=8+13+7+5$
$(15,7)$	$15=7+5+3$	$(25,11)$	$25=11+11+3$	$(33,3)$	$33=9+16+5+3$
$(15,11)$	$15=11+4$	$(25,13)$	$25=13+12$	$(33,5)$	$33=5+13+7+5+3$
$(15,13)$	$15=13+2$	$(25,17)$	$25=17+8$	$(33,7)$	$33=7+16+7+3$
$(16,2)$	$16=16$	$(25,19)$	$25=19+6$	$(33,11)$	$33=11+15+7$
$(16,3)$	$16=9+7$	$(25,23)$	$25=23+2$	$(33,13)$	$33=13+13+7$
$(16,5)$	$16=5+7+4$	$(26,2)$	$26=8+11+7$	$(33,17)$	$33=17+16$
$(16,7)$	$16=7+7+2$	$(26,3)$	$26=9+12+5$	$(33,19)$	$33=19+14$
$(16,11)$	$16=11+5$	$(26,5)$	$26=5+11+7+3$	$(33,23)$	$33=23+10$
$(16,13)$	$16=13+3$	$(26,7)$	$26=7+11+5+3$	$(33,29)$	$33=29+4$
$(17,2)$	$17=8+5+4$	$(26,11)$	$26=11+11+4$	$(33,31)$	$33=31+2$
$(17,3)$	$17=9+8$	$(26,13)$	$26=13+11+2$	$(34,2)$	$34=8+15+7+4$
$(17,5)$	$17=5+7+3+2$	$(26,17)$	$26=17+9$	$(34,3)$	$34=9+13+7+5$
$(17,7)$	$17=7+7+3$	$(26,19)$	$26=19+7$	$(34,5)$	$34=5+13+9+5+2$
$(17,11)$	$17=11+6$	$(26,23)$	$26=23+3$	$(34,7)$	$34=7+13+9+5$
$(17,13)$	$17=13+4$	$(27,2)$	$27=8+13+6$	$(34,11)$	$34=11+16+7$
$(17,17)$	$17=17$	$(27,3)$	$27=9+13+5$	$(34,13)$	$34=13+16+5$
$(18,2)$	$18=4+7+5+2$	$(27,5)$	$27=5+13+5+4$	$(34,17)$	$34=17+15+2$
$(18,3)$	$18=9+5+4$	$(7)27,$	$27=7+13+5+2$	$(34,19)$	$34=19+15$
$(18,7)$	$18=7+8+3$	$(27,11)$	$27=11+13+3$	$(34,23)$	$34=23+11$
$(18,11)$	$18=11+7$	$(27,13)$	$27=13+11+3$	$(34,29)$	$34=29+5$
$(18,13)$	$18=13+5$	$(27,17)$	$27=17+10$	$(34,31)$	$34=31+3$
$(19,2)$	$19=8+7+4$	$(27,19)$	$27=19+8$	$(35,2)$	$35=8+13+9+5$
$(19,3)$	$19=9+7+3$	$(27,23)$	$27=23+4$	$(35,3)$	$35=9+17+5+4$
$(19,5)$	$19=5+7+5+2$	$(28,2)$	$28=8+13+7$	$(35,5)$	$35=5+13+7+5+3+2$
$(19,7)$	$19=7+7+5$	$(28,3)$	$28=9+13+6$	$(35,7)$	$35=7+17+8+3$
$(19,11)$	$19=11+8$	$(28,5)$	$28=5+13+7+3$	$(35,11)$	$35=11+17+7$
$(19,13)$	$19=13+6$	$(28,7)$	$28=7+13+5+3$	$(35,13)$	$35=13+17+5$
$(19,17)$	$19=17+2$	$(28,11)$	$28=11+13+4$	$(35,17)$	$35=17+13+5$
$(19,19)$	$19=19$	$(28,13)$	$28=13+13+2$	$(35,19)$	$35=19+16$
$(20,2)$	$20=8+7+5$	$(28,17)$	$28=17+11$	$(35,23)$	$35=23+12$
$(20,3)$	$20=9+8+3$	$(28,19)$	$28=19+9$	$(35,29)$	$35=29+6$
$(20,5)$	$20=5+7+5+3$	$(28,23)$	$28=23+5$	$(35,31)$	$35=31+4$

Поступила 8.06.2006

СПИСОК ЛИТЕРАТУРЫ

1. **Hall P., Higman G.** The p-length of p-soluble groups and reduction theorems for Burnside's problem // Proc. London Math. Soc., Ser. III. 1956. V. 6. P. 1–42.
2. **Mazurov V.D.** Characterizations of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, no. 1. P. 129–140.
3. **Заварницин А.В., Мазуров В.Д.** О порядках элементов в накрытиях симметрических и знакопеременных групп // Алгебра и логика. 1999. Т. 38, № 3. С. 296–315.
4. **Заварницин А.В.** Веса неприводимых $\mathrm{SL}_3(q)$-модулей в характеристике определения // Сиб. мат. журн. 2004. Т. 45, № 2. С. 319–328.
5. **Заварницин А.В.** Порядки элементов в накрытиях $L_n(q)$ и распознавание знакопеременной группы A_{16}: Препринт № 48 // Новосибирск: НИИДМИ, 2000.
6. **Мазуров В.Д.** О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.
7. **Brandl R., Shi W.** The characterization of $\mathrm{PSL}_2(q)$ by its element orders // J. Algebra. 1994. V. 163, no. 1. P. 109–114.
8. **Darafsheh M.R., Moghaddamfar A.R.** Corrigendum: Characterization of the groups $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$ and $\mathrm{PSL}_7(2)$ [*Comm. Algebra*, **29**, no. 1 (2001), 465–475] // Comm. Algebra. 2003. V. 31, no. 9. P. 4651–4653.

9. **Grechkoseeva M.A., Lucido M.S., Mazurov V.D., Moghaddamfar A.R., Vasil'ev A.V.** On recognition of the projective special linear groups over the binary field // Sib. Elektron. Mat. Izv. 2005. V. 2. P. 253–263.
10. Нерешенные вопросы теории групп: Коуровская тетрадь. Новосибирск: Ин-т математики СО РАН, 1999.
11. **Kleidman P., Liebeck M.** The subgroup structure of the finite classical groups // London Math. Soc. Lect. Note Ser. Cambridge: Cambridge University Press, 1990. V. 129.
12. **Zsigmondy K.** Zur Theorie der Potenzreste // Monatsh. für Math. und Phys. 1892. V. 3. C. 256–284.
13. **Васильев А.В., Гречкосеева М.А.** О распознавании по спектру конечных простых линейных групп над полями характеристики 2 // Сиб. мат. журн. 2005. Т. 46, № 4. С. 749–758.
14. **Hanson D.** On a theorem of Sylvester and Schur // Canad. Math. Bull. 1973. V. 16. P. 195–199.
15. **Suprunenko I.D., Zalesskii A.E.** Fixed vectors for elements in modules for algebraic groups // Intern. J. Algebra Comput. 2007. V. 17, no. 4. P. 773–785.