УДК 512.542

Критерий смежности в графе простых чисел конечной простой группы[1]

А. В. Васильев, Е. П. Вдовин

Пусть G — конечная группа, $\pi(G)$ — множество всех простых делителей ее порядка и $\omega(G)$ — спектр группы G, т. е. множество порядков всех ее элементов. Граф $GK(G) = \langle V(GK(G)), E(GK(G))\rangle$, где $V(GK(G))$ — множество вершин и $E(GK(G))$ — множество ребер, называется *графом Грюнберга — Кегеля* (или *графом простых чисел*) группы G, если $V(GK(G)) = \pi(G)$ и ребро (r, s) лежит в $E(GK(G))$ тогда и только тогда, когда $rs \in \omega(G)$. Простые числа $r, s \in \pi(G)$ называются *смежными*, если они смежны как вершины графа $GK(G)$, т. е. $(r, s) \in E(GK(G))$. В противном случае, r и s называются *несмежными*.

Свойства графа простых чисел $GK(G)$ дают богатую информацию о структуре группы G (см. [1–4] и параграфы 5 и 7 настоящей работы). Основная цель статьи — указать исчерпывающий арифметический критерий смежности в графе простых чисел $GK(G)$ для каждой конечной неабелевой простой группы G. Параграфы 1–4 посвящены этой цели. В параграфе 5 обсуждаются некоторые новые результаты о графе простых чисел конечной группы, которые явились стимулом для написания настоящей работы. Кроме того, объясняется важность так называемых чисел неплотности графа простых чисел для исследований групповой структуры. В параграфе 6 найдены указанные инварианты для всех конечных неабелевых простых групп (результирующие таблицы собраны в параграфе 8). Приложения полученных нами результатов рассматриваются в параграфе 7.

1 Предварительные обозначения и результаты

Наши обозначения стандартны. Если n — натуральное число, π — множество простых чисел, то через $\pi(n)$ обозначается множество всех простых делителей числа n, через n_π обозначается наибольший делитель t числа n такой, что $\pi(t) \subseteq \pi$. Заметим, что для конечной группы G по определению $\pi(G) = \pi(|G|)$.

Критерий смежности двух простых делителей для знакопеременных групп очевиден и может быть сформулирован следующим образом.

Предложение 1.1. *Пусть $G = Alt_n$ — знакопеременная группа степени n.*

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05–01–00797), Совета по грантам президента РФ и государственной поддержке ведущих научных школ (код проекта НШ–2069.2003.1), программы Рособразования «Развитие научного потенциала высшей школы» по проекту 8294, программы «Университеты России» (код проекта УР.04.01.202), а также гранта Президиума СО РАН (№86-197).

(1) *Пусть* $r, s \in \pi(G)$ *нечетны. Тогда* r *и* s *несмежны в том и только в том случае, когда* $r + s > n$.

(2) *Пусть* $r \in \pi(G)$ *нечетно. Тогда* 2 *и* r *несмежны в том и только в том случае, когда* $r + 4 > n$.

Информацию о смежности вершин в графе простых чисел для всех спорадических групп и группы Титса ${}^2F_4(2)'$ можно извлечь из [5] или [6]. Таким образом, нам требуется рассмотреть лишь простые группы лиева типа.

Для групп лиева типа и линейных алгебраических групп наши обозначения согласуются с обозначениями в [7] и [8] соответственно. Обозначим через G_{sc} универсальную группу лиева типа. Тогда каждая фактор-группа G_{sc}/Z, где $Z \leq Z(G_{sc})$, называется *группой лиева типа*. Почти во всех случаях группа $G_{sc}/Z(G_{sc})$ проста и мы будем говорить, что $G_{ad} = G_{sc}/Z(G_{sc})$ — группа *присоединенного типа*. Некоторые группы лиева типа над небольшими полями не являются простыми. В таблице 1 мы собрали информацию из [7, теоремы 11.1.2 и 14.4.1] и указали все такие исключения. Иногда мы используем обозначения $A_n^\varepsilon(q), D_n^\varepsilon(q)$ и $E_6^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$, и $A_n^+(q) = A_n(q)$, $A_n^-(q) = {}^2A_n(q)$, $D_n^+(q) = D_n(q)$, $D_n^-(q) = {}^2D_n(q)$, $E_6^+(q) = E_6(q)$, $E_6^-(q) = {}^2E_6(q)$.

Если G изоморфна ${}^2A_n(q)$, ${}^2D_n(q)$ или ${}^2E_6(q)$, будем говорить, что G определена над полем $GF(q^2)$, если $G \simeq {}^3D_4(q)$, будем говорить, что G определена над $GF(q^3)$, и будем говорить, что G определена над $GF(q)$ для всех остальных групп лиева типа. Поле $GF(q)$ во всех случаях называется *основным полем* группы G. Если G — универсальная группа лиева типа с основным полем $GF(q)$, то существуют натуральное число $N (= |\Phi^+|$ в большинстве случаев) и многочлен $f(t) \in \mathbb{Z}[t]$ такие, что $|G| = f(q) \cdot q^N$ и $(q, f(q)) = 1$ (см. [7, теоремы 9.4.10 и 14.3.1]). Этот многочлен мы обозначим через $f_G(t)$. Если G не является универсальной, то найдется универсальная группа K такая, что $G = K/Z$, где $Z \leq Z(K)$, и мы определим $f_G(t) = f_K(t)$.

Предположим, что $\overline{G}$ — связная простая линейная алгебраическая группа над алгебраически замкнутым полем положительной характеристики p. Пусть σ — эндоморфизм группы $\overline{G}$ такой, что $\overline{G}_\sigma = C_{\overline{G}}(\sigma)$ — конечное множество. Тогда σ называется *отображением Фробениуса* и $G = O^{p'}(\overline{G}_\sigma)$ является конечной группой лиева типа. Более того, все конечные группы лиева типа, скрученные и нескрученные, могут получены таким способом. Далее мы полагаем, что для каждой конечной группы G лиева типа зафиксирована (некоторым способом) линейная алгебраическая группа $\overline{G}$ и отображение Фробениуса σ так, что $G = O^{p'}(\overline{G}_\sigma)$. Если группа $\overline{G}$ односвязна, то $G = \overline{G}_\sigma = O^{p'}(\overline{G}_\sigma)$, и если $\overline{G}$ — присоединенного типа, то $\overline{G}_\sigma = \widehat{G}$ — группа внутренне-диагональных автоморфизмов группы G (см. [9, § 12]).

Если $\overline{R}$ — σ-инвариантная редуктивная подгруппа группы $\overline{G}$, то $\overline{R}_\sigma \cap G = \overline{R} \cap G$ называется *редуктивной подгруппой* группы G. Если $\overline{R}$ имеет максимальный ранг, то говорят, что $\overline{R}_\sigma \cap G$ также имеет *максимальный ранг*. Заметим, что если $\overline{R}$ — σ-инвариантная редуктивная подгруппа максимального ранга, то $\overline{R} = \overline{T} \cdot \overline{G}_1 * \ldots * \overline{G}_k$, где $\overline{T}$ — некоторый σ-инвариантный максимальный тор группы $\overline{R}$ и $\overline{G}_1, \ldots, \overline{G}_k$ — подсистемные подгруппы группы $\overline{G}$. Кроме того, $\overline{G}_1 * \ldots * \overline{G}_k = \left[\overline{R}, \overline{R}\right]$. Известно, что $\overline{R}_\sigma = \overline{T}_\sigma G_1 * \ldots * G_m$, подгруппы $G_1, \ldots, G_m$ называются *подсистемными подгруппами* группы G. В общем случае, $m \leqslant k$ и для всех i основное поле группы G_i равно $GF(q^{\alpha_i})$, где $\alpha_i \geqslant 1$. Существует эффективный алгоритм, принадлежащий Борелю и де Зибенталю, для определения всех подсистемных подгрупп группы $\overline{G}$ (см. [10], а также [11]). Требуется рассмотреть расширенную диаграмму Дынкина группы $\overline{G}$ и исключить любое количество вершин. Связные компоненты получившегося графа являются диаграммами Дынкина подсистемных подгрупп группы $\overline{G}$, и диаграммы Дынкина всех подсистемных подгрупп могут быть получены таким способом.

Если $\overline{T}$ — σ-инвариантный тор группы $\overline{G}$, то $T = \overline{T} \cap G = \overline{T}_\sigma \cap G$ называется *тором* группы G. Если $\overline{T}$ максимален, то T — *максимальный тор* группы G. Если G не является группой Сузуки или группой Ри, то для каждого максимального тора T выполняется $|\overline{T}_\sigma| = g(q)$, где $GF(q)$ — основное поле группы G, $g(t)$ — многочлен степени n, делящий $f_G(t)$, и n — ранг группы $\overline{G}$. Для более подробной информации см. [12, глава 1].

Таблица 1. Группы лиева типа, не являющиеся простыми

Группа	Свойства
$A_1(2)$	Группа разрешима
$A_1(3)$	Группа разрешима
$B_2(2)$	$B_2(2) \simeq \mathrm{Sym}_6$
$G_2(2)$	$[G_2(2), G_2(2)] \simeq {}^2A_2(3)$
${}^2A_2(2)$	Группа разрешима
${}^2B_2(2)$	Группа разрешима
${}^2G_2(3)$	$[{}^2G_2(3), {}^2G_2(3)] \simeq A_1(8)$
${}^2F_4(2)$	$[{}^2F_4(2), {}^2F_4(2)] = {}^2F_4(2)'$ — группа Титса

В леммах 1.2 и 1.3 собрана информация о максимальных торах в конечных простых группах лиева типа.

Лемма 1.2. (см. [13, Предложения 7–10] и [14]) *Пусть $\overline{G}$ — связная простая классическая алгебраическая группа присоединенного типа и $G = O^{p'}(\overline{G}_\sigma)$ — конечная простая классическая группа.*

1. *Каждый максимальный тор T группы $G = A_{n-1}^{\varepsilon}(q)$ имеет порядок*

$$\frac{1}{(n, q-(\varepsilon 1))(q-(\varepsilon 1))}(q^{n_1}-(\varepsilon 1)^{n_1}) \cdot (q^{n_2}-(\varepsilon 1)^{n_2}) \cdot \ldots \cdot (q^{n_k}-(\varepsilon 1)^{n_k})$$

   для подходящего разбиения $n_1 + n_2 + \ldots + n_k = n$ числа n. Более того, для любого разбиения существует тор соответствующего порядка.

2. *Каждый максимальный тор T группы G, где $G = B_n(q)$ или $G = C_n(q)$ имеет порядок*

$$\frac{1}{(2, q-1)}(q^{n_1}-1) \cdot (q^{n_2}-1) \cdot \ldots \cdot (q^{n_k}-1) \cdot (q^{l_1}+1) \cdot (q^{l_2}+1) \cdot \ldots \cdot (q^{l_m}+1)$$

   для подходящего разбиения $n_1+n_2+\ldots+n_k+l_1+l_2+\ldots+l_m = n$ числа n. Более того, для любого разбиения существует тор соответствующего порядка.

3. *Каждый максимальный тор T группы $G = D_n^{\varepsilon}(q)$ имеет порядок*

$$\frac{1}{(4, q^n - \varepsilon 1)} \cdot (q^{n_1} - 1) \cdot (q^{n_2} - 1) \cdot \ldots \cdot (q^{n_k} - 1) \cdot (q^{l_1} + 1) \cdot (q^{l_2} + 1) \cdot \ldots \cdot (q^{l_m} + 1)$$

   для подходящего разбиения $n_1 + n_2 + \ldots + n_k + l_1 + l_2 + \ldots + l_m = n$ числа n, где m четно, если $\varepsilon = +$, и m нечетно, если $\varepsilon = -$. Более того, для любого разбиения существует тор соответствующего порядка.

Лемма 1.3. (см. [14] и [15]) *Пусть $\overline{G}$ — связная простая исключительная алгебраическая группа присоединенного типа и $G = O^{p'}(\overline{G}_\sigma)$ — конечная простая исключительная группа лиева типа.*

1. *Каждый максимальный тор T группы $G = G_2(q)$ имеет один из следующих порядков:*

$$(q \pm 1)^2, q^2 - 1, q^2 \pm q + 1.$$

   Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

2. *Каждый максимальный тор T группы $G = F_4(q)$ имеет один из следующих порядков:*

$$(q \pm 1)^4, (q \pm 1)^2 \cdot (q^2 \pm 1), (q^2 \pm 1)^2, (q \pm 1)(q^3 \pm 1), q^4 \pm 1, (q^2 \pm q + 1)^2, q^4 - q^2 + 1.$$

   Здесь и ниже символ $\pm$ означает, что можно выбрать либо "+ либо "−" независимо для каждого множителя, т. е., $(q \pm 1)^2(q^2 \pm 1)$ равно либо $(q-1)^2(q^2-1)$, либо $(q+1)^2(q^2-1)$, либо $(q-1)^2(q^2+1)$, либо $(q+1)^2(q^2+1)$. Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

3. *Для каждого максимального тора T группы $G = E_6^{\varepsilon}(q)$, число $(3, q - \varepsilon 1)|T|$ равно одному из следующих чисел:*

   $(q - \varepsilon 1)^k \cdot (q + \varepsilon 1)^{6-k}$, $2 \leqslant k \leqslant 6$; $(q^k - (\varepsilon 1)^k) \cdot (q^{6-k} - (\varepsilon 1)^{6-k})$, $1 \leqslant k \leqslant 5$;
   $(q^k - (\varepsilon 1)^k) \cdot (q - \varepsilon 1)^{6-k}$, $3 \leqslant k \leqslant 6$; $(q^3 - \varepsilon 1)(q^2 - 1)(q \pm 1)$; $(q^5 - \varepsilon 1)(q + \varepsilon 1)$;
   $(q^3 + \varepsilon 1)(q^2 \pm 1)(q - \varepsilon 1)$; $(q^4 + 1)(q^2 - 1)$; $(q^2 + 1)^2(q - \varepsilon 1)^2$; $(q^2 + \varepsilon q + 1)^3$;
   $(q^2 + \varepsilon q + 1)^2(q^2 - 1)$; $(q^4 - 1)(q + \varepsilon 1)^2$; $(q^3 + \varepsilon 1)(q^2 + \varepsilon q + 1)(q + \varepsilon 1)$;
   $(q^4 - q^2 + 1)(q^2 + \varepsilon q + 1)$; $q^6 + \varepsilon q^3 + 1$; $(q^2 + \varepsilon q + 1)(q^2 - \varepsilon q + 1)^2$. *Более того, для каждого числа n из приведенных выше, существует тор T, для которого $(3, q - \varepsilon 1)|T| = n$.*

4. *Для каждого максимального тора T группы $G = E_7(q)$, число $(2, q-1)|T|$ равно одному из следующих чисел:*

   $(q^{n_1} \pm 1) \cdot \ldots \cdot (q^{n_k} \pm 1)$, $n_1 + \ldots + n_k = 7$ *и* $(2, q-1)|T| \neq (q \pm 1)(q^6 + 1)$;
   $(q - \epsilon 1) \cdot (q^2 + \epsilon q + 1)^3$; $(q^5 - \epsilon 1) \cdot (q^2 + \epsilon q + 1)$; $(q^3 \pm 1) \cdot (q^4 - q^2 + 1)$; $(q - \epsilon 1) \cdot (q^6 + \epsilon q^3 + 1)$;
   $(q^3 - \epsilon 1) \cdot (q^2 - \epsilon q + 1)^2$, *где $\epsilon = \pm$. Более того, для каждого числа n из приведенных выше, существует тор T, для которого $(2, q-1)|T| = n$.*

5. *Каждый максимальный тор T группы $G = E_8(q)$ имеет один из следующих порядков:*

   $(q^{n_1} \pm 1) \cdot \ldots \cdot (q^{n_k} \pm 1)$, $n_1 + \ldots + n_k = 8$ *и* $|T| \neq q^8 + 1$;

   $(q-\epsilon 1)\cdot(q^2+\epsilon q+1)^3\cdot(q\pm 1)$; $(q^5-\epsilon 1)\cdot(q^2+\epsilon q+1)\cdot(q\pm 1)$; $(q^3\pm 1)\cdot(q^4-q^2+1)\cdot(q\pm 1)$;

   $(q-\epsilon 1)\cdot(q^6+\epsilon q^3+1)\cdot(q\pm 1)$; $(q^3-\epsilon 1)\cdot(q^2-\epsilon q+1)^2\cdot(q\pm 1)$; q^8-q^4+1;

   $q^8+q^7-q^5-q^4-q^3+q+1$; $q^8-q^6+q^4-q^2+1$; $(q^4-q^2+1)^2$; $(q^6+\epsilon q^3+1)(q^2+\epsilon q+1)$;

   $q^8-q^7+q^5-q^4+q^3-q+1$; $(q^4+\epsilon q^3+q^2+\epsilon q+1)^2$; $(q^4-q^2+1)(q^2\pm q+1)^2$;

   $(q^2-q+1)^2\cdot(q^2+q+1)^2$; $(q^2\pm q+1)^4$, *где* $\epsilon = \pm$. *Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.*

6. *Каждый максимальный тор T группы $G = {}^3D_4(q)$ имеет один из следующих порядков:*

   $$(q^3 \pm 1)(q \pm 1); (q^2 \pm q + 1)^2; q^4 - q^2 + 1.$$

   Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

7. *Каждый максимальный тор T группы $G = {}^2B_2(2^{2n+1})$ имеет один из следующих порядков:*

   $$q - 1; q \pm \sqrt{2q} + 1,$$

   где $q = 2^{2n+1}$. Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

8. *Каждый максимальный тор T группы $G = {}^2G_2(3^{2n+1})$ имеет один из следующих порядков:*

   $$q \pm 1; q \pm \sqrt{3q} + 1,$$

   где $q = 3^{2n+1}$. Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

9. *Каждый максимальный тор T группы $G = {}^2F_4(2^{2n+1})$, где $n \geqslant 1$, имеет один из следующих порядков:*

   $$(q\pm 1)^2; q^2\pm 1; q^2-q+1; (q\pm\sqrt{2q}+1)^2; q^2-\epsilon q\sqrt{2q}+\epsilon\sqrt{2q}-1; q^2+\epsilon q\sqrt{2q}+q+\epsilon\sqrt{2q}+1,$$

   где $q = 2^{2n+1}$ и $\epsilon = \pm$. Более того, для любого из приведенных выше чисел существует тор соответствующего порядка.

Если q — натуральное число, r — нечетное простое число и $(r, q) = 1$, то через $e(r, q)$ мы обозначим наименьшее натуральное число n, удовлетворяющее условию $q^n \equiv 1 (\mathrm{mod}\ r)$. Если q нечетно, положим $e(2, q) = 1$ при $q \equiv 1 (\mathrm{mod}\ 4)$, и $e(2, q) = 2$ при $q \equiv -1 (\mathrm{mod}\ 4)$.

Основным техническим средством в параграфе 6 является следующее утверждение.

Лемма 1.4. (следствие теоремы Жигмонди [16]) *Пусть q — натуральное число, большее 1. Тогда для каждого $n \in \mathbb{N}$ найдется простое число r такое, что $e(r,q) = n$, исключая следующий случай: $n = 6$, $q = 2$.*

Простое число r, удовлетворяющее условию $e(r,q) = n$, называется *примитивным простым делителем* числа $q^n - 1$. По лемме 1.4 оно существует, исключая указанный выше случай. Если q фиксировано, мы обозначим через r_n некоторый примитивный простой делитель числа $q^n - 1$ (очевидно, $q^n - 1$ может иметь более одного такого делителя). Заметим, что в соответствии с нашим определением каждый простой делитель числа $q-1$ является примитивным простым делителем числа $q-1$ за единственным исключением: 2 не является примитивным делителем числа $q-1$ при $e(2,q) = 2$. В последнем случае, 2 — примитивный делитель числа $q^2 - 1$.

В силу [7, теоремы 9.4.10 и 14.3.1] порядок любой конечной простой группы лиева типа G ранга n над полем $GF(q)$ характеристики p равен

$$|G| = \frac{1}{d} q^N (q^{m_1} \pm 1) \cdot \ldots \cdot (q^{m_n} \pm 1).$$

Поэтому любой простой делитель r числа $|G|$, отличный от характеристики p, является примитивным делителем числа $q^m - 1$ для некоторого натурального числа m. Таким образом, лемма 1.4 позволяет нам «находить» простые делители числа $|G|$. Более того, если G не является группой Сузуки или группой Ри, из лемм 1.2 и 1.3 следует, что для фиксированного m каждые два примитивных делителя числа $q^m - 1$ смежны в $GK(G)$.

Для групп Сузуки и Ри мы будем использовать следующую лемму.

Лемма 1.5. *Пусть n — натуральное число.*

1. *Пусть* $m_1(B,n) = 2^{2n+1} - 1$,
   $m_2(B,n) = 2^{2n+1} - 2^{n+1} + 1$,
   $m_3(B,n) = 2^{2n+1} + 2^{n+1} + 1$.
   Тогда $(m_i(B,n), m_j(B,n)) = 1$, *если* $i \neq j$.
2. *Пусть* $m_1(G,n) = 3^{2n+1} - 1$,
   $m_2(G,n) = 3^{2n+1} + 1$,
   $m_3(G,n) = 3^{2n+1} - 3^{n+1} + 1$,
   $m_4(G,n) = 3^{2n+1} + 3^{n+1} + 1$.
   Тогда $(m_1(G,n), m_2(G,n)) = 2$ *и* $(m_i(G,n), m_j(G,n)) = 1$, *в остальных случаях.*
3. *Пусть* $m_1(F,n) = 2^{4n+2} - 1$,
   $m_2(F,n) = 2^{4n+2} + 1$,
   $m_3(F,n) = 2^{4n+2} - 2^{2n+1} + 1$,
   $m_5(F,n) = 2^{4n+2} - 2^{3n+2} + 2^{2n+1} - 2^{n+1} + 1$,
   $m_6(F,n) = 2^{4n+2} + 2^{3n+2} + 2^{2n+1} + 2^{n+1} + 1$.
   Тогда $(m_1(F,n), m_3(F,n)) = 3$ *и* $(m_i(F,n), m_j(F,n)) = 1$ *в остальных случаях.*

Доказательство. Это легко проверить прямым вычислением. □

По лемме 1.3 каждый отличный от характеристики простой делитель s порядка группы Сузуки ${}^2B_2(2^{2n+1})$ делит одно из чисел $m_i(B,n)$, определенных в лемме 1.5. То же самое верно для групп Ри ${}^2G_2(3^{2n+1})$, ${}^2F_2(2^{2n+1})$ и всех делителей чисел

$m_i(G,n)$, $m_i(F,n)$ соответственно. Таким образом, лемма 1.5 позволяет нам находить простые делители порядков групп Сузуки и Ри. Более того, из леммы 1.3 вытекает, что для фиксированного числа k каждые два простых делителя числа $m_k(B,n)$ смежны в $GK(^2B_2(2^{2n+1}))$. То же верно для групп Ри и всех простых делителей чисел $m_k(G,n)$ и $m_k(F,n)$.

2 Смежность нечетных простых чисел

В этом параграфе мы рассмотрим, смежны ли два нечетных простых числа, отличных от характеристики, в графе Грюнберга — Кегеля конечной группы лиева типа.

Предложение 2.1. *Пусть $G = A_{n-1}(q)$ — конечная простая группа лиева типа над полем характеристики p. Пусть r, s — нечетные простые числа и $r, s \in \pi(G) \setminus \{p\}$. Обозначим $k = e(r,q)$, $l = e(s,q)$ и предположим, что $2 \leqslant k \leqslant l$. Тогда r и s несмежны в том и только в том случае, когда $k + l > n$ и k не делит l.*

Доказательство. Во-первых, заметим, что для любого нечетного простого числа $c \neq p$ выполняется:

$$\text{\textit{число} } c \text{ \textit{делит} } q^x - 1 \text{ \textit{тогда и только тогда, когда} } e(c,q) \text{ \textit{делит} } x. \qquad (1)$$

Действительно, по определению c делит $q^{e(c,q)} - 1$ и не делит $q^y - 1$ для любого $y < e(c,q)$, т. е. $e(c,q)$ — это порядок q в мультипликативной группе $GF(c)^*$ конечного поля $GF(c)$. Следовательно, если c делит $q^z - 1$, то $q^z = 1$ в $GF(c)^*$, откуда $e(c,q)$ делит z. Предположим теперь, что $e(c,q)$ делит z. Тогда $q^z - 1 = (q^{e(c,q)} - 1)f(q)$ для некоторого $f(t) \in \mathbb{Z}[t]$, откуда c делит $q^z - 1$.

Предположим, что $k + l \leqslant n$. Рассмотрим максимальный тор T группы G порядка

$$\frac{1}{(n, q-1)(q-1)}(q^k - 1) \cdot (q^l - 1) \cdot (q-1)^{n-k-l}.$$

Тор T — абелева подгруппа группы G, и $r, s \in \pi(T)$. Следовательно, T содержит элемент порядка rs, а значит, числа r, s смежны. Если k делит l, то оба числа r и s делят $q^l - 1$, следовательно, максимальный тор порядка $\frac{1}{(n,q-1)}(q^l - 1)(q-1)^{n-l-1}$ содержит элемент порядка rs.

Предположим теперь, что $k + l > n$, k не делит l, и пусть g — элемент группы G порядка rs. Тогда $(|g|, p) = 1$, и значит, g — полупростой элемент. Следовательно, найдется максимальный тор T такой, что $g \in T$. По лемме 1.2 порядок тора T равен

$$\frac{1}{(n, q-1)(q-1)}(q^{n_1} - 1) \cdot (q^{n_2} - 1) \cdot \ldots \cdot (q^{n_x} - 1)$$

для подходящего разбиения $n_1 + n_2 + \ldots + n_x = n$ числа n. Поскольку r, s просты, существуют числа n_i, n_j такие, что r делит $q^{n_i} - 1$ и s делит $q^{n_j} - 1$. В силу (1) имеем $n_i = a \cdot k$, $n_j = b \cdot l$ для некоторых чисел $a, b \geqslant 1$. Более того, поскольку $k + l > n$ и $k \leqslant l$, выполняется $b = 1$. Действительно, иначе $n_j \geqslant l + l \geqslant k + l > n$, что противоречит равенству $n_1 + \ldots + n_x = n$. Поскольку k не делит l, имеем $n_i \neq n_j$. Значит, $n_1 + n_2 + \ldots + n_x \geqslant n_i + n_j = a \cdot k + l > n$; противоречие. $\square$

Предложение 2.2. *Пусть $G = {}^2A_{n-1}(q)$ — конечная простая группа лиева типа над полем характеристики p. Определим функцию*

$$\nu(m) = \begin{cases} m & , \text{ если } m \equiv 0 (\mathrm{mod}\ 4), \\ \frac{m}{2} & , \text{ если } m \equiv 2 (\mathrm{mod}\ 4), \\ 2m & , \text{ если } m \equiv 1 (\mathrm{mod}\ 2). \end{cases}$$

Пусть r, s — нечетные простые числа, и $r, s \in \pi(G) \setminus \{p\}$. Обозначим $k = e(r, q)$, $l = e(s, q)$ и предположим, что $2 \leqslant \nu(k) \leqslant \nu(l)$. Тогда r и s несмежны в том и только в том случае, когда $\nu(k) + \nu(l) > n$ и $\nu(k)$ не делит $\nu(l)$.

Доказательство. Во-первых, заметим, что для любого нечетного простого числа $c \neq p$ выполняется:

$$\text{число } c \text{ делит } q^x - (-1)^x \text{ тогда и только тогда, когда } \nu(e(c, q)) \text{ делит } x. \tag{2}$$

Вначале предположим, что $e(c, q)$ нечетно. Если c делит $q^z - (-1)^z$, то c делит $q^{2z} - 1$, значит, в силу (1) число $e(c, q)$ делит $2z$. Поскольку $e(c, q)$ нечетно, $e(c, q)$ делит z и, следовательно, (вновь в силу (1)) c делит $q^z - 1$. Так как c нечетно, число $q^z + 1$ не делится на c, значит, $q^z - (-1)^z = q^z - 1$, т. е. z четно. Однако $e(c, q)$ нечетно, откуда $2e(c, q) = \nu(e(c, q))$ делит z. Предположим, что $\nu(e(c, q))$ делит z. Тогда z четно, значит, $q^z - (-1)^z = q^z - 1$ и c делит $q^z - (-1)^z$ в силу (1). Поэтому (2) верно в этом случае.

Предположим, что $e(c, q) \equiv 2 (\mathrm{mod}\ 4)$. Если c делит $q^z - (-1)^z$, то c делит $q^{2z} - 1$, откуда $e(c, q)$ делит $2z$. Но $\nu(e(c, q)) = \frac{e(c,q)}{2}$, следовательно, $\nu(e(c, q))$ делит z. Если $\nu(e(c, q))$ делит z, и z нечетно, то $q^z - (-1)^z = q^z + 1$. Поскольку $e(c, q)$ делит $2z$, число c делит $q^{2z} - 1$. Имеем $q^{2z} - 1 = (q^z - 1) \cdot (q^z + 1)$. Поскольку z нечетно, $e(c, q)$ не делит z, следовательно, по (1) число c не делит $q^z - 1$, откуда c делит $q^z + 1 = q^z - (-1)^z$. Если $\nu(e(c, q))$ делит z, и z четно, то $2\nu(e(c, q)) = e(c, q)$ делит z, значит, по (1) число c делит $q^z - (-1)^z = q^z - 1$. Таким образом, (2) верно и в этом случае.

Наконец, предположим, что $e(c, q) \equiv 0 (\mathrm{mod}\ 4)$. Если c делит $q^z - (-1)^z$, то, как и выше, c делит $q^{2z} - 1$, откуда $e(c, q)$ делит $2z$ и $\frac{e(c,q)}{2}$ делит z. Но $\frac{e(c,q)}{2}$ четно, значит, z четно и $q^z - (-1)^z = q^z - 1$. Отсюда $e(c, q) = \nu(e(c, q))$ делит z. Если $\nu(e(c, q)) = e(c, q)$ делит z, то z четно и в силу (1) число c делит $q^z - (-1)^z = q^z - 1$.

Предположим, что $\nu(k) + \nu(l) \leqslant n$. Рассмотрим максимальный тор T группы G порядка

$$\frac{1}{(n, q + 1)(q + 1)}(q^{\nu(k)} - (-1)^{\nu(k)}) \cdot (q^{\nu(l)} - (-1)^{\nu(l)}) \cdot (q + 1)^{n-\nu(k)-\nu(l)}.$$

Тор T — абелева подгруппа группы G, и $r, s \in \pi(T)$. Следовательно, T содержит элемент порядка rs, откуда числа r, s смежны. Если $\nu(k)$ делит $\nu(l)$, то оба числа r и s делят $q^{\nu(l)} - (-1)^{\nu(l)}$, следовательно, максимальный тор порядка $\frac{1}{(n,q+1)}(q^{\nu(l)} - (-1)^{\nu(l)})(q + 1)^{n-\nu(l)-1}$ содержит элемент порядка rs.

Предположим теперь, что $\nu(k) + \nu(l) > n$, $\nu(k)$ не делит $\nu(l)$, и предположим, что $g \in {}^2A_{n-1}(q)$ имеет порядок rs. Тогда $(|g|, p) = 1$, откуда g — полупростой элемент. Следовательно, найдется максимальный тор T такой, что $g \in T$. Используя (2) и лемму 1.2, мы приходим к противоречию как при доказательстве предложения 2.1. $\square$

Предложение 2.3. *Пусть G — одна из конечных простых групп лиева типа $B_n(q)$ или $C_n(q)$ над полем характеристики p. Определим функцию*

$$\eta(m) = \begin{cases} m & \text{, если } m \text{ нечетно,} \\ \frac{m}{2} & \text{, если } m \text{ четно.} \end{cases}$$

Пусть r, s — нечетные простые числа и $r, s \in \pi(G) \setminus \{p\}$, Обозначим $k = e(r, q)$, $l = e(s, q)$ и предположим, что $1 \leqslant \eta(k) \leqslant \eta(l)$. Тогда r и s несмежны в том и только в том случае, когда $\eta(k) + \eta(l) > n$ и $\eta(k)$, $\eta(l)$ удовлетворяют условию (3):

$$\textit{Либо } \frac{\eta(l)}{\eta(k)} \textit{ не является нечетным целым числом, либо } \eta(k) = \eta(l) \text{ и } k \neq l. \qquad (3)$$

Заметим, что (3) выполняется в следующих случаях:

1. Оба числа k и l четны, и либо $\eta(k)$ не делит $\eta(l)$, либо $\frac{\eta(l)}{\eta(k)}$ четно. В этом случае $q^{\eta(k)} + (-1)^k = q^{\eta(k)} + 1$ не делит $q^{\eta(l)} + (-1)^l = q^{\eta(l)} + 1$.

2. Оба числа k и l нечетны, и $\eta(k)$ не делит $\eta(l)$. В этом случае $q^{\eta(k)} + (-1)^k = q^k - 1$ не делит $q^{\eta(l)} + (-1)^l = q^l - 1$.

3. Число k нечетно и l четно. В этом случае $q^{\eta(k)} + (-1)^k = q^k - 1$ не делит $q^{\eta(l)} + (-1)^l = q^{\eta(l)} + 1$.

4. Число k четно, l нечетно, и либо $\eta(k)$ не делит $\eta(l)$, либо $\frac{\eta(l)}{\eta(k)}$ является четным числом или $\frac{\eta(l)}{\eta(k)}$ равно 1. В этом случае $q^{\eta(k)} + (-1)^k = q^{\eta(k)} + 1$ не делит $q^{\eta(l)} + (-1)^l = q^l - 1$.

Вышесказанное означает, что $\eta(k)$, $\eta(l)$ удовлетворяют условию (3) тогда и только тогда, когда $q^{\eta(k)} + (-1)^k$ не делит $q^{\eta(l)} + (-1)^l$.

Доказательство. Во-первых, мы докажем, что для любого нечетного простого числа $c \neq p$ выполняется:

$$\textit{если } c \textit{ делит } q^x \pm 1, \textit{ то } \eta(e(c, q)) \textit{ делит } x. \qquad (4)$$

Предположим вначале, что $e(c, q)$ нечетно и c делит $q^z \pm 1$. В силу (1) число $e(c, q)$ делит $2z$. Но $e(c, q)$ нечетно, откуда $e(c, q) = \eta(e(c, q))$ делит z. Предположим теперь, что $e(c, q)$ четно и c делит $q^z \pm 1$. Тогда c делит $q^{2z} - 1$, откуда $e(c, q)$ делит $2z$ и $\frac{e(c,q)}{2} = \eta(e(c, q))$ делит z.

Если теперь $\eta(k) + \eta(l) \leqslant n$, мы можем рассмотреть максимальный тор T порядка $\frac{1}{(2,q-1)}(q^{\eta(k)} + (-1)^k) \cdot (q^{\eta(l)} + (-1)^l) \cdot (q-1)^{n-\eta(k)-\eta(l)}$. Тор T — абелева группа и $r, s \in \pi(T)$. Значит, T содержит элемент порядка rs. Если $\eta(k)$, $\eta(l)$ не удовлетворяют условию (3), то $q^{\eta(k)} + (-1)^k$ делит $q^{\eta(l)} + (-1)^l$, а следовательно, оба числа r и s делят $q^{\eta(l)} + (-1)^l$. Таким образом, максимальный тор порядка $\frac{1}{(2,q-1)}(q^{\eta(l)} + (-1)^l)(q-1)^{n-\eta(l)}$ содержит элемент порядка rs.

Предположим, что $\eta(k)+\eta(l)>n$, $\eta(k)$ и $\eta(l)$ удовлетворяют условию (3), и предположим, что существует элемент $g\in G$ порядка rs. Поскольку $(|g|,p)=1$, элемент g полупрост. Поэтому найдется максимальный тор T, содержащий g. В силу леммы 1.2 порядок $|T|$ равен

$$\frac{1}{(2,q-1)}(q^{n_1}\pm 1)\cdot(q^{n_2}\pm 1)\cdot\ldots\cdot(q^{n_x}\pm 1)$$

для подходящего разбиения $n_1+n_2+\ldots+n_x=n$ числа n. Используя (4), мы приходим к противоречию как при доказательстве предложения 2.1. □

Предложение 2.4. *Пусть $G=D_n^\varepsilon(q)$ — конечная простая группа лиева типа над полем характеристики p, и функция $\eta(m)$ определена в предложении 2.3. Пусть r,s — нечетные простые числа и $r,s\in\pi(D_n^\varepsilon(q))\setminus\{p\}$. Обозначим $k=e(r,q)$, $l=e(s,q)$ и предположим, что $1\leqslant\eta(k)\leqslant\eta(l)$. Тогда r и s несмежны в том и только в том случае, когда $2\cdot\eta(k)+2\cdot\eta(l)>2n-(1-\varepsilon(-1)^{k+l})$ и $\eta(k)$, $\eta(l)$ удовлетворяют условию (3).*

Доказательство. Используя (4) и лемму 1.2, мы доказываем это предложение как предыдущие. □

Предложение 2.5. *Пусть G — конечная простая исключительная группа лиева типа над полем характеристики p, пусть r,s — нечетные простые числа и $r,s\in\pi(G)\setminus\{p\}$, $k=e(r,q)$, $l=e(s,q)$ и $1\leqslant k\leqslant l$. Тогда r и s несмежны в том и только в том случае, когда $k\neq l$ и выполняется одно из следующих утверждений:*

1. *$G=G_2(q)$ и либо $r\neq 3$ и $l\in\{3,6\}$, либо $r=3$ и $l=9-3k$.*

2. *$G=F_4(q)$ и либо $l\in\{8,12\}$, либо $k\in\{3,4\}$ и $l=6$, либо $k=3$ и $l=4$.*

3. *$G=E_6(q)$ и либо $l=5$ и $k\geqslant 3$, либо $l=6$ и $k=5$, либо $l=8$, $k\geqslant 3$, либо $l=8$ и $r=3$ при $(q-1)_3=3$, либо $l=9$, либо $l=12$, $k\neq 3$ и $r\neq 3$.*

4. *$G={}^2E_6(q)$ и либо $l=8$, $k\geqslant 3$, либо $l=8$ и $r=3$ при $(q+1)_3=3$, либо $l=10$ и $k\geqslant 3$, либо $l=12$, $k\neq 6$ и $r\neq 3$, либо $l=18$.*

5. *$G=E_7(q)$ и либо $l\in\{14,18\}$ и $k\neq 2$, либо $l\in\{7,9\}$ и $k\geqslant 2$, либо $l=8$ и $k=7$, либо $l=10$ и $k\geqslant 3, k\neq 4,6$, либо $l=12$ и $k\geqslant 4, k\neq 6$.*

6. *$G=E_8(q)$ и либо $l\in\{7,14\}$ и $k\geqslant 3$, либо $l=9$ и $k\geqslant 4$, либо $l\in\{8,10,12\}$ и $k\geqslant 5, k\neq 6$, либо $l=18$ и $k\neq 1,2,6$, либо $l=20$ и $r\cdot k\neq 20$, либо $l\in\{15,24,30\}$.*

7. *$G={}^3D_4(q)$ и либо $l=6$ и $k=3$, либо $l=12$.*

Доказательство. Как и для классических групп лиева типа, простые делители $r,s\in\pi(G)$, удовлетворяющие условиям предложения смежны, тогда и только тогда, когда rs делит порядок некоторого максимального тора группы G. Таким образом, используя лемму 1.3 вместо леммы 1.2, мы доказываем это предложение как предыдущие. □

Предложение 2.6. *Пусть G — конечная простая группа Сузуки или группа Ри над полем характеристики p, пусть r, s — нечетные простые числа и $r, s \in \pi(G) \setminus \{p\}$. Тогда r и s несмежны тогда и только тогда, когда выполняется одно из утверждений:*

1. $G = {}^2B_2(2^{2n+1})$, *r делит $m_k(B, n)$, s делит $m_l(B, n)$ и $k \neq l$.*

2. $G = {}^2G_2(3^{2n+1})$, *r делит $m_k(G, n)$, s делит $m_l(G, n)$ и $k \neq l$.*

3. $G = {}^2F_4(2^{2n+1})$, *r делит $m_k(F, n)$, s делит $m_l(F, n)$, $k \neq l$ и если $\{k, l\} = \{1, 3\}$, то $r \neq 3 \neq s$.*

Числа $m_i(B, n)$, $m_i(G, n)$ и $m_i(F, n)$ определены в лемме 1.5.

Доказательство. Мы используем лемму 1.3, лемму 1.5 и аргументы, аналогичные тем, что мы использовали при доказательстве предыдущих предложений параграфа. □

3 Смежность с характеристикой

В этом параграфе мы рассмотрим, смежны ли простое число r и характеристика p основного поля конечной группы лиева типа.

Предложение 3.1. *Пусть $G = O^{p'}(\overline{G}_\sigma)$ — конечная простая классическая группа лиева типа над полем характеристики p. Пусть $r \in \pi(G)$ и $r \neq p$. Тогда r и p несмежны в том и только в том случае, когда выполняется одно из следующих утверждений:*

1. $G = A_{n-1}(q)$, *r нечетно и $e(r, q) > n - 2$.*

2. $G = {}^2A_{n-1}(q)$, *r нечетно и $\nu(e(r, q)) > n - 2$. Функция $\nu(m)$ определена в предложении* 2.2.

3. $G = C_n(q)$, $\eta(e(r, q)) > n - 1$. *Функция $\eta(m)$ определена в предложении* 2.3.

4. $G = B_n(q)$, $\eta(e(r, q)) > n - 1$. *Функция $\eta(m)$ определена в предложении* 2.3.

5. $G = D_n^\varepsilon(q)$, $\eta(e(r, q)) > n - 2$. *Функция $\eta(m)$ определена в предложении* 2.3.

6. $G = A_1(q)$, $r = 2$.

7. $G = A_2^\varepsilon(q)$, $r = 3$ *и* $(q - \varepsilon 1)_3 = 3$.

Доказательство. Очевидно, что 2 и p смежны во всех классических группах кроме групп $A_1(q)$. Значит, мы можем полагать, что r нечетно.

Вначале кратко изложим общую идею доказательства. Мы будем использовать [13] как техническое средство в нашем доказательстве, поэтому мы сохраняем обозначения из [13]. Для того, чтобы доказать, что r и p смежны, мы находим связную редуктивную подгруппу R максимального ранга группы G такую, что $R = T(G_1 * G_2)$, где T — максимальный тор, G_1 и G_2 — нетривиальные группы лиева типа такие, что $r \in \pi(G_1)$. Тогда G_1 содержит элемент порядка r, который централизует G_2. Поскольку G_2 нетривиальна, она содержит элемент порядка p, и, следовательно, $G \geq R$ содержит элемент порядка rp.

Для того, чтобы доказать, что r и p несмежны, рассматривается произвольный элемент g порядка r и его связный централизатор $G \cap C_{\overline{G}}(g)^0$. Напомним, что $C_{\overline{G}}(g)^0 = \overline{S} * \overline{L}$, где $\overline{S} = Z(C_{\overline{G}}(g)^0)$ — центральный тор и $\overline{L}$ — полупростая часть. Ясно, что $g \in \overline{S} \cap G \leq \overline{S}_\sigma$, откуда r делит $|\overline{S}_\sigma|$. Это условие влечет тривиальность $\overline{L}_\sigma$, а значит, $C_{\overline{G}}(g)^0$ не содержит унипотентных элементов. Но каждый унипотентный элемент централизатора $C_{\overline{G}}(g)$ содержится в $C_{\overline{G}}(g)^0 \leq N_{\overline{G}}(\overline{T})^0 = \overline{T}$. Поэтому ни один из унипотентных элементов группы G не централизует g. Теперь мы рассмотрим все классические группы поочередно.

$A_1(q)$. Известно, что если g — элемент порядка $r \neq p$, то $(|C_{A_1(q)}(g)|, p) = 1$ (см. [13, предложение 7]). Поэтому r, p несмежны для каждого $r \in \pi(A_1(q)) \setminus \{p\}$.

$A_2(q)$. Используя [13, предложение 7], мы получаем, что только простые делители числа $\frac{q-1}{(3,q-1)}$ смежны с p, и предложение верно в этом случае.

$A_{n-1}(q)$ и $n \geqslant 4$. В нашем случае T — подгруппа Картана, $G_1 = A_{n-3}(q)$ и $G_2 = A_1(q)$. Существование такой подгруппы доказывается с использованием [13, предложение 7]. Таким образом, каждое простое число r, удовлетворяющее условию $e(r,q) \leqslant n-2$, делит $|G_1|$, а значит, смежно с p. Пусть теперь $e(r,q) = n-1$ и g — элемент порядка r. В силу (1) имеем, число $q^{n-1}-1$ должно делить $|\overline{S}_\sigma| \cdot (q-1)$. Из [13, предложение 7] следует, что $G \cap C_{\overline{G}}(g)^0$ — максимальный тор порядка $\frac{1}{(n,q-1)}(q^{n-1}-1)$. Значит $|\overline{L}_\sigma| = 1$ и r, p несмежны. Если $e(r,q) = n$ и g имеет порядок r, то в силу (1) число $q^n - 1$ должно делить $|\overline{S}_\sigma| \cdot (q-1)$. Снова используя [13, предложение 7], получаем, что $G \cap C_{\overline{G}}(g)^0$ — максимальный тор порядка $\frac{1}{(n,q-1)}\frac{q^n-1}{q-1}$. Поэтому $|\overline{L}_\sigma| = 1$ в этом случае, и каждое простое число r, удовлетворяющее условию $e(r,q) > n-2$, несмежно с p.

${}^2A_2(q)$. Используя [13, предложение 8], получаем, что только простые делители числа $\frac{q+1}{(3,q+1)}$ смежны с p и предложение верно в этом случае.

${}^2A_{n-1}(q)$ и $n \geqslant 4$. Вновь T — подгруппа Картана, $G_1 = {}^2A_{n-3}(q)$ и $G_2 = A_1(q)$. Существование такой подгруппы доказывается с использованием [13, предложение 8]. Таким образом, каждое простое число r, удовлетворяющее условию $\nu(e(r,q)) \leqslant n-2$, делит $|G_1|$, а значит, смежно с p. Пусть теперь $\nu(e(r,q)) = n-1$ и g — элемент порядка r. Тогда в силу (2) имеем, число $q^{n-1} - (-1)^{n-1}$ делит $|\overline{S}| \cdot (q+1)$. Из [13, предложение 8] следует, что $G \cap C_{\overline{G}}(g)^0$ — максимальный тор порядка $\frac{1}{(n,q+1)}(q^{n-1} - (-1)^{n-1})$. Отсюда $|\overline{L}_\sigma| = 1$ и r, p несмежны. Если $\nu(e(r,q)) = n$ и g — элемент порядка r, то в силу (2) число $q^n - (-1)^n$ делит $|\overline{S}_\sigma| \cdot (q+1)$. Используя [13, предложение 8], получаем, что $G \cap C_{\overline{G}}(g)^0$ — максимальный тор порядка $\frac{1}{(n,q+1)}\frac{q^n-(-1)^n}{q+1}$. Следовательно, $|\overline{L}_\sigma| = 1$ и каждое простое число r, удовлетворяющее условию $\nu(e(r,q)) > n-2$, несмежно с p.

$C_n(q)$. Выберем R так, что T — подгруппа Картана, $G_1 = C_{n-1}(q)$, $G_2 = A_1(q)$. Такая подгруппа R существует в силу [13, предложения 9 и 12]. Вновь каждое простое число r, удовлетворяющее условию $\eta(e(r,q)) \leqslant n-1$, делит $|G_1|$, а значит, смежно с p. Если $\eta(e(r,q)) = n$ и g — элемент порядка r, то из (4) следует, что либо $q^n - 1$, либо $q^n + 1$ делит $|\overline{S}_\sigma|$. Из [13, предложения 9 и 12] получаем, что $G \cap C_{\overline{G}}(g)^0$ — максимальный тор порядка $\frac{1}{(2,q-1)}(q^n \pm 1)$ соответственно, откуда $|\overline{L}_\sigma| = 1$ и r, p несмежны.

$B_n(q)$. Поскольку $B_2(q) \simeq C_2(q)$ и $B_n(2^t) \simeq C_n(2^t)$, можно полагать, что p нечетно и $n \geqslant 3$. Мы можем выбрать в качестве T подгруппу Картана, $G_1 = B_{n-2}(q)$ и $G_2 = D_2(q)$. Такая подгруппа R существует в силу [13, предложение 11]. Поскольку каждое простое число r, удовлетворяющее условию $\eta(e(r,q)) \leqslant n-2$, делит порядок G_1, получаем, что r и p несмежны, если $\eta(e(r,q)) \leqslant n-2$. Если $\eta(e(r,q)) = n-1$, то вновь по [13, предложение 11], существует редуктивная подгруппа R такая, что $|\overline{S}_\sigma| = q^{\eta(e(r,q))} + (-1)^{e(r,q)}$ и $\overline{L}_\sigma = B_1(q) \simeq A_1(q)$. Значит r, p смежны в G. Предположим теперь, что $\eta(e(r,q)) = n$ и g — элемент порядка r в G. Тогда порядок $|\overline{S}_\sigma|$ дан в [13, предложение 11], он равен $\prod_i (q^{n_i} \pm 1)$, где $\sum_i n_i \leqslant n$. Используя (4), получаем, что $\eta(e(r,q)) = n$ делит n_i для некоторого i. Значит, либо $q^n - 1$, либо $q^n + 1$ делит $|S_\sigma|$. В силу [13, предложение 11] имеем, $|\overline{L}_\sigma| = 1$, откуда r, p несмежны.

$D_n^\varepsilon(q)$. Пусть T — подгруппа Картана, $G_1 = D_{n-2}^\varepsilon(q)$, $G_2 = A_1(q)$. Существование такой подгруппы R доказывается с использованием [13, предложение 10]. Поэтому r, p смежны для всех r, удовлетворяющих условию $\eta(e(r,q)) \leqslant n-2$, исключая случай: $\eta(e(r,q)) = n-2$ и r делит $q^{n-2} + \varepsilon 1$. В этом последнем случае, мы получаем, что существует редуктивная подгруппа R такая, что $|\overline{S}_\sigma| = q^{n-2} + \varepsilon 1$ и $\overline{L}_\sigma \simeq D_2^\varepsilon(q)$. Значит, и в этом исключительном случае r, p также смежны. Если теперь $\eta(e(r,q)) \geqslant n-1$ и g — элемент группы G порядка r, то как и ранее получаем, что $q^{\eta(e(r,q))} + (-1)^{e(r,q)}$ делит $|\overline{S}_\sigma|$ и из [13, предложение 10] следует, что $\overline{L}_\sigma$ тривиальна. Следовательно, r и p несмежны в этом случае. □

Предложение 3.2. *Пусть G — конечная простая исключительная группа лиева типа над полем характеристики p. Пусть $r \in \pi(G)$, $k = e(r,q)$ и $r \neq p$. Тогда r и p несмежны в том и только в том случае, когда выполняется одно из утверждений*:

1. $G = G_2(q)$, $k \in \{3, 6\}$.
2. $G = F_4(q)$, $k \in \{8, 12\}$.
3. $G = E_6(q)$, $k \in \{8, 9, 12\}$.
4. $G = {}^2E_6(q)$, $k \in \{8, 12, 18\}$.
5. $G = E_7(q)$, $k \in \{7, 9, 14, 18\}$.
6. $G = E_8(q)$, $k \in \{15, 20, 24, 30\}$.
7. $G = {}^3D_4(q)$, $k = 12$.

Доказательство. Все утверждения получаются с использованием информации о централизаторах полупростых элементов из [15] и [17]. □

Предложение 3.3. *Пусть G — конечная простая группа Сузуки или Ри над полем характеристики p, пусть $r \in \pi(G) \setminus \{p\}$. Тогда r, p несмежны в том и только в том случае, когда выполняется одно из утверждений*:

1. $G = {}^2B_2(2^{2n+1})$, r *делит* $m_k(B, n)$.

2. $G = {}^2G_2(3^{2n+1})$, *r делит $m_k(G,n)$ и $r \neq 2$.*

3. $G = {}^2F_4(2^{2n+1})$, *r делит $m_k(F,n)$, $r \neq 3$ и $k > 2$.*

Числа $m_i(B,n)$, $m_i(G,n)$ и $m_i(F,n)$ определены в лемме 1.5.

Доказательство. Все утверждения получаются с использованием информации о централизаторах полупростых элементов из [15]. □

4 Смежность с числом 2

В этом параграфе мы рассмотрим, смежны ли число 2 и нечетное простое число r, если оба они не равны характеристике p основного поля. Мы начнем с групп $A_n^{\varepsilon}(q)$. Напомним, что в параграфе 2 для них не рассматривался критерий смежности для простых делителей числа $q-\varepsilon 1$. Дело в том, что его естественнее рассмотреть вместе с критерием для 2, что и сделано в двух следующих предложениях.

Предложение 4.1. *Пусть $G = A_{n-1}(q)$ — конечная простая группа лиева типа. Пусть r — простой делитель числа $q-1$ и s — нечетное простое число, отличное от характеристики. Обозначим $k = e(s,q)$. Тогда s и r несмежны в том и только в том случае, когда выполняется одно из следующих утверждений*:

1. *$k = n$, $n_r \leqslant (q-1)_r$, и если $n_r = (q-1)_r$, то $2 < (q-1)_r$.*

2. *$k = n-1$ и $(q-1)_r \leqslant n_r$.*

Доказательство. Вначале докажем следующие утверждение

$$\left(\frac{q^n-1}{q-1}\right)_r = n_r, \text{ если } (q-1)_r \geqslant n_r \text{ и } (q-1)_r > 2,$$

$$\left(\frac{q^n-1}{q-1}\right)_2 > 2, \text{ если } (q-1)_2 = n_2 = 2. \quad (5)$$

Предположим, что r нечетно. Тогда $n = r^k \cdot l$, где $(l,r) = 1$ и $q = r^k \cdot m + 1$. Имеем $q^n - 1 = (q^{r^k} - 1) \cdot (q^{n-r^k} + q^{n-2r^k} + \ldots + q^{r^k} + 1)$. Второй сомножитель является суммой l чисел вида q^i, и $q^i \equiv 1 (\mathrm{mod}\ r)$ для всех i. Поскольку $(l,r) = 1$, второй сомножитель взаимно прост с r. Таким образом, $\left(\frac{q^n-1}{q-1}\right)_r = \left(\frac{q^{r^k}-1}{q-1}\right)_r$. Вспомним теперь, что $q = r^k \cdot m + 1$, откуда

$$\frac{q^{r^k}-1}{q-1} = (r^k \cdot m)^{r^k-1} + r^k \cdot (r^k \cdot m)^{r^k-2} + \ldots + \frac{1}{2} r^k (r^k - 1)(r^k \cdot m) + r^k.$$

Поскольку r^{k+1} делит все слагаемые за исключением последнего и r^{k+1} не делит r^k, получаем, что r^k делит $\left(\frac{q^{r^k}-1}{q-1}\right)_r$, а r^{k+1} не делит $\left(\frac{q^{r^k}-1}{q-1}\right)_r$. Следовательно, в этом случае $\left(\frac{q^{r^k}-1}{q-1}\right)_r = n_r$.

Предположим теперь, что $r=2$, $n=2^k\cdot l$, где l нечетно, и $q=2^k\cdot m+1$. Тогда

$$\left(\frac{q^n-1}{q-1}\right)_2=\left(\frac{q^l-1}{q-1}\right)_2\cdot(q^l+1)\cdot(q^{2l}+1)\cdot\ldots\cdot(q^{2^{k-1}l}+1).$$

Поскольку l нечетно, выполняется $\left(\frac{q^l-1}{q-1}\right)_2=1$. Если $(q-1)_2>2$, то $(q^i+1)_2=2$ для всех i. Следовательно,

$$\left(\frac{q^n-1}{q-1}\right)_2=(q^l+1)_2\cdot(q^{2l}+1)_2\cdot\ldots\cdot(q^{2^{k-1}l}+1)_2=2^k=n_2.$$

Второй случай, когда $(q-1)_2=n_2=2$, очевиден.

Предположим, что $k\leqslant n-2$. Из леммы 1.2 следует, что существует максимальный тор T группы G порядка $\frac{1}{(n,q-1)}(q^k-1)(q-1)^{n-k-1}$. Тор T — абелева подгруппа группы G, и оба числа r,s делят $|T|$. Следовательно, T содержит элемент порядка rs.

Предположим, что $k=n$. В силу (1) и леммы 1.2 каждый элемент порядка s содержится в максимальном торе T порядка $\frac{1}{(n,q-1)}\frac{q^n-1}{q-1}$. В силу (5) число r не делит $|T|$ тогда и только тогда, когда имеет место условие 1 предложения.

Предположим, что $k=n-1$. В силу (1) и леммы 1.2 каждый элемент порядка s содержится в максимальном торе T порядка $\frac{1}{(n,q-1)}(q^{n-1}-1)$. Имеем $(q^{n-1}-1)=(q-1)(q^{n-2}+q^{n-3}+\ldots+q+1)$ и $(q^{n-2}+q^{n-3}+\ldots+q+1)_r=1$. Следовательно, r не делит $|T|$ тогда и только тогда, когда $(q-1)_r\leqslant n_r$, и мы получаем условие 2 предложения. □

Предложение 4.2. *Пусть $G={}^2A_{n-1}(q)$ — конечная простая группа лиева типа. Пусть r — простой делитель числа $q+1$ и s — нечетное простое число, отличное от характеристики. Обозначим $k=e(s,q)$. Тогда s и r несмежны в том и только в том случае, когда выполняется одно из следующих утверждений*:

1. $\nu(k)=n$, *$n_r\leqslant(q+1)_r$, и если $n_r=(q+1)_r$, то $2<(q+1)_r$.*
2. $\nu(k)=n-1$ *и* $(q+1)_r\leqslant n_r$.

Функция $\nu(m)$ определена в предложении 2.2.

Доказательство. Как и в предыдущем предложении, вначале мы показываем, что

$$\left(\frac{q^n-(-1)^n}{q+1}\right)_r=n_r,\text{ если }(q+1)_r\geqslant n_r\text{ и }(q+1)_r>2,$$
$$\left(\frac{q^n-(-1)^n}{q+1}\right)_2>2,\text{ если }(q+1)_2=n_2=2.\quad(6)$$

Предположим, что r нечетно. Тогда $n=r^k\cdot l$, где $(l,r)=1$, и $q=r^k\cdot m-1$. Имеем $q^n-(-1)^n=(q^{r^k}+1)\cdot(q^{n-r^k}-q^{n-2r^k}+\ldots+(-1)^{l-1}q^{r^k}+(-1)^l)$. Второй сомножитель является суммой l чисел вида $(-1)^tq^{n-(t+1)r^k}$ и $q^{n-(t+1)r^k}\equiv(-1)^{n+t-1}(\mathrm{mod}\ r)$ для всех t. Значит, второй множитель сравним с $(-1)^{n-1}l$ по модулю r. Поскольку $(l,r)=$

1, второй сомножитель взаимно прост с r. Таким образом, $\left(\frac{q^n-(-1)^n}{q+1}\right)_r = \left(\frac{q^{r^k}+1}{q+1}\right)_r$. Вспомним теперь, что $q = r^k \cdot m - 1$, откуда

$$\frac{q^{r^k}+1}{q+1} = (r^k \cdot m)^{r^k-1} - r^k \cdot (r^k \cdot m)^{r^k-2} + \ldots + (-1)^{k-2}\frac{1}{2}r^k(r^k-1)(r^k \cdot m) + (-1)^{k-1}r^k.$$

Поскольку r^{k+1} делит все слагаемые исключая последнее и r^{k+1} не делит r^k, получаем, что r^k делит $\left(\frac{q^{r^k}+1}{q+1}\right)_r$, а r^{k+1} не делит $\left(\frac{q^{r^k}+1}{q+1}\right)_r$. Следовательно, в этом случае $\left(\frac{q^{r^k}+1}{q+1}\right)_r = n_r$.

Предположим теперь, что $r = 2$, $n = 2^k \cdot l$, где l нечетно, и $q = 2^k \cdot m - 1$. Тогда

$$\left(\frac{q^n-(-1)^n}{q+1}\right)_2 = \left(\frac{q^l+1}{q+1}\right)_2 \cdot (q^l-1) \cdot (q^{2l}+1) \cdot \ldots \cdot (q^{2^{k-1}l}+1).$$

Поскольку l нечетно, выполняется $\left(\frac{q^l+1}{q+1}\right)_2 = 1$. Если $(q+1)_2 > 2$, то $(q^{2i}+1)_2 = 2$ для всех $i \geqslant 1$ и $(q^l-1)_2 = 2$. Следовательно,

$$\left(\frac{q^n-(-1)^n}{q+1}\right)_2 = (q^l-1)_2 \cdot (q^{2l}+1)_2 \cdot \ldots \cdot (q^{2^{k-1}l}+1)_2 = 2^k = n_2.$$

Второй случай, когда $(q+1)_2 = n_2 = 2$, очевиден.

Предположим, что $\nu(k) \leqslant n-2$. Из леммы 1.2 следует, что существует максимальный тор T группы G порядка $\frac{1}{(n,q+1)}(q^{\eta(k)} - (-1)^{\eta(k)})(q+1)^{n-k-1}$. Тор T — абелева подгруппа группы G, и оба числа r, s делят $|T|$. Следовательно, T содержит элемент порядка rs.

Предположим, что $\nu(k) = n$. В силу (2) и леммы 1.2 каждый элемент порядка s содержится в максимальном торе T порядка $\frac{1}{(n,q+1)}\frac{q^n-(-1)^n}{q+1}$. В силу (6) число r не делит $|T|$ тогда и только тогда, когда выполняется условие 1 предложения.

Предположим теперь, что $\nu(k) = n-1$. В силу (2) и леммы 1.2 каждый элемент порядка s содержится в максимальном торе T порядка $\frac{1}{(n,q+1)}(q^{n-1} - (-1)^{n-1})$. Имеем $(q^{n-1} - (-1)^{n-1}) = (q+1)(q^{n-2} - q^{n-3} + \ldots + (-1)^{n-3}q + (-1)^{n-2})$ и $(q^{n-2} - q^{n-3} + \ldots + (-1)^{n-3}q + (-1)^{n-2})_r = 1$. Следовательно, r не делит $|T|$ тогда и только тогда, когда $(q+1)_r \leqslant n_r$, и мы получаем условие 2 предложения. $\square$

Предложение 4.3. *Пусть $G = B_n(q)$ или $G = C_n(q)$ — конечная простая группа лиева типа над полем нечетной характеристики p. Пусть r — нечетный простой делитель числа $|G|$, $r \neq p$ и $k = e(r,q)$. Тогда числа 2 и r несмежны в том и только в том случае, когда $\eta(k) = n$ и выполняется одно из следующих утверждений:*

1. *n нечетно и $k = (3 - e(2,q))n$.*

2. *n четно и $k = 2n$.*

Функция $\eta(m)$ определена в предложении 2.3.

Доказательство. Если $\eta(k) \leqslant n-1$, то по лемме 1.2 найдется максимальный тор T порядка $\frac{1}{2}(q^{\eta(k)}+(-1)^k)(q-1)^{n-\eta(k)}$. Тор T — абелева подгруппа группы G и оба числа 2 и r делят $|T|$. Значит, T содержит элемент порядка $2r$ и числа $2, r$ смежны.

Таким образом, мы можем полагать, что $\eta(k)=n$. В силу (4) и леммы 1.2 каждый элемент g порядка r содержится в максимальном торе T порядка $\frac{1}{2}(q^n+(-1)^k)$. Следовательно, 2 и r несмежны тогда и только тогда, когда 2 не делит $|T|$, и предложение доказано. □

Предложение 4.4. *Пусть $G=D_n^{\varepsilon}(q)$ — конечная простая группа лиева типа над полем нечетной характеристики p. Пусть r — нечетный простой делитель числа $|G|$, $r \neq p$ и $k=e(r,q)$. Тогда числа 2 и r несмежны в том и только в том случае, когда выполняется одно из следующих утверждений*:

1. $\eta(k)=n$ *и* $(4, q^n-\varepsilon 1)=(q^n-\varepsilon 1)_2$.
2. $\eta(k)=k=n-1$, *n четно, $\varepsilon=+$, и* $e(2,q)=2$.
3. $\eta(k)=\frac{k}{2}=n-1$, *$\varepsilon=+$ и* $e(2,q)=1$.
4. $\eta(k)=\frac{k}{2}=n-1$, *n нечетно, $\varepsilon=-$, и* $e(2,q)=2$.

Функция $\eta(m)$ определена в предложении 2.3.

Доказательство. Вначале заметим, что если $\eta(k) \leqslant n-2$, то по лемме 1.2 найдется максимальный тор T порядка $\frac{1}{(4,q^n-\varepsilon 1)}(q^{\eta(k)}+(-1)^k)(q+(-\varepsilon 1)^k)(q-1)^{n-\eta(k)-1}$. Оба числа $2, r$ делят $|T|$, откуда $2, r$ смежны.

Теперь рассмотрим случай $G={}^2D_n(q)$ (т. е. $\varepsilon=-$). Если $\eta(k)=n-1$, то в силу (4) и леммы 1.2 каждый элемент порядка r содержится в максимальном торе T порядка $\frac{1}{(4,q^n+1)}(q^{n-1}+(-1)^k)(q-(-1)^k)$. Тогда 2 не делит $|T|$ в том и только в том случае, когда выполняется условие 4 предложения. Если $\eta(k)=n$, то в силу (4) и леммы 1.2 каждый элемент порядка r содержится в максимальном торе T порядка $\frac{1}{(4,q^n+1)}(q^n+1)$ (в частности, $k=2\eta(k)$). Тогда 2 не делит $|T|$ в том и только в том случае, когда $(4,q^n+1)=(q^n+1)_2$, и предложение для скрученных групп доказано.

Предположим теперь, что $G=D_n(q)$. Если $\eta(k)=n-1$, то в силу (4) и леммы 1.2 получаем, что каждый элемент порядка r содержится в максимальном торе T порядка $\frac{1}{(4,q^n-1)}(q^{n-1}+(-1)^k)(q+(-1)^k)$ и $k=n-1$, если k нечетно. Тогда 2 не делит $|T|$ в том и только в том случае, когда выполняются условие 2 или условие 3 предложения. Если $\eta(k)=n$, то n нечетно и в силу (4) и леммы 1.2 каждый элемент порядка r содержится в максимальном торе T порядка $\frac{1}{(4,q^n-1)}(q^n-1)$. Ясно, что 2 не делит $|T|$ в том и только в том случае, когда $(4,q^n-1)=(q^n-1)_2$, и предложение доказано. □

Предложение 4.5. *Пусть G — конечная простая исключительная группа лиева типа над полем нечетной характеристики p. Пусть r — нечетный простой делитель числа $|G|$, $r \neq p$ и $k=e(r,q)$. Тогда числа 2 и r несмежны в том и только в том случае, когда выполняется одно из следующих утверждений*:

1. $G=G_2(q)$, $k \in \{3,6\}$.

2. $G = F_4(q)$, $k = 12$.

3. $G = E_6(q)$, $k \in \{9, 12\}$.

4. $G = {}^2E_6(q)$, $k \in \{12, 18\}$.

5. $G = E_7(q)$, *и либо* $k \in \{7, 9\}$ *и* $e(2, q) = 2$, *либо* $k \in \{14, 18\}$ *и* $e(2, q) = 1$.

6. $G = E_8(q)$, $k \in \{15, 20, 24, 30\}$.

7. $G = {}^3D_4(q)$, $k = 12$.

8. $G = {}^2G_2(3^{2n+1})$, *и* r *делит* $m_3(G, n)$ *или* $m_4(G, n)$, *где* $m_i(G, n)$ *определены в лемме* 1.5.

Доказательство. Предложение прямо вытекает из лемм 1.3 и 1.5. □

5 О связи между свойствами графа простых чисел $GK(G)$ и структурой группы G

Пусть $GK(G)$ — граф простых чисел конечной группы G. Очевидно, что спектр $\omega(G)$ однозначно определяет структуру $GK(G)$. Обозначим через $s(G)$ число компонент связности графа $GK(G)$ и через $\pi_i(G)$, $i = 1, \ldots, s(G)$, его i-ю связную компоненту. Если G имеет четный порядок, то положим $2 \in \pi_1(G)$. Обозначим через $\omega_i(G)$ множество чисел $n \in \omega(G)$ таких, что каждый простой делитель числа n принадлежит $\pi_i(G)$.

Грюнберг и Кегель получили следующее описание конечных групп с несвязным графом простых чисел.

Теорема 5.1. (теорема Грюнберга — Кегеля) (см. [1]) *Если* G *— конечная группа с несвязным графом* $GK(G)$, *то выполняется одно из следующих утверждений*:

(a) $s(G) = 2$, *и* G *— группа Фробениуса*;

(b) $s(G) = 2$, *и* G *— двойная группа Фробениуса, т. е.* $G = ABC$, *где* A, AB *— нормальные подгруппы группы* G; AB, BC *— группы Фробениуса с ядрами* A, B *и дополнениями* B, C *соответственно*;

(c) *существует неабелева простая группа* S *такая, что* $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, *где* K *— максимальная нормальная разрешимая подгруппа группы* G. *Кроме того,* K *и* $\overline{G}/S$ *являются* $\pi_1(G)$*-подгруппами, граф* $GK(S)$ *несвязен,* $s(S) \geqslant s(G)$, *и для каждого* i, $2 \leqslant i \leqslant s(G)$, *найдется* j, $2 \leqslant j \leqslant s(S)$, *такое, что* $\omega_i(G) = \omega_j(S)$.

Вместе с классификацией конечных простых групп с несвязным графом простых чисел, полученной Уильямсом и Кондратьевым (см. [1] и [2]), теорема Грюнберга — Кегеля имела целый ряд важных следствий (см., например, [1, теоремы 3–6] и [2, теоремы 2–3]). В последние годы эта теорема используется для доказательства распознаваемости конечных групп по спектру (подробнее см. [3] и [4]).

Доказательство теоремы Грюнберга — Кегеля существенно использует тот факт, что в группе G (если ее порядок четен) найдется элемент нечетного порядка, несвязанный в $GK(G)$ с простым числом 2. Оказывается, что требование несвязности графа простых чисел $GK(G)$ в большинстве случаев может быть успешно заменено более слабым требованием несмежности числа 2 с хотя бы одним нечетным простым числом.

Обозначим через $t(G)$ наибольшее число простых делителей порядка группы G, попарно несмежных в $GK(G)$. Другими словами, $t(G)$ — наибольшее число вершин в независимых множествах графа $GK(G)$ (множество вершин графа называется *независимым*, если его элементы попарно несмежны). В теории графов это число принято называть *числом вершинной независимости* или *неплотностью* графа. По аналогии мы обозначим через $t(r,G)$ наибольшее число вершин в независимых множествах графа $GK(G)$, содержащих простое число r. Мы назовем это число *r-неплотностью.*

Теорема 5.2. (см. [4]) *Пусть G — конечная группа, удовлетворяющая двум условиям*:

(а) *существует три простых числа из $\pi(G)$, попарно несмежных в $GK(G)$, т. е. $t(G) \geqslant 3$;*

(б) *существует нечетное простое число из $\pi(G)$, несмежное в $GK(G)$ с числом 2, т. е. $t(2,G) \geqslant 2$.*

Тогда существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, $t(S) \geqslant t(G)-1$, и выполняется одно из следующих утверждений:

(1) *$S \simeq Alt_7$ или $A_1(q)$ для некоторого нечетного числа q и $t(S) = t(2,S) = 3$.*

(2) *Для каждого простого числа $r \in \pi(G)$, несмежного с 2 в $GK(G)$, силовская r-подгруппа группы G изоморфна силовской r-подгруппе группы S. В частности, $t(2,S) \geqslant t(2,G)$.*

Заметим, что условие (а) теоремы 5.2 влечет неразрешимость группы G и из теоремы Фейта — Томпсона следует, что G имеет четный порядок. Более того, условие (а) может быть заменено на более слабое условие неразрешимости группы G (см. [4, предложения 2–3]). Вместе с [18, теорема 2] теорема 5.2 влечет следующее утверждение.

Теорема 5.3. (см. [4, предложение 4]) *Пусть L — конечная простая группа с $t(2,L) \geqslant 2$, неизоморфная группам $A_2(3)$, ${}^2A_3(3)$, $C_2(3)$ и Alt_{10}. Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда для группы G имеет место заключение теоремы 5.2. В частности, G имеет единственный неабелев композиционный фактор.*

На самом деле, указанные результаты (теорема 5.2 и теорема 5.3) стали стимулом для настоящей работы. В параграфе 6, используя результаты параграфов 1–4, мы вычисляем значения неплотности и 2-неплотности для всех конечных неабелевых простых групп. Кроме того, для каждой конечной неабелевой простой группы лиева типа над полем характеристики p, мы также определяем p-неплотность $t(p,G)$.

6 Неплотность

Для конечной группы G обозначим через $\rho(G)$ (через $\rho(r,G)$) некоторое независимое множество в $GK(G)$ (содержащее r) с наибольшим числом вершин. Таким образом,

$|\rho(G)| = t(G)$ и $|\rho(r,G)| = t(r,G)$. Для данной конечной неабелевой простой группы мы укажем некоторые множества $\rho(G)$ и $\rho(2,G)$ (очевидно, они могут быть определены неоднозначно) и, следовательно, определим $t(G)$ и $t(2,G)$.

Предложение 6.1. *Пусть G — спорадическая группа. Тогда $\rho(G)$, $t(G)$, $\rho(2,G)$ и $t(2,G)$ перечислены в таблице 2. Кроме того, множество $\rho(2,G)$ определено однозначно.*

Доказательство. Результат несложно получить, используя [5] или [6]. □

Теперь мы займемся знакопеременными группами.

Предложение 6.2. *Пусть $G = Alt_n$ — знакопеременная группа степени $n \geqslant 5$. Пусть s'_n — наибольшее простое число, не превосходящее $n/2$, и s''_n — наименьшее простое число, большее чем $n/2$. Обозначим через $\tau(n)$ множество $\{s \mid s$ — простое число, $n/2 < s \leqslant n\}$ и через $\tau(2,n)$ множество $\{s \mid s$ — простое число, $n-3 \leqslant s \leqslant n\}$. Тогда $\rho(G)$, $t(G)$, $\rho(2,G)$ и $t(2,G)$ перечислены в таблице 3. Кроме того, множество $\rho(2,G)$ определено однозначно.*

Доказательство. Результат сразу следует из предложения 1.1. □

Теперь мы рассмотрим группы лиева типа. Поскольку задача в этом случае существенно сложнее, мы разделим процесс ее решения на несколько естественных этапов. Основными техническими средствами будут леммы 1.4 и 1.5 и наши результаты из параграфов 2–4. Напомним, что для данного натурального числа q мы обозначаем через r_n некоторый примитивный простой делитель числа q^n-1 (если он существует). Заметим, что примитивный простой делитель r_{2m} числа $q^{2m}-1$ делит q^m+1 и не делит q^k+1 для каждого натурального числа $k < m$. Полезно также напомнить, что для простых чисел r, s равенство $r^n = s^k+1$ возможно лишь в следующих случаях: либо $r^n = 9$, $s^k = 8$; либо $r = 2^k+1$ — простое число Ферма и $n = 1$; либо $s = 2^n-1$ — простое число Мерсенна и $k = 1$ (как и лемма 1.4, этот факт — следствие теоремы Жигмонди [16]).

Поскольку рассуждения в ситуации, когда 2 является характеристикой поля определения, подходят для любой характеристики p, мы начнем с определения $t(p,G)$.

Предложение 6.3. *Пусть G — конечная простая группа лиева типа над полем характеристики p и порядка q. Тогда $\rho(p,G)$ и $t(p,G)$ перечислены в таблице 4 для классических групп и таблице 5 для исключительных групп.*

Доказательство. (1) $G = A^{\varepsilon}_{n-1}(q)$.

Пусть $G = A_1(q)$. Поскольку группы $A_1(2)$ и $A_1(3)$ не просты, мы можем полагать, что $q > 3$. По лемме 1.4 существуют примитивные простые делители r_1 и r_2 чисел $q-1$ и $q+1$. Они несмежны между собой в $GK(G)$. В силу предложения 3.1 они несмежны с p. Значит, $\rho(p,G) = \{p, r_1, r_2\}$.

Предположим, что $n > 2$. Для того, чтобы рассматривать группы $A_{n-1}(q)$ и ${}^2A_{n-1}(q)$ одновременно, мы определим новую функцию:

$$\nu_{\varepsilon}(m) = \begin{cases} m & \text{, если либо } \varepsilon = +, \text{ либо } \varepsilon = - \text{ и } m \equiv 0 (\mathrm{mod}\ 4), \\ \frac{m}{2} & \text{, если } \varepsilon = - \text{ и } m \equiv 2 (\mathrm{mod}\ 4), \\ 2m & \text{, если } \varepsilon = - \text{ и } m \equiv 1 (\mathrm{mod}\ 2). \end{cases}$$

Очевидно, что $\nu_\varepsilon(m)$ — тождественное отображение, если $\varepsilon = +$, и $\nu_\varepsilon(m) = \nu(m)$, если $\varepsilon = -$. Несложно проверить, что ν_ε есть биекция на $\mathbb{N}$, и таким образом, функция ν_ε^{-1} корректно определена.

Пусть $n = 3$ и $G = A_2^\varepsilon(q)$. Тогда из предложения 3.1 следует, что $r_{\nu_\varepsilon^{-1}(2)}$ и $r_{\nu_\varepsilon^{-1}(3)}$ несмежны с числом p. Более того, если $(q-\varepsilon 1)_3 = 3$, то в силу предложения 3.1, число 3 несмежно с p, и в силу предложений 4.1 и 4.2 в этом случае 3 несмежно с $r_{\nu_\varepsilon^{-1}(2)}$ и $r_{\nu_\varepsilon^{-1}(3)}$. По лемме 1.4 $r_{\nu_\varepsilon^{-1}(3)}$ существует для всех q, исключая случай, когда $\varepsilon = -$ и $q = 2$. Но группа ${}^2A_2(2)$ не проста и мы ее не рассматриваем. Следовательно, в нашем случае $r_{\nu_\varepsilon^{-1}(3)}$ существует для всех простых групп. Если существует нечетный примитивный делитель $r_{\nu_{\varepsilon^{-1}(2)}}$, то он не связан с характеристикой и выполнена одна из первых двух возможностей среди четырех, приведенных ниже. Если единственный примитивный делитель $r_{\nu_{\varepsilon^{-1}(2)}}$ равен 2, то $q + \varepsilon 1$ является степенью числа 2, т. е. является простым числом Мерсенна в случае $\varepsilon = +$ и является простым числом Ферма или числом 9 в случае $\varepsilon = -$. Ввиду предложения 3.1 число 2 смежно с характеристикой, поэтому выполнена одна из последних двух возможностей среди четырех, приведенных ниже. Таким образом, имеем

$$\rho(p,G) = \begin{cases} \{p, 3, r_{\nu_\varepsilon^{-1}(2)}, r_{\nu_\varepsilon^{-1}(3)}\}, & \text{если } (q-\varepsilon 1)_3 = 3 \text{ и } q+\varepsilon \neq 2^k; \\ \{p, r_{\nu_\varepsilon^{-1}(2)}, r_{\nu_\varepsilon^{-1}(3)}\}, & \text{если } (q-\varepsilon 1)_3 \neq 3 \text{ и } q+\varepsilon \neq 2^k; \\ \{p, 3, r_{\nu_\varepsilon^{-1}(3)}\}, & \text{если } (q-\varepsilon 1)_3 = 3 \text{ и } q+\varepsilon = 2^k; \\ \{p, r_{\nu_\varepsilon^{-1}(3)}\}, & \text{если } (q-\varepsilon 1)_3 \neq 3 \text{ и } q+\varepsilon = 2^k. \end{cases}$$

Заметим, что мы избегаем использования функций $e(r,q)$ и ν_ε в таблицах в параграфе 8.

Пусть $G = A_4(2), A_5(2)$ или ${}^2A_3(2)$. Поскольку число $2^6 - 1$ не имеет примитивных простых делителей, то в силу предложения 3.1 выполняется $\rho(2, A_5(2)) = \{2, 31\}$, $\rho(2, A_6(2)) = \{2, 127\}$ и $\rho(2, {}^2A_3(2)) = \{2, 5\}$.

Во всех остальных случаях по лемме 1.4 найдутся примитивные простые делители $r_{\nu_\varepsilon^{-1}(n-1)}$ и $r_{\nu_\varepsilon^{-1}(n)}$. В силу леммы 1.2 имеем $r_{\nu_\varepsilon^{-1}(n-1)}, r_{\nu_\varepsilon^{-1}(n)} \in \pi(G)$. По предложениям 2.1 и 2.2 эти делители несмежны в $GK(G)$. Теперь в силу предложения 3.1 для группы $G = A_{n-1}^\varepsilon(q)$ выполняется $\rho(p,G) = \{p, r_{\nu_\varepsilon^{-1}(n-1)}, r_{\nu_\varepsilon^{-1}(n)}\}$.

(2) $G = C_n(q)$ or $B_n(q)$.

Из предложения 2.3, предложения 3.1 и предложения 4.3 следует, что графы простых чисел групп $C_n(q)$ и $B_n(q)$ совпадают. Поэтому мы рассмотрим эти группы одновременно и, для краткости, будем использовать символ $C_n(q)$ в обоих случаях.

Пусть $G = C_3(2)$. Поскольку не существует простых чисел r, удовлетворяющих условию $e(r,2) = 6$, только 7, как примитивный простой делитель числа $2^3 - 1$ несмежен с 2.

Пусть $G = C_n(q)$, $n \geqslant 2$ и $(n,q) \neq (3,2)$. Если n четно, то по предложению 3.1 только примитивные простые делители числа $q^n + 1$ несмежны с p. Таким образом, в этом случае $\rho(G) = \{p, r_{2n}\}$. Если n нечетно, предложения 2.3 и 3.1 показывают, что $\rho(G) = \{p, r_n, r_{2n}\}$.

(3) $G = D_n^\varepsilon(q)$.

С учетом хорошо известных изоморфизмов между группами малых лиевых рангов мы можем полагать, что $n \geqslant 4$. Пусть $n = 4$ и $q = 2$. Поскольку $2^6 - 1$ не имеет примитивных простых делителей, только число 7, как примитивный простой делитель числа 2^3-1, несмежно с 2 в случае $G=D_4(2)$, и лишь 7 и 17, как примитивные делители чисел 2^3-1 и 2^8-1 несмежны с 2 в случае $G={}^2D_4(2)$. Все остальные случаи могут быть легко описаны в прямом соответствии с предложением 2.4 и предложением 3.1. Результаты этого описания можно увидеть в таблице 4.

(4) Результат для исключительных групп, отличных от групп Сузуки и Ри, может быть получен с использованием предложения 2.5, предложения 3.2 и леммы 1.4.

(5) G — конечная группа Сузуки или Ри.

Пусть $G={}^2B_2(2^{2m+1})$, и s_i — простой делитель числа $m_i(B,n)$, где $i=1,2,3$ (см. лемму 1.5). В силу предложения 2.6 простые числа s_i и s_j смежны тогда и только тогда, когда $i=j$. С другой стороны, каждый s_i, где $i=1,2,3$, несмежен с $p=2$. Таким образом, $\rho(p,G)=\{p,s_1,s_2,s_3\}$ и $t(p,G)=4$ в этом случае. Аналогичные рассуждения можно применить к группам Ри и простым делителям чисел $m_i(G,n)$ и $m_i(F,n)$. □

В общем случае, примитивный простой делитель r_m числа q^m-1 может быть выбран несколькими способами. Таким образом, для конечной простой группы G лиева типа множество $\rho(p,G)$ может быть определено неоднозначно. Однако, оказывается, что значения $e(r,q)$ для всех примитивных простых делителей r из $\rho(p,G)$ являются инвариантами для данной группы G лиева типа.

Предложение 6.4. *Пусть G — конечная простая группа лиева типа над полем характеристики p и порядка q. Предположим, что G неизоморфна группам ${}^2B_2(q)$, ${}^2G_2(q)$, ${}^2F_4(2)'$ и ${}^2F_4(q)$. Пусть $\rho(p,G)=\{p,s_1,s_2,\dots,s_m\}$ — независимое множество в $GK(G)$, содержащее p, с наибольшим числом вершин и $k_i=e(s_i,q)$. Тогда множество $\{k_1,\dots,k_m\}$ определено однозначно.*

Доказательство. Это следует из результатов параграфов 2–4. □

Если мы заменим примитивные простые делители на делители чисел, определенных в лемме 1.5, то получим аналогичное утверждение для групп Сузуки и Ри.

Предложение 6.5. *Пусть G — конечная простая группа Сузуки или группа Ри над полем характеристики p. Пусть $\rho(p,G)=\{p,s_1,\dots,s_k\}$.*

1. *Если $G={}^2B_2(2^{2n+1})$, то с точностью до перенумерации s_i делят $m_i(B,n)$. В частности, $k=3$.*

2. *Если $G={}^2G_2(3^{2n+1})$, то все s_i нечетны и с точностью до перенумерации s_i делят $m_i(G,n)$. В частности, $k=4$.*

3. *Если $G={}^2F_4(2^{2n+1})$, то с точностью до перенумерации s_i делят $m_{i+2}(F,n)$ и $s_1\neq 3$. В частности, $k=3$.*

Числа $m_i(B,n)$, $m_i(G,n)$ и $m_i(F,n)$ определены в лемме 1.5.

Теперь мы определим $t(2,G)$. Очевидно, что для группы лиева типа над полем четной характеристики p-неплотность и 2-неплотность совпадают. Таким образом, мы можем полагать, что G определена над полем нечетной характеристики.

Предложение 6.6. *Пусть G — конечная простая группа лиева типа над полем нечетной характеристики p и порядка q. Тогда $\rho(2,G)$ и $t(2,G)$ перечислены в таблице 6 для классических групп и в таблице 7 для исключительных групп.*

Доказательство. (1) $G = A^{\varepsilon}_{n-1}(q)$.

Пусть $G = A_1(q)$ и $q > 3$. Поскольку q нечетно, каждый простой делитель $r \neq p$ числа $|G|$ делит $(q-1)/2$ или $(q+1)/2$. Если $e(2,q) = 1$, то 2 несмежно некоторому простому делителю r_2 числа $(q+1)/2$ и $\tau(G) = \{2, p, r_2\}$. Если $e(2,q) = 2$, то 2 несмежно некоторому делителю r_1 числа $(q-1)/2$ и $\tau(G) = \{2, p, r_1\}$.

Пусть $G = A^{\varepsilon}_{n-1}(q)$ и $n \geqslant 3$. Если $(q-\varepsilon 1)_2 < n_2$, то в силу предложений 4.1 и 4.2 только примитивный простой делитель $r_{\nu_\varepsilon^{-1}(n-1)}$ несмежен с 2. Заметим, что в этом случае $n_2 \geqslant 4$, поскольку для $n_2 \leqslant 2$ неравенство $(q-\varepsilon 1)_2 < n_2$ невозможно. По лемме 1.4 примитивный простой делитель $r_{\nu_\varepsilon^{-1}(n-1)}$ всегда существует. Таким образом, $\rho(2,G) = \{2, r_{\nu_\varepsilon^{-1}(n-1)}\}$.

Если $(q-\varepsilon 1)_2 > n_2$ или $(q-\varepsilon 1)_2 = n_2 = 2$, то в силу предложений 4.1 и 4.2 каждый примитивный простой делитель $r_{\nu_\varepsilon^{-1}(n)}$ несмежен с 2. Следовательно, $\rho(2,G) = \{2, r_{\nu_\varepsilon^{-1}(n)}\}$.

Наконец, пусть $(q-\varepsilon 1)_2 = n_2 > 2$. В силу предложений 4.1 и 4.2 только примитивные простые делители $r_{\nu_\varepsilon^{-1}(n-1)}$ и $r_{\nu_\varepsilon^{-1}(n)}$ несмежны с 2. С другой стороны, в силу предложений 2.1 и 2.2 простые числа $r_{\nu_\varepsilon^{-1}(n-1)}$ и $r_{\nu_\varepsilon^{-1}(n)}$ несмежны между собой. Таким образом, $\rho(2,G) = \{2, r_{\nu_\varepsilon^{-1}(n-1)}, r_{\nu_\varepsilon^{-1}(n)}\}$.

(2) $G = C_n(q)$ или $B_n(q)$.

Результаты таблицы прямо следуют из предложения 4.3.

(3) $G = D^{\varepsilon}_n(q)$.

Результаты вновь являются прямым следствием предложения 4.4. Заметим, что равенство $t(2,G) = 2$ имеет место для большинства групп типа D_n над полями нечетного порядка. Исключения следующие: n нечетно и $q \equiv 5 (\mathrm{mod}\ 8)$ для $G = D_n(q)$, и $q \equiv 3 (\mathrm{mod}\ 8)$ для $G = {}^2D_n(q)$.

(4) Теперь, чтобы завершить доказательство предложения, можно воспользоваться предложением 4.5, а также леммой 1.5 для групп Сузуки и Ри и леммой 1.4 для остальных исключительных групп. ☐

Рассмотрим теперь вопрос о единственности множества $\rho(2,G)$. Ситуация здесь очень похожа на ситуацию с $\rho(p,G)$.

Предложение 6.7. *Пусть G — конечная простая группа лиева типа над полем нечетной характеристики p и порядка q. Предположим, что G неизоморфна группам $A_1(q)$ и ${}^2G_2(q)$. Пусть $\rho(2,G) = \{2, s_1, s_2, \ldots, s_m\}$ — независимое множество в $GK(G)$, содержащее 2, с наибольшим число вершин и $k_i = e(s_i, q)$. Тогда $\{k_1, \ldots, k_m\}$ определены однозначно.*

Доказательство. Это следует из результатов параграфов 2–4. ☐

Предложение 6.8. *Пусть G — либо группа $A_1(q)$, где q нечетно, либо группа ${}^2G_2(3^{2n+1})$, и пусть $\rho(2,G) = \{2, s_1, s_2\}$.*

1. *Если $G = A_1(q)$, q нечетно, то с точностью до перенумерации $s_1 = p$ и $e(s_2, q) = 3 - e(2,q)$.*

2. *Если* $G = {}^2G_2(3^{2n+1})$, *то с точностью до перенумерации* $s_i = m_{i+2}(G, n)$.

Числа $m_i(G, n)$ *определены в лемме* 1.5.

Доказательство. Это следует из результатов параграфов 2–4. $\square$

Наша последняя задача — определить для каждой конечной простой группы G лиева типа некоторое независимое множество $\rho(G)$ в $GK(G)$ с наибольшим числом вершин.

Предложение 6.9. *Пусть G — конечная простая группа лиева типа над полем характеристики p и порядка q. Тогда $\rho(G)$ и $t(G)$ перечислены в таблице* 8 *для классических групп и таблице* 9 *для исключительных групп.*

Доказательство. (1) $G = A^{\varepsilon}_{n-1}(q)$.

Если $G = A_1(q)$ или $G = A^{\varepsilon}_2(q)$, то рассуждая как при доказательстве предложения 6.3, получим $\rho(G) = \rho(p, G)$.

Предположим, что $n = 4$. В силу предложения 6.3 и таблицы 4 имеет место $t(p, G) = 3$ во всех случаях кроме группы ${}^2A_3(2)$. Используя предложение 6.6 и таблицу 6, получаем $t(2, G) \leqslant 3$. Из предложений 4.1 и 4.2 следует, что $t(r_{\nu_\varepsilon^{-1}(1)}, G) \leqslant 3$. Кроме того, имеется не более трех других примитивных делителей $r_{\nu_\varepsilon^{-1}(2)}$, $r_{\nu_\varepsilon^{-1}(3)}$ и $r_{\nu_\varepsilon^{-1}(4)} = r_4$. Поэтому $t(G) = t(p, G) = 3$, исключая случай: $t({}^2A_3(2)) = t(2, {}^2A_3(2)) = 2$.

Пусть $G = A^{\varepsilon}_{n-1}(q)$, $n \geqslant 5$ и $q \neq 2$. По лемме 1.4 найдутся примитивные простые делители $r_{\nu_\varepsilon^{-1}(k)}$ для любого $k > 2$. Обозначим через m число $[n/2]$, т. е. целую часть числа $n/2$. В силу предложений 2.1 и 2.2 множество

$$\rho = \{r_{\nu_\varepsilon^{-1}(m+1)}, r_{\nu_\varepsilon^{-1}(m+2)}, \ldots, r_{\nu_\varepsilon^{-1}(n)}\}$$

является независимым в $GK(G)$. С другой стороны, в силу предложений 2.1, 2.2, 3.1, 4.1 и 4.2 каждые два простых делителя из $\pi\left(q\prod_{i=1}^{m}(q^i - (\varepsilon 1)^i)\right)$ смежны в $GK(G)$. Кроме того, каждый из них смежен по крайней мере с одним числом из ρ. Поскольку каждое простое число $s \in \pi(G) \setminus \left(\rho \cup \pi\left(q\prod_{i=1}^{m}(q^i - (\varepsilon 1)^i)\right)\right)$ имеет вид r_i для некоторого $i > m$, то каждое независимое множество в $GK(G)$, содержащее простой делитель из $\pi\left(q\prod_{i=1}^{m}(q^i - 1)\right)$, содержит не более $|\rho|$ вершин. Таким образом, $\rho(G) = \rho$ и $t(G) = |\rho| = [(n+1)/2]$.

Пусть $q = 2$. Поскольку $\nu_+^{-1}(6) = \nu_-^{-1}(3) = 6$, результаты предыдущего абзаца верны для групп $A_{n-1}(2)$ при $n \geqslant 12$ и групп ${}^2A_{n-1}(2)$ при $n \geqslant 6$. Если $n = 5$ и $\varepsilon = -$, то несложно проверить, что для ${}^2A_4(2)$ имеет место $\rho(G) = \rho(2, G) = \{2, 5, 11\}$ и $t(G) = 3$. Поэтому мы можем считать, что $G = A_{n-1}(2)$. Если $n = 5, 6$, то $\rho(G) = \{r_3, r_4, r_5\} = \{5, 7, 31\}$ и $t(G) = 3$. Если $7 \leqslant n \leqslant 11$, то мы должны исключить делители числа $2^6 - 1$ из $\rho(G)$, а в остальном рассуждать как в предыдущем абзаце. В этом случае $\rho(G) = \{r_i \mid i \neq 6, [n/2] < i \leqslant n\}$ и $t(G) = [(n-1)/2]$.

(2) $G = C_n(q)$ или $B_n(q)$. Напомним, что $GK(C_n(q)) = GK(B_n(q))$, и мы рассмотрим эти группы одновременно.

$G = C_2(q)$, $q > 2$. Поскольку каждые два простых делителя числа $q(q^2 - 1)$ смежны, имеем $\rho(G) = \rho(p, G) = \{p, r_4\}$.

Пусть $n \geqslant 3$ при $q > 2$ и $n \geqslant 7$ при $q = 2$. Определим множество ρ следующим образом:

$$\rho = \{r_{2i} \mid [n+1/2] < i \leqslant n\} \cup \{r_i \mid [n/2] < i \leqslant n, i \equiv 1 (\mathrm{mod}\ 2)\}.$$

Используя результаты параграфов 1–4 и рассуждения как при доказательстве для групп $A^{\varepsilon}_{n-1}(q)$, получаем, что $\rho(G) = \rho$ и, как легко проверить, $t(G) = [(3n+5)/4]$.

Если $q = 2$ и $3 \leqslant n \leqslant 5$, то все рассуждения остаются такими же, но требуется исключить из ρ делители вида r_6. Таким образом, в этом случае $t(G) = [(3n+1)/4]$. Наконец, если $(n, q) = (6, 2)$, мы должны исключить из ρ делитель типа r_6, но вместо него можно добавить примитивный простой делитель 7 числа $2^3 - 1$. Таким образом, $t(G) = [(3n+5)/4]$ как и в общем случае.

(3) $G = D^{\varepsilon}_n(q)$.

Мы рассуждаем как в двух предыдущих частях доказательства. Используя предложение 2.4, получаем множество $\rho(G)$ в общей ситуации, а затем рассматриваем исключения, возникающие из-за исключения в лемме 1.4.

(4) Мы получаем результаты для исключительных групп, используя предложения 2.5 и 2.6, таблицы 5 и 6, а также леммы 1.4 и 1.5. □

7 Приложения

В этом параграфе мы применим наши результаты в духе параграфа 5. Прежде всего наши исследования показывают, что условие $t(2, G) > 1$ реализуется для очень широкого класса конечных простых групп.

Теорема 7.1. *Пусть G — конечная неабелева простая группа, удовлетворяющая условию $t(2, G) = 1$, тогда G — знакопеременная группа Alt_n, где n таково, что $\tau(2, n) = \{s \mid s$ — простое число, $n - 3 \leqslant s \leqslant n\} = \varnothing$.*

Доказательство. См. предложения 6.1–6.9 и соответствующие таблицы в параграфе 8. □

Таким образом, мы можем применить результаты теорем 5.2 и 5.3 следующим образом.

Следствие 7.2. *Пусть L — конечная неабелева простая группа, отличная от групп $A_2(3)$, ${}^2A_3(3)$, $C_2(3)$, Alt_{10} и групп Alt_n с условием $\tau(2, n) = \varnothing$. Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, $t(S) \geqslant t(G) - 1$ и выполняется одно из следующих утверждений:*

(1) $S \simeq Alt_7$ или $A_1(q)$ для некоторого нечетного q и $t(S) = t(2, S) = 3$.

(2) Для каждого простого числа $r \in \pi(G)$, несмежного в $GK(G)$ с числом 2, силовская r-подгруппа группы G изоморфна силовской r-подгруппе группы S. В частности, $t(2, S) \geqslant t(2, G)$.

Доказательство. Это прямое следствие теоремы 5.3 и теоремы 7.1. □

Если G является одной из групп: $A_2(3)$, ${}^2A_3(3)$, $C_2(3)$, Alt_{10}, то $t(2, G) \geqslant 2$ и выполняется также

Следствие 7.3. *Пусть L — конечная простая группа, отличная от групп Alt_n с условием $\tau(2, n) = \varnothing$. Пусть G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда G имеет не более одного неабелева композиционного фактора.*

Для произвольного подмножества ω множества $\mathbb{N}$ натуральных чисел обозначим через $h(\omega)$ число попарно неизоморфных конечных групп G таких, что $\omega(G) = \omega$. Мы будем говорить, что для конечной группы G *проблема распознаваемости решена*, если мы знаем значение $h(\omega(G))$ (для краткости, $h(G)$). В частности, группа G называется *распознаваемой по спектру* (кратко, распознаваемой), если $h(G) = 1$. В последние двадцать лет проблема распознаваемости была решена для многих конечных неабелевых простых и почти простых групп (обзор результатов в этой области см. в [3]). Но большинство таких групп имеют несвязный граф простых чисел, поскольку теорема Грюнберга — Кегеля и классификация конечных простых групп с несвязным графом простых чисел, полученная Уильямсом и Кондратьевым, являлись важной частью доказательства. Основной результат из [4] (теорема 5.2 здесь) и результаты настоящей работы дают возможность работать с группами, граф простых чисел которых связен. Конечная неабелева простая группа L называется *квазираспознаваемой по спектру*, если каждая конечная группа с тем же спектром имеет ровно один неабелев композиционный фактор S и S изоморфен L. Таким образом, исследование квазираспознаваемости является важным шагом при определении, является ли данная группа распознаваемой по спектру. В [4] первый автор дал набросок доказательства следующего утверждения.

Теорема 7.4. ([4, предложение 5]) *Пусть $L = {}^2D_n(q)$, $q = 2^k$, k, n — натуральные числа, n четно и $n \geqslant 16$. Тогда L квазираспознаваема по спектру.*

Фактически, этот результат был доказан по модулю результатов параграфа 6 настоящей работы. Таким образом, теперь он полностью доказан.

Теперь мы хотели бы выделить одно утверждение, упомянутое нами ранее.

Предложение 7.5. *Пусть $G = B_n(q)$ и $H = C_n(q)$. Тогда графы простых чисел $GK(G)$ и $GK(H)$ совпадают.*

Доказательство. Это следует из результатов параграфов 2–4. □

В заключение мы упомянем один недавно опубликованный результат о графах простых чисел конечных групп. Напомним, что множество вершин графа называется кликой, если все вершины из этого множества попарно смежны. В [18, теорема 1] Лучидо и Могхаддамфар описали все конечные неабелевы простые группы, компоненты связности графов простых чисел которых образуют клики. Мы проверили их список таких групп, используя результаты настоящей работы. К сожалению, в списке содержатся некоторые неточности. На самом деле, для групп $G = A_2^{\varepsilon}(q)$, где $q = 2^k - \varepsilon 1$ и $(q - \varepsilon 1)_3 = 3$, имеет место $3, p \in \pi_1(G)$ и $3p \notin \omega(G)$. Поэтому компонента связности $\pi_1(G)$ не является кликой для этих групп, что противоречит утверждению теоремы 1 в [18]. Ниже в следствии 7.6 мы даем уточненный список рассматриваемых групп.

Следствие 7.6. *Пусть G — конечная неабелева простая группа и все связные компоненты ее простого графа $GK(G)$ являются кликами. Тогда G — одна из следующих групп*:

1. *Спорадические группы M_{11}, M_{22}, J_1, J_2, J_3, HiS.*

2. *Знакопеременные группы Alt_n, где $n = 5, 6, 7, 9, 12, 13$.*

3. *Группы лиева типа $A_1(q)$, где $q > 3$; $A_2(4)$; $A_2(q)$, где $(q-1)_3 \neq 3$, $q+1 = 2^k$; ${}^2A_3(3)$; ${}^2A_5(2)$; ${}^2A_2(q)$, где $(q+1)_3 \neq 3$, $q-1 = 2^k$; $C_3(2)$, $C_2(q)$, где $q > 2$; $D_4(2)$; ${}^3D_4(2)$; ${}^2B_2(q)$, где $q = 2^{2k+1}$; $G_2(q)$, где $q = 3^k$.*

Доказательство. Все связные компоненты графа простых чисел $GK(G)$ конечной группы G являются кликами тогда и только тогда, когда число $s(G)$ компонент равно неплотности $t(G)$ графа $GK(G)$. Для каждой конечной неабелевой простой группы значения $s(G)$ и $t(G)$ теперь известны. Таким образом, используя таблицы 2a–2c из [3] для значений $s(G)$ и таблицы 2–9 из параграфа 8 настоящей работы для $t(G)$, получаем результат следствия. $\square$

8 Таблицы

В нижеследующих таблицах предполагается, что n, k — натуральные числа. Через $[x]$ обозначается целая часть числа x. Для конечной группы G мы обозначаем через $\rho(G)$ (через $\rho(r, G)$) некоторое независимое множество в $GK(G)$ (содержащее r) с наибольшим числом вершин и полагаем, что $t(G) = |\rho(G)|$, $t(r, G) = |\rho(r, G)|$. В таблице 3 через $\tau(n)$ обозначено множество $\{s \mid s$ — простое число, $n/2 < s \leqslant n\}$, а через $\tau(2, n)$ — множество $\{s \mid s$ — простое число, $n - 3 \leqslant s \leqslant n\}$. Через s'_n обозначено наибольшее простое число, не превосходящее $n/2$, а через s''_n — наименьшее простое число, большее чем $n/2$. В таблицах 4–9 предполагается, что G — конечная неабелева простая группа лиева типа над полем характеристики p и порядка q. Через r_m обозначается примитивный простой делитель числа $q^m - 1$. Если p нечетно, то мы говорим, что 2 является примитивным простым делителем числа $q - 1$, если $q \equiv 1 (\mathrm{mod}\ 4)$, и примитивным делителем числа $q^2 - 1$, если $q \equiv -1 (\mathrm{mod}\ 4)$.

Таблица 2. Спорадические группы

G	$t(G)$	$\rho(G)$	$t(2,G)$	$\rho(2,G)$
M_{11}	3	$\{3,5,11\}$	3	$\{2,5,11\}$
M_{12}	3	$\{3,5,11\}$	2	$\{2,11\}$
M_{22}	4	$\{3,5,7,11\}$	4	$\{2,5,7,11\}$
M_{23}	4	$\{3,7,11,23\}$	4	$\{2,5,11,23\}$
M_{24}	4	$\{5,7,11,23\}$	3	$\{2,11,23\}$
J_1	4	$\{5,7,11,19\}$	4	$\{2,7,11,19\}$
J_2	2	$\{5,7\}$	2	$\{2,7\}$
J_3	3	$\{5,17,19\}$	3	$\{2,17,19\}$
J_4	7	$\{7,11,23,29,31,37,43\}$	6	$\{2,23,29,31,37,43\}$
Ru	4	$\{5,7,13,29\}$	2	$\{2,29\}$
He	3	$\{5,7,17\}$	2	$\{2,17\}$
McL	3	$\{5,7,11\}$	2	$\{2,11\}$
HN	3	$\{7,11,19\}$	2	$\{2,19\}$
HiS	3	$\{5,7,11\}$	3	$\{2,7,11\}$
Suz	4	$\{5,7,11,13\}$	3	$\{2,11,13\}$
Co_1	4	$\{7,11,13,23\}$	2	$\{2,23\}$
Co_2	4	$\{5,7,11,23\}$	3	$\{2,11,23\}$
Co_3	4	$\{5,7,11,23\}$	2	$\{2,23\}$
Fi_{22}	4	$\{5,7,11,13\}$	2	$\{2,13\}$
Fi_{23}	5	$\{7,11,13,17,23\}$	3	$\{2,17,23\}$
Fi'_{24}	6	$\{7,11,13,17,23,29\}$	4	$\{2,17,23,29\}$
O'N	5	$\{5,7,11,19,31\}$	4	$\{2,11,19,31\}$
LyS	6	$\{5,7,11,31,37,67\}$	4	$\{2,31,37,67\}$
F_1	11	$\{11,13,17,19,23,29,31,41,47,59,71\}$	5	$\{2,29,41,59,71\}$
F_2	8	$\{7,11,13,17,19,23,31,47\}$	3	$\{2,31,47\}$
F_3	5	$\{5,7,13,19,31\}$	4	$\{2,13,19,31\}$

Таблица 3. Простые знакопеременные группы

G	Условия	$t(G)$	$\rho(G)$	$t(2,G)$	$\rho(2,G)$
Alt_n	$n=5,6$	3	$\{2,3,5\}$	3	$\{2,3,5\}$
	$n=8$	3	$\{2,5,7\}$	3	$\{2,5,7\}$
	$n\geqslant 7$, $s'_n+s''_n>n$	$\lvert\tau(n)\rvert+1$	$\tau(n)\cup\{s'_n\}$	$\lvert\tau(2,n)\rvert+1$	$\tau(2,n)\cup\{2\}$
	$n\geqslant 9$, $s'_n+s''_n\leqslant n$	$\lvert\tau(n)\rvert$	$\tau(n)$	$\lvert\tau(2,n)\rvert+1$	$\tau(2,n)\cup\{2\}$

Таблица 4. p-неплотность для конечных простых классических групп

G	Условия	$t(p,G)$	$\rho(p,G)$
$A_{n-1}(q)$	$n=2$, $q>3$	3	$\{p,r_1,r_2\}$
	$n=3$, $(q-1)_3=3$ и $q+1\neq 2^k$	4	$\{p,3,r_2,r_3\}$
	$n=3$, $(q-1)_3\neq 3$ и $q+1\neq 2^k$	3	$\{p,r_2,r_3\}$
	$n=3$, $(q-1)_3=3$ и $q+1=2^k$	3	$\{p,3,r_3\}$
	$n=3$, $(q-1)_3\neq 3$ и $q+1=2^k$	2	$\{p,r_3\}$
	$n=6$, $q=2$	2	$\{2,31\}$
	$n=7$, $q=2$	2	$\{2,127\}$
	$n>3$ $(n,q)\neq(6,2),(7,2)$	3	$\{p,r_{n-1},r_n\}$
${}^2A_{n-1}(q)$	$n=3$, $q\neq 2$, $(q+1)_3=3$ и $q-1\neq 2^k$	4	$\{p,3,r_1,r_6\}$
	$n=3$, $(q+1)_3\neq 3$ и $q-1\neq 2^k$	3	$\{p,r_1,r_6\}$
	$n=3$, $(q+1)_3=3$ и $q-1=2^k$	3	$\{p,3,r_6\}$
	$n=3$, $(q+1)_3\neq 3$ и $q-1=2^k$	2	$\{p,r_6\}$
	$n=4$, $q=2$	2	$\{2,5\}$
	$n\equiv 0(\mathrm{mod}\ 4)$, $(n,q)\neq(4,2)$	3	$\{p,r_{2n-2},r_n\}$
	$n\equiv 1(\mathrm{mod}\ 4)$	3	$\{p,r_{n-1},r_{2n}\}$
	$n\equiv 2(\mathrm{mod}\ 4)$, $n\neq 2$	3	$\{p,r_{2n-2},r_{n/2}\}$
	$n\equiv 3(\mathrm{mod}\ 4)$, $n\neq 3$	3	$\{p,r_{(n-1)/2},r_{2n}\}$
$B_n(q)$ или $C_n(q)$	$n=3$, $q=2$	2	$\{2,7\}$
	n четно	2	$\{p,r_{2n}\}$
	$n>1$ нечетно, $(n,q)\neq(3,2)$	3	$\{p,r_n,r_{2n}\}$
$D_n(q)$	$n=4$, $q=2$	2	$\{2,7\}$
	$n\equiv 0(\mathrm{mod}\ 2)$, $n\geqslant 4$, $(n,q)\neq(4,2)$	3	$\{p,r_{n-1},r_{2n-2}\}$
	$n\equiv 1(\mathrm{mod}\ 1)$, $n>4$	3	$\{p,r_n,r_{2n-2}\}$
${}^2D_n(q)$	$n=4$, $q=2$	3	$\{2,7,17\}$
	$n\equiv 0(\mathrm{mod}\ 2)$, $n\geqslant 4$, $(n,q)\neq(4,2)$	4	$\{p,r_{n-1},r_{2n-2},r_{2n}\}$
	$n\equiv 1(\mathrm{mod}\ 2)$, $n>4$	3	$\{p,r_{2n-2},r_{2n}\}$

Таблица 5. p-неплотность для конечных простых исключительных групп лиева типа

G	Условия	$t(p,G)$	$\rho(p,G)$
$G_2(q)$	$q>2$	3	$\{p, r_3, r_6\}$
$F_4(q)$	нет	3	$\{p, r_8, r_{12}\}$
$E_6(q)$	нет	4	$\{p, r_8, r_9, r_{12}\}$
${}^2E_6(q)$	нет	4	$\{p, r_8, r_{12}, r_{18}\}$
$E_7(q)$	нет	5	$\{p, r_7, r_9, r_{14}, r_{18}\}$
$E_8(q)$	нет	5	$\{p, r_{15}, r_{20}, r_{24}, r_{30}\}$
${}^3D_4(q)$	нет	2	$\{p, r_{12}\}$
${}^2B_2(2^{2n+1})$	$n \geqslant 1$	4	$\{2, s_1, s_2, s_3\}$, где s_1 делит $2^{2n+1}-1$, s_2 делит $2^{2n+1}-2^{n+1}+1$ s_3 делит $2^{2n+1}+2^{n+1}+1$
${}^2G_2(3^{2n+1})$	$n \geqslant 1$	5	$\{3, s_1, s_2, s_3, s_4\}$, где $s_1 \neq 2$ делит $3^{2n+1}-1$ $s_2 \neq 2$ делит $3^{2n+1}+1$ s_3 делит $3^{2n+1}-3^{n+1}+1$ s_4 делит $3^{2n+1}+3^{n+1}+1$
${}^2F_4(2^{2n+1})$	$n \geqslant 1$	4	$\{2, s_1, s_2, s_3\}$, где $s_1 \neq 3$ и делит $2^{4n+2}-2^{2n+1}+1$ s_2 делит $2^{4n+2}+2^{3n+2}+2^{2n+1}+2^{n+1}+1$ s_3 делит $2^{4n+2}-2^{3n+2}+2^{2n+1}-2^{n+1}+1$
${}^2F_4(2)'$	нет	2	$\{2, 13\}$

Таблица 6. 2-неплотность для конечных простых классических групп характеристики $p \neq 2$

G	Условия	$t(2,G)$	$\rho(2,G)$
$A_{n-1}(q)$	$n = 2$, $q \equiv 1 (\mathrm{mod}\ 4)$	3	$\{2, r_2, p\}$
	$n = 2$, $q \equiv 3 (\mathrm{mod}\ 4)$, $q \neq 3$	3	$\{2, r_1, p\}$
	$n \geqslant 3$ и $n_2 < (q-1)_2$	2	$\{2, r_n\}$
	$n \geqslant 3$ и либо $n_2 > (q-1)_2$,	2	$\{2, r_{n-1}\}$
	либо $n_2 = (q-1)_2 = 2$		
	$2 < n_2 = (q-1)_2$	3	$\{2, r_{n-1}, r_n\}$
$^2A_{n-1}(q)$	$n_2 > (q+1)_2$	2	$\{2, r_{2n-2}\}$
	$n_2 = 1$	2	$\{2, r_{2n}\}$
	$2 < n_2 < (q+1)_2$	2	$\{2, r_n\}$
	$n \geqslant 3$, $2 = n_2 \leqslant (q+1)_2$	2	$\{2, r_{n/2}\}$
	$2 < n_2 = (q+1)_2$	3	$\{2, r_{2n-2}, r_n\}$
$B_n(q)$ или	$n > 1$ нечетно и $(q-1)_2 = 2$	2	$\{2, r_n\}$
$C_n(q)$	n четно или $(q-1)_2 > 2$	2	$\{2, r_{2n}\}$
$D_n(q)$	$n \equiv 0 (\mathrm{mod}\ 2)$, $n \geqslant 4$, $q \equiv 3 (\mathrm{mod}\ 4)$	2	$\{2, r_{n-1}\}$
	$n \equiv 0 (\mathrm{mod}\ 2)$, $n \geqslant 4$, $q \equiv 1 (\mathrm{mod}\ 4)$	2	$\{2, r_{2n-2}\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 3 (\mathrm{mod}\ 4)$	2	$\{2, r_n\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 1 (\mathrm{mod}\ 8)$	2	$\{2, r_{2n-2}\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 5 (\mathrm{mod}\ 8)$	3	$\{2, r_n, r_{2n-2}\}$
$^2D_n(q)$	$n \equiv 0 (\mathrm{mod}\ 2)$, $n \geqslant 4$	2	$\{2, r_{2n}\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 1 (\mathrm{mod}\ 4)$	2	$\{2, r_{2n}\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 7 (\mathrm{mod}\ 8)$	2	$\{2, r_{2n-2}\}$
	$n \equiv 1 (\mathrm{mod}\ 2)$, $n > 4$, $q \equiv 3 (\mathrm{mod}\ 8)$	3	$\{2, r_{2n-2}, r_{2n}\}$

Таблица 7. 2-неплотность для конечных простых исключительных групп лиева типа характеристики $p \neq 2$

G	Условия	$t(2,G)$	$\rho(2,G)$
$G_2(q)$	нет	3	$\{2, r_3, r_6\}$
$F_4(q)$	нет	2	$\{2, r_{12}\}$
$E_6(q)$	нет	3	$\{2, r_9, r_{12}\}$
$^2E_6(q)$	нет	3	$\{2, r_{12}, r_{18}\}$
$E_7(q)$	$q \equiv 1 (\mathrm{mod}\ 4)$	3	$\{2, r_{14}, r_{18}\}$
	$q \equiv 3 (\mathrm{mod}\ 4)$	3	$\{2, r_7, r_9\}$
$E_8(q)$	нет	5	$\{2, r_{15}, r_{20}, r_{24}, r_{30}\}$
$^3D_4(q)$	нет	2	$\{2, r_{12}\}$
$^2G_2(3^{2n+1})$	нет	3	$\{2, s_1, s_2\}$, где
			s_1 делит $3^{2n+1} - 3^{n+1} + 1$,
			s_2 делит $3^{2n+1} + 3^{n+1} + 1$.

Таблица 8. Неплотность для конечных простых классических групп

G	Условия	$t(G)$	$\rho(G)$
$A_{n-1}(q)$	$n = 2$, $q > 3$	3	$\{p, r_1, r_2\}$
	$n = 3$, $(q-1)_3 = 3$ и $q+1 \neq 2^k$	4	$\{p, 3, r_2, r_3\}$
	$n = 3$, $(q-1)_3 \neq 3$ и $q+1 \neq 2^k$	3	$\{p, r_2, r_3\}$
	$n = 3$, $(q-1)_3 = 3$ и $q+1 = 2^k$	3	$\{p, 3, r_3\}$
	$n = 3$, $(q-1)_3 \neq 3$ и $q+1 = 2^k$	2	$\{p, r_3\}$
	$n = 4$	3	$\{p, r_{n-1}, r_n\}$
	$n = 5, 6$, $q = 2$	3	$\{5, 7, 31\}$
	$7 \leqslant n \leqslant 11$, $q = 2$	$\left[\frac{n-1}{2}\right]$	$\{r_i \mid i \neq 6, \left[\frac{n}{2}\right] < i \leqslant n\}$
	$n \geqslant 5$ и $q > 2$ или $n \geqslant 12$ и $q = 2$	$\left[\frac{n+1}{2}\right]$	$\{r_i \mid \left[\frac{n}{2}\right] < i \leqslant n\}$
${}^2A_{n-1}(q)$	$n = 3, q \neq 2, (q+1)_3 = 3$ и $q-1 \neq 2^k$	4	$\{p, 3, r_1, r_6\}$
	$n = 3$, $(q+1)_3 \neq 3$ и $q-1 \neq 2^k$	3	$\{p, r_1, r_6\}$
	$n = 3$, $(q+1)_3 = 3$ и $q-1 = 2^k$	3	$\{p, 3, r_6\}$
	$n = 3$, $(q+1)_3 \neq 3$ и $q-1 = 2^k$	2	$\{p, r_6\}$
	$n = 4$, $q = 2$	2	$\{2, 5\}$
	$n = 4$, $q > 2$	3	$\{p, r_4, r_6\}$
	$n = 5$, $q = 2$	3	$\{2, 5, 11\}$
	$n \geqslant 5$ и $(n, q) \neq (5, 2)$	$\left[\frac{n+1}{2}\right]$	$\{r_{i/2} \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 2(\mathrm{mod}\ 4)\} \cup$ $\cup \{r_{2i} \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 1(\mathrm{mod}\ 2)\}$ $\cup \{r_i \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 0(\mathrm{mod}\ 4)\}$
$B_n(q)$ или $C_n(q)$	$n = 2$, $q > 2$	2	$\{p, r_4\}$
	$n = 3$ и $q = 2$	2	$\{5, 7\}$
	$n = 4$ и $q = 2$	3	$\{5, 7, 17\}$
	$n = 5$ и $q = 2$	4	$\{7, 11, 17, 31\}$
	$n = 6$ и $q = 2$	5	$\{7, 11, 13, 17, 31\}$
	$n > 2$, $(n, q) \neq (3, 2), (4, 2), (5, 2), (6, 2)$	$\left[\frac{3n+5}{4}\right]$	$\{r_{2i} \mid \left[\frac{n+1}{2}\right] \leqslant i \leqslant n\} \cup$ $\cup \{r_i \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 1(\mathrm{mod}\ 2)\}$
$D_n(q)$	$n = 4$ и $q = 2$	2	$\{5, 7\}$
	$n = 5$ и $q = 2$	4	$\{5, 7, 17, 31\}$
	$n = 6$ и $q = 2$	4	$\{7, 11, 17, 31\}$
	$n \geqslant 4$, $(n, q) \neq (4, 2), (5, 2), (6, 2)$	$\left[\frac{3n+1}{4}\right]$	$\{r_{2i} \mid \left[\frac{n+1}{2}\right] \leqslant i < n\} \cup$ $\cup \{r_i \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 1(\mathrm{mod}\ 2)\}$
${}^2D_n(q)$	$n = 4$ и $q = 2$	3	$\{5, 7, 17\}$
	$n = 5$ и $q = 2$	3	$\{7, 11, 17\}$
	$n = 6$ и $q = 2$	5	$\{7, 11, 13, 17, 31\}$
	$n = 7$ и $q = 2$	5	$\{11, 13, 17, 31, 43\}$
	$n \geqslant 4$, $n \not\equiv 1(\mathrm{mod}\ 4)$, $(n, q) \neq (4, 2), (6, 2), (7, 2)$	$\left[\frac{3n+4}{4}\right]$	$\{r_{2i} \mid \left[\frac{n}{2}\right] \leqslant i \leqslant n\} \cup$ $\cup \{r_i \mid \left[\frac{n}{2}\right] < i \leqslant n,$ $i \equiv 1(\mathrm{mod}\ 2)\}$
	$n > 4$, $n \equiv 1(\mathrm{mod}\ 4)$, $(n, q) \neq (5, 2)$	$\left[\frac{3n+4}{4}\right]$	$\{r_{2i} \mid \left[\frac{n}{2}\right] < i \leqslant n\} \cup$ $\cup \{r_i \mid \left[\frac{n}{2}\right] < i < n,$ $i \equiv 1(\mathrm{mod}\ 2)\}$

Таблица 9. Неплотность для конечных простых исключительных групп лиева типа

G	Условия	$t(G)$	$\rho(G)$
$G_2(q)$	$q > 2$	3	$\{p, r_3, r_6\}$
$F_4(q)$	$q = 2$	4	$\{5, 7, 13, 17\}$
	$q > 2$	5	$\{r_3, r_4, r_6, r_8, r_{12}\}$
$E_6(q)$	$q = 2$	5	$\{5, 13, 17, 19, 31\}$
	$q > 2$	6	$\{r_4, r_5, r_6, r_8, r_9, r_{12}\}$
${}^2E_6(q)$	нет	5	$\{r_4, r_8, r_{10}, r_{12}, r_{18}\}$
$E_7(q)$	нет	7	$\{r_7, r_8, r_9, r_{10}, r_{12}, r_{14}, r_{18}\}$
$E_8(q)$	нет	11	$\{r_7, r_8, r_9, r_{10}, r_{12}, r_{14}, r_{15}, r_{18}, r_{20}, r_{24}, r_{30}\}$
${}^3D_4(q)$	$q = 2$	2	$\{2, 13\}$
	$q > 2$	3	$\{r_3, r_6, r_{12}\}$
${}^2B_2(2^{2n+1})$	$n \geqslant 1$	4	$\{2, s_1, s_2, s_3\}$, где s_1 делит $2^{2n+1} - 1$, s_2 делит $2^{2n+1} - 2^{n+1} + 1$ s_3 делит $2^{2n+1} + 2^{n+1} + 1$
${}^2G_2(3^{2n+1})$	$n \geqslant 1$	5	$\{3, s_1, s_2, s_2, s_3, s_4\}$, где $s_1 \neq 2$ делит $3^{2n+1} - 1$ $s_2 \neq 2$ делит $3^{2n+1} + 1$ s_3 делит $3^{2n+1} - 3^{n+1} + 1$ s_4 делит $3^{2n+1} + 3^{n+1} + 1$
${}^2F_4(2^{2n+1})$	$n \geqslant 2$,	5	$\{s_1, s_2, s_3, s_4, s_5\}$, где $s_1 \neq 3$ и делит $2^{2n+1} + 1$, s_2 делит $2^{4n+2} + 1$, $s_3 \neq 3$ и делит $2^{4n+2} - 2^{2n+1} + 1$, s_4 делит $2^{4n+2} - 2^{3n+2} + 2^{2n+1} - 2^{n+1} + 1$, s_5 делит $2^{4n+2} + 2^{3n+2} + 2^{2n+1} + 2^{n+1} + 1$,
${}^2F_4(2)'$	нет	3	$\{3, 5, 13\}$
${}^2F_4(8)$	нет	4	$\{7, 19, 37, 109\}$

Список литературы

[1] *J.S.Williams*, Prime graph components of finite groups, J. Algebra, **69**, N 2 (1981), 487–513.

[2] *А.С.Кондратьев*, О компонентах графа простых чисел конечных простых групп, Матем. сб., **180**, N 6 (1989), 787–797.

[3] *V.D.Mazurov*, Characterization of groups by arithmetic properties, Algebra Colloc., **11**, N 1 (2004), 129–140.

[4] *А.В.Васильев*, О связи между строением конечной группы и свойствами ее графа простых чисел, Сиб. мат. журн., **46**, N 3 (2005), 511–522.

[5] *J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson*, Atlas of finite groups, Clarendon Press, Oxford, 1985.

[6] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4, 2004; (http://www.gap-system.org).

[7] *R.W.Carter*, Simple groups of Lie type, John Wiley and Sons, London, 1972.

[8] *J.E.Humphreys*, Linear algebraic groups, Springer-Verlag, New York, 1972.

[9] *R.Steinberg*, Endomorphisms of algebraic groups, Mem. AMS, **80**, 1968.

[10] *A.Borel, J. de Siebental*, Les-sous-groupes fermés de rang maximum des groupes de Lie clos, Comment.Math.Helv., **23**, (1949), 200–221.

[11] *Е.Б.Дынкин*, Полупростые подалгебры полупростых алгебр Ли, Матем. сб., **30**, N 2 (1952), 349–462.

[12] *R.W.Carter*, Finite groups of Lie type, conjugacy classes and complex characters, John Wiley and Sons, 1985.

[13] *R.W.Carter*, Centralizers of semisimple elements in the finite classical groups, Proc. London Math. Soc., (3), **42**, N 1 (1981), 1–41.

[14] *R.W.Carter*, Conjugacy classes in the Weyl group, Compositio Mathematica, **25**, N 1 (1972), 1–59.

[15] *D.Deriziotis*, Conjugacy classes and centralizers of semisimple elements in finite groups of Lie type, Vorlesungen aus dem Fachbereich Mathematic der Universität Essen, 1984, Heft 11.

[16] *K.Zsigmondy*, Zur Theorie der Potenzreste, Monatsh. für Math. und Phys., **3**, (1892), 265–284.

[17] *D.Deriziotis*, The centralizers of semisimple elements of the Chevalley groups E_7 and E_8, Tokyo J. Math., **6**, N 1 (1983), 191–216.

[18] *M.S.Lucido, A.R.Moghaddamfar*, Groups with complete prime graph connected components, J. Group Theory, **7**, N 3 (2004), 373–384.

Аннотация: В статье для каждой конечной неабелевой простой группы указан исчерпывающий арифметический критерий смежности вершин в ее графе простых чисел. С использованием этого критерия для графа простых чисел каждой конечной простой группы найдены: независимое множество с наибольшим числом вершин, независимое множество, содержащее 2, с наибольшим числом вершин и порядки этих множеств. Эта информация собрана в таблицах в конце работы. Рассматриваются некоторые приложения полученных результатов к различным вопросам теории конечных групп, в частности, к вопросу о распознаваемости конечной группы по спектру.

Ключевые слова: конечная группа, конечная простая группа, группа лиева типа, спектр конечной группы, распознавание по спектру, граф простых чисел конечной группы, неплотность графа простых чисел, 2-неплотность графа простых чисел

Адреса авторов:

Васильев Андрей Викторович
Институт математики им. Соболева СО РАН
пр. Академика Коптюга, 4
Новосибирск 630090
`vdr@gorodok.net`

Вдовин Евгений Петрович
Институт математики им. Соболева СО РАН
пр. Академика Коптюга, 4
Новосибирск 630090
`vdovin@math.nsc.ru`