Сибирский математический журнал
Июль—август, 2012. Том 53, № 4

УДК 512.542

ПОЧТИ РАСПОЗНАВАЕМОСТЬ ПО СПЕКТРУ КОНЕЧНЫХ ПРОСТЫХ ЛИНЕЙНЫХ ГРУПП ПРОСТОЙ РАЗМЕРНОСТИ

М. А. Гречкосеева, Д. В. Лыткин

Аннотация. Спектром группы называется множество порядков ее элементов. Пусть $L = PSL_n(q)$, где n — простое число, большее трех. Показано, что любая конечная группа, спектр которой совпадает со спектром группы L, изоморфна расширению группы L посредством некоторой подгруппы группы внешних автоморфизмов группы L.

Ключевые слова: простая линейная группа, граф простых чисел, квазираспознаваемость по спектру.

Введение

Спектром $\omega(G)$ конечной группы G называется множество всех порядков ее элементов. Множество $\omega(G)$ замкнуто относительно взятия делителей и, следовательно, определяется своим подмножеством $\mu(G)$, состоящим из максимальных по делимости элементов. Группы G и H называются *изоспектральными*, если $\omega(G) = \omega(H)$. Конечная группа G называется *распознаваемой по спектру*, если для любой конечной группы H изоспектральность групп G и H влечет их изоморфизм. Иными словами, если через $h(G)$ обозначить число попарно не изоморфных конечных групп, изоспектральных группе G, то G распознаваема, если $h(G) = 1$. Если $h(G) < \infty$, то G называется *почти распознаваемой по спектру*, и если $h(G)$ бесконечно, то G называется *нераспознаваемой по спектру*. Говорят, что для группы G решена проблема распознаваемости по спектру, если известно значение $h(G)$.

В [1] Ши показал, что группа, имеющая нетривиальную нормальную разрешимую подгруппу, обязательно нераспознаваема. Следовательно, каждая распознаваемая группа является расширением прямого произведения M неабелевых простых групп с помощью некоторой подгруппы из $\operatorname{Out} M$. Поэтому основной интерес проблема распознаваемости представляет для конечных неабелевых простых групп. Почти распознаваемость неабелевой простой группы L может быть доказана следующим образом. Назовем L *квазираспознаваемой по спектру*, если любая группа, изоспектральная L, обладает единственным неабелевым композиционным фактором и этот фактор изоморфен L. Также

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 11–01–91158), Совета по грантам президента РФ и государственной поддержке ведущих научных школ (код проекта НШ–3669.2010.1 и МК–2136.2010.1), а также программы Рособразования «Развитие научного потенциала высшей школы» (код проекта 2.1.1.10726).

назовем L *распознаваемой по спектру среди накрытий*, если любая группа, гомоморфно отображающаяся на L и изоспектральная L, изоморфна L. Пусть теперь L квазираспознаваема и распознаваема среди накрытий и $\omega(G) = \omega(L)$. Из квазираспознаваемости следует, что $L \leq G/K \leq \operatorname{Aut} L$ для некоторой нормальной разрешимой подгруппы K группы G. Полный прообраз группы L в G изоспектрален L и из распознаваемости среди накрытий следует, что $K = 1$. Таким образом, $L \leq G \leq \operatorname{Aut} L$, и, значит, $h(L)$ не превосходит числа подгрупп в $\operatorname{Out} L$.

В настоящей работе рассматриваются простые линейные группы $PSL_n(q)$. Нам удобнее пользоваться лиевой нотацией, поэтому далее эти группы записываются как $A_{n-1}(q)$. Более точно, будут рассматриваться простые линейные группы, граф простых чисел которых является несвязным. *Графом простых чисел* $GK(G)$ группы G называется граф, множество вершин которого — это множество простых делителей порядка группы G и в котором две различные вершины p и q смежны тогда и только тогда, когда $pq \in \omega(G)$. Известно, что все конечные простые группы с тремя и более компонентами связности в графе простых чисел, кроме знакопеременной группы степени 6, квазираспознаваемы по спектру [2]. Для всех конечных простых групп с двумя компонентами связности в графе простых чисел, кроме групп $A_{n-1}(q)$, $A_n(q)$, ${}^2A_{n-1}(q)$, ${}^2A_n(q)$, где $n > 3$ — простое число, и $G_2(q)$, доказана квазираспознаваемость или решена проблема распознаваемости (см. [3–7]). Кроме того, установлено, что группы $A_{n-1}(2^k)$ распознаваемы по спектру [8, 9] и что $h(A_{n-1}(3)) \leq 2$ для любого простого числа n, большего трех [10].

Цель данной работы — доказать квазираспознаваемость всех групп $A_{n-1}(q)$, где n — простое число, большее трех. Как указано выше, группы $A_{n-1}(2^k)$ распознаваемы по спектру, поэтому достаточно рассматривать только нечетные q. Кроме того, группы $A_{n-1}(q)$, где $n \geq 5$, распознаваемы по спектру среди накрытий [11], значит, основной результат настоящей работы может быть сформулирован как

Теорема. *Пусть $L = A_{n-1}(q)$, где n — простое число, $n \geq 5$, и G — конечная группа такая, что $\omega(G) = \omega(L)$. Тогда $L \leq G \leq \operatorname{Aut} L$. В частности, $h(L) < \infty$.*

§ 1. Предварительные сведения и обозначения

Множество простых делителей натурального числа n обозначается через $\pi(n)$. Для простого числа p через $n_{\{p\}}$ обозначается p-часть числа n, т. е. наибольшая степень числа p, делящая n. Наибольший общий делитель и наименьшее общее кратное чисел $n_1, \dots, n_s$ обозначаются через $(n_1, \dots, n_s)$ и $[n_1, \dots, n_s]$ соответственно. Через $[x]$ обозначается целая часть числа x.

Множество простых делителей порядка группы G обозначается через $\pi(G)$. Через $m_1(G)$ и $m_2(G)$ обозначаются самый большой и второй по величине элементы в $\omega(G)$ соответственно. Под *периодом* группы G подразумевается некоторое натуральное число n такое, что $g^n = 1$ для любого $g \in G$.

Число компонент связности графа $GK(G)$ обозначается через $s(G)$, а сами компоненты связности — через $\pi_i(G)$, где $1 \leq i \leq s(G)$. Если порядок группы G четен, то считаем, что $2 \in \pi_1(G)$. Разобьем множество $\mu(G)$ на классы $\mu_i(G)$ так, чтобы каждое $\mu_i(G)$ состояло из всех $\pi_i(G)$-чисел в $\mu(G)$ для любого $1 \leq i \leq s(G)$. В [12] показано, что если G — простая группа с несвязным графом простых чисел, то все $\mu_i(G)$ для $2 \leq i \leq s(G)$ состоят из единственного элемента. Условимся обозначать этот элемент через $n_i(G)$.

Множество вершин графа называется *кокликой*, если вершины, принадлежащие этому множеству, попарно не смежны. Мощность коклики с наибольшим числом вершин называется *неплотностью* графа. Обозначим через $t(G)$ неплотность графа $GK(G)$.

Лемма 1 [13–15]. *Пусть L — конечная неабелева простая группа с несвязным графом простых чисел и $t(L) \geq 3$, а G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда выполняются следующие утверждения:*

(а) *существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, где K — нормальная нильпотентная подгруппа группы G;*

(б) *$s(S) \geq s(G)$ и для любого i, $2 \leq i \leq s(G)$, существует j, $2 \leq j \leq s(S)$, такое, что $n_i(G) = n_j(S)$, а группы K и $\overline{G}/S$ являются $\pi_1(G)$-группами;*

(в) *для каждой коклики ρ графа $GK(G)$, порядок которой больше 2, не более чем одно число из ρ делит произведение $|K| \cdot |\overline{G}/S|$; в частности, $t(S) \geq t(G) - 1$.*

Лемма 2 [16, лемма 1]. *Пусть G — конечная группа, $N \lhd G$ и G/N — группа Фробениуса с 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 $p \in \pi(N)$.*

Лемма 3 [17, следствие 3]. *Пусть $L = A_{n-1}(q)$, где $n \geq 2$ и q — степень простого числа p. Положим $d = (n, q-1)$. Тогда $\omega(L)$ состоит из всех делителей следующих чисел:*

(а) $\frac{q^n-1}{d(q-1)}$;

(б) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ *для $n_1, n_2 > 0$ таких, что $n_1 + n_2 = n$;*

(в) $[q^{n_1} - 1, q^{n_2} - 1, \dots, q^{n_s} - 1]$ *для $s \geq 3$ и $n_1, n_2, \dots, n_s > 0$ таких, что $n_1 + n_2 + \dots + n_s = n$;*

(г) $p^k \frac{q^{n_1}-1}{d}$ *для $k, n_1 > 0$ таких, что $p^{k-1} + 1 + n_1 = n$;*

(д) $p^k[q^{n_1} - 1, q^{n_2} - 1, \dots, q^{n_s} - 1]$ *для $s \geq 2$ и $k, n_1, n_2, \dots, n_s > 0$ таких, что $p^{k-1} + 1 + n_1 + n_2 + \dots + n_s = n$;*

(е) p^k, *если $p^{k-1} + 1 = n$ для $k > 0$.*

Лемма 4. *Пусть $L = A_{n-1}(q)$, где $n \geq 3$ и $(n, q) \neq (3, 2)$. Положим $d = (n, q-1)$. Тогда*

$$m_1(L) = \frac{q^n - 1}{d(q-1)} \quad \text{и} \quad m_2(L) = \frac{(q^{\alpha(n)} - 1)(q^{n-\alpha(n)} - 1)}{d(q-1)},$$

где $\alpha(n) = [(n-1)/2]$ при $n \not\equiv 2 \pmod 4$ и $\alpha(n) = (n-4)/2$ при $n \equiv 2 \pmod 4$.

Доказательство. Несложно показать, что утверждение леммы верно при $n = 3$ и $n = 4$, поэтому далее считается, что $n > 4$. Пусть q — степень простого числа p. Положим $a = (q^n - 1)/(d(q-1))$ и $b = (q^{\alpha(n)} - 1)(q^{n-\alpha(n)} - 1)/(d(q-1))$. Несложно проверить, что $a > b$, поэтому достаточно показать, что все числа из пп. (б)–(е) леммы 3 не превосходят b. Будем использовать неравенства

$$(q^x - 1)(q^y - 1) < (q^{x+y} - 1), \quad (q^x - 1)(q^y - 1) < (q^u - 1)(q^v - 1),$$

где x, y, u, v — натуральные числа, $x < u \leq v$ и $x + y = u + v$, а также тот факт, что $k \leq p^{k-1}$ при $k \geq 1$. Кроме того, отметим, что $b > q^{n-3}$.

Пусть $c = [q^{n_1} - 1, q^{n_2} - 1]/\big(n/(n_1, n_2), q-1\big)$, где $0 < n_1 \leq n_2$ и $n_1 + n_2 = n$. Если $(n_1, n_2) = 1$, то $n_1 \leq \alpha(n)$ и, значит, $c \leq b$. Предположим, что $(n_1, n_2) \geq 2$.

Тогда $[q^{n_1}-1,q^{n_2}-1]\le(q^{n_1}-1)(q^{n_2}-1)/(q^2-1)$. Если $n_1\le\alpha(n)$, то $c\le b$, поэтому можно считать, что $n_1>\alpha(n)$. Поскольку $n_1\ge n/2$, это возможно только при четном n и либо $n_1=n/2$, либо $n\equiv 2\pmod 4$, $n_1=n/2-1$. Если $n_1=n/2$, то $c=(q^{n/2}-1)/(2,q-1)<q^{n/2}\le q^{n-3}<b$. Если $n\equiv 2\pmod 4$ и $n_1=n/2-1$, то

$$\frac{d(q^2-1)c}{(2,q-1)}=\frac{(n,q-1)(q^n-q^{n/2+1}-q^{n/2-1}+1)}{(2,q-1)(n/2,q-1)}=q^n-q^{n/2+1}-q^{n/2-1}+1,$$

$$\frac{d(q^2-1)b}{(2,q-1)}=\frac{(q^n-q^{n/2+2}-q^{n/2-2}+1)(q+1)}{(2,q-1)}\ge 2(q^n-q^{n/2+2}-q^{n/2-2}+1).$$

Поскольку $2(q^n-q^{n/2+2}-q^{n/2-2}+1)>q^n-q^{n/2+1}-q^{n/2-1}+1$ при $n\ge 6$, получаем, что $c<b$.

Пусть $c=[q^{n_1}-1,q^{n_2}-1,\dots,q^{n_s}-1]$, где $s\ge 3$, $0<n_1\le n_2\le\dots\le n_s$ и $n_1+n_2+\dots+n_s=n$. Тогда

$$c\le\frac{(q^{n_1}-1)(q^{n_2}-1)\dots(q^{n_s}-1)}{(q-1)^{s-1}}<\frac{(q^{n_1}-1)(q^{n-n_1}-1)}{(q-1)^2}.$$

Если $n_1\le\alpha(n)$, то $c<b$. Предположим, что $n_1>\alpha(n)$. Тогда $n\ge sn_1\ge 3(\alpha(n)+1)$, откуда $n=6$. При этом $n_1>1$, поэтому $c=q^2-1<(q^5-1)/d=b$.

Пусть $c=p^k(q^{n_1}-1)/d$, где $k,n_1>0$ и $p^{k-1}+1+n_1=n$. Тогда

$$\begin{aligned}d(q-1)c\le p^{p^{k-1}}(q^{n_1}-1)(q-1)=p^{n-n_1-1}(q^{n_1}-1)(q-1)&\\<(q^{n-1}-1)(q-1)\le d(q-1)b.&\end{aligned}$$

Отметим, что при $s\ge 2$

$$p^k[q^{n_1}-1,q^{n_2}-1,\dots,q^{n_s}-1]\le p^k\frac{q^{n_1+\dots+n_s}-1}{q-1}\le p^k\frac{q^{n_1+\dots+n_s}-1}{d},$$

поэтому каждое число из п. (д) оценивается сверху подходящим числом из п. (г).

Пусть, наконец, $n=p^{k-1}+1$ и $c=p^k$. Если $n>5$, то $k\ge 2$ и $(k,p)\ne(2,2),(2,3),(3,2)$, тем самым $k\le p^{k-1}-2=n-3$ и, значит, $c\le q^{n-3}\le b$. Если $n=5$, то $k=3$, $p=2$ и $c=8<21=b$.

Отметим, что для нечетного q утверждение леммы доказано в [18].

Если q — натуральное число, r — нечетное простое число и $(q,r)=1$, то через $e(r,q)$ обозначается мультипликативный порядок числа q по модулю r. Для нечетного q положим $e(2,q)=1$, если $q\equiv 1\pmod 4$, и $e(2,q)=2$, если $q\equiv 3\pmod 4$. Простое число r называется *примитивным простым делителем* для q^m-1, если $e(r,q)=m$.

Лемма 5 (Жигмонди [19]). *Пусть q — натуральное число и $q>1$. Тогда для каждого натурального числа m найдется простое число r такое, что $e(r,q)=m$, за исключением случаев, когда $(q,m)\in\{(2,1),(2,6),(3,1)\}$.*

Для данных q и m обозначим через $R_m(q)$ множество всех примитивных простых делителей числа q^m-1. Для $m>2$ произведение чисел $(q^m-1)_{\{r\}}$ по всем $r\in R_m(q)$ называется *наибольшим примитивным делителем числа* q^m-1.

Лемма 6. *Пусть q, m, k — натуральные числа. Тогда $R_{mk}(q) \subseteq R_m(q^k)$. Если дополнительно $(m,k) = 1$, то $R_m(q) \subseteq R_m(q^k)$. В частности, $|R_m(q^k)| > 1$ для любых взаимно простых $m \geq 4$ и $k \geq 2$, исключая случай $m = 6$ и $q = 2$.*

Доказательство. Пусть $r \in R_{mk}(q)$ и $r \neq 2$, т. е. r делит число $q^{mk} - 1$ и не делит ни одно из чисел $q^i - 1$, $i = 1, \dots, mk-1$. Тогда оно, в частности, не делит ни одно из чисел $(q^k)^j - 1$, $j = 1, \dots, m-1$, значит, принадлежит множеству $R_m(q^k)$. Пусть $2 \in R_{mk}(q)$. Тогда $mk = 1$ или $mk = 2$. При $k = 1$ утверждение очевидно. Пусть $k = 2$ и $m = 1$, т. е. $2 \in R_2(q)$. Тогда $2 \in R_m(q^k) = R_1(q^2)$, поскольку $q^2 \equiv 1 \pmod 4$.

Пусть $r \in R_m(q)$ и $r \neq 2$. Тогда порядок элемента q в группе обратимых элементов кольца вычетов по модулю r равен m. Следовательно, при $(m,k) = 1$ порядок элемента q^k также равен m, т. е. $r \in R_m(q^k)$. Пусть $2 \in R_m(q)$. Тогда $m = 1$ или $m = 2$. Если $2 \in R_1(q)$, то $q \equiv 1 \pmod 4$, значит, также $q^k \equiv 1 \pmod 4$, и, следовательно, $2 \in R_1(q^k)$. Если же $2 \in R_2(q)$, то $q \equiv 3 \pmod 4$. Условие $(m,k) = 1$ в этом случае означает, что k нечетно, и, следовательно, $q^k \equiv 3 \pmod 4$, и $2 \in R_2(q^k)$.

Из доказанного следует, что $R_m(q) \cup R_{mk}(q) \subseteq R_m(q^k)$. Множества $R_m(q)$ и $R_{mk}(q)$ не пересекаются и при наложенных ограничениях непусты по лемме Жигмонди. Значит, $|R_m(q^k)| > 1$.

Лемма 7 [20, табл. 2]. *Пусть $L = A_{n-1}(q)$, где $n \geq 5$, и $\rho = \{r_i \mid \frac{n+1}{2} \leq i \leq n\}$, где для каждого i число r_i — некоторый элемент множества $R_i(q)$, если таковое непусто. Тогда ρ является кокликой максимального размера в графе $GK(L)$. В частности, $t(L) = \left[\frac{n-1}{2}\right]$ при $q = 2$ и $7 \leq n \leq 11$, и $t(L) = \left[\frac{n+1}{2}\right]$ иначе.*

Доказательство следующей леммы не представляет труда.

Лемма 8. *Пусть q — нечетное число, $q > 1$ и $\varepsilon = \pm 1$. Если n четно, то $(q^n + 1)_{\{2\}} = 2$. Если n нечетно, то $(q^n - \varepsilon)_{\{2\}} = (q - \varepsilon)_{\{2\}}$.*

Лемма 9. *Пусть q — нечетное число, $q > 1$, n — простое число, $n \geq 5$ и n делит $q - 1$. Тогда $(q^n - 1 - n(q-1))_{\{n\}} = n(q-1)^2_{\{n\}}$.*

Доказательство. Пусть $(q-1)_{\{n\}} = n^k$ и $q - 1 = n^k t$. Тогда

$$q^n \equiv 1 + n \cdot n^k t + n(n-1)/2 \cdot n^{2k} t^2 \pmod{n^{3k+1}}.$$

Значит, $q^n - 1 - n(q-1) \equiv n(n-1)/2 \cdot n^{2k} t^2 \pmod{n^{3k+1}}$. Таким образом, $(q^n - 1 - n(q-1))_{\{n\}} = n^{2k+1} = n(q-1)^2_{\{n\}}$.

§ 2. Доказательство теоремы

Пусть $L = A_{n-1}(q)$, где n — простое число, $n \geq 5$, q нечетно, и G — конечная группа такая, что $\omega(G) = \omega(L)$. В [13] посчитано, что $s(L) = 2$ и $n_2(L) = (q^n - 1)/((n, q-1)(q-1))$. Кроме того, по лемме 7 группа L удовлетворяет условию $t(L) \geq 3$. Значит, по лемме 1 найдется неабелева простая группа S такая, что

$$S \leq \overline{G} = G/K \leq \operatorname{Aut} S,$$

где K — нормальная нильпотентная подгруппа группы G. Более того, $s(S) \geq 2$, и найдется i, $2 \leq i \leq s(S)$, такое, что $n_i(S) = n_2(G)$. Поскольку $n_2(G)$ — самый большой по модулю элемент в $\omega(G)$ в силу леммы 4 и $\omega(S) \subseteq \omega(G)$, получаем равенства

$$n_2(G) = n_i(S) = m_1(S).$$

Также отметим, что $t(G) = (n+1)/2$, поэтому из неравенства $t(S) \geq t(G) - 1$ вытекает неравенство $n \leq 2t(S) + 1$. Неплотности графов простых чисел простых групп, приводимые ниже в доказательстве, взяты из [20].

Как отмечено во введении, для доказательства теоремы достаточно показать, что $S \simeq L$. В [21] установлено, что S не может быть изоморфна знакопеременной или спорадической группе, а также группе Титса ${}^2F_4(2)'$. Таким образом, группа S должна быть группой лиева типа. Более того, по [21, теорема 3] можно считать, что группа S определена над полем, порядок которого взаимно прост с q.

Группы лиева типа с несвязным графом простых чисел приведены в табл. 1–3. В этих таблицах r означает нечетное простое число. Все колонки, кроме последних, взяты из [16]. В последних колонках указан некоторый элемент спектра группы. Принадлежность этого числа спектру устанавливается с помощью информации о спектрах классических групп из [17, 22] и о строении максимальных торов исключительных групп из [18] (см. также [23]). Несложно проверить, что для всех групп S из табл. 2–4, кроме групп, указанных в табл. 1, этот элемент больше $n_i(S)$ для любого $2 \leq i \leq s(S)$ и, значит, $n_i(S) \neq m_1(S)$ для любого $2 \leq i \leq s(S)$. Таким образом, S изоморфна одной из групп в табл. 1. В последнем столбце табл. 1 для некоторых групп указано число $\exp(S)$, являющееся периодом группы S.

Таблица 1. Конечные простые группы лиева типа с $s(S) = 2$

S	Условия на S	n_2	$a \in \omega(S)$
$A_{r-1}(u)$	$(r,u) \neq (3,2),(3,4)$	$(u^r-1)/((u-1)(r,u-1))$	$(u^r-1)/((u-1)(r,u-1))$
$A_r(u)$	$(u-1)\|(r+1)$	$(u^r-1)/(u-1)$	$(u^{r+1}-1)/(u-1)^2$
${}^2A_{r-1}(u)$		$(u^r+1)/((u+1)(r,u+1))$	$(u^{r-1}-1)/(r,u+1)$
${}^2A_r(u)$	$(u+1)\|(r+1)$, $(r,u) \neq (3,3),(5,2)$	$(u^r+1)/(u+1)$	$u^{r-1}-1$
$B_m(u)$	$m = 2^k \geq 4$	$(u^m+1)/(2,u-1)$	$(u^{m-1}-1)(u+1)/(2,u-1)$
$B_r(3)$		$(3^r-1)/2$	$(3^r+1)/2$
$C_m(u)$	$m = 2^k \geq 2$	$(u^m+1)/(2,u-1)$	$(u^{m-1}-1)(u+1)/(2,u-1)$
$C_r(u)$	$u = 2,3$	$(u^r-1)/(2,u-1)$	$(u^r+1)/(2,u-1)$
$D_r(u)$	$r \geq 5$, $u = 2,3,5$	$(u^r-1)/(4,u-1)$	$(u^{r-1}+1)(u+1)/(4,u-1)$
$D_{r+1}(u)$	$u = 2,3$	$(u^r-1)/(2,u-1)$	$(u^{r+1}-1)/(2,u-1)$
${}^2D_m(u)$	$m = 2^k \geq 4$	$(u^m+1)/(2,u-1)$	$(u^{m-1}-1)(u+1)/(2,u-1)$
${}^2D_m(2)$	$m = 2^k+1 \geq 5$	$2^{m-1}+1$	2^m+1
${}^2D_r(3)$	$7 \leq r \neq 2^k+1$	$(3^r+1)/4$	$10(3^{r-3}-3)$
${}^2D_m(3)$	$9 \leq m = 2^k+1$, m составное	$(3^{m-1}+1)/2$	$(3^m+1)/4$
$G_2(u)$	$2 < u \equiv \varepsilon(3)$, $\varepsilon = \pm 1$	$u^2-\varepsilon u+1$	u^2+u+1
${}^3D_4(u)$		u^4-u^2+1	$(u^3-1)(u+1)$
$F_4(u)$	u нечетно	u^4-u^2+1	$(u^3-1)(u+1)$
$E_6(u)$		$(u^6+u^3+1)/(3,u-1)$	$(u+1)(u^5-1)/(3,u-1)$
${}^2E_6(u)$	$u > 2$	$(u^6-u^3+1)/(3,u+1)$	$(u+1)(u^2+1)(u^3-1)/(3,u+1)$

Таблица 2. Конечные простые группы лиева типа с $s(S)=3$

S	Условия на S	n_2	n_3	$a \in \omega(S)$
$A_1(u)$	$3 < u \equiv \varepsilon \pmod 4$, $\varepsilon = \pm 1$, u простое	u	$(u+\varepsilon)/2$	u
$A_1(u)$	$3 < u \equiv \varepsilon \pmod 4$, $\varepsilon = \pm 1$, u составное	$\pi(u)$	$(u+\varepsilon)/2$	$(u+1)/2$
$A_1(u)$	$u = 2^k \geq 4$	$u-1$	$u+1$	$u+1$
${}^2A_3(3)$		5	7	12
${}^2A_5(2)$		7	11	18
${}^2D_r(3)$	$r = 2^k+1 \geq 5$	$(3^{r-1}+1)/2$	$(3^r+1)/4$	$5(3^{r-2}-1)/2$
$G_2(u)$	$u \equiv 0 \pmod 3$	u^2-u+1	u^2+u+1	u^2+u+1
${}^2G_2(u)$	$u = 3^{2k+1} > 3$	$u-\sqrt{3u}+1$	$u+\sqrt{3u}+1$	$u+\sqrt{3u}+1$
$F_4(u)$	u четно	u^4+1	u^4-u^2+1	$(u^3-1)(u+1)$
${}^2F_4(u)$	$u = 2^{2k+1} > 2$	$u^2-\sqrt{2u^3}+u-$ $-\sqrt{2u}+1$	$u^2+\sqrt{2u^3}+u+$ $+\sqrt{2u}+1$	$u^2+\sqrt{2u^3}+u+\sqrt{2u}+1$
$E_7(u)$	$u = 2,3$	u^6+u^3+1	$(u^7-1)/(u-1)$	$(u^5-1)(u^2+u+1)/(u-1)$

Таблица 3. Конечные простые группы лиева типа с $s(S)>3$

$s(S)$	S	Условия на S	n_2	n_3	n_4	n_5	$a \in \omega(S)$
4	$A_2(4)$		3	5	7		7
	${}^2B_2(u)$	$u = 2^{2k+1} > 2$	$u-1$	$u-\sqrt{2q}+1$	$u+\sqrt{2q}+1$		$u+\sqrt{2q}+1$
	${}^2E_6(2)$		13	17	19		35
	$E_8(u)$	$u \equiv 2,3 \pmod 5$	$\frac{u^{10}-u^5+1}{u^2-u+1}$	$\frac{u^{10}+u^5+1}{u^2+u+1}$	u^8-u^4+1		$(u+1)(u^2+u+1)$ $\times(u^5-1)$
5	$E_8(u)$	$u \not\equiv 2,3 \pmod 5$	$\frac{u^{10}-u^5+1}{u^2-u+1}$	$\frac{u^{10}+u^5+1}{u^2+u+1}$	u^8-u^4+1	$\frac{u^{10}+1}{u^2+1}$	$(u+1)(u^2+u+1)$ $\times(u^5-1)$

Предложение 1. *Группа S не изоморфна ни ${}^2F_4(u)$, ни ${}^2B_2(u)$.*

Доказательство. Предположим противное. Тогда $t(S) \leq 5$ в силу [20, табл. 4] и, значит, $n \leq 11$.

Предположим, что $S \simeq {}^2F_4(u)$. Вычитая из обеих частей равенства $n_2(G) = m_1(S)$ единицу и разлагая правую часть на множители, получаем

$$\frac{q^n-1}{(n,q-1)(q-1)} - 1 = \sqrt{2u}(\sqrt{u/2}+1)(u+1). \tag{1}$$

Используя равенство числа $\sqrt{2u}$ и 2-части числа $b = (q^n-1)/((n,q-1)(q-1))-1$, покажем, что $\sqrt{2u} \leq (q+1)/2$.

Пусть $(n,q-1)=1$. Тогда $b = q(q^{n-1}-1)/(q-1)$. Если $n=7$ или $n=11$, то $b_{\{2\}} = (q^{(n-1)/2}+1)_{\{2\}}(q^{(n-1)/2}-1)_{\{2\}}/(q-1)_{\{2\}} = (q+1)_{\{2\}}$, где последнее равенство выполнено по лемме 8. Если $n=5$, то $b_{\{2\}} = (q^2+1)_{\{2\}}(q+1)_{\{2\}} = 2(q+1)_{\{2\}}$. В любом случае $\sqrt{2u}$ делит $2(q+1)$. Непосредственной подстановкой

Таблица 4

S	Условия на S	$m_1(S)$	$\exp(S)$
$A_{m-1}(u)$	m простое, $m>3$	$\frac{u^m-1}{(m,u-1)(u-1)}$	
$A_2(u)$		$\frac{u^2+u+1}{(3,u-1)}$	$u^2(u^3-1)(u+1)$
$A_1(u)$	$u>3$ простое	u	$u(u^2-1)/2$
$A_1(u)$	$3<u\equiv 1 \pmod 4$ сост.	$(u+1)/2$	$u(u^2-1)/2$
$A_1(u)$	$u>2$ четное	$u+1$	$u(u^2-1)$
$G_2(u)$	$2<u\equiv\varepsilon \pmod 3$, $\varepsilon=0,2$	u^2+u+1	$u^6(u^6-1)$
${}^2G_2(u)$	$u=3^{2k+1}>3$	$u+\sqrt{3u}+1$	$u^3(u^3+1)(u-1)$
${}^2F_4(u)$	$u=2^{2k+1}>2$	$u^2+\sqrt{2u^3}+u+\sqrt{2u}+1$	
${}^2B_2(u)$	$u=2^{2k+1}>2$	$u+\sqrt{2u}+1$	

в (1) убеждаемся, что $\sqrt{2u}\neq 2(q+1)$, $q+1$. Таким образом, в этом случае $\sqrt{2u}\leq (q+1)/2$.

Пусть $(n,q-1)=n$. Тогда $q\geq 11$ и

$$b=(q^{n-1}+q^{n-2}+\dots+1-n)/n=(q-1)(q^{n-2}+2q^{n-3}+\dots+(n-2)q+n-1)/n.$$

Если $q\equiv 1 \pmod 4$, то $nb/(q-1)\equiv n(n-1)/2 \pmod 4$. Если $q\equiv -1 \pmod 4$, то $nb/(q-1)\equiv (n-1)/2 \pmod 4$. Поскольку $(n-1)_{\{2\}}\leq 4$, получаем, что $b_{\{2\}}\leq 2(q-1)_{\{2\}}$. Следовательно, $\sqrt{2u}$ делит $2(q-1)$, причем, как и выше, можно показать, что $\sqrt{2u}\neq 2(q-1)$, $q-1$. Значит, $\sqrt{2u}\leq (q-1)/2$.

Таким образом, в любом случае $\sqrt{2u}\leq (q+1)/2$. Стало быть, $\sqrt{u/2}+1\leq (q+5)/4<q/2$ и $u+1\leq (q+1)^2/8+1<q^2/4$. Отсюда $\sqrt{2u}(\sqrt{u/2}+1)(u+1)\leq q^3(q+1)/16$. С другой стороны,

$$b\geq (q(q+1)(q^2+1)-10)/11>(q(q+1)(q^2+1)-q(q+1))/11=q^3(q+1)/11,$$

и равенство (1) невозможно.

Если $S\simeq {}^2B_2(u)$, то из $n_2(G)=m_1(S)$ следует, что

$$\frac{q^n-1}{(n,q-1)(q-1)}-1=\sqrt{2u}(\sqrt{u/2}+1),$$

поэтому этот случай разбирается аналогичным образом. Предложение доказано.

Таким образом, S — это либо линейная группа, либо $G_2(u)$, либо ${}^2G_2(u)$. По лемме 1 группы K и $\overline{G}/S$ являются $\pi_1(G)$-группами. Получим более сильные ограничения на порядки этих группы. Далее v обозначает характеристику поля, над которым определена группа S.

Предложение 2. $\pi(K)\subseteq\{2,v\}$. *В частности,* $t(\overline{G})\geq t(G)$.

Доказательство. Предположим противное. Пусть $t\in\pi(K)$ и $t\notin\{2,v\}$. Группа K нильпотентна, поэтому $K=R_1\times R_2\times\dots\times R_s$, где R_i, $i=1,\dots,s$, — все силовские подгруппы в K и R_1 — силовская t-подгруппа. Положим $\widetilde{G}=G/(\Phi(R_1)\times R_2\times\dots\times R_s)$ и $\widetilde{K}=K/(\Phi(R_1)\times R_2\times\dots\times R_s)$. Тогда $\widetilde{K}$ — элементарная абелева t-группа и $\widetilde{G}/\widetilde{K}\simeq G/K\geq S$. Обозначим полный прообраз группы S в $\widetilde{G}$ через $\widetilde{S}$.

Так как S — простая группа, $C_{\widetilde{S}}(\widetilde{K})/\widetilde{K}$ не может содержаться в S собственным образом. Предположим, что $C_{\widetilde{S}}(\widetilde{K})/\widetilde{K} = S$. Поскольку $t \in \pi_1(G)$, число $tm_1(S)$ должно содержаться в спектре $\omega(G)$, но это противоречит максимальности числа $m_1(S) = m_1(G)$. Таким образом, $C_{\widetilde{S}}(\widetilde{K}) \leq \widetilde{K}$.

Пусть $S \simeq A_{m-1}(u)$, где $m \geq 2$. По [24, лемма 5] группа S содержит группу Фробениуса с ядром порядка u^{m-1} и циклическим дополнением порядка $(u^{m-1}-1)/(m, u-1)$. Поскольку $(u, t) = 1$, выполняются все условия леммы 2, значит, $b = t(u^{m-1}-1)/(m, u-1) \in \omega(G)$. Мы придем к противоречию, показав, что $m_1(G) < b$. Если $m > 2$ или u — составное число, то $m_1(S) = (u^m - 1)/((u-1)(m, u-1))$ и $u^{m-1} \geq 4$. Следовательно,

$$m_1(G) = m_1(S) < 2u^{m-1}/(m, u-1) < 3(u^{m-1}-1)/(m, u-1) \leq b.$$

Если $m = 2$ и $u > 3$ — простое число, то $m_1(G) = m_1(S) = u < 3(u-1)/2 \leq b$.

Пусть $S \simeq G_2(u)$, где $u > 2$ и $u \not\equiv 1 \pmod 3$. В S есть подгруппа, изоморфная $SL_3(u)$ (см. [25, 26]). В силу условия на u эта подгруппа изоморфна $A_2(u)$. Значит, в S есть группа Фробениуса с ядром порядка u^2 и циклическим дополнением порядка $u^2 - 1$. Следовательно, $t(u^2-1) \in \omega(G)$. С другой стороны, $t(u^2-1) \geq 3(u^2-1) > u^2 + u + 1 = m_1(S) = m_1(G)$.

Пусть, наконец, $S \simeq {}^2G_2(u)$, где $u = 3^{2k+1} > 3$. В S есть подгруппа, изоморфная $A_1(u)$ (см., например, [25]), поэтому, рассуждая как выше, получаем, что $t(u-1)/2 \in \omega(G)$. Это противоречит цепочке неравенств

$$t(u-1)/2 \geq 5(u-1)/2 > u + \sqrt{3u} + 1 = m_1(S) = m_1(G).$$

Таким образом, $\pi(K) \subseteq \{2, v\}$. Следовательно, $\pi(\overline{G}) = \pi(G)$, значит, $t(\overline{G}) \geq t(G)$. Предложение доказано.

Предложение 3. (а) *Пусть $S \simeq A_{m-1}(u)$, где m — простое число и $u = v^k$. Тогда $\pi(\overline{G}/S) \subseteq \{2, m\}$. Если при этом $(m, k) = 1$, то $\pi(\overline{G}/S) \subseteq \{2, (m, u-1)\}$.*

(б) *Если $S \simeq G_2(u)$, то $\pi(\overline{G}/S) \subseteq \{2, 3\}$.*

(в) *Пусть $S \simeq {}^2G_2(u)$. Тогда либо $\pi(\overline{G}/S) \subseteq \{3\}$, либо $u = 3^f$, где f — нечетное простое число, $f \equiv 5, 7 \pmod{12}$ и $\pi(\overline{G}/S) = \{f\}$. В любом случае $t(S) \geq t(\overline{G})$.*

Доказательство. Напомним, что $\pi(\overline{G}/S) \subseteq \pi_1(G)$. Кроме того, $\pi_2(G)$ — компонента связности графа $GK(\overline{G})$, не содержащая число 2, поэтому $s(\overline{G}) > 1$. Почти простые группы с несвязным графом простых чисел описаны в [27, 28]. Отметим, что в (б) и (в) группа $\overline{G}$ расщепляется над S (см., например, [29]).

(а) Хорошо известно, что $\pi(\mathrm{Out}\, S) \subseteq \{2\} \cup \pi((m, u-1)) \cup \pi(k)$. Обозначим фактор $\overline{G}/S$ через $\widehat{G}$ и будем обозначать образ элемента $x \in \overline{G}$ при естественном гомоморфизме в $\widehat{G}$ через $\hat{x}$. Пусть s — простой делитель порядка $|\widehat{G}|$, отличный от 2 и $(m, u-1)$. Тогда $s \in \pi(k)$. В группе $\overline{G}$ найдется элемент g такой, что порядок элемента $\hat{g}$ равен s. Представим g в виде $g = \iota \cdot \varphi \cdot \gamma^{\varepsilon}$, где ι, φ и γ — внутренне-диагональный, полевой и графовый автоморфизмы соответственно, $\varepsilon \in \{0, 1\}$. Можем считать, что $\varepsilon = 0$, в противном случае ввиду нечетности s можем перейти от $\hat{g}$ к $\hat{g}^2$. Кроме того, $\widehat{\varphi}$ также имеет порядок s.

Обозначим через $\mathrm{Out\,diag}\, S$ образ группы внутренне-диагональных автоморфизмов в $\mathrm{Out}\, S$. Группа $\mathrm{Out\,diag}\, S$ имеет порядок $(m, u-1)$, который взаимно прост с s. Поэтому элементы $\hat{g}$ и $\widehat{\varphi}$ порождают силовские s-подгруппы в группе $\mathrm{Out\,diag}\, S \leftthreetimes \langle \hat{g} \rangle$. Значит, подгруппы $\langle \hat{g} \rangle$ и $\langle \widehat{\varphi} \rangle$ сопряжены некоторым элементом из $\operatorname{Out} S$, и, следовательно, их полные прообразы также сопряжены в $\operatorname{Aut} S$. Таким образом, $\omega(\langle S,\varphi\rangle)=\omega(\langle S,g\rangle)\subseteq\omega(G)$.

По [30, предложение 4.9.1] централизатор автоморфизма φ в S содержит секцию, изоморфную $A_{m-1}(u^{1/s})$. По лемме Жигмонди множество $R_m(u^{1/s})$ непусто. Тогда $s\cdot R_m(u^{1/s})\subseteq\omega(G)$ и, значит, $R_m(u^{1/s})\subseteq\pi_1(G)$. Если $s\neq m$, то в силу леммы 6 выполняется включение $R_m(u^{1/s})\subseteq R_m(u)=\pi_2(S)=\pi_2(G)$. Следовательно, $s=m$.

(б) Требуемое следует из [27, теорема 5].

(в) Предположим, что $\pi(\overline{G}/S)\not\subseteq\{3\}$. Тогда по [27, теорема 5; 28, предложение 1] имеем $u=3^f$, где f — простое число, большее трех, и $\pi(\overline{G}/S)=\{f\}$, причем числа $2f$ и $3f$ лежат в $\omega(\overline{G})$. Кроме того, как указано в доказательстве [28, предложение 1], если $f\equiv 1,11\pmod{12}$, то $\pi_1(\overline{G})=\pi(u(u^2-1)f)\cup\pi(u+\sqrt{3u}+1)$, а если $f\equiv 5,7\pmod{12}$, то $\pi_1(\overline{G})=\pi(u(u^2-1)f)\cup\pi(u-\sqrt{3u}+1)$. Поскольку $\pi(u+\sqrt{3u}+1)=\pi_2(G)$, случай $f\equiv 1,11\pmod{12}$ невозможен.

Предположим, что $t(\overline{G})>t(S)=5$. Это означает, что $\pi(\overline{G})\neq\pi(S)$, т. е. $\pi(\overline{G}/S)=\{f\}$, где $f>3$, и в $GK(\overline{G})$ найдется коклика ρ размера 6, содержащая f. Тогда $\rho\setminus\{f\}$ — коклика размера 5 в $GK(S)$ и, значит, $\rho\setminus\{f\}$ содержит 3 (см. [20]). Это противоречит тому, что $3f\in\omega(\overline{G})$. Предложение доказано.

Предложение 4. *Группа S изоморфна группе $A_{m-1}(u)$, где m — простое число и $m\geq 5$.*

Доказательство. Предположим противное. По лемме 7 в графе $GK(G)$ есть коклика из $(n+1)/2$ чисел, причем среди этих чисел нет ни 2, ни 3. Если S изоморфна одной из групп $A_1(u)$, $A_2(u)$ и $G_2(u)$, то в силу предложений 2 и 3 выполнено равенство $\pi(S)=\pi(G)$ и, значит, в $GK(S)$ тоже должна быть коклика из $(n+1)/2$ чисел, не содержащая ни 2, ни 3. Используя информацию о максимальных кокликах из [20], заключаем, что $n=5$. Если $S\simeq {}^2G_2(u)$, то из $t(S)\geq t(G)$ следует, что $n=5$ или $n=7$.

Рассмотрим уравнение $n_2(G)=m_1(S)$. Умножая на $(n,q-1)$ и вычитая 1 из обеих частей, получаем

$$q(q^{n-1}-1)/(q-1)=(n,q-1)m_1(S)-1.$$

Левая часть этого равенства делится на наибольший примитивный делитель числа $q^{n-1}-1$, который будем обозначать через $k_{n-1}(q)$. Это число лежит в спектре группы G, оно нечетно и не делится на 3. Значит, при выполнении условий $(k_{n-1}(q),u)=1$ и $S\not\simeq {}^2G_2(u)$ из предложений 2 и 3 следует, что $k_{n-1}(q)\in\omega(S)$ и, значит, наибольший общий делитель чисел $(n,q-1)m_1(S)-1$ и $\exp(S)$ делится на $k_{n-1}(q)$.

1. Пусть $S\simeq A_2(u)$, где $(3,u-1)=1$, или $S\simeq G_2(u)$. Тогда $n=5$ и

$$q(q^4-1)/(q-1)=(5,q-1)(u^2+u+1)-1.$$

Предположим, что $(5,q-1)=1$. Тогда $q(q+1)(q^2+1)=u(u+1)$. Напомним, что u и q взаимно просты. Пусть u нечетно. Тогда u делит одно из чисел $q+1$ и q^2+1. Следовательно, $u(u+1)\leq(q^2+1)(q^2+2)<q(q+1)(q^2+1)$; противоречие. Пусть теперь u четно. Тогда u делит $2(q+1)$ и опять $u(u+1)<q(q+1)(q^2+1)$.

Предположим, что $(5,q-1)=5$. Тогда $q(q+1)(q^2+1)=5(u^2+u+1)-1$. Из этого равенства и равенства $(5(u^2+u+1)-1,u)=(4,u)$ следует, что $k_4(q)=(q^2+1)/2$ взаимно просто с u. Значит, наибольший общий делитель чисел $b=5(u^2+u+1)-1$ и u^6-1 делится на $(q^2+1)/2$. Несложно проверить, что

$(b, u-1) = (14, u-1)$, $(b, u+1) = (4, u+1)$ и $(b, u^2-u+1) = (7\cdot 13, u+9)$. По малой теореме Ферма число 7 не может быть делителем числа $k_4(q)$, поэтому $q^2+1 = 26$, откуда $q = 5$. Это противоречит условию $(5, q-1) = 5$.

2. Пусть $S \simeq A_2(u)$, где $(3, u-1) = 3$. Тогда $n = 5$ и

$$q(q^4-1)/(q-1) = (5, q-1)(u^2+u+1)/3 - 1.$$

Предположим, что $(5, q-1) = 1$. Тогда $q(q+1)(q^2+1) = (u+2)(u-1)/3$. Пусть сначала $u = 2^k$. Но тогда при $k > 1$ имеем

$$4 \le (q(q+1)(q^2+1))_{\{2\}} = (u+2)(u-1)_{\{2\}} = 2.$$

Если же $k = 1$, то $(u-1, 3) = 1$. Пусть теперь u нечетно. Несложно вывести, что $(q^2+1)/2$ взаимно просто с u, поэтому наибольший общий делитель чисел $(u+2)(u-1)/3$ и $(u^3-1)(u+1)$ делится на $(q^2+1)/2$. Отсюда вытекает, что $(q^2+1)/2$ делит $u-1$. Тогда $q^2+1 \le (u-1)/3$ и, в частности, $u+2 \ge 3q^2+6$. Значит, $(u+2)(u-1)/3 \ge (3q^2+6)(q^2+1) > q(q+1)(q^2+1)$; противоречие.

Предположим, что $(5, q-1) = 5$. Тогда $q(q+1)(q^2+1) = (5u^2+5u+2)/3$. Стало быть, $((q^2+1)/2, u) = 1$. Поскольку $(5u^2+5u+2, u-1) = (12, u-1)$ и $(5u^2+5u+2, u+1) = (2, u+1)$, наибольший общий делитель чисел $5u^2+5u+2$ и $(u^3-1)(u+1)$ не делится на $(q^2+1)/2$; противоречие.

3. Пусть $S \simeq A_1(u)$, где $u > 3$. Тогда $n = 5$. Более того, все коклики размера 3 в $GK(S)$ содержат характеристику v, поэтому u нечетно.

Предположим, что $(5, q-1) = 1$. Тогда $q(q+1)(q^2+1) = u-1$ или $q(q+1)(q^2+1) = (u-1)/2$. В S есть элемент порядка $(u-1)/2$, значит, в G есть элемент порядка $q(q^2+1)/2$. Это противоречит тому, что элементы множества $R_4(q)$ не смежны с характеристикой поля $GF(q)$ в $GK(G)$ по лемме 3.

Предположим, что $(5, q-1) = 5$. Тогда $q(q+1)(q^2+1) = 5u-1$ или $q(q+1)(q^2+1) = (5u+3)/2$. Учитывая, что q^2+1 не делится на 3, получаем, что числа $(q^2+1)/2$ и u взаимно просты. Поскольку $(5u-1, u^2-1) = (24, u-5)$ и $(5u+3, u^2-1) = (16, u+7)$, наибольший общий делитель чисел $5m_1(S)-1$ и $\exp(S)$ не делится на $(q^2+1)/2$; противоречие.

4. Пусть $S \simeq {}^2G_2(u)$, где $u = 3^{2k+1} > 3$. Тогда $n = 5$ или $n = 7$.

Предположим, что $(n, q-1) = 1$. Тогда

$$q(q^{(n-1)/2}+1)\frac{q^{(n-1)/2}-1}{q-1} = \sqrt{3u}(\sqrt{u/3}+1).$$

Ровно одно из чисел $q^{(n-1)/2}+1$ и $q^{(n-1)/2}-1$ делится на 3, поэтому $\sqrt{3u} < q^{(n-1)/2}+1$. Тогда $\sqrt{u/3}+1 < (q^{(n-1)/2}+4)/3 \le q^{(n-1)/2} < q(q^{(n-1)/2}-1)/(q-1)$; противоречие.

Предположим, что $(n, q-1) = n$. Тогда

$$q\frac{q^{n-1}-1}{q-1} = n(u+\sqrt{3u}+1)-1.$$

Если некоторый делитель числа $(q^{n-1}-1)/(q-1)$ лежит в $\omega(S)$, то он одновременно делит $b = n(u+\sqrt{3u}+1)-1$ и $\exp(S)$. В силу формул

$$(b, u-1) = (3\sqrt{u/3}+n-2, (n-2)\sqrt{u/3}+1),$$

$$(b, u+1) = (3n+1, \sqrt{u/3}+n),$$

$$(b, u-\sqrt{3u}+1) = (12n^2-6n+1, \sqrt{u/3}+2n-1),$$

которые несложно вывести с помощью алгоритма Евклида, $(b, \exp(S))$ делит $2 \cdot 16 \cdot 271 \cdot u$ при $n = 5$ и $2 \cdot 22 \cdot 547 \cdot u$ при $n = 7$.

Пусть $n = 5$. Любой делитель числа $k_4(q)$ должен быть сравним с 1 по модулю 4, а $271 \equiv 3 \pmod 4$, поэтому ни один из делителей числа $k_4(q)$ не лежит в $\pi(S)$. Тогда из предложений 2 и 3 вытекает, что $k_4(q) \in \omega(\overline{G}/S)$ и, значит, $k_4(q)$ — простое число, сравнимое с 5 или 7 по модулю 12. Однако $k_4(q) - 1 = (q^2 - 1)/2$ делится на 12; противоречие.

Пусть $n = 7$. Поскольку $\pi(K) \cup \pi(\overline{G}/S) \subseteq \{2, 3, f\}$, где f зависит только от u, хотя бы одно из чисел $k_6(q)$ и $k_3(q)$ лежит в $\omega(S)$. Следовательно, одно из этих чисел делит $11 \cdot 547$. Простые делители чисел $k_6(q)$ и $k_3(q)$ должны быть сравнимы с 1 по модулю 3, поэтому выполнено равенство $q^2 + \varepsilon q + 1 = (3, q - \varepsilon)547$, где $\varepsilon = \pm 1$. Отсюда $q = 41$, что противоречит условию $(7, q - 1) = 7$. Предложение доказано.

Предложение 5. *Если S изоморфна группе $A_{m-1}(u)$, где m — простое число и $m \geq 5$, то $t(S) = t(G)$ и $m = n$.*

Доказательство. Пусть $u = v^k$, где v — простое число. Напомним, что по предложениям 2 и 3 $\pi(K) \cup \pi(\overline{G}/S) \subseteq \{2, v, m\}$, причем если $(m, k) = 1$, то $\pi(K) \cup \pi(\overline{G}/S) \subseteq \{2, v\} \cup \pi(u - 1)$. В частности, $\pi(S) = \pi(G)$. Следовательно, для доказательства равенства $t(S) = t(G)$ достаточно в $GK(S)$ найти коклику максимального размера, не содержащую ни одного делителя порядков $|K|$ и $|\overline{G}/S|$.

По лемме 7 множество $\rho = \{r_i \mid \frac{m+1}{2} \leq i \leq m\}$, где $r_i \in R_i(u)$, является кокликой максимального размера в $GK(S)$, и эта коклика не содержит v. Поскольку $(m+1)/2 \geq 3$, множество ρ также не содержит ни 2, ни делителей числа $u - 1$. Остается рассмотреть случай, когда k делится на m и $m \in \rho$. По теореме Ферма если $m \in R_i(u)$, то i делит $m - 1$. Значит, $m \in R_{m-1}(u)$. Но поскольку m делит k, получаем, что $|R_{m-1}(u)| = |R_{m-1}((v^{k/m})^m)| > 1$, где последнее неравенство выполняется в силу леммы 6 для всех пар m и u, кроме пары $m = 7$ и $u = 2^7$. Однако $7 \in R_3(2^7)$. Поэтому в качестве r_{m-1} в коклике максимального размера графа $GK(S)$ можно выбрать число, отличное от m. Таким образом, $t(S) = t(G) = (n+1)/2$.

Если $S \not\simeq A_6(2), A_{10}(2)$, то $t(S) = (m+1)/2$ и тогда $m = n$. Если $S \simeq A_{10}(2)$, то $t(S) = 5$, а значит, $n = 9$; противоречие. Если $S \simeq A_6(2)$, то $t(S) = 3$ и $n = 5$. Следовательно, $q(q+1)(q^2+1) = (5, q-1)127 - 1$. Левая часть этого равенства делится на 4, а правая нет. Это противоречие завершает доказательство предложения.

Таким образом, $S \simeq A_{n-1}(u)$, и выполнено равенство

$$\frac{q^n - 1}{(n, q-1)(q-1)} = \frac{u^n - 1}{(n, u-1)(u-1)}.$$

Если $(n, q-1) = (n, u-1)$, то $u = q$ и, значит, $S \simeq L$, как и требовалось. Будем считать, что $(n, q-1) \neq (n, u-1)$.

Предположим, что $(n, q-1) = 1$. Тогда

$$\frac{q^n - 1}{q - 1} = \frac{u^n - 1}{n(u-1)}. \tag{2}$$

Ясно, что $u > q$. Множество $\omega(S)$ содержится в $\omega(G)$, значит, $m_2(S) \leq m_2(G)$, откуда по лемме 4 следует неравенство

$$\frac{(u^{(n+1)/2} - 1)(u^{(n-1)/2} - 1)}{n(u-1)} \leq \frac{(q^{(n+1)/2} - 1)(q^{(n-1)/2} - 1)}{q - 1}.$$

Разделив это неравенство на равенство (2), получим

$$\frac{(u^{(n+1)/2}-1)(u^{(n-1)/2}-1)}{u^n-1} \le \frac{(q^{(n+1)/2}-1)(q^{(n-1)/2}-1)}{q^n-1}.$$

Но функция

$$\frac{(x^{(n+1)/2}-1)(x^{(n-1)/2}-1)}{x^n-1} = 1-\frac{x^{(n+1)/2}-1}{x^n-1}-\frac{x^{(n-1)/2}-1}{x^n-1}$$

строго возрастает по x при $x \ge 2$; противоречие.

Предположим, что $(n, q-1) = n$. Тогда

$$\frac{q^n-1}{n(q-1)} = \frac{u^n-1}{u-1}, \tag{3}$$

откуда

$$u(u^{n-1}-1) = (u-1)\cdot\left(\frac{q^n-1}{n(q-1)}-1\right). \tag{4}$$

Из леммы 9 следует, что $u_{\{n\}}(u^{n-1}-1)_{\{n\}} = (q-1)_{\{n\}}$. Предположим, что n делит u. Тогда $u = (q-1)_{\{n\}}$ и, в частности, $u \le (q-1)/2$. Следовательно,

$$\frac{u^n-1}{u-1} \le 2u^{n-1} \le \frac{q^{n-1}}{2^{n-2}} < \frac{q^{n-1}}{n} < \frac{q^n-1}{n(q-1)},$$

но это противоречит (3). Значит, $(u^{n-1}-1)_{\{n\}} = (q-1)_{\{n\}}$. В группе S, а стало быть, и в группе G есть элемент порядка $u^{n-1}-1$. Следовательно, $u^{n-1}-1$ делит одно из чисел, указанных в лемме 3. Несложно проверить, что n-части чисел, указанных в пп. (а), (б), (г) и (е), меньше, чем $(q-1)_{\{n\}}$, поэтому $u^{n-1}-1$ делит число из п. (в) или (д). Значит,

$$u^{n-1}-1 < (q^n-q^{(n+1)/2})/(q-1)^2$$

(см. доказательство леммы 4). С другой стороны, $(u-1)/u \ge 1/2$ и $2n \le q-1$, поэтому из (4) следует, что

$$u^{n-1}-1 \ge \frac{q^n-1}{2n(q-1)}-\frac{1}{2} \ge \frac{q^n-1-(q-1)^2}{(q-1)^2} \ge \frac{q^n-q^2}{(q-1)^2}.$$

Полученное противоречие завершает доказательство теоремы.

ЛИТЕРАТУРА

1. *Shi W.* The characterization of the sporadic simple groups by their element orders // Algebra Colloq. 1994. V. 1, N 2. P. 159–166.
2. *Алексеева О. А., Кондратьев А. С.* Квазираспознаваемость одного класса конечных простых групп по множеству порядков элементов // Сиб. мат. журн. 2003. Т. 44, № 2. С. 241–255.
3. *Кондратьев А. С.* О распознаваемости по спектру конечных простых ортогональных групп. II // Владикавк. мат. журн. 2009. Т. 11, № 4. С. 32–43.
4. *Мазуров В. Д.* Группы с заданным спектром // Изв. Урал. гос. ун-та. 2005. Т. 36. С. 119–138.
5. *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7. P. 81–97.
6. *Заварницин А. В.* Распознавание простых групп $U_3(q)$ по порядкам элементов // Алгебра и логика. 2006. Т. 45, № 2. С. 185–202.

7. *Darafsheh M. R., Farjami Y., Sadrudini A.* A characterization property of the simple group $\mathrm{PSL}_4(5)$ by the set of its element orders // Arch. Math., Brno. 2007. V. 43, N 1. P. 31–37.
8. *Мазуров В. Д., Чен Г. Ю.* Распознаваемость по спектру конечных простых групп $L_4(2^m)$ и $U_4(2^m)$ // Алгебра и логика. 2008. Т. 47, № 1. С. 83–93.
9. *Васильев А. В., Гречкосеева М. А.* Распознавание по спектру конечных простых линейных групп малых размерностей над полями характеристики 2 // Алгебра и логика. 2008. Т. 47, № 5. С. 558–570.
10. *Darafsheh M. R.* Recognition of the projective special linear group over GF(3) // Acta Math. Sin., Engl. Ser. 2010. V. 26, N 3. P. 477–488.
11. *Заварницин А. В.* Свойства порядков элементов в накрытиях групп $L_n(q)$ и $U_n(q)$ // Сиб. мат. журн. 2008. Т. 49, № 2. С. 308–321.
12. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–369.
13. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
14. *Васильев А. В.* О связи между строением конечной группы и свойствами ее графа простых чисел // Сиб. мат. журн. 2005. Т. 46, № 3. С. 511–522.
15. *Васильев А. В., Горшков И. Б.* О распознавании конечных простых групп со связным графом простых чисел // Сиб. мат. журн. 2009. Т. 50, № 2. С. 292–299.
16. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
17. *Бутурлакин А. А.* Спектры конечных линейных и унитарных групп // Алгебра и логика. 2008. Т. 47, № 2. С. 157–173.
18. *Kantor W. M., Seress A.* Large element orders and the characteristic of Lie-type simple groups // J. Algebra. 2009. V. 322, N 3. P. 802–832.
19. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284
20. *Васильев А. В., Вдовин Е. П.* Коклики максимального размера в графе простых чисел конечной простой группы // Алгебра и логика. 2011. Т. 50, № 4. С. 425–470.
21. *Васильев А. В., Гречкосеева М. А., Старолетов А. М.* О конечных группах, изоспектральных простым линейным и унитарным группам // Сиб. мат. журн. 2011. Т. 52, № 1. С. 39–53.
22. *Бутурлакин А. А.* Спектры конечных симплектических и ортогональных групп // Мат. тр. 2010. Т. 13, № 2. С. 33–83.
23. *Kantor W. M., Seress A.* Prime power graphs for groups of Lie type // J. Algebra. 2002. V. 247. P. 370–434.
24. *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.
25. *Kleidman P. B.* The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree group ${}^2G_2(q)$, and of their automorphism groups // J. Algebra. 1998. V. 117. P. 30–71.
26. *Cooperstein B. N.* Maximal subgroups of $G_2(2^n)$ // J. Algebra. 1981. V. 70. P. 23–36.
27. *Lucido M. S.* Prime graph components of finite almost simple groups // Rend. Semin. Mat. Univ. Padova. 1999. V. 102. P. 1–22.
28. *Lucido M. S.* Addendum to "Prime graph components of finite almost simple groups" // Rend. Semin. Mat. Univ. Padova. 2002. V. 107. P. 1–2.
29. *Lucchini A., Menegazzo F., Morigi M.* On the existence of a complement for a finite simple group in its automorphism group // Illinois J. Math. 2003. . V. 47, N 1/2. P. 395–418.
30. *Gorenstein D., Lyons R., Solomon R.* The classification of the finite simple groups. Number 3. Providence, RI: Amer. Math. Soc., 1998. (Math. Surveys Monogr.; V. 40).

Статья поступила 2 сентября 2011 г.

Гречкосеева Мария Александровна
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
grechkoseeva@gmail.com

Лыткин Даниил Всеволодович
Новосибирский гос. университет,
ул. Пирогова, 2, Новосибирск 630090
dan.lytkin@gmail.com