*Сибирский математический журнал*
*Январь—февраль, 2006. Том 47, № 1*

*УДК 519.542*

# РАСПОЗНАВАНИЕ НЕКОТОРЫХ ЛИНЕЙНЫХ ГРУПП НАД БИНАРНЫМ ПОЛЕМ ПО ИХ СПЕКТРАМ

**М. С. Лючидо, А. Р. Могхаддамфар**

**Аннотация:** Исследованы линейные группы $L_n(2)$ и получены некоторые общие результаты для этих групп. Показано, что линейные группы $L_p(2)$, где 2 — первообразный корень по модулю $p$ ($p$ простое нечетное), распознаваемы по их спектрам. Например, линейные группы $L_3(2)$, $L_5(2)$, $L_{11}(2)$, $L_{13}(2)$, $L_{19}(2)$, $L_{29}(2)$, $L_{37}(2)$, $L_{53}(2)$ и т. д. распознаваемы по их спектрам.

**Ключевые слова:** граф Грюнберга — Кегеля, специальная проективная линейная группа, распознавание по спектрам.

## 1. Введение

Всюду ниже все группы предполагаются конечными и все простые группы — неабелевыми. Некоторые интересные задачи в теории конечных групп касаются арифметических структур. Для группы $G$ к арифметическим структурам относятся порядок $G$, обозначаемый через $|G|$, множество простых делителей $|G|$, обозначаемое через $\pi(G)$, множество $\omega(G)$ порядков всех элементов $G$, называемое *спектром* $G$, и т. д.

Спектр $\omega(G)$ группы $G$ определяет *граф Грюнберга — Кегеля* $\mathrm{GK}(G)$ с множеством вершин $\pi(G)$, в котором вершины $p$ и $q$ соединены ребром, если $pq \in \omega(G)$. Обозначим через $s(G)$ число компонент связности $\mathrm{GK}(G)$ и через $\pi_i = \pi_i(G)$, $i = 1, 2, \dots, s(G)$, — $i$-ю компоненту связности $\mathrm{GK}(G)$. Если $2 \in \pi(G)$, то мы предполагаем, что $2 \in \pi_1(G)$. Обозначим через $\mu(G)$ множество чисел в $\omega(G)$, максимальных относительно отношения делимости. Обозначим через $\mu_i = \mu_i(G)$ ($\omega_i = \omega_i(G)$) множество чисел $n \in \mu(G)$ ($n \in \omega(G)$) таких, что каждый простой делитель $n$ принадлежит $\pi_i$.

Для множества $\Omega \subset \mathbb{N}$ натуральных чисел определим $h(\Omega)$ как число (возможно, $\infty$) неизоморфных конечных групп $G$ со спектром $\Omega$ и положим $h(G) = h(\omega(G))$. Группу $G$ называют *распознаваемой по спектру*, если $h(G) = 1$. Некоторый перечень простых групп, распознаваемых или нет, дан в [1].

Для $m \in \mathbb{N}$ обозначим через $\pi(m)$ множество простых делителей $m$. Для краткости будем обозначать $\mathrm{PSL}(n, q)$ через $L_n(q)$, так что $L_n(2) = \mathrm{GL}(n, 2)$. Согласно [2] имеем

$$s(L_n(2)) = \begin{cases} 1, & \text{если } n \neq p,\ p+1, \\ 2, & \text{если } n = p \text{ или } p+1, \end{cases}$$

This work has been supported by a grant from K. N. Toosi University of Technology and by the Research Institute for Fundamental Sciences Tabriz, Iran.

где $p > 3$ простое. Если $n$ равно $p$ или $p+1$, то $L_n(2)$ имеет две компоненты связности, одна из которых

$$\pi_1 = \pi\left(2\prod_{i=1}^{p-1}(2^i-1)\right), \quad \text{соответственно } \pi_1 = \pi\left(2(2^{p+1}-1)\prod_{i=1}^{p-1}(2^i-1)\right),$$

а другая в любом случае

$$\pi_2 = \pi(2^p - 1).$$

Для простой степени $q$ обозначим через $\mathbb{F}_q$ конечное поле порядка $q$. Значения $s(G)$ и $h(G)$ для некоторых линейных групп над полем $\mathbb{F}_2$ можно найти в табл. 1.

Таблица 1

| $G$ | $s(G)$ | $h(G)$ | Ссылки |
|---|---|---|---|
| $L_3(2) \cong L_2(7)$ | 3 | 1 | [3] |
| $L_4(2) \cong A_8$ | 2 | 1 | [4] |
| $L_5(2)$ | 2 | 1 | [5] |
| $L_6(2)$ | 2 | 1 | [5, 6] |
| $L_7(2)$ | 2 | 1 | [5, 7] |
| $L_8(2)$ | 2 | 1 | [8] |
| $L_9(2)$ | 1 | Неизвестно | |
| $L_{10}(2)$ | 1 | Неизвестно | |
| $L_{11}(2)$ | 2 | 1 | [9] |

Как видно из табл. 1, ничего не указано для $h(G)$ в случаях $G = L_9(2)$ и $L_{10}(2)$. Так происходит потому, что наш способ распознавания связан с группами, граф Грюнберга — Кегеля которых несвязен, а группы $L_9(2)$ и $L_{10}(2)$ имеют связный граф Грюнберга — Кегеля. Тем самым можно поставить следующую задачу (см. также [6]).

**Задача.** *Могут ли специальные проективные линейные группы $L_9(2)$ и $L_{10}(2)$ быть распознаваемы по их спектрам?*

Так как до сих пор не известно никакого $n \geq 3$, для которого $h(L_n(2)) \neq 1$, сделаем следующее

**Предположение.** *Специальные проективные линейные группы $L_n(2)$ для всех целых $n \geq 3$ распознаваемы по их спектрам.*

Примитивные простые делители впервые были рассмотрены Жигмонди [10]. Сформулируем теорему Жигмонди следующим образом.

**Теорема Жигмонди** [10]. *Пусть $a$ и $n$ суть целые, большие 1. Существует простой делитель $p$ числа $a^n - 1$ такой, что $p$ не делит $a^i - 1$ для всех $1 \leq i < n$, кроме как в следующих случаях:*

(1) $n = 2$, $a = 2^s - 1$, *где* $s \geq 2$;

(2) $n = 6$, $a = 2$.

Такое простое $p$ назовем *примитивным простым делителем* $a^n - 1$ и будем при этом использовать обозначение $a_{[n]}$. Разумеется, может быть более одного примитивного простого делителя у $a^n - 1$, и символ $a_{[n]}$ относится к какому-либо из них. Например, примитивными простыми делителями числа $47^4 - 1$ будут 5, 13, 17, и через $47_{[4]}$ обозначается одно из них. Очевидно, что если $a_{[n]}$ — примитивный простой делитель $a^n - 1$, то $a$ имеет порядок $n$ по модулю $a_{[n]}$ и тем самым $a_{[n]} \equiv 1 \bmod (n)$. Итак, $a_{[n]} \geq n + 1$.

Будем говорить, что $a$ — *примитивный корень по модулю* $p$, если $(a, p) = 1$ и $a_{[p-1]} = p$. Целочисленный вариант гипотезы Артина о примитивных корнях утверждает, что для фиксированного целого $a$, не являющегося точным корнем и не равного $-1$, есть бесконечно много простых чисел таких, что $(a, p) = 1$ и $a_{[p-1]} = p$. В предположении выполнения гипотезы Римана для некоторого числового поля гипотеза Артина была доказана в [11].

В данной статье, используя классификационную теорему для конечных простых групп, мы докажем, что наше предположение также верно для линейных групп $L_p(2)$, где 2 — примитивный корень по модулю $p$ ($p$ простое нечетное). В завершение будет доказана

**Основная теорема.** *Пусть $p$ простое нечетное. Если 2 — примитивный корень по модулю $p$, то линейная группа $L_p(2)$ распознаваема по спектру.*

Например, линейные группы $L_3(2)$, $L_5(2)$, $L_{11}(2)$, $L_{13}(2)$, $L_{19}(2)$, $L_{29}(2)$, $L_{37}(2)$, $L_{53}(2)$ и т. д. распознаваемы по их спектрам.

Введем некоторые обозначения. Будем через $A \rtimes B$ обозначать полупрямое произведение $A$ и $B$. Будем писать $\mathbb{Z}_n$ для циклической группы порядка $n$ и обозначать через $\lfloor n \rfloor$ наибольшее целое, не превосходящее $n$. Для элемента $x$ группы $G$ обозначим через $o(x)$ порядок $x$. Все другие обозначения стандартны и могут быть найдены, например, в [12, 13].

## 2. О спектре $L_n(2)$

В [9] найдено $\mu(L_{11}(2))$. Точно таким же путем были найдены $\mu(L_n(2))$ для $n = 9, 10$, указанные в табл. 2.

Таблица 2

| $G$ | $\mu(G)$ |
|---|---|
| $L_9(2)$ | 16, 56, 120, 124, 186, 210, 217, 252, 254, 255, 381, 465, 511 |
| $L_{10}(2)$ | 16, 120, 168, 248, 252, 315, 372, 381, 420, 434, 465, 508, 510, 511, 651, 889, 1023 |

Этот же путь можно проделать для нахождения $\mu(L_n(2))$ при $n \geq 12$, но это связано с длинным вычислением, и так как мы в основном имеем дело со специальными числами в $\mu(L_n(2))$, то мы можем опустить получение всего множества $\mu(L_n(2))$, а ограничиться лишь некоторыми числами в $\mu(L_n(2))$, играющими важную роль в распознаваемости групп по их спектрам.

Здесь мы используем обозначения, аналогичные [9], и все они, по существу, восходят к [14].

Пусть $f(t)=t^d+a_{d-1}t^{d-1}+\dots+a_0$ — полином над $\mathbb{F}_2$ степени $d$. Определим матрицы

$$U(f)=U_1(f):=\begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0\\ 0 & 0 & 1 & 0 & \dots & 0\\ 0 & 0 & 0 & 1 & \dots & 0\\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots\\ 0 & 0 & 0 & 0 & \dots & 1\\ a_0 & a_1 & a_2 & a_3 & \dots & a_{d-1}\end{bmatrix},$$

$$U_m(f):=\begin{bmatrix} U(f) & 1_d & 0 & \dots & 0\\ 0 & U(f) & 1_d & \dots & 0\\ \vdots & \vdots & \vdots & \dots & \vdots\\ 0 & 0 & 0 & \dots & U(f)\end{bmatrix}$$

с $m$ диагональными блоками $U(f)$, $1_d$ — единичная матрица. Наконец, если $\lambda=\{l_1,l_2,\dots,l_p\}$ — разложение положительного целого $k$ в сумму $p$ слагаемых, записанных в порядке убывания: $l_1\geq l_2\geq\dots\geq l_p>0$, то

$$U_\lambda(f):=\operatorname{diag}\{U_{l_1}(f),U_{l_2}(f),\dots,U_{l_p}(f)\}$$

и ее характеристический полином $\det(t1-U_\lambda(f))$ есть $f(t)^k$. Пусть $A\in\mathrm{GL}(n,q)$ имеет характеристический полином

$$f_1^{k_1}f_2^{k_2}\dots f_N^{k_N},$$

где $f_1,f_2,\dots,f_N$ суть различные неприводимые полиномы над $\mathbb{F}_q$, $k_i\geq 0$ ($i=1,2,\dots,N$), и если $d_1,d_2,\dots,d_N$ — соответствующие степени $f_1,f_2,\dots,f_N$ с $\sum\limits_{i=1}^{N}k_id_i=n$, то $A$ сопряжена с

$$\operatorname{diag}\{U_{\nu_1}(f_1),U_{\nu_2}(f_2),\dots,U_{\nu_N}(f_N)\},$$

в $\mathrm{GL}(n,2)$, где $\nu_1,\nu_2,\dots,\nu_N$ — некоторые разбиения $k_1,k_2,\dots,k_N$ соответственно. В таком случае классы сопряженности $c$ группы $A$ обозначим символом

$$c=\left(f_1^{\nu_1}f_2^{\nu_2}\dots f_N^{\nu_N}\right).$$

Кроме того, если $B$ сопряжена с $\operatorname{diag}\{U_{k_1}(f_1),U_{k_2}(f_2),\dots,U_{k_N}(f_N)\}$, то

$$o(B)=\mathrm{l.c.m.}\{o(U_{k_1}(f_1)),o(U_{k_2}(f_2)),\dots,o(U_{k_N}(f_N))\}.\tag{1}$$

С другой стороны, легко видеть, что $o(A)$ делит $o(B)$. Следовательно, среди всех элементов $\mathrm{GL}(n,2)$, имеющих один тот же характеристический полином $f_1^{k_1}f_2^{k_2}\dots f_N^{k_N}$, у $B$ наибольший порядок.

Определение. Пусть $f\in\mathbb{F}_q[t]$ — ненулевой полином. Если $f(0)\neq 0$, то наименьшее положительное целое $e$, для которого $f(t)$ делит $t^e-1$, называют *порядком* $f$ и обозначают через $\operatorname{ord}(f)$.

Если $A$ — элемент из $\mathrm{GL}(n,q)$ с характеристическим полиномом $f(t)$, то известно, что порядок $A$ в $\mathrm{GL}(n,q)$ равен $\operatorname{ord}(f)$. Поэтому нахождение порядков полиномов над $\mathbb{F}_q$ важно для нахождения порядков элементов в общих линейных группах и мы будем интересоваться $\mathrm{GL}(n,2)$.

Пусть $w(d,2)$ — число неприводимых полиномов $f(t)$ степени $d$ над $\mathbb{F}_2$. Далее, если $w(d,2)=k$, то найдутся $k$ неприводимых полиномов степени $d$ над $\mathbb{F}_2$, допустим, $g_1,g_2,\dots,g_k$. Разумеется, $o(U_1(g_i))=\operatorname{ord}(g_i)$ делит $2^d-1$, а также существует $g_j$, $1\leq j\leq k$, такое, что $o(U_1(g_j))=\operatorname{ord}(g_j)=2^d-1$.

Сформулируем наш первый результат.

**Лемма 1.** *Пусть* $n = \sum\limits_{i=1}^{N} k_i d_i$, *где* $k_1, k_2, \dots, k_N, d_1, d_2, \dots, d_N$ — *положительные целые и* $n \geq 3$. *Пусть* $e = \mathrm{l.\,c.\,m.}\{2^{d_1}-1, 2^{d_2}-1, \dots, 2^{d_N}-1\}$ *и* $m$ — *наименьшее целое такое, что* $2^m \geq \max\{k_1, k_2, \dots, k_N\}$. *Тогда* $2^m e \in \omega(L_n(2))$.

Доказательство. Пусть $A \in L_n(2)$ имеет характеристический полином

$$f = f_1^{k_1} f_2^{k_2} \dots f_N^{k_N},$$

где $f_1, f_2, \dots, f_N$ суть различные неприводимые полиномы над $\mathbb{F}_2$ степеней $d_1, d_2, \dots, d_N$ соответственно и $o(U_1(f_i)) = \mathrm{ord}(f_i) = 2^{d_i} - 1$. Предположим, что $A$ сопряжена с

$$\mathrm{diag}\{U_{k_1}(f_1), U_{k_2}(f_2), \dots, U_{k_N}(f_N)\}.$$

Тогда по теореме 3.8 из [15] имеем

$$o(U_{k_i}(f_i)) = 2^{m_i}\,\mathrm{ord}(f_i) = 2^{m_i}(2^{d_i}-1), \quad i = 1, 2, \dots, N,$$

где $m_i$ — наименьшее целое с $2^{m_i} \geq k_i$. Также по (1) получим

$$\begin{aligned} o(A) &= \mathrm{l.c.m.}\{o(U_{k_1}(f_1)), o(U_{k_2}(f_2)), \dots, o(U_{k_N}(f_N))\} \\ &= \mathrm{l.c.m.}\{2^{m_1}(2^{d_1}-1), 2^{m_2}(2^{d_2}-1), \dots, 2^{m_N}(2^{d_N}-1)\} \\ &= 2^m \times \mathrm{l.c.m.}\{2^{d_1}-1, 2^{d_2}-1, \dots, 2^{d_N}-1\}, \end{aligned}$$

где $m = \max\{m_1, m_2, \dots, m_N\}$. $\square$

В следующем результате мы установим некоторые свойства множества $\omega(L_n(2))$. Их доказательства основаны на изучении структуры классов сопряженности $L_n(2)$ и некоторых арифметических рассуждениях.

**Следствие 1.** *Справедливы следующие утверждения.*

(a) *Для* $n \geq 3$ *имеет место включение* $\omega(L_n(2)) \subset \omega(L_{n+1}(2))$. *В частности,* $2^i - 1 \in \omega(L_n(2))$ *для каждого* $1 \leq i \leq n$.

(b) $(q^n-1)/d(q-1)$ *и* $(q^{n-1}-1)/d$ *принадлежат* $\mu(L_n(q))$, *где* $d = (n, q-1)$. *В частности,* $2^{n-1}-1, 2^n-1 \in \mu(L_n(2))$.

(c) *Если* $s$ — *наименьшее целое такое, что* $2^s \geq n$, *то* $2^s$ — *2-период* $L_n(2)$, *тем самым* $s \in \mathbb{N}$ *таково, что* $2^s \in \omega(L_n(2))$ *и* $2^{s+1} \notin \omega(L_n(2))$.

(d) *Если* $A \in L_n(2)$, *то* $o(A) \leq 2^n - 1$.

(e) $k(2^{n-2}-1) \in \omega(L_n(2))$ *тогда и только тогда, когда* $k$ *равно* $1, 2$ *или* $3$. *Кроме того, если* $m \in \mu(L_n(2))$ *и* $m$ *четно, то* $m \leq 2(2^{n-2}-1)$.

(f) *Пусть* $n = \sum\limits_{i=1}^{N} d_i$, *где* $d_1, d_2, \dots, d_N$ — *целые положительные и* $(d_i, d_j) = 1$ *для любых* $i, j = 1, 2, \dots, N$. *Тогда* $\prod\limits_{i=1}^{N}(2^{d_i}-1) \in \mu(L_n(2))$.

Доказательство. (a) Очевидно, $L_n(2) \hookrightarrow L_{n+1}(2)$ для любого $n \geq 2$, так что $\omega(L_n(2)) \subseteq \omega(L_{n+1}(2))$. Кроме того, $L_i(2)$ содержит цикл Зингера порядка $2^i - 1$. Это завершает доказательство п. (a).

(b) См. лемму 14 в [16].

(c) Пусть сначала $s$ — наименьшее целое такое, что $2^s \geq n$. Тогда по лемме 1 заключаем, что $2^s \in \omega(L_n(2))$. Далее, предположим, что $c = \left(f_1^{k_1} f_2^{k_2} \dots f_N^{k_N}\right)$

представляет произвольный класс сопряженности в $L_n(2)$, где $f_i$ — неприводимый полином над $\mathbb{F}_2$ степени $d_i$ и $B \in c$. Пусть $|k|_p$ — $p$-часть числа $k$. Рассуждения, аналогичные приведенным в доказательстве леммы 1, показывают, что $|o(B)|_2$ делит $2^m$, где $m$ — наименьшее целое такое, что $2^m \geq \max\{k_1, k_2, \ldots, k_N\}$. Очевидно, что $\max\{k_1, k_2, \ldots, k_N\} \leq n$, когда $\sum\limits_{i=1}^{N} k_i d_i = n$, откуда заключаем, что $2^m \leq 2^s$ и, следовательно, $|o(B)|_2 \leq 2^s$. Поэтому $2^s$ — 2-период $L_n(2)$.

(d) Пусть $A \in L_n(2)$ имеет характеристический полином $f = f_1^{k_1} f_2^{k_2} \ldots f_N^{k_N}$, где $f_i$ — неприводимый полином над $\mathbb{F}_2$ степени $d_i$. Допустим, что $m$ и $e$, как в лемме 1. Очевидно, что $o(A)$ делит $2^m e$. Замечая, что $\sum\limits_{i=1}^{N} d_i k_i = n$, заключаем, что

$$o(A) \leq 2^m e \leq 2^m (2^{d_1} - 1)(2^{d_2} - 1) \ldots (2^{d_N} - 1) \leq 2^{\left(m + \sum\limits_{i=1}^{N} d_i\right)} - 1 \leq 2^n - 1,$$

и это завершает доказательство п. (d).

(e) Пусть $A \in L_n(2)$. Ясно, что $A \in \left(f_{n-2} f_i^k\right)$ тогда и только тогда, когда $(i, k)$ равно $(1, 2)$ или $(2, 1)$. Используя (1), в первом случае имеем $o(A) = 2(2^{n-2} - 1)$, а в последнем —

$$o(A) = \begin{cases} 2^{n-2} - 1, & \text{если } n \text{ четно}, \\ 3(2^{n-2} - 1), & \text{если } n \text{ нечетно}. \end{cases}$$

Отсюда $k(2^{n-2} - 1) \in \omega(L_n(2))$ тогда и только тогда, когда $k$ равно 1, 2 или 3. Рассуждая, как в доказательстве п. (d), можно доказать, что $2(2^{n-2} - 1)$ — наибольшее четное в $\omega(L_n(2))$, откуда $2(2^{n-2} - 1) \in \mu(L_n(2))$.

(f) Пусть $A \in (f_1 f_2 \ldots f_N)$, где $f_i$ — неприводимый полином над $\mathbb{F}_2$ степени $d_i$, и $o(U_1(f_i)) = 2^{d_i} - 1$. По лемме 1 легко показать, что

$$o(A) = \text{l.c.m.}\{2^{d_1} - 1, 2^{d_2} - 1, \ldots, 2^{d_N} - 1\} = \prod_{i=1}^{N} (2^{d_i} - 1),$$

так как $(2^{d_i} - 1, 2^{d_j} - 1) = 2^{(d_i, d_j)} - 1 = 1$.

Докажем теперь, что $o(A) \in \mu(L_n(2))$. Предположим, что $L_n(2)$ содержит элемент, пусть $B$, такой, что $o(A)$ делит $o(B)$. Предположим, что $B \in \left(g_1^{k_1} g_2^{k_2} \ldots g_z^{k_z}\right)$, где $g_j$, $1 \leq j \leq z$, — неприводимый полином над $\mathbb{F}_2$ степени $m_j$, $\sum\limits_{j=1}^{z} k_j m_j = n$ и $o(U_1(g_j)) = 2^{m_j} - 1$. Из леммы 1 имеем $o(B) = 2^t e$, где $t$ — наименьшее положительное целое такое, что $2^t \geq \max\{k_1, k_2, \ldots, k_z\}$ и $e = \text{l.c.m.}\{2^{m_1} - 1, 2^{m_2} - 1, \ldots, 2^{m_z} - 1\}$. Поскольку $o(A)$ делит $o(B)$, для каждого $i$ найдется $j_{(i)}$ такое, что $d_i \mid m_{j_{(i)}}$, $1 \leq i \leq N$. Тогда $d_i \leq m_{j_{(i)}}$ влечет $\sum\limits_{i=1}^{N} d_i \leq \sum\limits_{i=1}^{N} m_{j_{(i)}}$. С другой стороны, так как $k_i \geq 1$, получаем

$$\sum_{j=1}^{z} m_j \leq \sum_{j=1}^{z} k_j m_j = n = \sum_{i=1}^{N} d_i \leq \sum_{i=1}^{N} m_{j_{(i)}}.$$

Следовательно, имеет место равенство, откуда $N = z$, $k_i = 1$ и $m_{j_{(i)}} = d_i$ для всех $i$, $1 \leq i \leq N$. Тем самым $A = B$. Следствие доказано. $\square$

## 3. Предварительные результаты

Начнем с известных теорем Грюнберга и Кегеля.

**Теорема Грюнберга — Кегеля** (см. [17, теорема A]). *Если $G$ — конечная группа с несвязным графом $\mathrm{GK}(G)$, то имеет место одно из следующих свойств:*

(1) *$s(G) = 2$, $G$ фробениусова или 2-фробениусова.*

(2) *$G$ — расширение $\pi_1(G)$-группы $N$ посредством группы $G_1$, где $P \leq G_1 \leq \mathrm{Aut}(P)$, $P$ — неабелева простая группа и $G_1/P$ — $\pi_1(G)$-группа. Кроме того, $s(P) \geq s(G)$, и для каждого $i$, $2 \leq i \leq s(G)$, существует $j$, $2 \leq j \leq s(P)$, такое, что $\omega_j(P) = \omega_i(G)$.*

**Лемма 2** (см. [18]). *Пусть $P$ — конечная простая группа с несвязным графом $\mathrm{GK}(P)$. Тогда $|\mu_i(P)| = 1$ для $2 \leq i \leq s(P)$. Пусть $n_i(P)$ — единичный элемент в $\mu_i(P)$ для $i \geq 2$. Тогда значения $P$, $\pi_1(P)$ и $n_i(P)$ при $2 \leq i \leq s(P)$ таковы, как в табл.* 2a–2c *из* [19].

**Лемма 3** [16, лемма 14]. *Имеют место следующие утверждения.*

(a) $(q^n-1)/(q+1)(n,q+1) \in \omega(U_n(q))$ *для четного $n$ и* $(q^{n-1}-1)/(n,q+1) \in \omega(U_n(q))$ *для нечетного $n$.*

(b) $3^{n-1} - 1 \in \omega(^2D_n(3))$.

**Лемма 4** (см. [20]). *Пусть $a, b \in L_n(q)$, $q = r^m$, $n \geq 4$, $o(a) = r$ и $[a, b] = 1$. Тогда $\pi(o(b)) \subseteq \pi(\mathrm{SL}(n-2, q))$.*

В качестве непосредственного следствия из леммы 4 отметим, что в графе $\mathrm{GK}(L_p(2))$ вершина 2 не соединена с $2_{[p-1]}$. Другими словами, получаем

**Следствие 2.** $2 \cdot 2_{[p-1]} \notin \omega(L_p(2))$.

С другой стороны, в следующей лемме мы докажем, что существует внешний автоморфизм $L_p(2)$ порядка $2 \cdot 2_{[p-1]}$, и это несомненно доказывает, что $\omega(L_p(2)) \subsetneq \omega(\mathrm{Aut}(L_p(2)))$.

**Лемма 5.** $2 \cdot 2_{[p-1]} \in \omega(\mathrm{Aut}(L_p(2)))$.

Доказательство. Достаточно рассмотреть графовый автоморфизм $\alpha$ порядка 2 группы $K = L_p(2)$. Тогда, так как $p$ нечетно, имеем

$$C_K(\alpha) \cong PSO^+(p,2) \quad \text{порядка } 2^{((p-1)/2)^2}(2^2-1)(2^4-1)\dots(2^{p-1}-1).$$

(см. 19.9 в [21]). □

В следующей лемме будет доказано существование фробениусовой группы типа $2^{n-1} : 2^{n-1} - 1$ в $L_n(2)$.

**Лемма 6.** *Линейная группа $L_n(2)$, $n \geq 3$, содержит фробениусову подгруппу $KC$, ядро которой $K$ является элементарной абелевой 2-группой порядка $2^{n-1}$, дополнение которой $C$ есть циклическая группа порядка $2^{n-1} - 1$.*

Доказательство. Пусть $H = \langle A \rangle$, где $A \in GL(n-1, 2)$ и $o(A) = 2^{n-1} - 1$. Тогда

$$L = \left\{ \left[ \begin{array}{c|c} 1 & a_1 a_2 \dots a_{n-1} \\ \hline 0 & X \end{array} \right] \mid X \in H,\ a_i \in \mathbb{F}_2,\ 1 \leq i \leq n-1 \right\} \leq L_n(2).$$

Положим

$$K = \left\{ \left[ \begin{array}{c|c} 1 & a_1 a_2 \dots a_{n-1} \\ \hline 0 & I \end{array} \right] \mid a_i \in \mathbb{F}_2,\ 1 \leq i \leq n-1 \right\}$$

и

$$C = \left\{ \left[ \begin{array}{c|c} 1 & 0 \\ \hline 0 & X \end{array} \right] \mid X \in H \right\}.$$

Ясно, что $K$ — элементарная абелева 2-группа порядка $2^{n-1}$ и $C$ — циклическая группа порядка $2^{n-1}-1$. Кроме того, мы имеем полупрямое произведение $L = K \rtimes C$, являющееся группой Фробениуса, что и требовалось. $\square$

Покажем, как фробениусова подгруппа типа $2^p-1 : p$ может быть построена в $L_p(2)$.

**Лемма 7** (Заварницын). *Линейная группа $L_p(2)$, $p \geq 3$, содержит фробениусову подгруппу конфигурации $2^p - 1 : p$.*

Доказательство. Есть общий факт, что группа $\mathrm{GL}(n, q)$ содержит подгруппу, изоморфную $\mathbb{Z}_{q^n-1} : \mathbb{Z}_n$ — расширению циклической группы порядка $q^n - 1$ посредством циклической группы порядка $n$ (см. [22, п. 7.3]). Эта группа, вообще говоря, не фробениусова, но в случае $n = p$ (простое) и $q = 2$ является фробениусовой, ибо $2^p - 1 \in \mu(L_p(2))$. $\square$

**Лемма 8** [23]. *Пусть $G$ — конечная группа, $N$ — нормальная подгруппа в $G$ и $G/N$ — фробениусова группа с фробениусовым ядром $F$ и циклическим дополнением $C$. Если $(|F|, |N|) = 1$ и $F$ не содержится в $NC_G(N)/N$, то $p|C| \in \omega(G)$ для некоторого простого делителя $p$ числа $|N|$.*

## 4. Доказательство основной теоремы

Пусть $G$ — конечная группа такая, что $\omega(G) = \omega(L_p(2))$ с $p = 2_{[p-1]}$. В таком случае по следствию 2 будет $2p \notin \omega(G)$. Как было отмечено, простые группы $L_n(2)$ для $n = 3, 4, \dots, 8, 11$ распознаваемы, так что рассмотрим $p \geq 13$. Простые группы $L_p(2)$, где $p$ простое нечетное, имеют две компоненты связности:

$$\pi_1 = \pi\left(2 \prod_{i=1}^{p-1} (2^i - 1)\right) \quad \text{и} \quad \pi_2 = \pi(2^p - 1).$$

Докажем, что $G \cong L_p(2)$.

Следующая лемма сводит задачу к изучению простых групп.

**Лемма 9.** *Выполнен п. (2) теоремы Грюнберга — Кегеля.*

Доказательство вытекает из основного результата в [24]. $\square$

Далее будем использовать обозначения из п. (2) теоремы Грюнберга — Кегеля.

**Лемма 10.** $P \cong L_p(2)$.

Доказательство. Согласно классификации конечных простых групп мы знаем, что возможности для $P$ таковы:

(1) знакопеременные группы $A_n$, $n \geq 5$;

(2) 26 спорадических конечных простых групп;

(3) простые группы лиева типа.

Рассмотрим эти случаи по отдельности. Предположим сначала, что $P$ — знакопеременная группа $A_n$, $n \geq 5$. Из [17] известно, что $n_j(A_n)$ для $j \geq 2$ является простым нечетным. Отсюда $2^p - 1$ должно быть простым и $n \geq 2^p - 1$. Рассмотрим простое $r$ между $\lfloor \frac{2^p-1}{2} \rfloor$ и $2^p - 1$. Ясно, что $r > 2^{p-1} - 1$, тем самым

$$r \in \pi(A_n) \backslash \pi(G);$$

противоречие.

Предположим теперь, что $P$ — спорадическая простая группа. Так как согласно [17] $n_i(P)$, $i \geq 2$, для всех спорадических простых групп простые, меньшие 71, то $2^p - 1$ простое и $2^p - 1 < 71$, что приводит к противоречию с тем, что $p \geq 13$.

Наконец, пусть $P$ — простая группа лиева типа. Используем результаты, вошедшие в табл. $2a$–$2c$ из [19], для доказательства того, что $P$ изоморфно $L_p(2)$. Согласно числу компонент графа простых чисел группы $P$ докажем наше утверждение, рассмотрев соответствующие случаи.

Случай 1. $s(P) = 2$.

В этом случае имеем $n_2(P) = 2^p - 1$.

(1) Если $P \cong A_{r-1}(q)$, $(r, q) \neq (3, 2)$, $(3, 4)$, где $r$ простое нечетное, то $(q^r - 1)/(q-1)d = 2^p - 1$, где $d = (r, q-1)$.

Предположим сначала, что $d = 1$. В таком случае если $q = 2$, то $r = p$ и $P \cong L_p(2)$, что и требовалось. Тем самым мы можем считать, что $q > 2$. Вычислениями получаем, что $q^{r-1} - 1 = 2(q-1)(2^{p-1} - 1)/q$, и ввиду того, что $q^{r-1} - 1 \in \omega(A_{r-1}(q))$, имеем $2(q-1)(2^{p-1}-1)/q \in \omega(G)$. Если $q$ четно, то $q = 2$; противоречие. Если $q$ нечетно, то из $2(q-1)(2^{p-1}-1)/q > 2(2^{p-2}-1)$ получаем противоречие со следствием 1(e).

Пусть теперь $d = r$. Если $q$ четно, скажем $q = 2^m$, то

$$2^{mr} - 1 = r(2^m - 1)(2^p - 1).$$

Очевидно, что $mr > p \geq 13$. Рассмотрим теперь примитивный простой делитель $s = 2_{[mr]}$. Ясно, что $s \in \pi(2^{mr} - 1)$, но $s \notin \pi(r(2^m - 1)(2^p - 1))$, что невозможно. Тем самым можно считать, что $q$ нечетно. В таком случае имеем

$$\frac{q^{r-1} - 1}{r} = \left(\frac{q-1}{q}\right)\left[(2^p - 1) - \frac{1}{r}\right] > \frac{1}{2}(2^p - 2) = 2^{p-1} - 1 > 2(2^{p-2} - 1),$$

и так как по следствию 1(b) $(q^{r-1} - 1)/r \in \omega(P) \subset \omega(G)$, снова приходим к противоречию со следствием 1(e).

(2) Предположим, что $P \cong A_r(q)$, где $q-1$ делит $r+1$. Тогда $\frac{q^r - 1}{q-1} = 2^p - 1$. Поскольку $A_r(q)$ содержит элемент порядка $(q^{r+1}-1)/(q-1)^2 > 2^p - 1$, приходим к противоречию со следствием 1(d).

(3) Если $P \cong {}^2A_{r-1}(q)$, где $r$ простое нечетное, то $\frac{q^r+1}{(q+1)(r,q+1)} = 2^p - 1$. По лемме 3(a) $P$ содержит элемент порядка $(q^{r-1} - 1)/(r, q+1) > 2^p - 1$; противоречие.

(4) Случай, когда $P \cong {}^2A_r(q)$, $r$ простое нечетное, $q$ — простая степень, $(q+1) \mid (r+1)$ и $(r, q) \neq (3, 3), (5, 2)$, может быть рассмотрен аналогично.

(5) $P \cong {}^2A_3(2)$ или ${}^2F_4(2)'$. Так как $p \geq 13$, то $2^p - 1 > 13$.

(6) Если $P \cong B_n(q)$, $n = 2^m \geq 4$, $q$ нечетно, то $\frac{q^n+1}{2} = 2^p - 1$ и тем самым

$$4(2^{p-1} - 1) = q^n - 1 = (q^{\frac{n}{2}} - 1)(q^{\frac{n}{2}} + 1).$$

Поэтому 8 должно быть делителем $4(2^{p-1} - 1)$; противоречие.

(7) Если $P \cong B_r(3)$, где $r$ простое нечетное, то $\frac{3^r - 1}{2} = 2^p - 1$. Отсюда

$$4(2^{p-1} - 1) = 3(3^{r-1} - 1) = 3(3^{\frac{r-1}{2}} - 1)(3^{\frac{r-1}{2}} + 1)$$

и снова должно быть $8 \mid 4(2^{p-1}-1)$, что невозможно.

(8) Если $P \cong C_n(q)$, $n = 2^m \geq 4$, то $\frac{q^n+1}{(2,q-1)} = 2^p - 1$. Если $(2, q-1) = 1$, то $q$ нечетно и тогда $2^p - q^n = 2$; противоречие. Если $(2, q-1) = 2$, то $2^p - 1 = \frac{q^n+1}{2}$, и мы приходим к противоречию, как в (6).

(9) Допустим, что $P \cong C_r(q)$, где $r$ простое нечетное и $q = 2, 3$.

(i) Если $P \cong C_r(2)$, то из $2^r - 1 = 2^p - 1$ вытекает, что $r = p$ и $P \cong C_p(2)$. В таком случае имеем

$$\pi_1(P) = \pi\left(2(2^p+1)\prod_{i=1}^{p-1}(2^{2i}-1)\right).$$

Рассмотрим теперь примитивный простой делитель $s = 2_{[2p]} \in \pi(2^p+1)$. Ясно, что $s \in \pi(P) \backslash \pi(G)$; противоречие.

(ii) Если $P \cong C_r(3)$, то $\frac{3^r-1}{2} = 2^p - 1$, и мы приходим к противоречию, как в (7).

(10) $P \cong D_r(q)$, где $r \geq 5$ простое нечетное и $q = 2, 3, 5$.

(i) Если $P \cong D_r(2)$, то $2^r - 1 = 2^p - 1$ и тем самым $r = p$. Теперь

$$\pi_1(P) = \pi\left(2\prod_{i=1}^{p-1}(2^{2i}-1)\right)$$

и рассмотрим примитивный простой делитель $s = 2_{[2(p-1)]}$. Очевидно, что $s$ делит $2^{p-1}+1$, так что $s \in \pi(P) \backslash \pi(G)$; противоречие.

(ii) Если $P \cong D_r(3)$, то $\frac{3^r-1}{2} = 2^p - 1$, что невозможно, как в (7).

(iii) Если $P \cong D_r(5)$, где $r \geq 5$ нечетное простое, то $\frac{5^r-1}{4} = 2^p - 1$. Вычислениями получим, что $5(5^{r-1}+1) = 2(2^{p+1}+1)$. Но тогда $2_{[2(p+1)]} \in \pi(P) \backslash \pi(G)$; противоречие.

(11) Допустим, что $P \cong D_{r+1}(q)$, где $q = 2, 3$.

(i) Пусть сначала $q = 2$. Тогда $2^r - 1 = 2^p - 1$, откуда $r = p$ и $P \cong D_{p+1}(2)$. Далее,

$$\pi_1(P) = \pi\left(2(2^p+1)\prod_{i=1}^{p-1}(2^{2i}-1)\right),$$

и, как выше, рассмотрим примитивный простой делитель $s = 2_{[2p]}$. Вновь легко видеть, что $s \in \pi(P) \backslash \pi(G)$; противоречие.

(ii) Случай, когда $P \cong D_{r+1}(3)$, аналогичен (7).

(12) Если

$$P \cong {}^2D_n(q), \quad n = 2^m \geq 4,$$

то $\frac{q^n+1}{(2,q-1)} = 2^p - 1$, и доказательство аналогично таковому для (8).

(13) Если

$$P \cong {}^2D_n(2), \quad n = 2^m + 1 \geq 5,$$

то $2^{n-1} + 1 = 2^p - 1$, т. е. $2^p - 2^{n-1} = 2$; противоречие.

(14) Допустим, что $P \cong {}^2D_r(3)$, где $r$ простое нечетное и $5 \leq r \neq 2^m+1$. В таком случае $\frac{3^r+1}{4} = 2^p-1$. По лемме 3(b) $P$ содержит элемент порядка $3^{r-1}-1 > 2^p-1$; противоречие.

(15) Если

$$P \cong {}^2D_n(3), \quad 9 \leq n = 2^m+1 \neq r,$$

где $r$ нечетное простое, то $\frac{3^{n-1}+1}{2} = 2^p-1$, и приходим к противоречию по аналогии с (6).

(16) Предположим, что

$$P \cong G_2(q), \quad 2 < q \equiv \varepsilon \operatorname{mod} 3, \quad \varepsilon = \pm 1.$$

В этом случае $q^2 - \varepsilon q + 1 = 2^p - 1$. Рассмотрим два случая.

(i) $\varepsilon = +1$. В этой ситуации имеем

$$q(q-1) = 2(2^{p-1}-1) = 2(2^{\frac{p-1}{2}}-1)(2^{\frac{p-1}{2}}+1).$$

Ясно, что $q$ нечетно. Если $q$ делит $2^{\frac{p-1}{2}}-1$, то можно считать, что

$$q = \frac{2^{\frac{p-1}{2}}-1}{k}$$

для некоторого $k$, следовательно,

$$q \leq 2^{\frac{p-1}{2}}-1.$$

Кроме того,

$$q-1 = 2(2^{\frac{p-1}{2}}+1)k \geq 2(2^{\frac{p-1}{2}}+1).$$

Значит,

$$2 \cdot 2^{\frac{p-1}{2}} + 3 \leq q \leq 2^{\frac{p-1}{2}}-1;$$

противоречие. Если $q$ делит $2^{\frac{p-1}{2}}+1$, то

$$q = \frac{2^{\frac{p+1}{2}}-1}{k} \leq 2^{\frac{p+1}{2}}-1, \quad q-1 = 2(2^{\frac{p-1}{2}}-1)k \geq 2(2^{\frac{p-1}{2}}-1),$$

откуда

$$2(2^{\frac{p-1}{2}}-1) \leq q \leq 2^{\frac{p-1}{2}}+1,$$

или $2^{\frac{p-1}{2}} \leq 2$, и мы получили противоречие с тем, что $p \geq 13$.

(ii) $\varepsilon = -1$. Рассуждая, как выше, приходим к противоречию.

(17) Случаи, когда $P \cong {}^3D_4(q)$ или $P \cong F_4(q)$, $q$ нечетно, аналогичны (16).

(18) Рассуждения, подобные прежним, отклоняют случай, когда $P \cong E_6(q)$.

Случай 2. $s(P) = 3$.
Здесь имеем $n_2(P) = 2^p-1$ или $n_3(P) = 2^p-1$.

(1) Если

$$P \cong A_1(q), \quad 3 < q \equiv \varepsilon \operatorname{mod} 4, \quad \varepsilon = \pm 1, \quad q = r^m (r \text{ простое}),$$

то $r = 2^p-1$ или $\frac{q+\varepsilon}{2} = 2^p-1$.

(i) Допустим сначала, что $r = 2^p - 1$. Если $m > 1$, то $\frac{r^m+1}{2} > r = 2^p - 1$, а так как
$$\frac{r^m+1}{2} \in \omega(P) \subseteq \omega(G),$$
приходим к противоречию по следствию 1(d). Тем самым можно считать, что $m = 1$. В этом случае имеем $|P| = 2^p(2^{p-1}-1)(2^p-1)$ и $|\operatorname{Aut}(P) : P| = 2$. Ввиду того, что $P \leq G/N \leq \operatorname{Aut}(P)$, множество $\pi(N)$ содержит нечетное простое, скажем $s$. Рассмотрим фробениусову подгруппу $2^p - 1 : 2^{p-1} - 1$ группы $P$. Из леммы 8 следует, что $G$ содержит элемент порядка $s(2^{p-1}-1)$, что противоречит следствию 1(b).

(ii) Пусть теперь $\frac{q+\varepsilon}{2} = 2^p - 1$, где $\varepsilon = \pm 1$. Если $\varepsilon = -1$, то $q$ равно $2^{p+1} - 1$, которое делит $|P|$, но не $|G|$, а такое невозможно. Если $\varepsilon = +1$, то
$$|P| = 2^2(2^{p-1}-1)(2^p-1)(2^{p+1}-1).$$
Пусть $q = r^m$, где $r$ простое нечетное. Так как $r^m = 2^{p+1} - 3$, очевидно, $r > 3$ и $m < p - 1$. Рассмотрим теперь примитивный простой делитель $s := 2_{[p-2]}$. Ясно, что $s \geq p - 1 > m$, и поскольку
$$\operatorname{Aut}(P) \cong \mathrm{PGL}(2, q) \rtimes \mathbb{Z}_m,$$
имеем $s \notin \pi(\operatorname{Aut}(P))$. Отсюда $s \in \pi(N)$. Рассуждая, как в предыдущем разделе, можно показать, что рассматриваемый случай невозможен.

(2) Если $P \cong A_1(q)$, $q = 2^n > 2$, то $q-1 = 2^p-1$ или $q+1 = 2^p-1$. Допустим сначала, что $q - 1 = 2^p - 1$. Тогда $q = 2^p$ и рассмотрим примитивный простой делитель $2_{[2p]} \in \pi(2^p + 1) = \pi(q + 1)$. Ясно теперь, что $2_{[2p]} \in \pi(P) \setminus \pi(G)$; противоречие. Предположим, далее, что $q+1 = 2^p-1$. В этом случае получаем $2^p - 2^n = 2$; противоречие с тем, что $p \geq 13$.

(3) Предположим, что $P \cong {}^2D_r(3)$, где $r = 2^m + 1$ простое. Тогда должно быть $\frac{3^r+1}{4} = 2^p - 1$ или $\frac{3^{r-1}+1}{2} = 2^p - 1$. Рассмотрим эти случаи отдельно.

(i) Пусть сначала $\frac{3^r+1}{4} = 2^p - 1$. В этом случае получим $2^2(2^p + 1) = 3^2(3^{r-2} + 1)$. С другой стороны, имеем
$$\pi_1(P) = \pi_1({}^2D_r(3)) = \pi\left(3(3^{r-1}-1)\prod_{i=1}^{r-2}(3^{2i}-1)\right).$$
Рассмотрим теперь примитивный простой делитель $2_{[2p]}$. Ясно, что $2_{[2p]} \in \pi(2^p + 1)$, тем самым $2_{[2p]} \in \pi(3^{r-2} + 1) \subset \pi_1(P)$; противоречие с тем, что $2_{[2p]} \notin \pi(G)$.

(ii) Предположим, далее, что $\frac{3^{r-1}+1}{2} = 2^p - 1$. Тогда легко видеть, что $2^{p+1} = 3(3^{r-2} + 1)$; противоречие.

(4) Если $P \cong G_2(q)$, где $q = 3^n$, то $q^2+q+1 = 2^p-1$ или $q^2-q+1 = 2^p-1$. Воспользуемся методом, подобным использованному выше (случай 1(16)), для доказательства того, что такое невозможно.

(5) Предположим, что $P \cong {}^2G_2(q)$, где $q = 3^{2n+1} > 3$. В этом случае должно быть $3^{2n+1} - 3^{n+1} + 1 = 2^p - 1$ или $3^{2n+1} + 3^{n+1} + 1 = 2^p - 1$. Допустим, что $3^{2n+1} - 3^{n+1} + 1 = 2^p - 1$. Тогда легко вывести, что $2(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) =$

$3^{n+1}(3^n-1)$. Если $3^{n+1}$ делит $2^{\frac{p-1}{2}}-1$, то $3^n-1<3^{n+1}\le 2^{\frac{p-1}{2}}-1<2^{\frac{p-1}{2}}+1$. Тогда
$$3^{n+1}(3^n-1)<2(2^{\frac{p-1}{2}}-1)(2^{\frac{p-1}{2}}+1);$$
противоречие. Допустим теперь, что $3^{n+1}$ делит $2^{\frac{p-1}{2}}+1$. Тогда $2^{\frac{p-1}{2}}+1=k(3^{n+1})$ при некотором $k$ и тем самым $3^{n+1}\le 2^{\frac{p-1}{2}}+1$. С другой стороны, заметим, что $2k(2^{\frac{p-1}{2}}-1)=3^n-1$, так что $3^n-1\ge 2(2^{\frac{p-1}{2}}-1)$, т. е.
$$3^n\ge 2^{\frac{p+1}{2}}-1.$$
Поэтому
$$2^{\frac{p+1}{2}}-1\le 3^n<3^{n+1}\le 2^{\frac{p-1}{2}}+1;$$
противоречие. В остальных случаях обсуждения аналогичны.

(6) Если $P\cong F_4(q)$, $q$ четно, то $q^4+1=2^p-1$ или $q^4-q^2+1=2^p-1$. Первый случай, очевидно, невозможен. Для последнего случая рассуждения, подобные проведенным в случае 1(16), также приводят к противоречию.

(7) Если $P\cong {}^2F_4(q)$, где $q=2^{2m+1}>2$, то
$$2^{2(2m+1)}-2^{3m+2}+2^{2m+1}-2^{m+1}+1=2^p-1,$$
или
$$2^{2(2m+1)}+2^{3m+2}+2^{2m+1}+2^{m+1}+1=2^p-1.$$
Теперь нетрудно увидеть, что ни одно из этих равенств не может быть выполнено.

(8) Если $P\cong {}^2A_5(2)$, $E_7(2)$ или $E_7(3)$, то $2^p-1$ равно 7, 11, 73, 127, 757 или 1093, а это противоречит тому, что $p\ge 13$.

Случай 3. $s(P)=4,5$.

(1) Если $P\cong A_2(4)$, ${}^2E_6(2)$, то, так как $2^p>19$, этот случай не выполняется.

(2) Если $P\cong {}^2B_2(2^{2m+1})$ и $2^{2m+1}\pm 2^{m+1}+1=2^p-1$, то $m=0$ в противоречие с тем, что $m\ge 1$.

Если $2^{2m+1}-1=2^p-1$, то $p=2m+1$ и найдется элемент порядка $2_{[4p]}$ в $P$. Но такой элемент не может быть в $L_p(2)$.

(3) Если $P\cong E_8(q)$, то $2^p-1$ будет одним из следующих.

(i) $q^8-q^7+q^5-q^4+q^3-q+1$. Отсюда
$$2(2^{p-1}-1)=q(q-1)(q+1)(q^5-q^4+q^3+1)$$
в противоречие с тем, что 8 делит $(q^2-1)$, если $q$ нечетно. Если $q$ четно, то $q=2$ также приводит к противоречию.

(ii) $q^8+q^7-q^5-q^4-q^3+q+1$. Отсюда
$$2(2^{p-1}-1)=q(q-1)(q+1)(q^5+q^4+q^3-1),$$
а это противоречит тому, что 8 делит $(q^2-1)$, если $q$ нечетно. Если $q$ четно, то $q=2$ также дает противоречие.

(iii) $q^8-q^6+q^4-q^2+1$. Тогда
$$2(2^{p-1}-1)=q^2(q-1)(q+1)(q^4+q^2-1),$$
а это противоречит тому, что 8 делит $(q^2-1)$, если $q$ нечетно. Если $q$ четно, то $q^2=2$ также приводит к противоречию.

(iv) $q^8-q^4+1$. В этом случае
$$2(2^{p-1}-1)=q^4(q^4-1),$$
и мы снова приходим к противоречию. $\square$

**Лемма 11.** $N = 1$.

Доказательство. По лемме 10 $P \cong L_p(2)$. Так как $s(G) = 2$ и $N$ — $\pi_1$-группа, $\Lambda$-подгруппа группы $G$, где $\Lambda \subseteq \pi_2$, действует без неподвижных точек на $N$. Отсюда согласно результатам Томпсона (см. [13, с. 337]) $N$ нильпотентна. Предположим, что $N \neq 1$. Не уменьшая общности, можно считать, что $N$ — элементарная абелева $r$-подгруппа в $G$ для некоторого простого $r \in \pi_1(G)$. Предположим сначала, что $r \neq 2$. По лемме 6 $P$ содержит фробениусову подгруппу с ядром порядка $2^{p-1}$ и циклическим дополнением порядка $2^{p-1} - 1$. Применяя лемму 8 к этой фробениусовой группе, получаем, что $G$ содержит элемент порядка $r.(2^{p-1} - 1)$, что противоречит следствию 1(b). Итак, $N$ — нетривиальная 2-подгруппа. В таком случае по лемме 7 $P$ содержит фробениусову подгруппу конфигурации $2^p - 1 : p$ и $G$ будет содержать элемент порядка $2p$; противоречие. □

**Лемма 12.** $G = P \cong L_p(2)$.

Доказательство. По леммам 10 и 11 имеем $N = 1$ и $P \cong L_p(2)$. Очевидно, что $P \leq G \leq \mathrm{Aut}(P)$ и тем самым $G = P$ или $G = \mathrm{Aut}(P)$, потому что $|\mathrm{Out}(P)| = 2$. С другой стороны, по лемме 5 $\omega(G) \subsetneq \omega(\mathrm{Aut}(P))$, откуда $G = P$, что и требовалось. □

**Благодарности**

Авторы выражают благодарность рецензенту, а также А. В. Заварницыну за предоставленную им лемму (лемма 7).

## *ЛИТЕРАТУРА*

**1.** *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.
**2.** *Кондратьев В. А.* О компонентах графа простых чисел для конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
**3.** *Shi W. J.* A characteristic property of $\mathrm{PSL}_2(7)$ // J. Austral Math. Soc. Ser. A. 1984. V. 36, N 3. P. 354–356.
**4.** *Shi W. J.* A characteristic property of $A_8$ // Acta Math. Sin. New Ser. 1987. V. 3, N 1. P. 92–96.
**5.** *Darafsheh M. R., Moghaddamfar A. R.* Characterization of the groups $PSL_5(2)$, $PSL_6(2)$ and $PSL_7(2)$ // Comm. Algebra. 2001. V. 29, N 1. P. 465–475.
**6.** *Shi W. J., Wang L. H., Wang S. H.* The pure quantitative characterization of linear groups over the binary field (Chinese) // Chinese Ann. Math. Ser. A. 2003. V. 24A, N 6. P. 675–682.
**7.** *Darafsheh M. R., Moghaddamfar A. R.* Corrigendum to: "Characterization of the groups $PSL_5(2)$, $PSL_6(2)$ and $PSL_7(2)$" // Comm. Algebra. 2003. V. 32, N 9. P. 4651–4653.
**8.** *Darafsheh M. R., Moghaddamfar A. R.* A characterization of groups related to the linear groups $PSL(n, 2)$, $n = 5, 6, 7, 8$ // Pure Math. Appl. 2000. V. 11, N 4. P. 629–637.
**9.** *Moghaddamfar A. R., Zokayi A. R., Khademi M.* A characterization of the finite simple group $L_{11}(2)$ by its element orders // Taiwanese J. Math. 2005. V. 9, N 3. P. 445–455.
**10.** *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
**11.** *Hooley C.* On Artin's conjecture // J. Reine Angew. Math. 1967. V. 225. P. 209–220.
**12.** *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
**13.** *Gorenstein D.* Finite group. New York: Harper and Row, 1968.
**14.** *Green J. A.* The characters of the finite general linear groups // Trans. Amer. Math. Soc. 1955. V. 80. P. 402–447.
**15.** *Lidl R., Niederreiter H.* Finite fields. Massachusets: Addison-Wesly Publ. Comp., Inc., 1983.
**16.** *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7, N 1. P. 81–97.

**17.** *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.

**18.** *Кондратьев В. А., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–369.

**19.** *Mazurov V. D.* Characterization of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, N 1. P. 129–140.

**20.** *Shi W. J., Bi J.* A characteristic property for each finite projective special linear group // Groups–Canberra 1989. Berlin; Heidelberg; New York; London; Paris; Tokyo; Hong Kong; Barcelona: Springer-Verl., 1990. (Lecture Notes in Math.; 1456). P. 171–180.

**21.** *Aschbacher M., Seitz G. M.* Involutions in Chevalley groups over fields of even order // Nagoya Math. J. 1976. V. 63. P. 1–91.

**22.** *Huppert B.* Endliche Gruppen I. New York: Springer-Verl., 1983.

**23.** *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.

**24.** *Алеева М. Р.* О конечных простых группах с множеством порядков элементов, как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, № 3. С. 323–339.

*Статья поступила 27 октября 2004 г., окончательный вариант — 28 апреля 2005 г.*

*Maria Silvia Lucido (Лючидо Мария Сильвия)*
*Dipartimento di Matematica e Informatica*
*Università di Udine*
*via delle Scienze 200, I-33100 Udine, Italy*
`mslucido@dimi.uniud.it`

*Ali Reza Moghaddamfar (Могхаддамфар Али Реза)*
*Department of Mathematics, Faculty of Science*
*K. N. Toosi University of Technology,*
*P.O. Box 16315-1618, Tehran, Iran*
`moghadam@iust.ac.ir`