Сибирский математический журнал
Март—апрель, 2000. Том 41, № 2

УДК 519.542

РАСПОЗНАВАНИЕ ЗНАКОПЕРЕМЕННЫХ ГРУПП ПРОСТОЙ СТЕПЕНИ ПО ПОРЯДКАМ ИХ ЭЛЕМЕНТОВ

А. С. Кондратьев, В. Д. Мазуров

Аннотация: Доказывается, что конечная группа, множество порядков элементов которой такое же, как у знакопеременной группы A_r простой степени $r \geq 5$, изоморфна A_r. Библиогр. 10.

К 60-летию Юрия Леонидовича Ершова

Для конечной группы G обозначим через $\omega(G)$ множество всех порядков элементов группы G. Это множество замкнуто и частично упорядочено относительно делимости и поэтому однозначно определяется подмножеством $\mu(G)$, состоящим из максимальных относительно делимости элементов из $\omega(G)$.

Цель работы состоит в доказательстве следующего результата.

Теорема. *Пусть G — конечная группа, для которой $\omega(G) = \omega(A_r)$, где A_r — знакопеременная группа степени r и $r > 3$ — простое число. Тогда G изоморфна A_r.*

Доказательство. Предположим противное. Пусть G — противоречащий пример. В силу [1–3] можно предполагать, что $r \geq 17$.

Напомним, что множество $\omega(H)$ конечной группы H определяет *граф Грюнберга — Кегеля* $GK(H)$, вершинами которого служат простые делители порядка группы H, и два простых числа p, q соединены ребром, если H содержит элемент порядка pq. Обозначим через $s(H)$ число связных компонент в графе $GK(H)$, а через $\pi_i = \pi_i(H), i = 1, \dots, s(H)$, — i-ю связную компоненту. Для группы H четного порядка положим $2 \in \pi_1$. Обозначим через $\mu_i = \mu_i(H)$ множество тех $n \in \mu(H)$, для которых каждый простой делитель числа n принадлежит π_i.

В рассматриваемом случае граф $GK(G)$ несвязен и имеет компоненту связности, состоящую из единственного простого числа r. Наше доказательство основано на описании групп P с несвязным графом $GK(P)$ [4, 5] и следствия из основного результата работы [6], утверждающего, что для любого натурального числа $n \geq 119$ сегмент $[n, 1.073n]$ содержит по меньшей мере одно простое число.

Лемма 1. *Если $n \geq 6$ — натуральное число, то существует по меньшей мере $s(n)$ простых чисел p_i таких, что $(n+1)/2 < p_i < n$, где*

$s(n) = 6$ для $n \geq 48$,

$s(n) = 5$ для $42 \leq n \leq 47$,

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99–01–00550).

$s(n) = 4$ *для* $38 \le n \le 41$,
$s(n) = 3$ *для* $18 \le n \le 37$,
$s(n) = 2$ *для* $14 \le n \le 17$,
$s(n) = 1$ *для* $6 \le n \le 13$.

В частности, для любого натурального числа $n > 6$ *существует нечетное простое число* p *такое, что* $(n+1)/2 < p < n-1$, *и для любого натурального числа* $n > 3$ *существует нечетное простое число* p *такое, что* $n - p < p < n$.

Доказательство. Предположим вначале, что $n > 739$, и положим $n = 185u + v$, где $u \ge 4$ — натуральное число, а $0 \le v < 185$. Согласно [6] существуют простые числа $p_1, \dots, p_6$ такие, что $119u < p_1 < 128u < p_2 < 138u < p_3 < 149u < p_4 < 160u < p_5 < 172u < p_6 < 185u \le n$. Если $119u \le (n+1)/2$, то $119u \le (185u + 185)/2$ и $u < 4$. Поэтому $n \le 185 \cdot 3 + 184 = 739$ вопреки предположению. Тогда $n \le 739$ и заключение легко проверить перебором.

Лемма 2. *Если* $n \ge 2$, *то* $\omega(A_n) \subsetneqq \omega(A_{n+1})$. *Если* $n \ge 2$ *и* $n \ne 5$, *то* $\omega(S_n) \subsetneqq \omega(S_{n+1})$.

Доказательство проведем индукцией по n. Для $n \le 18$ утверждение леммы легко проверить непосредственно. Пусть $n > 18$. По лемме 1 существуют нечетные простые числа p_1, p_2, p_3, для которых $n/2 < p_3 < p_2 < p_1 < n-1$. Если $n - p_2 = 5$, то n четно, $(n+1) - p_1 < p_1 \le n-3, n - p_1 \ne 5$, и по индукции A_{n-p_1+1} (соответственно S_{n-p_1+1}) содержит элемент x такой, что $|x| \notin \omega(A_{n-p_1})$ (соответственно $|x| \notin \omega(S_{n-p_1})$). Если мы добавим к x цикл длины p_1, то получим элемент y из A_{n+1} (соответственно из S_{n+1}) такой, что $|y| = p_1|x| \notin \omega(A_n)$ (соответственно $|y| \notin \omega(S_n)$). Если $n - p_2 \ne 5$, то годятся те же рассуждения с заменой p_1 на p_2.

Лемма 3. *Существует нильпотентная нормальная подгруппа* N *группы* G *такая, что* $P \le G/N \le \mathrm{Aut}(P)$ *для некоторой неабелевой простой группы* P *с несвязным графом* $GK(P)$ *и* $\mu_i(P) = \{r\}$ *для некоторого числа* $i > 1$.

Доказательство. Согласно [4] верно одно из следующих утверждений:

(а) G — группа Фробениуса с ядром F и дополнением C, и $\pi(F), \pi(C)$ — компоненты связности графа $GK(G)$;

(б) $G = ABC$, где A, AB — нормальные подгруппы группы G и AB, BC — группы Фробениуса с ядрами A, B и дополнениями B, C соответственно;

(в) G является расширением $\pi_1(G)$-группы N посредством группы A, где $P \le A \le \mathrm{Aut}(P)$, P — простая неабелева группа с несвязным графом $GK(P)$, а A/P — $\pi_1(G)$-группа.

Предположим, что выполнен п. (а). По теореме Томпсона [7] подгруппа F нильпотентна.

Если r делит $|F|$, то F является r-группой, $\omega(C) \cup \{r\} = \omega(G) = \omega(A_r)$ и $|C|$ — четное число. Поэтому C содержит центральный элемент порядка 2. Пусть p_1 — наибольшее простое число, для которого $p_1 \le r - 1$. По лемме 1 $p_1 > r - p_1$ и p_1 нечетно. Если $r - p_1 \ge 3$, то по лемме 1 существует нечетное простое число p_2, для которого $r - p_1 - p_2 < p_2 \le r - p_1$. Продолжив этот процесс, мы получим простые числа $r > p_1 > \dots > p_t > 2$ такие, что $r - 2 \le p_1 + \dots + p_t \le r$. Это означает, что A_r содержит элемент порядка $p_1 \cdots p_t \ne r$, но не содержит элементов порядка $2p_1 \cdots p_t$. С другой стороны, C содержит элемент порядка $p_1 \cdots p_t$ и тем самым содержит элемент порядка $2p_1 \cdots p_t$. Это противоречие показывает, что r не может делить $|F|$.

Таким образом, $|C| = r$. Пусть t — натуральное число такое, что $2^t + 2 < r < 2^{t+1} + 2$. Тогда A_r содержит элемент порядка 2^t и $2^t + 2 > r/2$. Пусть q — наибольшее простое число, для которого $q < r$. Тогда $q > r/2 > 2$, и поэтому A_r содержит элемент порядка q, но не содержит элементов порядка $2^t q$. С другой стороны, $2^t, q \in \omega(F)$, и поскольку подгруппа F нильпотентна, F содержит элемент порядка $2^t q$. Это противоречие показывает, что (а) не имеет места.

Предположим, что верен п. (б). Тогда $|B| = r$, и поэтому C — циклическая группа. По лемме 1 существуют различные простые числа p_1 и p_2 такие, что $(r+1)/2 < p_1,\ p_2 \leq r - 1$. Это означает, что G содержит элементы порядков p_1, p_2, но не содержит элементов порядка $p_1 p_2$. Ввиду строения группы G это невозможно, и поэтому верен п. (в).

Если r делит порядок группы N или фактор-группы A/P, то $r \in \pi_1(G)$, что невозможно. Следовательно, $\{r\}$ — компонента связности группы P, и подгруппа N нильпотентна по теореме Томпсона. Лемма доказана.

Лемма 4. *Пусть P — конечная простая группа с несвязным графом $GK(P)$. Тогда $|\mu_i(P)| = 1$ для $2 \leq i \leq s(P)$. Пусть n_i означает единственный элемент из $\mu_i(P)$ для $i > 1$. Тогда P, $\pi_1(P)$, n_i для $2 \leq i \leq s(P)$ такие, как в табл.* 1–3, *где p — нечетное простое число.*

Доказательство. Группы P и множества $\pi_i(P)$ были найдены Уильямсом и А. С. Кондратьевым [4, 5]. Мы объединяем их результаты в табл. 1–3, исправив опечатки и мелкие погрешности. Ими было также доказано, что в случае группы P лиева типа, за исключением групп $P = A_1(q)$, где число q нечетно, для $i > 1$ имеет место равенство $\mu_i(P) = \mu(T)$, где T — некоторый максимальный тор в P, являющийся изолированной в P подгруппой. Поэтому для доказательства леммы достаточно показать, что соответствующие торы T циклические.

Предположим, что тор T не является циклическим. Тогда существует подгруппа $E \simeq Z_p \times Z_p$ в T для некоторого нечетного простого числа p, отличного от характеристики группы P. Поскольку T — изолированная подгруппа в P, то $T = \langle C_P(e) \mid e \in E^{\#} \rangle$. По теореме 1 из [8] характеристика группы P равна 2 и либо $p = 3$, либо $p = 5$ и $P \simeq {}^2F_4(2)'$. Это противоречит результатам из [5].

Лемма 5. *Пусть p_1, p_2 — различные простые числа, делящие порядок группы G, и пусть $p_1, p_2 < r < p_1 + p_2$. Тогда в G нет элементов порядка $p_1 p_2$.*

Доказательство очевидно, поскольку в A_r нет таких элементов.

Лемма 6. *Пусть P и N такие, как в лемме* 3.

(а) *Если p_1, p_2 — различные простые числа, делящие порядок подгруппы N, то $r \geq p_1 + p_2$. В частности, существует самое большее одно простое число p такое, что $(r+1)/2 \geq p$ и p делит порядок подгруппы N.*

(б) *Группа P не изоморфна спорадической группе, знакопеременной группе или группе $L_2(r^n)$, $n > 1$.*

(в) *Если P не изоморфна ${}^2G_2(q)$, то для любого числа i существует самое большее одно простое число $s \in \pi_i(P)$ такое, что $(r+1)/2 < s < r$. Если P изоморфна ${}^2G_2(q)$, то существуют самое большее три простых числа $s \in \pi(P)$, для которых $(r+1)/2 < s < r$.*

Таблица 1. Конечные простые группы P с $s(P) = 2$

P	Ограничения на P	$\pi_1(P)$	n_2
A_n	$6 < n = p, p+1, p+2$; одно из $n, n-2$ не простое	$\pi((n-3)!)$	p
$A_{p-1}(q)$	$(p,q) \neq (3,2), (3,4)$	$\pi\Big(q\prod_{i=1}^{p-1}(q^i-1)\Big)$	$\frac{q^p-1}{(q-1)(p,q-1)}$
$A_p(q)$	$(q-1)\|(p+1)$	$\pi\Big(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-1)\Big)$	$\frac{q^p-1}{q-1}$
${}^2A_{p-1}(q)$		$\pi\Big(q\prod_{i=1}^{p-1}(q^i-(-1)^i)\Big)$	$\frac{q^p+1}{(q+1)(p,q+1)}$
${}^2A_p(q)$	$(q+1)\|(p+1)$, $(p,q) \neq (3,3), (5,2)$	$\pi\Big(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-(-1)^i)\Big)$	$\frac{q^p+1}{q+1}$
${}^2A_3(2)$		$\{2,3\}$	5
$B_n(q)$	$n = 2^m \geq 4$, q нечетно	$\pi\Big(q\prod_{i=1}^{n-1}(q^{2i}-1)\Big)$	$\frac{q^n+1}{2}$
$B_p(3)$		$\pi\Big(3(3^p+1)\prod_{i=1}^{p-1}(3^{2i}-1)\Big)$	$\frac{3^p-1}{2}$
$C_n(q)$	$n = 2^m \geq 2$	$\pi\Big(q\prod_{i=1}^{n-1}(q^{2i}-1)\Big)$	$\frac{q^n+1}{(2,q-1)}$
$C_p(q)$	$q = 2, 3$	$\pi\Big(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1)\Big)$	$\frac{q^p-1}{(2,q-1)}$
$D_p(q)$	$p \geq 5$, $q = 2, 3, 5$	$\pi\Big(q\prod_{i=1}^{p-1}(q^{2i}-1)\Big)$	$\frac{q^p-1}{q-1}$
$D_{p+1}(q)$	$q = 2, 3$	$\pi\Big(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1)\Big)$	$\frac{q^p-1}{(2,q-1)}$
${}^2D_n(q)$	$n = 2^m \geq 4$	$\pi\Big(q\prod_{i=1}^{n-1}(q^{2i}-1)\Big)$	$\frac{q^n+1}{(2,q+1)}$
${}^2D_n(2)$	$n = 2^m+1$, $m \geq 2$	$\pi\Big(2(2^n+1)\prod_{i=1}^{n-2}(2^{2i}-1)\Big)$	$2^{n-1}+1$
${}^2D_p(3)$	$5 \leq p \neq 2^m+1$	$\pi\Big(3\prod_{i=1}^{p-1}(3^{2i}-1)\Big)$	$\frac{3^p+1}{4}$
${}^2D_n(3)$	$n = 2^m+1 \neq p, m \geq 2$	$\pi\Big(3(3^n+1)\prod_{i=1}^{n-2}(3^{2i}-1)\Big)$	$\frac{3^{n-1}+1}{2}$
$G_2(q)$	$2 < q \equiv \varepsilon(3)$, $\varepsilon = \pm 1$	$\pi(q(q^2-1)(q^3-\varepsilon))$	$q^2-\varepsilon q+1$
${}^3D_4(q)$		$\pi(q(q^6-1))$	q^4-q^2+1
$F_4(q)$	q нечетно	$\pi(q(q^6-1)(q^8-1))$	q^4-q^2+1
${}^2F_4(2)'$		$\{2,3,5\}$	13
$E_6(q)$		$\pi(q(q^5-1)(q^8-1)(q^{12}-1))$	$\frac{q^6+q^3+1}{(3,q-1)}$

Окончание таблицы 1

P	Ограничения на P	$\pi_1(P)$	n_2
${}^2E_6(q)$	$q > 2$	$\pi(q(q^5+1)(q^8-1)(q^{12}-1))$	$\frac{q^6-q^3+1}{(3,q+1)}$
M_{12}		$\{2,3,5\}$	11
J_2		$\{2,3,5\}$	7
Ru		$\{2,3,5,7,13\}$	29
He		$\{2,3,5,7\}$	17
McL		$\{2,3,5,7\}$	11
Co_1		$\{2,3,5,7,11,13\}$	23
Co_3		$\{2,3,5,7,11\}$	23
Fi_{22}		$\{2,3,5,7,11\}$	13
F_5		$\{2,3,5,7,11\}$	19

(г) *Для любого простого числа s, удовлетворяющего неравенству $(r+1)/2 < s < r$, порядок фактор-группы* $\mathrm{Aut}(P)/P$ *не делится на s.*

Доказательство. Поскольку подгруппа N нильпотентна, утверждение (а) следует из леммы 5 .

Докажем (б). Предположим, что группа P изоморфна спорадической группе. Поскольку r — наибольший простой делитель числа $|G|$ и $|G|$ делится на любое простое число $p < r$, по (а) и лемме 4 группа P изоморфна Fi_{23} или Fi'_{24}, а $|N|$ делится на 19. Но в этом случае P содержит подгруппу Фробениуса порядка $23 \cdot 11$, и поэтому G содержит элемент порядка $19 \cdot 23$ или $19 \cdot 11$. Поскольку $r < 30$, получаем противоречие с леммой 5.

Предположим, что P изоморфна A_n. По лемме 4 $n = r$, $r+1$ или $r+2$. Поскольку по лемме 2 $\omega(A_n) \subsetneqq \omega(A_{n+1})$, то $n = r$, и ввиду [9] $N = 1$. Так как $\mathrm{Aut}(A_r) = S_r$ и $\omega(A_r) \neq \omega(S_r)$, то $G = A_r$.

Предположим, что P изоморфна $L_2(r^n)$, $n > 1$. Тогда силовская r-подгруппа R из P нециклическая, и поэтому $N = 1$. Поскольку $N_G(R)$ — группа Фробениуса, то $|N_G(R) : R| \leq |R| - 1$, $|G : P| \leq 2$ и тем самым все элементы нечетного порядка из G содержатся в P. Так как $r^{2n} - 1$ делится на 3, то 3 делит $r^n + \varepsilon$, где $\varepsilon = \pm 1$, и число $m = (r^n - \varepsilon)/2$ взаимно просто с 3 и равно порядку некоторого элемента x в A_r. Пусть $m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, где $p_1, \dots, p_t$ — различные простые числа. Если m нечетно, то выберем элемент x в виде произведения $c = c_1 \cdots c_t$ независимых циклов $c_1, \dots, c_t$ таких, что длина c_i равна $p_i^{\alpha_i}$, а если m четно, то положим $x = cc_{t+1}$, где c_{t+1} — транспозиция, независимая со всеми c_i, $i \leq t$. Если m — степень простого числа, то $m < r$, что невозможно, поскольку $r < (r+1) \cdot (r-1)/2 = (r^2-1)/2 \leq (r^n-1)/2 \leq m$. Поэтому $m = uv$, где $u \neq 1 \neq v, (u,v) = 1$, и число u нечетно. Очевидно, что элемент x^v имеет порядок u и оставляет неподвижными по меньшей мере три точки при естественном действии группы A_r. Поскольку u не делится на 3, A_r содержит элемент порядка $3u \notin \omega(P)$. Следовательно, P не изоморфна $L_2(r^n)$, $n > 1$.

Чтобы доказать (в) и (г), исследуем отдельно каждую возможность, представленную в табл. 1–3. Обозначим $A = \mathrm{Aut}(P)$. Пусть s — простой делитель числа $|A|$, удовлетворяющий условию $(r+1)/2 < s < r$.

Таблица 2. Конечные простые группы P с $s(P) = 3$

P	Ограничения на P	$\pi_1(P)$	n_2	n_3
A_n	$n > 6$, $n = p, p-2$ просты	$\pi((n-3)!)$	p	$p-2$
$A_1(q)$	$3 \leq q \equiv \varepsilon(4)$, $\varepsilon = \pm 1$	$\pi(q-\varepsilon)$	$\pi(q)$	$(q+\varepsilon)/2$
$A_1(q)$	$q > 2$, q четно	$\{2\}$	$q-1$	$q+1$
$^2A_5(2)$		$\{2,3,5\}$	7	11
$^2D_p(3)$	$p = 2^m+1$, $m \geq 1$	$\pi\left(3(3^{p-1}-1) \times \prod_{i=1}^{p-2}(3^{2i}-1)\right)$	$(3^{p-1}+1)/2$	$(3^p+1)/4$
$G_2(q)$	$q \equiv 0(3)$	$\pi(q(q^2-1))$	q^2-q+1	q^2+q+1
$^2G_2(q)$	$q = 3^{2m+1} > 3$	$\pi(q(q^4-1))$	$q-\sqrt{3q}+1$	$q+\sqrt{3q}+1$
$F_4(q)$	$q > 2$, q четно	$\pi(q(q^4-1)(q^6-1))$	q^4+1	q^4-q^2+1
$^2F_4(q)$	$q = 2^{2m+1} > 2$	$\pi(q(q^3+1)(q^4-1))$	$q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$
$E_7(2)$		$\{2,3,5,7,11,13,17,19,31,43\}$	73	127
$E_7(3)$		$\{2,3,5,7,11,13,19,37,41,61,73,547\}$	757	1093
M_{11}		$\{2,3\}$	5	11
M_{23}		$\{2,3,5,7\}$	11	23
M_{24}		$\{2,3,5,7\}$	11	23
J_3		$\{2,3,5\}$	17	19
HiS		$\{2,3,5\}$	7	11
Suz		$\{2,3,5,7\}$	11	13
Co_2		$\{2,3,5,7\}$	11	23
Fi_{23}		$\{2,3,5,7,11,13\}$	17	23
F_3		$\{2,3,5,7,13\}$	19	31
F_2		$\{2,3,5,7,11,13,17,19,23\}$	31	47

Предположим, что $s(P) = 2$. В силу (б) можно считать, что P — простая группа лиева типа ранга > 1 над $GF(q)$, где $q = t^k$ для некоторого простого числа t. Тогда $\pi(A/P) \subseteq \pi(6k(q^2-1))$.

Пусть $P = A_m^\varepsilon(q)$, $m > 1$, $\varepsilon = \pm 1$. По лемме 4

$$\pi(P) = \pi\left(q\prod_{i=1}^{f}(q^i - \varepsilon^i)\right)$$

для некоторого натурального числа f и для некоторого нечетного простого чис-

Таблица 3. Конечные простые группы P с $s(P) > 3$

$s(P)$	P	Ограничения на P	$\pi_1(P)$	n_2	n_3	n_4	n_5	n_6
4	$A_2(4)$		$\{2\}$	3	5	7		
	${}^2B_2(q)$	$q{=}2^{2m+1} > 2$	$\{2\}$	$q{-}1$	$q-\sqrt{2q}+1$	$q+\sqrt{2q}+1$		
	${}^2E_6(2)$		$\{2,3,5,7,11\}$	13	17	19		
	$E_8(q)$	$q \equiv 2,3(5)$	$\pi(q(q^8{-}1)(q^{14}{-}1)(q^{12}{-}1)(q^{18}{-}1)(q^{20}{-}1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	$q^8{-}q^4{+}1$		
	M_{22}		$\{2,3\}$	5	7	11		
	J_1		$\{2,3,5\}$	7	11	19		
	$O'N$		$\{2,3,5,7\}$	11	19	31		
	LyS		$\{2,3,5,7,11\}$	31	37	67		
	Fi'_{22}		$\{2,3,5,7,11,13\}$	17	23	29		
	F_1		$\{2,3,5,7,11,13,17,19,23,29,31,47\}$	41	59	71		
5	$E_8(q)$	$q \equiv 0,1,4(5)$	$\pi(q(q^8{-}1)(q^{10}{-}1)(q^{12}{-}1)(q^{14}{-}1)(q^{18}{-}1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	$q^8{-}q^4{+}1$	$\frac{q^{10}+1}{q^2+1}$	
6	J_4		$\{2,3,5,7,11\}$	23	29	31	37	43

ла p верно одно из следующих утверждений:

(i) $m = p-1$, $r = (q^p-\varepsilon)/(q-\varepsilon)(p,q-\varepsilon)$;

(ii) $m = p$, $r = (q^p-\varepsilon)/(q-\varepsilon)$, $(q-\varepsilon)|(p+1)$.

Заметим, что

$$(r+1)/2 > q+1. \tag{1}$$

Предположив противное, получим, что $17 \le r \le 2q+1$, т. е. $q \ge 8$ и

$$(q^p-\varepsilon)/(q-\varepsilon)(p,q-\varepsilon) \le 2q+1.$$

Если $p \ge 5$, то

$$q^5-\varepsilon \le q^p-\varepsilon \le (2q+1)(q-\varepsilon)(q-\varepsilon,p) \le (2q+1)(q-\varepsilon)^2 < 2q^4-\varepsilon$$

и $q^5 < 2q^4$, что невозможно. Поэтому $p = 3$ и мы последовательно получаем $(q^3-\varepsilon)/3(q-\varepsilon) \le r \le 2q+1$, $q^2+\varepsilon q+1 \le 6q+3$, $q^2+(\varepsilon-6)q-2 \le 0$, $q \le 7$, что невозможно.

По (1) s не делит A/P. В частности, верно (г), и s делит $(q^i-\varepsilon^i)/(q-\varepsilon)$ для некоторого числа i, $2 \le i \le m+1$. Заметим, что

$$(q^i-\varepsilon^i)/(q-\varepsilon) < s \quad \text{для} \quad i \le p-2. \tag{2}$$

Действительно, по (1) можно предполагать, что $p \geq 5$ и $2 \leq i \leq p-2$. Если $\varepsilon = 1$, то

$$(q^i-1)/(q-1) \leq (q^{p-2}-1)/(q-1) \leq (q^p-1)/2(q-1)^2 \leq r/2 < s.$$

Пусть $\varepsilon = -1$. Тогда для $q > 2$

$$(q^p+1)/2(q+1) - (q^{p-2}+1) = ((q-3)/2 + 1/2(q+1))q^{p-2} - (2q+1)/(2q+2) > 0$$

и, следовательно,

$$(q^i-(-1)^i)/(q+1) \leq (q^{p-2}+1)/(q+1) \leq (q^p+1)/2(q+1)^2 \leq r/2 < s.$$

Если $q = 2$, то

$$(q^i-(-1)^i)/(q+1) \leq (2^{p-2}+1)/3 = (2^p/4+1)/3 < (2^p+1)/6 = r/2 < s.$$

Покажем, что

$$q^{(p-1)/2} + 1 \leq (r+1)/2. \tag{3}$$

Предположим противное. По (1) $p > 3$. Если $\varepsilon = 1$, то

$$2q^{(p-1)/2} \geq r \geq (q^p-1)/(q-1)^2 > q^{p-2},$$

следовательно, $2 > q^{(p-3)/2}$. Это неравенство невозможно.

Пусть $\varepsilon = -1$. Тогда при $q > 3$

$$(q^p+1)/(q+1)^2 - 2q^{p-3} > q^p/(q+1)^2 - 2q^{p-3} = q^{p-3}(q^3-2q^2-4q-2)/(q+1)^2 > 0,$$

откуда

$$2q^{(p-1)/2} \geq r \geq (q^p+1)/(q+1)^2 > 2q^{p-3}$$

и $2 > 2q^{(p-5)/2}$, что невозможно. Если $q = 2, 3$, то справедливость (3) легко проверить непосредственно.

Пусть выполнено (i). По (2) s делит

$$(q^{p-1}-1)/(q+\varepsilon) = (q^{(p-1)/2}+1)(q^{(p-1)/2}-1)/(q+\varepsilon),$$

что по (3) невозможно.

Пусть выполнено (ii). По (2) и (3) s делит $(q^{p+1} \pm 1)/(q^2-1)$, т. е. s делит $q^{(p+1)/2}+1$. Чтобы получить противоречие, достаточно доказать, что при $r \geq 17$

$$q^{(p+1)/2} + 1 \leq (r+1)/2 = ((q^p-\varepsilon)/(q-\varepsilon)+1)/2. \tag{4}$$

Если $p = 3$, то по условию $(q-\varepsilon)|(p+1)$ при $\varepsilon = 1$ значение q равно 2, 3 или 5 и $r = 7, 13, 31$ соответственно, а при $\varepsilon = -1$ будет $q = 3$ и $r = 7$. Поэтому $q = 5$, $\varepsilon = 1$ и $r = 31$, что противоречит выбору s. Если $p = 5$, то (4) верно. Пусть $p \geq 7$ и (4) не верно. Тогда

$$2(q-\varepsilon)(q^{(p+1)/2}+1) > q^p + q - 2\varepsilon$$

и

$$2q^{(p+3)/2} + q > q^p + 2\varepsilon q^{(p+1)/2}. \tag{5}$$

Поскольку очевидно, что $4q^{(p+3)/2} \leq q^p$, $q^{(p+1)/2} + q < q^{(p+3)/2}$ и $q < 2q^{(p+1)/2}$, неравенство (5) невозможно.

Предположим, что P равно $B_n(q)$, q нечетно, $C_n(q)$ или ${}^2D_n(q)$, где $n = 2^m$. Тогда по лемме 4 $\pi_1(P) = \pi\left(q\prod_{i=1}^{n-1}(q^{2i}-1)\right)$ и $r = (q^n+1)/(2, q-1)$. Как и выше, можно показать, что (1) и, следовательно, (г) выполнены. Далее, $s|(q^i \pm 1)$ для некоторого числа i, $1 \leq i \leq n-1$. По (1) $i > 1$ и поэтому $n \geq 4$. Если $s|(q^i - 1)$, то

$$s|(q^i - 1)/(q-1) \leq (q^{n-1} - 1)/(q-1) \leq (q^n - 1)/2(q-1) < r/2 < s.$$

Отсюда $s|(q^i + 1)$. Пусть $i \leq n-2$. Если $q = 2$, то $q^i + 1 \leq 2^{n-2} + 1 \leq (2^n + 1)/2 \leq r/2 < s$. Следовательно, $q > 2$ и $q^i + 1 \leq q^{n-2} + 1 \leq (q^n + 3)/4 \leq (r+1)/2 < s$. Поэтому $s|(q^{n-1} + 1)/(q+1) \leq (q^n + 1)/2(q+1) \leq r/2 < s$, что невозможно.

Предположим, что $P = B_p(q)$, $q = 3$, $C_p(q)$, $q = 2, 3$, или $P = D_{p+1}(q)$, $q = 2, 3$, где p — нечетное простое число. Тогда по лемме 4

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

и $r = (q^p - 1)/(2, q-1)$. Как и выше, показывается, что (1) и (г) верны и s делит $q^{p-1} + 1$ или $q^p + 1$. Пусть $s|(q^{p-1} + 1)$. Если $q = 3$, то $(3^{p-1} + 1)/2 \leq (3^p - 1)/4 = r/2 < s$. Если $q = 2$, то $s|(2^{p-1} + 1)$. Так как $2^{p-1} = (r+1)/2 < s$, то $s = (2^{p-1} + 1)$. Пусть $s|(q^p + 1)$. Тогда $s|(q^p + 1)/(q+1)$. Если $q = 2$, то $s|(2^p + 1)/3$ и $(r+1)/2 - (2^p + 1)/3 = (2^{p-1} - 1)/3 > 0$. Если $q = 3$, то $s|(3^p + 1)/4 = (r+1)/2$ и (в) верно.

Предположим, что $P = D_p(q)$, где $p \geq 5$ — нечетное простое число и $q = 2, 3, 5$. Тогда по лемме 4

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

и $r = (q^p - 1)/(q-1)$. Как и выше, доказывается, что (1) и (г) верны и $s|(q^i + 1)$ для некоторого числа i, $2 \leq i \leq p-1$. Если $i \leq p-2$, то $q^i + 1 \leq q^{p-2} + 1$ и $(r+1)/2 - (q^{p-2} + 1) = (q^{p-2}(q^2 - 2q + 2) - q)/2(q-1) \geq 0$, т. е. $s \leq (r+1)/2$. Следовательно, $s|(q^{p-1} + 1)$. Если q нечетно, то $s|(q^{p-1} + 1)/2$ и $(r+1)/2 - (q^{p-1} + 1)/2 = (q^{p-1} - 1)/2(q-1) > 0$. Поэтому $q = 2$ и $s|(2^{p-1} + 1)$. Так как $2^{p-1} = (r+1)/2 < s$, то $s = (2^{p-1} + 1)$ и (в) верно.

Пусть $P = {}^2D_n(q)$, $n \geq 4$. Тогда по лемме 4 для некоторого нечетного простого числа p верно одно из следующих утверждений:

(i) выполнены равенства

$$n = 2^m + 1,\ q \leq 3,\ r = (q^{n-1} + 1)/(2, q-1),\ \pi_1(P) = \pi\left(q(q^n + 1)\prod_{i=1}^{n-2}(q^{2i} - 1)\right);$$

(ii) справедливы равенства

$$n = p, \quad q = 3, \quad r = (3^p + 1)/4, \quad \pi_1(P) = \pi\left(q\prod_{i=1}^{n-2}(q^{2i} - 1)\right).$$

Так же, как и раньше, доказывается, что (1) и (г) верны и $s|(q^i \pm 1)$ для некоторого числа i, $2 \leq i \leq n-2$, или же $s|(q^n + 1)/(q+1)$. Прямой проверкой показывается, что в случае, когда $s|(q^i \pm 1)$, $2 \leq i \leq n-2$, имеет место невозможное неравенство $s \leq (r+1)/2$. Следовательно, $s|(q^n + 1)/(q+1)$. Если $q = 3$, то $s|(3^n + 1)/4 > r = (3^{n-1} + 1)/2$ и поэтому $s \leq (3^n + 1)/8 < (r+1)/2$, что невозможно. Таким образом, $q = 2$, $s|(2^n + 1)/3$ и $(r+1)/2 = 2^{n-2} + 1$. Если $s < (2^n + 1)/3$, то $s \leq (r+1)/2$. Итак, $s = (2^n + 1)/3$, и (в) выполнено.

Если $P = G_2(q)$, $2 < q \equiv \varepsilon(3)$, $\varepsilon = \pm 1$, то $q \geq 4$, $r = q^2 - \varepsilon q + 1$ и s делит $q \pm 1$ или $(q^2 + \varepsilon q + 1)/3$. Каждое из этих чисел не превосходит $(r+1)/2$.

Если $P = {}^3D_4(q)$, то $r = q^4 - q^2 + 1$ и s делит одно из чисел $q \pm 1$ или $(q^2 \pm q + 1)/3$, каждое из которых не превосходит $(r+1)/2$.

Пусть $P = F_4(q)$, q нечетно. Тогда $r = q^4 - q^2 + 1$ и s делит $q \pm 1$, $q^2 + 1$, $(q^2 \pm q + 1)$ или $(q^4 + 1)/2$. Все эти числа, исключая $(q^4 + 1)/2$, не превосходят $(r+1)/2$. Поэтому $s|(q^4 + 1)/2$. Так как $(q^4 + 1)/2 < ((r+1)/2)^2$, существует самое большее одно такое число s.

Пусть $P = E_6^\varepsilon(q)$, $\varepsilon = \pm 1$ и $q > 2$ для $\varepsilon = -1$. Тогда $r = (q^6 + \varepsilon q^3 + 1)/(3, q - \varepsilon)$ и s делит $q \pm 1$, $q^2 + 1$, $(q^2 \pm q + 1)$, $q^4 + 1$, $q^4 - q^2 + 1$ или $(q^5 - \varepsilon)/(q - \varepsilon)$. Все эти числа меньше, чем $(r+1)/2$.

Предположим, что $s(P) \geq 3$. Тогда $r = n_t$ для некоторого числа t. Поскольку во всех случаях для каждой пары i, j верно неравенство $n_i < ((n_j + 1)/2)^2$, существует не более одного простого делителя s числа n_i, для которого $s > (r+1)/2$.

Кроме того, легко заметить, что в этом случае $|A/P| < (n_j + 1)/2$ при $j > 1$ и поэтому (г) выполнено.

Пусть $s > (r+1)/2$ — простое число из $\pi_1(P)$. Если $P = {}^2D_p(3)$, $p = 2^m + 1 \geq 5$, то s делит $(3^{p-1} - 1)/4$ или $(3^i \pm 1)/2$ при $i < p - 1$, но все эти числа меньше, чем $(n_j + 1)/2$ при $j > 1$. Если $P = G_2(q)$, q — степень числа 3, то s делит число $(q \pm 1)/2$, которое меньше, чем $(n_j + 1)/2$ при $j > 1$. Если $P = {}^2G_2(q), q = 3^{2m+1} > 3$, то s делит $(q+1)/4, (q-1)/2$ или $(q^2 + 1)/10$. Так как первое число меньше, чем $(n_j + 1)/2$ при j, равном 2 или 3, второе может делиться на s, только если оно простое, а третье меньше, чем $(n_j + 1)/2)^2$ при $j > 1$, то существуют самое большее два простых числа $s \in \pi_1(P)$, для которых $s > (r+1)/2$. Если $P = F_4(q)$, $q = 2^m > 2$, то s делит одно из чисел $q \pm 1, q^2 + 1$ или $q^2 \pm q + 1$, каждое из которых меньше, чем $(n_j + 1)/2$ при $j > 1$. Если $P = {}^2F_4(q)$, $q = 2^{2m+1} > 2$, то s делит одно из чисел $q \pm 1$, $(q^2 - q + 1)/3$ или $(q^2 + 1)/5$, каждое из которых не больше, чем $(n_j + 1)/2$ при $j > 1$. Если $P = E_8(q)$, то s делит $q^i \pm 1, i \leq 7$, $q^6 \pm q^3 + 1$ или $q^{10} + 1$. Если $q = 2$, то $r = n_2 = 331$ и все эти числа, исключая $q^{10} + 1$, меньше, чем $(r+1)/2$. Если $q > 2$, то все эти числа, исключая $q^{10} + 1$, меньше, чем $(n_j + 1)/2$ при $j > 1$. Поэтому s делит $q^{10} + 1$. Поскольку $q^{10} + 1 < ((n_j + 1)/2)^2$ для $j = 2, 3, 4$, существует не более одного такого числа s. Все остальные случаи очевидны.

Лемма 7. *Если $s(P) = 2$, то $r = 17$. Если $s(P) = 3$, то $r \leq 37$. Если $s(P) = 4$, то $r \leq 41$. Если $s(P) = 5$, то $r \leq 47$.*

Доказательство вытекает из лемм 6 и 1.

Лемма 8. *Все случаи, указанные в лемме 7, невозможны.*

Доказательство. Если $s(P) = 2$, то $r = 17$, и из табл. 1 получаем, что P равно $C_4(2)$, ${}^2D_4(2)$ или ${}^2D_5(2)$. В первом и втором случаях $11, 13 \notin \omega(\mathrm{Aut}(P))$, что противоречит п. (а) леммы 6. Если $P = {}^2D_5(2)$, то $13 \in \pi(N)$, и поскольку силовская 5-подгруппа в P нециклическая, G содержит элемент порядка $5 \cdot 13 \notin \omega(A_{17})$.

Если $s(P) > 2$, то $r \leq 47$ только в следующих случаях:

(а) $P = {}^2B_2(32)$, $r = 41$;

(б) $P = {}^2G_2(27)$, $r = 37$;

(в) $P = {}^2E_6(2)$, $r = 19$;

(г) $P = A_1(q)$, $q \leq 96$.

В случаях (а) и (б) $|N|$ делится на 23 и 29, что невозможно по п. (а) леммы 6.

Предположим, что выполнено (в). Множество $\omega(\mathrm{Aut}(P))$ можно извлечь из [10]. Так как $P.2$ содержит элемент порядка 48, а $P.3$ — элемент порядка $3 \cdot 17$, то $G/N = P$. Поскольку A_{19} содержит элемент порядка $7 \cdot 11 \notin \omega(P)$, $|N|$ делится на 7 или 11, и поэтому $13 \notin \omega(N)$. Так как $5 \cdot 13 \notin \omega(P)$, то $|N|$ делится на 5. Ясно, что 17 не делит $|N|$ и элемент порядка 17 действует на N без неподвижных точек. Но P содержит подгруппу Фробениуса порядка $17 \cdot 8$, значит, G содержит элемент порядка $5 \cdot 7 \cdot 8$ или $5 \cdot 11 \cdot 8$. Для A_{19} это неверно.

В случае (г) прямыми вычислениями легко установить, что существуют два простых числа $> (r+1)/2$, делящие $|N|$, вопреки п. (а) леммы 6.

Лемма и теорема доказаны.

ЛИТЕРАТУРА

1. *Shi W.* A characteristic property of A_5 // J. Southwest-China Teachers Univ. 1986. V. 3. P. 11–14 (in Chinese).

2. *Brandl R., Shi W.* Finite groups whose element orders are consecutive integers // J. Algebra. 1991. V. 143, N 2. P. 388–400.

3. *Praeger C. E., Shi W.* A characterization of some alternating and symmetric groups // Comm. Algebra. 1994. V. 22, N 5. P. 1507–1530.

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

5. *Кондратьев А. С.* О компонентах графа простых чисел для конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.

6. *Rohrbach H., Weis J.* Zum finiten Fall des Bertrandschen Postulates // J. Reine Angew. Math. 1964. V. 214, N 5. P. 432–440.

7. *Thompson J. G.* Normal p-complements for finite groups // Math Z. 1960. Bd 72, N. 2. S. 332–354.

8. *Seitz G. M.* Generation of finite groups of Lie type // Trans. Amer. Math. Soc. 1882. V. 271, N 2. P. 351–407.

9. *Заварницин А. В., Мазуров В. Д.* О порядках элементов в накрытиях симметрических и знакопеременных групп // Алгебра и логика. 1999. Т. 38, № 3. С. 296–315.

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

Статья поступила 14 декабря 1998 г.

г. Екатеринбург
Институт математики и механики УрО РАН
a.s.kondratiev@imm.uran.ru

г. Новосибирск
Институт математики им. С. Л. Соболева СО РАН
mazurov@math.nsc.ru