Сибирский математический журнал
Январь—февраль, 2021. Том 62, № 1

УДК 512.542

О СОВПАДЕНИИ КЛАССОВ КОНЕЧНЫХ ГРУПП E_{π_x} И D_{π_x}

К. А. Ильенко, Н. В. Маслова

Аннотация. Пусть π_x — множество всех простых чисел, больших x. Доказано, что для любого $x \in \mathbb{R}$ классы конечных групп D_{π_x} и E_{π_x} совпадают, т. е. конечная группа G обладает π_x-холловой подгруппой тогда и только тогда, когда в G выполняется полный аналог теорем Силова для π_x-подгрупп.

DOI 10.33048/smzh.2021.62.105

Ключевые слова: π-холлова подгруппа, силовские свойства, свойства E_{π_x}, C_{π_x} и D_{π_x}.

Посвящается Юрию Леонидовичу Ершову к 80-летию

1. Введение

Всюду в работе будем употреблять термин «группа» в значении «конечная группа». Наши терминология и обозначения, в основном, стандартны, их можно найти в [1].

Пусть π — некоторое множество простых чисел. Через π' обозначим множество всех простых чисел, не лежащих в π, через $\pi(n)$ — множество всех простых делителей натурального числа n, а для конечной группы G через $\pi(G)$ — множество $\pi(|G|)$. Группа с условием $\pi(G) \subseteq \pi$ называется *π-группой*. Подгруппа H группы G называется *π-холловой подгруппой*, если $\pi(H) \subseteq \pi$ и $\pi(|G : H|) \subseteq \pi'$.

Будем говорить, что группа G *принадлежит классу E_π*, если в G имеется π-холлова подгруппа. Если при этом любые две π-холловы подгруппы группы G сопряжены, то будем говорить, что она *принадлежит классу C_π*. Если, к тому же, любая π-подгруппа группы G содержится в некоторой π-холловой подгруппе, то будем говорить, что G *принадлежит классу D_π*. Включение $D_\pi \subseteq C_\pi \subseteq E_\pi$ выполняется по определению. Естественной является следующая проблема, сформулированная в [2, проблема 7.20].

Проблема 1. *Для каких множеств π простых чисел одно или оба включения в цепочке*

$$D_\pi \subseteq C_\pi \subseteq E_\pi$$

являются равенствами?

Тривиальные примеры выполнения равенств $D_\pi = C_\pi = E_\pi$ дают пустое множество, множество всех простых чисел и ввиду теорем Силова любое одноэлементное множество π. В 1956 г. Холлом высказана гипотеза о том, что для любого множества простых чисел π такого, что $2 \notin \pi$, имеет место равенство

Работа выполнена за счет Российского научного фонда (проект 19–71–10067).

классов групп $E_\pi = D_\pi$. В 1982 г. Арад и Уард [3, теорема 4.9], используя классификацию конечных простых групп, доказали, что если $\pi = 2'$, то $D_\pi = E_\pi$. В 1984 г. Гросс [4] опроверг гипотезу Холла, доказав, что для любого конечного множества нечетных простых чисел π, содержащего более одного элемента, существует группа из класса E_π, не принадлежащая классу D_π. Тем не менее в 1987 г. с использованием классификации конечных простых групп Гросс доказал ослабленный аналог гипотезы Холла [5, 6], а именно, показал, что если множество π простых чисел не содержит число 2, то $E_\pi = C_\pi$. Не так давно Д. О. Ревиным [1, предложение 3] было показано, что если множество простых чисел π содержит числа 2 и 3 и отлично от множества всех простых чисел, то включение $D_\pi \subset C_\pi$ строгое.

Пусть x — действительное число. Положим

$$\pi_x = \{p \mid p \text{ — простое число, } p > x\}.$$

В 2009 г. Д. О. Ревиным [1, теорема 1] показано, что $E_{\pi_x} = D_{\pi_x}$ для всех $x \geqslant 7$. Кроме того, в этой же работе [1, проблема 8] сформулирована следующая

Проблема 2. *Верно ли, что $E_{\pi_x} = D_{\pi_x}$ для любого действительного числа x?*

Отметим, что проблема 2 также приведена в обзорной статье Е. П. Вдовина и Д. О. Ревина [2, проблема 7.30].

В работе [1] Д. О. Ревин высказал гипотезу о том, что проблема 2 имеет положительное решение. В настоящей работе подтверждена гипотеза Д. О. Ревина и получено положительное решение проблемы 2. Доказана следующая

Теорема. *$E_{\pi_x} = D_{\pi_x}$ для любого действительного числа x.*

2. Вспомогательные результаты

Приведем несколько вспомогательных результатов, которые понадобятся для доказательства теоремы.

Если r — нечетное простое число, а $q > 1$ — натуральное число, взаимно простое с r, то положим

$$e(q,r) = \min\{k \in \mathbb{N} \mid q^k \equiv 1 \pmod r\}.$$

Множество простых чисел r таких, что $e(q,r) = m$, будем обозначать через $R_m(q)$.

Лемма 1 (теорема Жигмонди, см. [7]). *Пусть q, m — натуральные числа, причем $q, m > 1$. Тогда найдется такое нечетное простое число r, что $e(q,r) = m$, за исключением следующих случаев:*

(1) $q = 2$ *и* $m = 6$*;*

(2) $q = 2^l - 1$ *для некоторого* $l > 1$ *и* $m = 2$.

Ввиду леммы 1 множество $R_m(q)$, за исключением описанных в лемме случаев, непусто. По определению $R_i(q) \cap R_j(q) = \varnothing$ при различных i и j, и если q — степень простого числа, то $R_i(q) \cap \pi(q) = \varnothing$ для любого i. Любое простое число $r \in R_m(q)$ будем обозначать для краткости через $r_m(q)$.

Следующее утверждение известно и доказывается элементарно.

Лемма 2. *Пусть r — нечетное простое число, $q > 1$ — натуральное число и r делит $q^i - 1$ для некоторого i. Тогда число $e(q, r)$ делит i.*

Всюду далее считаем, что π — некоторое множество простых чисел. Символ x означает некоторое действительное число, а π_x — множество всех простых чисел из интервала $(x, +\infty)$.

Лемма 3 [8, 9]. *Пусть G — конечная группа. Следующие утверждения эквивалентны:*
(1) *G разрешима;*
(2) *$G \in D_\pi$ для любого множества π простых чисел;*
(3) *$G \in C_\pi$ для любого множества π простых чисел;*
(4) *$G \in E_\pi$ для любого множества π простых чисел.*

Лемма 4. *Пусть G — конечная группа и A — ее нормальная подгруппа. Тогда справедливы следующие утверждения.*
(1) *Если $G \in E_\pi$, то $A \in E_\pi$ и $G/A \in E_\pi$.*
(2) *Если $A \in D_\pi$ и $G/A \in D_\pi$, то $G \in D_\pi$.*

Доказательство. (1) См. [10, лемма 1].
(2) См. [11, теорема 7.7].

Лемма 5 (см. [5, теорема 6.14]). *Если π — некоторое множество нечетных простых чисел и G — простая спорадическая группа или группа Титса такая, что $G \in E_\pi \setminus D_\pi$, то $G = O'N$ и $\pi \cap \pi(G) = \{3, 5\}$.*

Лемма 6. *Если π — некоторое множество нечетных простых чисел и $G = A_n$ — знакопеременная группа такая, что $G \in E_\pi$, то $|\pi \cap \pi(G)| \le 1$. В частности, $G \in D_\pi$.*

Доказательство следует из [11, теорема 4.3; 10, теорема A4; 12].

Лемма 7 (см. [1, лемма 7][1)]). *Пусть π — некоторое множество нечетных простых чисел, G — простая группа лиева типа с базовым полем $\mathbb{F}_q$ характеристики $p > 0$, причем $G \in E_\pi \setminus D_\pi$. Положим $r = \min \pi \cap \pi(G)$ и $\tau = \pi \cap \pi(G) \setminus \{r\}$. Тогда имеет место одно из следующих утверждений.*

(1) *$p \in \pi$, p делит $|W|$ (порядок группы Вейля W группы G, см. табл. 1), любое число t из $\pi \cap \pi(G) \setminus \{p\}$ делит $q - 1$ и не делит $|W|$;*

(2) *$p \notin \pi$ и выполнено одно из следующих условий*:

(2.1) *$G = A_{n-1}(q)$, $e(q, r) = r - 1$, $(q^{r-1} - 1)_r = r$, $[n/(r - 1)] = [n/r]$ и для всех $t \in \tau$ выполнено $e(q, t) = 1$ и $n < t$;*

(2.2) *$G = {}^2A_{n-1}(q)$, $r \equiv 1 \pmod 4$, $e(q, r) = r - 1$, $(q^{r-1} - 1)_r = r$, $[n/(r - 1)] = [n/r]$ и для всех $t \in \tau$ выполнены $e(q, t) = 2$ и $n < 2t$;*

(2.3) *$G = {}^2A_{n-1}(q)$, $r \equiv 3 \pmod 4$, $e(q, r) = [(r - 1)/2]$, $(q^{r-1} - 1)_r = r$, $[n/(r - 1)] = [n/r]$ и для всех $t \in \tau$ выполнены $e(q, t) = 2$ и $n < 2t$;*

(2.4) *$G = E_6(q)$, $\pi \cap \pi(G) \subseteq \pi(q - 1)$, $3, 13 \in \pi \cap \pi(G)$, $5 \notin \pi \cap \pi(G)$;*

(2.5) *$G = {}^2E_6(q)$, $\pi \cap \pi(G) \subseteq \pi(q + 1)$, $3, 13 \in \pi \cap \pi(G)$, $5 \notin \pi \cap \pi(G)$;*

(2.6) *$G = E_7(q)$, $\pi \cap \pi(G)$ содержится в одном из множеств $\pi(q - 1)$ или $\pi(q + 1)$, $3, 13 \in \pi \cap \pi(G)$, $5, 7 \notin \pi \cap \pi(G)$;*

(2.7) *$G = E_8(q)$, $\pi \cap \pi(G)$ содержится в одном из множеств $\pi(q - 1)$ или $\pi(q + 1)$, $3, 13 \in \pi \cap \pi(G)$, $5, 7 \notin \pi \cap \pi(G)$;*

[1)] Текст формулировки утверждения [1, лемма 7] содержит опечатки: должно быть $e(q, r)$ и $e(q, t)$ вместо $e(r, q)$ и $e(t, q)$ соответственно.

Таблица 1. Простые группы лиева типа над полем $\mathbb{F}_q$

(2.8) *$G = E_8(q)$, $\pi \cap \pi(G)$ содержится в одном из множеств $\pi(q-1)$ или $\pi(q+1)$, $5, 31 \in \pi \cap \pi(G)$, $3, 7 \notin \pi \cap \pi(G)$;*

(2.9) *$G = F_4(q)$, $\pi \cap \pi(G)$ содержится в одном из множеств $\pi(q-1)$ или $\pi(q+1)$, $3, 13 \in \pi \cap \pi(G)$.*

3. Доказательство основного результата

В настоящем разделе докажем теорему. Заметим, что для этого достаточно показать, что $E_\pi = D_\pi$ в случае, когда π — одно из множеств:

$$\pi_1 = \{p \mid p \text{ — простое число и } p \geq 5\} \text{ или } \pi_2 = \{p \mid p \text{ — простое число и } p \geq 7\}.$$

Действительно, если $x < 2$, то множество π_x совпадает с множеством всех простых чисел и теорема выполняется тривиально. При $2 \leq x < 3$ теорема доказана в [3, теорема 4.9], а при $x \geq 7$ теорема следует из результата Д. О. Ревина [1, теорема 1]. Таким образом, осталось рассмотреть случай, когда $3 \leq x < 7$, т. е. когда π — одно из указанных множеств π_1 или π_2.

Предположим, что для некоторого множества π простых чисел $E_\pi \setminus D_\pi \neq \varnothing$ и $G \in E_\pi \setminus D_\pi$. Тогда ввиду леммы 3 группа G неразрешима. Из леммы 4 следует, что найдется неабелев композиционный фактор S группы G такой, что $S \in E_\pi \setminus D_\pi$. Поэтому для того, чтобы доказать теорему, достаточно показать, что пересечение множества $E_\pi \setminus D_\pi$, где π — одно из множеств π_1 или π_2, с множеством неабелевых простых групп пусто.

Пусть π — одно из множеств π_1 или π_2. Докажем, что в множестве $E_\pi \setminus D_\pi$ нет неабелевых простых групп. Из леммы 6 следует, что знакопеременные группы не содержатся в множестве $E_\pi \setminus D_\pi$. Поскольку $\{3, 5\} \nsubseteq \pi$, из леммы 5 вытекает, что спорадические группы и группа Титса не содержатся в множестве $E_\pi \setminus D_\pi$.

Пусть S является группой лиева типа над полем характеристики p. Конечные неабелевы простые группы лиева типа, лежащие в множестве $E_\pi \setminus D_\pi$, описаны в лемме 7.

Пусть S — исключительная группа лиева типа и $S \in E_\pi \setminus D_\pi$.

Предположим, что $p \in \pi$. Тогда $p \geq 5$ и, поскольку p делит $|W|$, из п. (1) леммы 7 и табл. 1 следует, что имеет место один из следующих случаев.

(a) $S \cong E_6(q)$ и $\pi = \pi_1$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{12}(q), r_9(q), r_8(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{8, 9, 12\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

(b) $S \cong E_7(q)$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{18}(q), r_{14}(q), r_{12}(q), r_{10}(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| \leq 3$, найдется индекс $i \in \{10, 12, 14, 18\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

(c) $S \cong E_8(q)$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{30}(q), r_{24}(q), r_{20}(q), r_{18}(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| \leq 3$, найдется индекс $i \in \{18, 20, 24, 30\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

Таким образом, $p \notin \pi$. Ввиду п. (2) леммы 7 имеем $\pi = \pi_1$, т. е. $p \in \{2, 3\}$ и $S \cong E_8(q)$. По малой теореме Ферма число 7 делит число $q^6 - 1$, которое делит число $q^{12} - 1$, которое делит порядок группы S. Кроме того, $7 \in \pi$, поэтому $7 \in \pi \cap \pi(S)$; получаем противоречие с пунктом (2.7) леммы 7.

Пусть S — классическая группа лиева типа и $S \in E_\pi \setminus D_\pi$. Далее рассмотрим случаи $\pi = \pi_1$ и $\pi = \pi_2$ отдельно.

1. Пусть $\pi = \pi_1$.

1.1. Предположим, что $p \in \pi$. Тогда $p \geq 5$ и, поскольку p делит $|W|$, из п. (1) леммы 7 и табл. 1 следует, что имеет место один из следующих случаев.

1.1.1. $S \cong A_n(q)$. Тогда p делит $(n+1)!$, поэтому $5 \leq p \leq n+1$, откуда $n \geq 4$. Если q не является простым числом Мерсенна, т. е. простым числом вида $2^l - 1$ для некоторого простого числа $l > 1$, то ввиду леммы 1 существуют и попарно различны числа

$$r_4(q), r_3(q), r_2(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{2, 3, 4\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

Если $q = p$ является простым числом Мерсенна, то $p \geq 7$, откуда $n \geq 6$. Ввиду леммы 1 существуют и попарно различны числа

$$r_5(q), r_4(q), r_3(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)),$$

поэтому снова найдется индекс $i \in \{3,4,5\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Получаем противоречие с тем, что $r_i(q)$ делит $q-1$.

1.1.2. $S \cong {}^2A_n(q)$. Тогда p делит $2\left[\frac{n+1}{2}\right]!$, поэтому $5 \leq p \leq \left[\frac{n+1}{2}\right]$, откуда $n \geq 9$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{18}(q), r_8(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{6,8,18\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

1.1.3. $S \cong B_n(q)$ или $C_n(q)$. Тогда p делит $2^n n!$, поэтому $5 \leq p \leq n$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{10}(q), r_8(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{6,8,10\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

1.1.4. $S \cong D_n(q)$. Тогда p делит $2^{n-1}n!$, поэтому $5 \leq p \leq n$. Ввиду леммы 1 существуют и попарно различны числа

$$r_8(q), r_6(q), r_4(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{4,6,8\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

1.1.5. $S \cong {}^2D_n(q)$. Тогда p делит $2^{n-1}(n-1)!$, поэтому $5 \leq p \leq n-1$, откуда $n \geq 6$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{10}(q), r_8(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 2$, найдется индекс $i \in \{6,8,10\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

Таким образом, $p \notin \pi$.

1.2. Предположим, что $p \in \pi' = \{2,3\}$. Положим $r = \min \pi \cap \pi(S)$, $\tau = \pi \cap \pi(S) \setminus \{r\}$. Ввиду п. (2) леммы 7 имеет место один из следующих случаев.

1.2.1. $S \cong A_{n-1}(q)$ и $e(q,r) = r-1$. Поскольку $r \in \pi$, имеем $r \geq 5$. С другой стороны, $r \in \pi(S)$, поэтому существует индекс i такой, что r делит $q^i - 1$. Отсюда

$$e(q,r) = (r-1) \leq i \leq n,$$

поэтому $n \geq 5-1 = 4$. Ввиду леммы 1 существуют и различны числа

$$r_3(q), r_4(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Заметим, что $r_3(q) \geq 5$ и $r_4(q) \geq 5$, так как числа 2 и 3 делят $q(q^2-1)$. Поэтому числа $r_3(q)$ и $r_4(q)$ лежат в $\pi \cap \pi(S)$; таким образом, хотя бы одно из чисел $r_3(q)$ и $r_4(q)$ лежит в τ. Противоречие с тем, что для всех $t \in \tau$ выполняется равенство $e(q,t) = 1$.

1.2.2. $S \cong {}^2A_{n-1}(q)$, $r \equiv 1 \pmod 4$ и $e(q,r) = r-1$. Поскольку $r \in \pi$, имеем $r \geq 5$. С другой стороны, $r \in \pi(S)$, поэтому существует индекс i такой, что либо i четно и r делит $q^i - 1$, либо i нечетно и r делит $q^i + 1$. Отсюда r делит $q^{2i} - 1$, поэтому по лемме 2 число $e(q,r) = (r-1)$ делит $2i$, при этом, поскольку $r \equiv 1 \pmod 4$, число $r-1$ делится на 4, поэтому i четно. Заключаем, что

$$e(q,r) = (r-1) \leq i \leq n.$$

Заметим, что $n \neq 4$, так как иначе $r = 5$ и $[n/(r-1)] \neq [n/r]$. Поэтому $n \geq 5$. Ввиду леммы 1 существуют и различны числа

$$r_{10}(q), r_4(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Заметим, что $r_{10}(q) \geq 5$ и $r_4(q) \geq 5$, так как числа 2 и 3 делят $q(q^2-1)$. Поэтому числа $r_{10}(q)$ и $r_4(q)$ лежат в $\pi \cap \pi(S)$; таким образом, хотя бы одно из чисел $r_{10}(q)$ и $r_4(q)$ лежит в τ. Противоречие с тем, что $e(q,s) = 2$ для любого $s \in \tau$.

1.2.3. $S \cong {}^2A_{n-1}(q)$, $r \equiv 3 \pmod 4$ и $e(q,r) = [(r-1)/2]$. Заметим, что $r \geq 7$, поэтому порядок группы S не делится на 5. Из [13, табл. 1] следует, что $S \cong {}^2A_2(q)$ или $S \cong {}^2A_1(q)$, где $2 < q \equiv \pm 2 \pmod 5$, в частности, q является нечетной степенью числа $p \in \{2,3\}$.

Поскольку $r \in \pi(S)$, либо r делит число $q^2 - 1$, либо r делит число $q^3 + 1$, которое делит число $q^6 - 1$. Из леммы 2 следует, что $e(q,r) = (r-1)/2$ делит одно из чисел 2 или 6, при этом, поскольку $r \equiv 3 \pmod 4$, число $(r-1)/2$ нечетно. Поэтому $(r-1)/2 = 1$ или $(r-1)/2 = 3$, откуда $r \in \{3,7\}$. Учитывая, что $r \geq 7$, заключаем, что $r = 7$. Теперь имеем $e(q,7) = [(r-1)/2] = 3$. Поэтому 7 не делит $q^2 - 1$ и $q^3 + 1$; противоречие.

2. Пусть $\pi = \pi_2$.

2.1. Предположим, что $p \in \pi$. Тогда $p \geq 7$ и, поскольку p делит $|W|$, из п. (1) леммы 7 и табл. 1 следует, что имеет место один из следующих случаев.

2.1.1. $S \cong A_n(q)$. Тогда p делит $(n+1)!$, поэтому $7 \leq p \leq n+1$, откуда $n \geq 6$. Ввиду леммы 1 существуют и попарно различны числа

$$r_6(q), r_5(q), r_4(q), r_3(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 3$, найдется индекс $i \in \{3,4,5,6\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

2.1.2. $S \cong {}^2A_n(q)$. Тогда p делит $2\left[\frac{n+1}{2}\right]!$, поэтому $p \leq \left[\frac{n+1}{2}\right]$, откуда $n \geq 13$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{12}(q), r_{10}(q), r_8(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 3$, найдется индекс $i \in \{6,8,10,12\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

2.1.3. $S \cong B_n(q)$ или $C_n(q)$. Тогда p делит $2^n n!$, поэтому $7 \le p \le n$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{14}(q), r_{12}(q), r_{10}(q), r_8(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 3$, найдется индекс $i \in \{8, 10, 12, 14\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

2.1.4. $S \cong D_n(q)$. Тогда p делит $2^{n-1} n!$, поэтому $7 \le p \le n$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{12}(q), r_{10}(q), r_8(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 3$, найдется индекс $i \in \{6, 8, 10, 12\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

2.1.5. $S \cong {}^2D_n(q)$. Тогда p делит $2^{n-1}(n-1)!$, поэтому $7 \le p \le n-1$, откуда $n \ge 8$. Ввиду леммы 1 существуют и попарно различны числа

$$r_{14}(q), r_{12}(q), r_{10}(q), r_8(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi'| = 3$, найдется индекс $i \in \{8, 10, 12, 14\}$ такой, что

$$r_i(q) \in (\pi(S) \setminus (\{p\} \cup \pi(q-1))) \cap \pi.$$

Противоречие с тем, что $r_i(q)$ делит $q-1$.

Таким образом, $p \notin \pi$.

2.2. Предположим, что $p \in \pi' = \{2, 3, 5\}$. Положим

$$r = \min \pi \cap \pi(S) \quad \text{и} \quad \tau = \pi \cap \pi(S) \setminus \{r\}.$$

Ввиду п. (2) леммы 7 имеет место один из следующих случаев.

2.2.1. $S \cong A_{n-1}(q)$ и $e(q, r) = r - 1$. Поскольку $r \in \pi$, имеем $r \ge 7$. С другой стороны, $r \in \pi(S)$, поэтому существует индекс i такой, что r делит $q^i - 1$. Отсюда

$$e(q, r) = (r-1) \le i \le n,$$

тем самым $n \ge 7 - 1 = 6$.

Предположим, что $(n, q) = (6, 2)$. Тогда $\pi(S) = \{2, 3, 5, 7, 31\}$, при этом $31 \in \tau$ и $e(2, 31) = 5$. Противоречие с тем, что $e(q, s) = 1$ для любого $s \in \tau$.

Предположим, что $(n, q) \ne (6, 2)$. Ввиду леммы 1 существуют и попарно различны числа

$$r_6(q), r_5(q), r_4(q), r_3(q) \in \pi(S) \setminus (\{p\} \cup \pi(q-1)).$$

Поскольку $|\pi' \setminus \{p\}| = 2$, найдется индекс $i \in \{3, 4, 5, 6\}$ такой, что $r_i(q) \in \tau$. Противоречие с тем, что $e(q, s) = 1$ для любого $s \in \tau$.

2.2.2. $S \cong {}^2A_{n-1}(q)$, $r \equiv 1 \,(\mathrm{mod}\, 4)$ и $e(q, r) = r - 1$. Поскольку $r \in \pi$ и $r \equiv 1 \,(\mathrm{mod}\, 4)$, имеем $r \ge 13$. С другой стороны, $r \in \pi(S)$, поэтому существует индекс i такой, что либо i четно и r делит $q^i - 1$, либо i нечетно и r делит $q^i + 1$. Отсюда

$$e(q, r) = (r-1) \le 2i \le 2n,$$

поэтому $n \geq 6$.

Предположим, что $(n, q) = (6, 2)$. Тогда $\pi(S) = \{2, 3, 5, 7, 11\}$, при этом $r = 7$. Противоречие с тем, что $r \equiv 1 \,(\mathrm{mod}\, 4)$.

Предположим, что $(n, q) \neq (6, 2)$. Ввиду леммы 1 существуют и различны числа

$$r_{10}(q), r_6(q) \in \pi(S) \setminus (\{p\} \cup \pi(q - 1)).$$

Заметим, что $r_{10}(q) \geq 7$ и $r_6(q) \geq 7$, так как по малой теореме Ферма числа 2, 3 и 5 делят $q(q^4 - 1)$. Поэтому числа $r_{10}(q)$ и $r_6(q)$ лежат в $\pi \cap \pi(S)$; таким образом, хотя бы одно из чисел $r_{10}(q)$ и $r_6(q)$ лежит в τ. Противоречие с тем, что $e(q, s) = 2$ для любого $s \in \tau$.

2.2.3. $S \cong {}^2A_{n-1}(q)$, $r \equiv 3 \,(\mathrm{mod}\, 4)$ и $e(q, r) = [(r - 1)/2]$. Напомним, что q является степенью числа $p \in \{2, 3, 5\}$.

Пусть $n \in \{2, 3, 4\}$. Поскольку $r \in \pi(S)$, либо r делит число $q^2 - 1$, либо r делит число $q^3 + 1$, которое делит число $q^6 - 1$, либо r делит число $q^4 - 1$. Из леммы 2 следует, что $e(q, r) = (r - 1)/2$ делит одно из чисел 2, 4 или 6, при этом, поскольку $r \equiv 3 \,(\mathrm{mod}\, 4)$, число $(r - 1)/2$ нечетно. Поэтому $(r - 1)/2 = 1$ или $(r - 1)/2 = 3$, откуда $r \in \{3, 7\}$. Учитывая, что $r \geq 7$, заключаем, что $r = 7$. Теперь имеем $e(q, 7) = [(r - 1)/2] = 3$. Поэтому число 7 не делит $q^2 - 1$, $q^3 + 1$ и $q^4 - 1$, откуда следует, что 7 не принадлежит $\pi(S)$; противоречие. Следовательно, $n \geq 5$.

Пусть $q = 2$. Заметим, что если $n = 5$, то $|\pi \cap \pi(S)| = 1$, поэтому ${}^2A_4(2) \in D_\pi$. Предположим, что $(n, q) = (6, 2)$. Тогда $\pi(S) = \{2, 3, 5, 7, 11\}$, при этом $11 \in \tau$ и $e(2, 11) = 10$. Противоречие с тем, что $e(q, s) = 2$ для любого $s \in \tau$. Поэтому $n \geq 7$. Ввиду леммы 1, существуют и различны числа

$$r_{10}(q), r_{14}(q) \in \pi(S) \setminus (\{p\} \cup \pi(q - 1)).$$

Кроме того, по малой теореме Ферма числа 2, 3 и 5 делят $q(q^4 - 1)$, откуда $r_{10}(q), r_{14}(q) \in \pi$. Поэтому найдется индекс $i \in \{10, 14\}$ такой, что $r_i(q) \in \tau$. Противоречие с тем, что $e(q, s) = 2$ для любого $s \in \tau$. Тем самым $q \neq 2$.

Ввиду леммы 1 существуют и различны числа

$$r_6(q), r_{10}(q) \in \pi(S) \setminus (\{p\} \cup \pi(q - 1)).$$

Кроме того, по малой теореме Ферма числа 2, 3 и 5 делят $q(q^4 - 1)$, откуда $r_6(q), r_{10}(q) \in \pi$. Поэтому найдется индекс $i \in \{6, 10\}$ такой, что $r_i(q) \in \tau$. Противоречие с тем, что $e(q, s) = 2$ для любого $s \in \tau$. $\square$

ЛИТЕРАТУРА

1. *Ревин Д. О.* Вокруг гипотезы Ф. Холла // Сиб. электрон. мат. изв. 2009. Т. 6. С. 144–158.
2. *Вдовин Е. П., Ревин Д. О.* Теоремы силовского типа // Успехи мат. наук. 2011. Т. 66, № 5. С. 3–46.
3. *Arad Z., Ward M. B.* New criteria for the solvability of finite groups // J. Algebra. 1982. V. 77, N 1. P. 234–246.
4. *Gross F.* Odd order Hall subgroups of $\mathrm{GL}(n, q)$ and $\mathrm{Sp}(2n, q)$ // Math. Z. 1984. Bd 187, Heft 2. S. 185–194.
5. *Gross F.* On a conjecture of Philip Hall // Proc. London Math. Soc., Ser. III. 1986. V. 52, N 3. P. 464–494.
6. *Gross F.* Conjugacy of odd order Hall subgroups // Bull. London Math. Soc. 1987. V. 19, N 4. P. 311–319.
7. *Zsigmondy K.* Zur Theorie der Potenzreste // J. Monatshefte Math. Phys. 1892. V. 3. P. 265–284.

8. *Hall P.* A characteristic property of soluble groups // J. London Math. Soc. 1937. V. 12. P. 198–200.

9. *Чунихин С. А.* О разрешимых группах // Изв. НИИММ Том. унив. 1938. Т. 2. С. 220–223.

10. *Hall P.* Theorems like Sylow's // Proc. London Math. Soc. 1956. V. 6, N 22. P. 286–304.

11. *Revin D. O., Vdovin E. P.* Hall subgroups of finite groups // Contemp. Math. 2006. V. 402. P. 229–265.

12. *Thompson J. G.* Hall subgroups of the symmetric groups // J. Comb. Th. 1966. V. 1, N 2. P. 271–279.

13. *Заварницин А. В.* О распознавании конечных групп по графу простых чисел // Алгебра и логика. 2006. Т. 45, № 4. С. 390–408.

Поступила в редакцию 28 апреля 2020 г.
После доработки 26 октября 2020 г.
Принята к публикации 18 ноября 2020 г.

Ильенко Кристина Альбертовна, Маслова Наталья Владимировна
Институт математики и механики им. Н. Н. Красовского УрО РАН,
ул. С. Ковалевской, 16, Екатеринбург 620990
christina.ilyenko@yandex.ru, butterson@mail.ru