Сибирский математический журнал
Январь—февраль, 2015. Том 56, № 1

УДК 512.54

О ХАРАКТЕРИЗУЕМОСТИ ЗНАКОПЕРЕМЕННЫХ ГРУПП ПОРЯДКОМ И ГРАФОМ ПРОСТЫХ ЧИСЕЛ

А. Махмудифар, Б. Хосрави

Аннотация. Имеется несколько графов, связанных со структурой конечной группы: например, граф простых чисел, разрешимый граф и некоммутативный граф конечной группы. В настоящей работе рассматривается характеризуемость знакопеременных групп порядком и графом простых чисел. В частности, показано, что существует тесная связь между характеризуемостью порядком и графом простых чисел для некоторых знакопеременных групп и гипотезой Гольдбаха. Обсуждаются некоторые вопросы и решается задача характеризуемости знакопеременных и симметрических групп порядком и образцом степеней из работы [R. Kogani-Moghaddam, A. R. Moghaddamfar, Groups with the same order and degree pattern, *Sci. China Math.*, 2012].

Ключевые слова: знакопеременная группа, симметрическая группа, разрешимый граф, граф простых чисел, образец степеней, гипотеза Гольдбаха.

1. Введение и предварительные результаты

Все группы в статье предполагаются конечными. Пусть n — натуральное число, и пусть G — группа. Символом $\pi(n)$ обозначим множество всех простых делителей числа n и вместо $\pi(|G|)$ будем писать $\pi(G)$. Множество всех простых чисел p таких, что $n/2 < p \leq n$, обозначается символом $\Pi(n)$. Для простого p через n_p обозначена p-часть числа n, т. е. $n_p = p^k$, если $p^k \mid n$, но $p^{k+1} \nmid n$.

Пусть $GK(G)$ — граф, у которого множество вершин есть $\pi(G)$ и два простых числа $p, q \in \pi(G)$ соединены ребром (пишем $p \sim q$ в $GK(G)$), когда в G есть элемент порядка pq. Этот граф называется *графом простых чисел* группы G. Пусть $\Gamma_{\mathrm{sol}}(G)$ — граф с множеством вершин $\pi(G)$, в котором два простых числа $p, q \in \pi(G)$ соединены ребром (пишем $p \sim q$ в $\Gamma_{\mathrm{sol}}(G)$), когда G содержит подгруппу порядка $p^\alpha q^\beta$, где $\alpha, \beta \geq 1$. Этот граф называется *разрешимым графом* группы G. Независимое подмножество графа — это множество его вершин такое, что не существует ребра между его элементами. Максимальный размер независимых подмножеств в $GK(G)$ обозначается символом $t(G)$. Все не объясняемые ниже обозначения стандартны и могут быть найдены в [1].

Заметим, что если $p \sim q$ в $GK(G)$, то $p \sim q$ в $\Gamma_{\mathrm{sol}}(G)$, хотя обратное, вообще говоря, неверно. В самом деле, если $p \sim q$ в $\Gamma_{\mathrm{sol}}(G)$, в то время как $p \nsim q$ в $GK(G)$, получаем, что в G имеется фробениусова подгруппа порядка $p^\alpha q^\beta$, где $\alpha, \beta \geq 1$. Тогда по свойству Фробениуса либо $p^\alpha \mid (q^\beta - 1)$ либо $q^\beta \mid (p^\alpha - 1)$. Отсюда следует, что если даны порядок и граф простых чисел группы G, то можно получить информацию о разрешимом графе группы G.

The second author was in part supported by a Grant from IPM (No 93200043).

Характеризуемость конечных знакопеременных и симметрических групп порядком и графом простых чисел рассматривалась некоторыми авторами (см. список литературы в [2]). В [3] были исследованы простые группы, имеющие тот же граф простых чисел, что и у знакопеременной группы. В данной работе рассмотрена характеризуемость знакопеременных и симметрических групп порядком и графом простых чисел.

В разд. 2 найдены все конечные группы того же порядка и разрешимого графа, что и у знакопеременной или симметрической группы, и получены некоторые результаты, полезные для характеризации порядком и графом простых чисел. Затем определено, какие знакопеременные группы характеризуются порядком и графом простых чисел. Наконец, в разд. 3 даны ответы на некоторые гипотезы и проблему, изложенные в [2].

В силу леммы 3 из [4] имеем следующее утверждение.

Лемма 1.1. *Если* $n \geq 21$, *то* $|\Pi(n)| \geq (0.366)n/\ln(n)$. *В частности,* $|\Pi(n)| \geq 3$.

Из леммы 2.11 в [5] вытекает

Лемма 1.2. *Если* n *— натуральное число и* $t \in \pi(n!)$, *то* $(n!)_t < t^{n/(t-1)}$.

Используя теорему Жигмонди [6], можно легко получить следующий результат.

Лемма 1.3. *Если* $n \geq 82$, *то* $\pi(n(n+1)) \nsubseteq \{2, 3, 5\}$.

Лемма 4 в [7] дает следующее утверждение.

Лемма 1.4 [8, предложение 1.1]. *Пусть* $G = A_n$ *или* S_n *— знакопеременная или симметрическая группа степени* n. *Предположим также, что* $r, s \in \pi(G) \setminus \{2\}$. *Тогда*

(1) G *имеет элемент порядка* rs *тогда и только тогда, когда* $r + s \leq n$.

(2) A_n *имеет элемент порядка* $2r$ *тогда и только тогда, когда* $r + 4 \leq n$.

(3) S_n *имеет элемент порядка* $2r$ *тогда и только тогда, когда* $r + 2 \leq n$.

Лемма 1.5 [9, лемма 1]. *Предположим, что* G *— конечная группа и* N *— нормальная подгруппа в* G. *Справедливы следующие утверждения.*

(1) *Если* $t \in \pi(G/N)$, $t' \in \pi(N)$ *и* $t \neq t'$, *то* $t \sim t'$ *в* $\Gamma_{\mathrm{sol}}(G)$.

(2) *Если* $t \sim t'$ *в* $\Gamma_{\mathrm{sol}}(G/N)$, *то* $t \sim t'$ *в* $\Gamma_{\mathrm{sol}}(G)$.

Наконец, используем очень известную гипотезу Гольдбаха.

Гипотеза Гольдбаха. *Для четного* $n > 6$ *существуют два простых числа* p *и* q *такие, что* $n = p + q$.

Эта гипотеза подтверждена (см., например, [10]) для четных чисел, не превосходящих 1.2×10^{18}. Также было установлено в [11, 12], что если существуют четные числа, не представимые в виде суммы двух простых, то их доля стремится к нулю с ростом n. Нам нужна более сильная гипотеза о том, что каждое четное число $n > 6$ является суммой двух различных простых. Это так для прямо проверяемых чисел, и нижняя грань для числа различных представлений n в виде суммы двух простых растет с ростом n.

Если $n = p + q$ таково, что $p > q$ — различные простые числа, то будем говорить, что $n = p + q$ — *разбиение Гольдбаха числа* n.

2. Основные результаты

Основной целью данного параграфа является доказательство следующей теоремы, которую можно применить к широкому классу конечных групп и которая является мощным средством в характеризации конечных групп их разрешимым графом или графом простых чисел.

Теорема 2.1. *Пусть G — конечная группа и T — независимое подмножество в $\Gamma_{\rm sol}(G)$, где $|T| \geq 2$. Тогда существует неабелева простая группа S такая, что*

$$S \leq \overline{G} := \frac{G}{N} \leq \mathrm{Aut}(S),$$

где $N = O_{T'}(G)$. При этом $T \subseteq \pi(S)$ и $\pi(\overline{G}/S) \cap T = \varnothing$. Кроме того, $C_G(N) \leq N$ или $S \leq C_G(N)N/N$.

Доказательство. Пусть S — произвольная минимальная нормальная подгруппа группы $\overline{G} := G/N$. Так как $N = O_{T'}(G)$, мы в силу выбора S получаем, что $\pi(S) \cap T \neq \varnothing$. Поскольку $|T| \geq 2$, если $\pi(\overline{G}/S) \cap T \neq \varnothing$, то существуют $t \in \pi(S) \cap T$ и $t' \in \pi(\overline{G}/S) \cap T$ такие, что $t \neq t'$. Следовательно, в силу леммы 1.5 $t \sim t'$ в $\Gamma_{\rm sol}(G)$; противоречие, так как T — независимое подмножество в $\Gamma_{\rm sol}(G)$. Поэтому $\pi(\overline{G}/S) \cap T = \varnothing$. Также по определению N получим $\pi(N) \cap T = \varnothing$. Ввиду $S \leq \overline{G} = G/N$ имеем $T \subseteq \pi(S)$.

Поскольку S — минимальная нормальная подгруппа группы $\overline{G}$, то $S = S_1 \times \cdots \times S_m$, где S_i, $1 \leq i \leq m$, — изоморфные простые группы. Из $T \subseteq \pi(S)$ вытекает, что $T \subseteq \pi(S_i)$ для каждого i, а из $|T| \geq 2$ следует, что каждая S_i — неабелева простая группа, где $1 \leq i \leq m$. Так как T — независимое подмножество в $\Gamma_{\rm sol}(G)$, то $m = 1$. Поэтому S — неабелева простая группа.

Утверждается, что S — единственная минимальная нормальная подгруппа группы G/N. В самом деле, в противном случае если S и H — две минимальные нормальные подгруппы в G/N и $H \neq S$, то в силу изложенного выше H и S — неабелевы простые группы такие, что $T \subseteq \pi(S) \cap \pi(H)$. Также имеем $H \times S \cong HS \leq G/N$; противоречие, так как T — независимое подмножество в $\Gamma_{\rm sol}(G)$. Значит, S — единственная минимальная нормальная подгруппа в G/N.

Поэтому в силу изложенного выше S — неабелева простая и всякая нетривиальная нормальная подгруппа группы G/N содержит S. Тогда $C_{G/N}(S) = 1$, поэтому

$$S \leq \overline{G} = \frac{G}{N} \leq \mathrm{Aut}(S).$$

Если $C_G(N) \not\leq N$, то $C_G(N)N/N$ — нетривиальная нормальная подгруппа в G/N, стало быть, $S \leq C_G(N)N/N$. $\square$

Лемма 2.2. *Пусть G — конечная группа и $p, q \in \pi(G)$ таковы, что $p \neq q$. Пусть $|G|_p = p$, $|G|_q = q$, $p \nmid (q-1)$ и $q \nmid (p-1)$. Тогда $p \sim q$ в $GK(G)$ если и только если $p \sim q$ в $\Gamma_{\rm sol}(G)$.*

Доказательство. Очевидно, что $p \sim q$ в $GK(G)$; тогда $p \sim q$ в $\Gamma_{\rm sol}(G)$. Пусть $p \nsim q$ в $GK(G)$ и $p \sim q$ в $\Gamma_{\rm sol}(G)$. Отсюда следует, что в G имеется нециклическая подгруппа H такая, что $|H| = pq$, потому что $|G|_p = p$ и $|G|_q = q$. Таким образом, H — фробениусова подгруппа в G. Тем самым $p \mid (q-1)$ или $q \mid (p-1)$; противоречие. $\square$

Следующий результат немедленно вытекает из лемм 2.2 и 1.1.

Следствие 2.3. *Пусть n — натуральное число и G — конечная группа такая, что $|G|_r = r$ для каждого $r \in \Pi(n)$. Тогда $\Pi(n)$ — независимое подмножество в $\Gamma_{\mathrm{sol}}(G)$ тогда и только тогда, когда $\Pi(n)$ — независимое подмножество в $GK(G)$. В частности, если $n \geq 21$ и $\Pi(n)$ — независимое подмножество в $\Gamma_{\mathrm{sol}}(G)$, то $t(G) \geq |\Pi(n)| \geq (0.366)n/\ln(n)$.*

Лемма 2.4. *Пусть $n \geq 13$ — натуральное число и p — наибольшее простое число, не превосходящее n. Предположим также, что G — конечная группа такая, что $|G| \mid n!$. Если $\Pi(n)$ — независимое подмножество в $\Gamma_{\mathrm{sol}}(G)$, то существует натуральное число m такое, что*

$$A_m \leq G/N \leq S_m,$$

где $N = O_{\Pi(n)'}(G)$ и $p \leq m$.

Доказательство. Если $13 \leq n \leq 20$, то $|\Pi(n)| \geq 2$. По лемме 1.1 если $n > 20$, то имеем $|\Pi(n)| \geq 3$. Отсюда $|\Pi(n)| \geq 2$ для $n \geq 13$.

В силу теоремы 2.1 существует неабелева простая группа S такая, что $S \leq G/N \leq \mathrm{Aut}(S)$, где $N = O_{\Pi(n)'}(G)$ и $\Pi(n) \subseteq \pi(S)$. Ввиду $|G| \mid n!$ если $r \in \Pi(n) \subseteq \pi(S)$, то $r \leq |S|_r \leq |G|_r \leq (n!)_r = r$, поэтому $|S|_r = r$.

В силу изложенного выше $\pi(S)$ содержит по крайней мере $|\Pi(n)|$ элементов. Пусть их число равно r, так что $n/2 < r \leq n$ и $|S|_r = r$. По предположению $p \in \Pi(n) \subseteq \pi(S)$ и p — максимальный элемент в $\pi(S)$. Кроме того, так как $|G| \mid n!$, получаем, что $|S| \mid n!$.

Если $13 \leq n \leq 54$, то, используя табл. 8 из [2], можно легко показать, что единственная возможность для S — быть знакопеременной группой, поскольку $\Pi(n) \subseteq \pi(S)$ и $|S| \mid n!$.

Предположим впредь, что $n \geq 55$. В силу следствия 2.3 имеем

$$t(S) \geq |\Pi(n)| \geq (0.366)(55)/\ln(55) > 5,$$

и потому $t(S) \geq 6$. Воспользуемся таблицами из [8] для рассмотрения всех возможностей для S:

(a) Пусть S — спорадическая простая группа. Так как $n \geq 55$, то $p \geq 53$. Поскольку $p \in \pi(S)$, в силу порядка спорадической группы заключаем, что $S \cong LyS$ или F_1 и $p = 67$ или $p = 71$. Отсюда следует, что в обоих случаях $61 \in \Pi(n)$, но $61 \notin \pi(S)$; противоречие.

(b) Пусть S — исключительная простая группа лиевского типа. Известно, что $t(S) \geq 6$. Согласно табл. 9 из [8] $t(E_7(q)) = 8$, $t(E_8(q)) = 12$, а для остальных исключительных простых групп $t(S) < 6$. Поэтому предположим, что $S \cong E_7(t^\alpha)$ или $E_8(t^\alpha)$, где t — простое число.

Если $S \cong E_7(2)$, то $127 \in \pi(S)$ и потому $8 = t(S) \geq (0.366)(127)/\ln(127) > 9$; противоречие.

Если $S \cong E_7(t^\alpha)$, где $t^\alpha \geq 3$, то по лемме 1.2 $t^{63\alpha} = |S|_t \leq |G|_t \leq (n!)_t < t^{n/(t-1)}$ и потому $n \geq 126$. Значит, $8 = t(S) \geq (0.366)(126)/\ln(126) > 9$, что невозможно.

Если $S \cong E_8(2)$, то $241 \in \pi(S)$, стало быть, $12 = t(S) \geq (0.366)(241)/\ln(241) > 16$; противоречие.

Если $S \cong E_8(t^\alpha)$, где $t^\alpha \geq 3$, то по лемме 1.2 $t^{120\alpha} = |S|_t \leq |G|_t \leq (n!)_t < t^{n/(t-1)}$, а значит, $n \geq 240$. Следовательно, $12 = t(S) \geq (0.366)(240)/\ln(240) > 16$, что невозможно.

(c) Пусть S — классическая простая группа лиевского типа. Можно предполагать в каждом случае, что $S \cong {}^dX_m(t^\alpha)$, где m — ранг S и t простое. В силу изложенного выше $n \geq 55$ и $t(S) \geq 6$. Поэтому из табл. 8 в [8] заключаем, что в каждом случае

$$\frac{3m+5}{4} \geq t(S) \geq \frac{(0.366)n}{\ln n} > 5 \Longrightarrow m \geq \frac{(0.488)n}{\ln n} - \frac{5}{3} \ \& \ m \geq 7. \tag{1}$$

С другой стороны,

$$t^{\frac{n}{t-1}} > (n!)_t \geq |G|_t \geq |S|_t \geq t^{\frac{\alpha m(m-1)}{2}} \Longrightarrow m < \sqrt{\frac{2n}{\alpha(t-1)} + \frac{1}{4}} + \frac{1}{2}. \tag{2}$$

Используя (1) и (2), заключаем, что

$$\sqrt{\frac{2n}{\alpha(t-1)} + \frac{1}{4}} + \frac{13}{6} - \frac{(0.488)n}{\ln n} > 0. \tag{3}$$

Так как $n \geq 55$, простое вычисление показывает, что если $\alpha(t-1) \geq 6$ или $n \geq 333$, то (3) невозможно.

Предположим, что $n < 333$ и $\alpha(t-1) < 6$. Тогда t^α равно 2, 2^2, 2^3, 2^4, 2^5, 3, 3^2 или 5. Заметим, что $683 \in \pi(2^{22}-1)$, $3851 \in \pi(3^{22}-1)$ и $5281 \in \pi(5^{22}-1)$. Это показывает, что если $\pi(t^{22}-1) \subseteq \pi(S)$, где t равно 2, 3 или 5, то $n \geq 683$, что противоречит условию $n < 333$.

Тогда в силу изложенного выше $\pi(t^{22}-1) \nsubseteq \pi(S)$. Сверившись с порядками классических простых групп, заключаем, что $m < 22$. Поэтому $S \cong {}^dX_m(t^\alpha)$, где $7 \leq m \leq 21$ и t^α равно $2, 3, 4, 5, 8, 9$ или 16. Простые выкладки показывают, что в этих случаях соотношения $p \in \Pi(n) \subseteq \pi(S)$ и $p = \max \pi(S)$ не выполнены.

Поэтому S неизоморфна спорадической, исключительной или классической простой группе. Таким образом, S изоморфна знакопеременной группе A_m. Также имеем $p \in \pi(S) = \pi(m!)$. Значит, $A_m \leq G/N \leq S_m$, где $p \leq m$. $\square$

Лемма 2.5. *Пусть $n \geq 13$ — натуральное число и p — наибольшее простое число, не превосходящее n. Предположим, что G — конечная группа, причем $|G| = n!$ или $|G| = n!/2$. Если $\Pi(n)$ — независимое подмножество в $\Gamma_{\mathrm{sol}}(G)$, то существует натуральное число m такое, что $A_m \leq G/N \leq S_m$, где $N = O_{\Pi(n)'}(G)$ и $p \leq m \leq n$. Кроме того, если $r \in \pi(N) \setminus \{2\}$, то или $r \leq n-p$ или G содержит элемент порядка pr.*

Доказательство. Согласно лемме 2.4 существует натуральное число m такое, что $A_m \leq G/N \leq S_m$, где $N = O_{\Pi(n)'}(G)$. В силу порядка группы G получаем, что $p \leq m \leq n$. Отсюда $|N| = 2(n!)/(m!)$, $n!/2(m!)$ или $n!/m!$.

Пусть $r \in \pi(N) \setminus \{2\}$ таково, что $p + r > n$. Утверждается, что r делит только одно число u со свойством $p < u \leq n$. Порядок группы N гарантирует существование по крайней мере одного числа u со свойствами $p < u \leq n$ и $r \mid u$. Если имеются два числа u и v такие, что $p < v < u \leq n$, $r \mid u$ и $r \mid v$, то $r \mid (u-v)$. Поэтому $r \leq u - v < n - p$; противоречие. Таким образом, r делит только одно число u такое, что $p < u \leq n$. Отсюда также вытекает, что $|N|_r = u_r \leq n$.

В силу аргумента Фраттини в G имеется подгруппа $R \rtimes G_p$, где $R \in \mathrm{Syl}_r(N)$ и $G_p \in \mathrm{Syl}_p(N_G(R))$. Если G не содержит элементов порядка pr, то $R \rtimes G_p$ — фробениусова подгруппа группы G и потому $p \mid (|R|-1)$. Следовательно, так как r нечетно, в силу изложенного выше получаем, что $2p \leq |R| - 1 = |N|_r - 1 \leq n - 1$. Это невозможно, ибо $n/2 < p \leq n$. $\square$

Лемма 2.6. *Пусть $n \geq 13$ — натуральное число и p — наибольшее простое число, не превосходящее n. Предположим, что G — конечная группа такая, что $|G| = |L|$ и $GK(G) = GK(L)$, где $L \in \{A_n, S_n\}$. Тогда существует натуральное число m такое, что $A_m \leq G/N \leq S_m$, где $N = O_{\Pi(n)'}(G)$, $p \leq m \leq n$ и $\pi(N) \subseteq \pi((n-p)!)$. Кроме того, если $2 \in \pi(N)$ и $2 \nsim p$ в $GK(G)$, то $p \mid (|N|_2 - 1)$.*

Доказательство. В силу леммы 2.5 имеем $A_m \leq G/N \leq S_m$, где $N = O_{\Pi(n)'}(G)$ и $p \leq m \leq n$. Отметим, что если $n = p$ или $n = p + 1$, то A_n и S_n характеризуемы порядком и графом простых чисел [2]. Поэтому предположим, что $n \geq p + 2$. Тогда $2 \in \pi((n-p)!)$. Покажем, что $\pi(N) \subseteq \pi((n-p)!)$.

В силу изложенного выше достаточно показать, что если $r \in \pi(N) \setminus \{2\}$, то $r \in \pi((n-p)!)$. Пусть $r \in \pi(N) \setminus \{2\}$. Если $p + r > n$, то с использованием леммы 2.5 получаем, что в G имеется элемент порядка pr, что невозможно по лемме 1.4, так как $GK(G) = GK(L)$. Таким образом, $p + r \leq n$, откуда $r \in \pi((n-p)!)$.

Наконец, предположим, что $2 \in \pi(N)$ и $2 \nsim p$ в $GK(G)$. Тогда G содержит фробениусову подгруппу $R \rtimes G_p$, где $R \in \mathrm{Syl}_2(N)$ и $G_p \in \mathrm{Syl}_p(N_G(R))$. Тем самым $|G|_p \mid (|R| - 1)$, а значит, $p \mid (|N|_2 - 1)$. $\square$

Теорема 2.7. *Пусть A_n — знакопеременная группа и p — наибольшее простое число, меньшее или равное n. Справедливы следующие утверждения.*

(1) *Если $p \leq n \leq p + 5$ или $\pi(n) \nsubseteq \pi((n-p)!)$, то A_n характеризуема порядком и графом простых чисел, кроме случая A_{10}.*

(2) *Если $\pi(n) \subseteq \pi((n-p)!)$, $n \geq p + 6$ и n — нечетное число, то A_n не характеризуема порядком и графом простых чисел. Более того, в этом случае A_n и $A_{n-1} \times N$, где N — группа порядка n, имеют те же порядок и граф простых чисел.*

(3) *Пусть $\pi(n) \subseteq \pi((n-p)!)$, $n \geq p + 6$ и n — четное число. Если n имеет по крайней мере два разбиения Гольдбаха, то A_n характеризуема порядком и графом простых чисел.*

Доказательство. Предположим, что G — конечная группа такая, что $|G| = |A_n|$ и $GK(G) = GK(A_n)$. Согласно [2] если $n \leq 100$, то A_n характеризуема порядком и графом простых чисел, кроме случая A_{10}. В дальнейшем пусть $n \geq 101$. Тогда по лемме 2.6 существует m такое, что $p \leq m \leq n$ и $A_m \leq G/N \leq S_m$, где $N = O_{\Pi(n)'}(G)$ и $\pi(N) \subseteq \pi((n-p)!)$.

(1) Заметим сначала, что если $n = p$ или $p + 1$, то в силу [2] A_n не характеризуема порядком и графом простых чисел. Поэтому будем предполагать, что $n \geq p + 2$.

(1.a) Пусть $\pi(n) \nsubseteq \pi((n-p)!)$. Если A_n не характеризуема порядком и графом простых чисел, то $m < n$. Следовательно, $n/(2,n) \mid |N|$, потому что $|N| = n!/(m!)$ или $n!/2(m!)$. Таким образом, $\pi(n/(2,n)) \subseteq \pi(N) \subseteq \pi((n-p)!)$, а значит, $\pi(n) \setminus \{2\} \subseteq \pi((n-p)!)$. Поэтому, так как $\pi(n) \nsubseteq \pi((n-p)!)$, получаем, что $\pi(n) = \{2\}$ и $2 \notin \pi((n-p)!)$. Тогда $n = p$ или $n = p + 1$; противоречие, ибо по предположению $n \geq p + 2$. Поэтому, когда $\pi(n) \nsubseteq \pi((n-p)!)$, знакопеременная группа A_n характеризуема порядком и графом простых чисел, A_n характеризуема порядком и графом простых чисел.

(1.b) Пусть $n = p + 2$. Так как $p > 2$, то $\pi(p+2) \neq \{2\}$ и потому $\pi(p+2) \nsubseteq \pi(2!)$. Тем самым в силу случая (1.a) группа A_{p+2} характеризуема порядком и графом простых чисел.

(1.c) Пусть $n = p + 3$. Согласно случаю (1.a) если $\pi(p+3) \nsubseteq \pi(3!)$, то A_{p+3} характеризуема порядком и графом простых чисел. Предположим, что

$\pi(p+3) \subseteq \pi(3!)$. Тогда $p+3 = 2^\alpha$, где $\alpha \geq 3$. Отсюда также получаем, что $(p+1)_2 = 2$. Поэтому если $m < n$, то $|N|_2$ равно $(p+3)/2$, $p+3$ или $2(p+3)$. Так как $2 \nsim p$ в $GK(A_{p+3})$, по лемме 2.6 получаем, что $p \mid (|N|_2 - 1)$. Ввиду значения $|N|_2$ приходим к противоречию.

(1.d) Пусть $n = p+4$. Известно, что $\pi(N) \subseteq \pi(4!)$. Ввиду $n \geq 100$ если $\pi((p+3)(p+4)/2) \subseteq \pi(N)$, то в силу леммы 1.3 получаем противоречие. Отсюда следует, что $p+3 \leq m \leq p+4$.

Если $m = p+3$, то $A_{p+3} \leq G/N \leq S_{p+3}$. Так как $|G| = ((p+3)!/2)(p+4)$ и число $p+4$ нечетно, имеем $|G/N| \neq |S_{p+3}|$. Следовательно, $G/N \cong A_{p+3}$ и $|N| = p+4$. С другой стороны, $2 \sim p$ в $GK(A_{p+4})$, в то время как $2 \nsim p$ в $GK(A_{p+3})$. Значит, $2 \mid |N|$, что невозможно, так как $|N| = p+4$.

(1.e) Наконец, пусть $n = p+5$. Если $p \leq m \leq p+3$, то $\pi((p+4)(p+5)/2) \subseteq \pi(N)$, но по лемме 1.3 $\pi((p+4)(p+5)/2) \nsubseteq \{2,3,5\}$. Поэтому $p+4 \leq m \leq p+5$. Далее, $5 \sim p$ в $GK(A_{p+5})$ и $5 \nsim p$ в $GK(A_{p+4})$. Таким образом, если $m = p+4$, то $5 \mid |N|$, где $|N|$ равно $p+5$ или $(p+5)/2$, что невозможно. Поэтому $m = p+5$, откуда вытекает, что группа A_{p+5} характеризуема порядком и графом простых чисел.

(2) Так как $n \geq p+6$, по предложению 1 из [3] $GK(A_n) = GK(A_{n-1})$. Значит, ввиду $\pi(n) \subseteq \pi((n-p)!)$ имеем $GK(A_n) = GK(A_{n-1} \times N)$, где N — группа такая, что $|N| = n$. Далее, поскольку $|A_n| = |A_{n-1} \times N|$, получаем требуемое.

(3) Так как n содержит по крайней мере два разбиения Гольдбаха, существуют два различных простых числа q и l такие, что $n = q + l$ и $q \neq p \neq l$. Поэтому можно предполагать, что $q > n/2 > l$. Так как $p \neq q$, то $p+l > q+l = n$ и потому $l \notin \pi((n-p)!)$. Таким образом, согласно лемме 2.6 имеем $l \notin \pi(N)$.

Далее, если A_n не характеризуема порядком и графом простых чисел, то $A_m \leq G/N \leq S_m$, где $m < n$. С другой стороны, $n = q + l$, а значит, $q \sim l$ в $GK(A_n)$, в то время как $q \nsim l$ в $GK(A_m)$. Поэтому $l \in \pi(N)$; противоречие. $\square$

Замечание 2.8. Пусть n — натуральное число. Если $n \leq 100$, то характеризуемость группы A_n порядком и графом простых чисел уже рассмотрена (см. [2]). Далее, если $101 \leq n \leq 119$ или $121 \leq n \leq 124$, то n удовлетворяет утверждению (1) теоремы 2.7 и потому A_n характеризуема порядком и графом простых чисел. Если $n = 120$, то, поскольку $120 = 113 + 7 = 109 + 11$, согласно утверждению (3) получаем, что группа A_{120} характеризуема порядком и графом простых чисел. Если $n = 125$, то $p = 113$ и $\pi(125) = \{5\} \subseteq \pi((n-p)!) = \pi(12!)$, поэтому в силу утверждения (2) теоремы 2.7 получаем, что A_{125} не характеризуема порядком и графом простых чисел.

Так как гипотеза Гольдбаха, по-видимому, верна в общем случае и нам представляется, что для каждого n можно найти два разбиения Гольдбаха, выдвинем следующую гипотезу.

Гипотеза 2.9. *Если n — четное число такое, что $n \neq 10$, то знакопеременная группа A_n характеризуема порядком и графом простых чисел.*

3. Приложения

В данном разделе используем основные результаты для проверки некоторых гипотез и решения проблемы из [2]. Определим образец степеней конечной группы.

Определение 3.1 [2]. Пусть G — группа, и пусть $\pi(G) = \{p_1, p_2, \dots, p_k\}$, где $p_1 < p_2 < \dots < p_k$. Тогда *образец степеней* группы G определяется следующим образом:

$$D(G) := (\deg(p_1), \deg(p_2), \dots, \deg(p_k)),$$

где $\deg(p_i)$, $1 \leq i \leq k$, — степень вершины p_i в $GK(G)$.

Определение 3.2 [2]. Пусть G — конечная группа. Говорят, что группа G *k-кратно* OD-*характеризуема*, если существуют в точности k неизоморфных групп того же порядка и образца степеней. В частности, если $k = 1$, то G называется OD-*характеризуемой.*

Ранее рассматривалась OD-характеризуемость некоторых конечных групп (см. список литературы в [2]). В [13] поставлена следующая проблема об OD-характеризуемости конечных простых групп (см. также [14, 2, 13]):

Вопрос 3.3. *Существует ли простая группа, являющаяся k-кратно OD-характеризуемой для $k \geq 3$?*

В [2] авторы выдвинули следующие гипотезы.

Гипотеза 3.4. *Все знакопеременные группы A_m, где $m \neq 10$,* OD-*характеризуемы.*

Гипотеза 3.5. *Все симметрические группы S_m при $m \neq 10$ не являются n-кратно* OD-*характеризуемыми, где $n \in \{1, 3\}$.*

Заметим сначала, что в силу леммы 2.15 из [2] для знакопеременных или симметрических групп характеризуемость порядком и образцом степеней эквивалентна характеризуемости порядком и графом простых чисел. В силу теоремы 2.7 группа A_{125} является контрпримером к гипотезе 3.4 и примером k-кратной OD-характеризуемой группы, где $k > 3$, что также дает ответ на проблему 3.3. Группа S_{125} является контрпримером к гипотезе 3.5.

Авторы выражают признательность рецензенту за ценные замечания, которые способствовали улучшению текста статьи.

ЛИТЕРАТУРА

1. *Gorenstein D.* Finite groups. New York: Harper and Row, 1968.
2. *Kogani-Moghaddam R., Moghaddamfar A. R.* Groups with the same order and degree pattern // Sci. China Math. 2012. V. 55, N 4. P. 701–720.
3. *Звездина М. А.* О неабелевых простых группах с графом простых чисел как у знакопеременных групп // Сиб. мат. журн. 2013. Т. 54, № 1. С. 65–76.
4. *Vakula I. A.* On the structure of finite groups isospectral to an alternating group // Proc. Steklov Inst. Math. 2011. V. 272, N 1. P. 271–286.
5. *Khosravi A., Khosravi B.* A new characterization of PSL(p, q) // Comm. Algebra. 2004. V. 32, N 6. P. 2325–2339.
6. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3, N 1. P. 265–284.
7. *Заварницын А. В., Мазуров В. Д.* О порядках элементов в накрытиях симметричных и знакопеременных групп // Алгебра и логика. 1999. Т. 38, № 3. С. 296–315.
8. *Васильев А. В., Вдовин Е. П.* Критерий смежности в графе простых чисел конечной простой группы // Алгебра и логика. 2005. Т. 44, № 6. С. 682–725.
9. *Abe S.* A characterization of some finite simple groups by orders of their solvable subgroups // Hokkaido Math. J. 2002. V. 31, N 2. P. 349–361.
10. *Weisstein E. W.* Goldbach Conjecture // http://mathworld.wolfram.com/GoldbachConjecture.html.
11. *Estermann T.* On Goldbach's problem: proof that almost all even positive integers are sums of two primes // Proc. London Math. Soc. 1938. V. s2-44, N 1. P. 307–314.

12. *Vinogradov I. M.* Some theorems concerning the theory of primes // Rec. Math. 1937. V. 44, N 2. P. 179–195.
13. *Moghaddamfar A. R., Zokayi A. R.* Recognizing finite groups through order and degree pattern // Algebra Colloq. 2008. V. 15, N 3. P. 449–456.
14. *Akbari B., Moghaddamfar A. R.* Recognizing by order and degree pattern of some projective special linear groups // Int. J. Algebra Comput. 2012. V. 22, N 6. P. 22.

Статья поступила 1 июня 2013 г.

Ali Mahmoudifar (Махмудифар Али)
Dept. of Pure Math., Faculty of Math. and Computer Sci.,
Amirkabir University of Technology (Tehran Polytechnic),
424, Hafez Ave., Tehran 15914, Iran
alimahmoudifar@gmail.com

Behrooz Khosravi (Хосрави Бехруз)
Dept. of Pure Math., Faculty of Math. and Computer Sci.,
Amirkabir University of Technology (Tehran Polytechnic),
424, Hafez Ave., Tehran 15914, Iran;
School of Mathematics,
Institute for Research in Fundamental sciences (IPM),
P.O.Box: 19395-5746, Tehran, Iran
khosravibbb@yahoo.com