Сибирский математический журнал
Июль—август, 2008. Том 49, № 4

УДК 519.542

2–РАСПОЗНАВАЕМОСТЬ $PSL(2, p^2)$ ПО ГРАФУ ПРОСТЫХ ЧИСЕЛ

А. Хосрави, Б. Хосрави

Аннотация. Пусть G — конечная группа и $\Gamma(G)$ — граф простых чисел группы G. Пусть p простое. Рассмотрены конечные группы G такие, что $\Gamma(G) = \Gamma(PSL(2, p^2))$, и доказано, что если $p \neq 2, 3, 7$ простое, то $k(\Gamma(PSL(2, p^2))) = 2$. Как следствие этого результата доказано, что если G — конечная группа такая, что $|G| = |PSL(2, p^2)|$, и $\Gamma(G) = \Gamma(PSL(2, p^2))$, то $G \cong PSL(2, p^2)$. С помощью этого факта даны новые доказательства некоторых теорем, например, гипотезы Ши и Би. Рассмотрены также применения этих результатов к задаче распознавания конечных групп по множеству порядков элементов.

Ключевые слова: простая группа, граф простых чисел, порядок элемента, линейная группа.

1. Введение

Для целого n обозначим через $\pi(n)$ множество всех простых делителей n. Если G — конечная группа, то множество $\pi(|G|)$ обозначается через $\pi(G)$, а множество порядков элементов из G — через $\pi_e(G)$. Очевидно, $\pi_e(G)$ частично упорядочено по делимости. Поэтому оно однозначно определяется множеством $\mu(G)$ его максимальных элементов. Построим *граф* $\Gamma(G)$ *простых чисел группы* G. Множество его вершин — это $\pi(G)$, и два различных простых числа p и q соединены ребром (записываем $p \sim q$), если в G есть элемент порядка pq. Пусть $t(G)$ — количество связных компонент $\Gamma(G)$ и $\pi_1(G), \pi_2(G), \dots, \pi_{t(G)}(G)$ — связные компоненты графа $\Gamma(G)$. Иногда мы будем использовать обозначение π_i вместо $\pi_i(G)$. Если $2 \in \pi(G)$, то всегда предполагаем, что $2 \in \pi_1$. Связные компоненты неабелевых простых групп, имеющих по крайней мере две компоненты связности, перечислены в [1].

Понятие графа простых чисел возникло при изучении некоторых когомологических вопросов, связанных с интегральными представлениями конечных групп. Было доказано, что для каждой конечной группы G выполнено неравенство $t(G) \leq 6$ [2–4] и диаметр $\Gamma(G)$ не более чем 5 (см. [5]). В [6] описаны конечные группы G, удовлетворяющие равенству $\Gamma(G) = \Gamma(S)$, где S — спорадическая простая группа.

Обозначим через $k(\Gamma(G))$ число попарно не изоморфных конечных групп H таких, что $\Gamma(G) = \Gamma(H)$. Тогда если G — конечная группа, то $k(\Gamma(G)) \geq 1$. Используя эту функцию, дадим следующее

Определение 1.1. Для данного натурального n конечную группу G называют *n-распознаваемой по графу простых чисел*, если $k(\Gamma(G)) = n$. Обычно

The second author was supported in part by the grant from IPM (N 84200024).

1-распознаваемые группы называют *характеризуемыми группами.* Если существует бесконечно много неизоморфных конечных групп H таких, что $\Gamma(G) = \Gamma(H)$, то будем говорить, что G — *нераспознаваемая группа.*

Если p простое, то $k(\Gamma(\mathbb{Z}_p)) = \infty$, поэтому каждая p-группа нераспознаваема. Отметим, что $\Gamma(\mathbb{Z}_6)$ — граф с двумя вершинами, т. е. $V = \{2,3\}$, и существует ребро между 2 и 3. Однако $\Gamma(\mathbb{Z}_3 \times \mathbb{Z}_{2^k}) = \Gamma(\mathbb{Z}_6)$ для любого $k > 0$. Кроме того, $S_3 \times \mathbb{Z}_{2^k}$, где $k > 0$, — неабелева группа и $\Gamma(S_3 \times \mathbb{Z}_{2^k}) = \Gamma(\mathbb{Z}_6)$. Поэтому есть бесконечно много неизоморфных групп G таких, что $\Gamma(G) = \Gamma(\mathbb{Z}_6)$. Отсюда $\mathbb{Z}_6$ — нераспознаваемая группа. Заметим также, что даже если $|G| = |M|$ и $\Gamma(G) = \Gamma(M)$, то мы не можем заключить, что $G \cong M$.

Поэтому разобьем множество всех групп на следующие два класса: нераспознаваемые группы и n-распознаваемые группы, где $n \geq 1$. Доказано, что если $q = 3^{2n+1}$ $(n > 0)$, то простая группа ${}^2G_2(q)$ однозначно определяется ее графом простых чисел [7, 8]. В [9] также доказано, что если $p > 11$ — простое число и $p \not\equiv 1 \pmod{12}$, то $PSL(2,p)$ характеризуема графом простых чисел.

В настоящей статье мы определим конечные группы G, графом простых чисел которых является $\Gamma(PSL(2,p^2))$, где p простое.

Всюду ниже все группы конечны и под простыми группами мы понимаем неабелевы простые группы. Все используемые, но необъясняемые понятия можно найти в [10]. Мы используем результаты из [2–4] о графах простых чисел и результаты из [11] о графе простых чисел почти простых групп. Через (a,b) обозначаем наибольший общий делитель целых a и b. Пусть m — положительное целое число и p — простое число. Тогда через $|m|_p$ обозначается p-часть m. Иными словами, $|m|_p = p^k$, если $p^k \| m$ (т. е. $p^k | m$, но $p^{k+1} \nmid m$).

2. Предварительные результаты

Замечание 2.1. Пусть N — нормальная подгруппа группы G и $p \sim q$ в $\Gamma(G/N)$. Тогда $p \sim q$ в $\Gamma(G)$. Действительно, если $xN \in G/N$ имеет порядок pq, то найдется степень x, имеющая порядок pq.

Определение 2.1 [12]. Конечная группа G называется 2-*фробениусовой*, если в ней есть нормальный ряд $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$, где K и G/H — фробениусовы группы с ядрами H и K/H соответственно.

Лемма 2.1 [4, теорема A]. *Если G — конечная группа, граф простых чисел которой имеет более одной компоненты, то G — одна из следующих групп:*

(a) *фробениусова или 2-фробениусова группа;*

(b) *простая группа;*

(c) *расширение π_1-группы простой группой;*

(d) *расширение простой группы π_1-группой;*

(e) *расширение π_1-группы посредством расширения простой группы с помощью π_1-группы.*

Лемма 2.2 [3]. *Если G — разрешимая группа с более чем одной компонентой графа простых чисел, то G либо фробениусова, либо 2-фробениусова и в ней есть в точности две компоненты, одна из которых состоит из простых делителей нижнего фробениусова дополнения.*

В следующей лемме собраны основные структурные свойства фробениусовой группы [12–14] и 2-фробениусовой группы [12].

Лемма 2.3. (a) *Пусть G — фробениусова группа и H, K — фробениусовы дополнение и ядро G соответственно. Тогда $t(G) = 2$, компонентами графа простых чисел группы G являются $\pi(H)$, $\pi(K)$ и G имеет одну из следующих структур:*

(i) $2 \in \pi(K)$ *и все силовские подгруппы H циклические;*

(ii) $2 \in \pi(H)$, *K — абелева группа, H — разрешимая группа, в которой силовские подгруппы нечетного порядка являются циклическими группами, и 2-силовские подгруппы в H суть циклические группы или группы кватернионов;*

(iii) $2 \in \pi(H)$, *K — абелева группа и существует $H_0 \leq H$ такое, что $|H : H_0| \leq 2$, $H_0 = Z \times SL(2,5)$, $\pi(Z) \cap \{2,3,5\} = \varnothing$ и силовские подгруппы в Z циклические.*

(b) *Если G 2-фробениусова, то $t(G) = 2$. В терминах определения 2.1 $\pi_1 = \pi(G/K) \cup \pi(H)$ и $\pi_2 = \pi(K/H)$.*

Лемма 2.4. *Если G — конечная группа и $\Gamma(G) = \Gamma(PSL(2,p^2))$, то в G есть нормальный ряд $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ такой, что G/K — π_1-группа, H — нильпотентная π_1-группа и K/H — неабелева простая группа с $t(K/H) \geq 3$ и $G/K \leq \mathrm{Out}(K/H)$. Кроме того, если $j \in \{2,3\}$, то найдется $i \geq 2$ такое, что $\pi_j(PSL(2,p^2)) = \pi_i(K/H)$.*

Доказательство. Первая часть леммы вытекает непосредственно из предыдущих лемм. Так как $t(G) \geq 2$, имеем $Z(G/H) = 1$. Если $xH \in G/H$ и $xH \notin K/H$, то xH индуцирует автоморфизм K/H, который тривиален тогда и только тогда, когда $xH \in Z(G/H)$. Поэтому $G/H \leq \mathrm{Aut}(K/H)$ и поскольку $Z(G/H) = 1$, то $G/K \leq \mathrm{Out}(K/H)$. □

Следующая лемма представляет собой известный результат теории чисел.

Лемма 2.5 [15, с. 29]. *Пусть $a > 1$, m и n положительные целые. Тогда*

$$(a^n - 1, a^m - 1) = a^{(m,n)} - 1.$$

Лемма 2.6 [3]. *Пусть $q > 1$, m и n положительные целые. Тогда*

$$\left(\frac{q^n - 1}{q^{(n,m)} - 1}, q^m - 1\right) = \left(\frac{n}{(n,m)}\ , q^{(n,m)} - 1\right).$$

Лемма 2.7 [16]. *Единственное решение диофантова уравнения $p^m - q^n = 1$, где p, q простые и $m, n > 1$, таково: $3^2 - 2^3 = 1$.*

Лемма 2.8 [16, 17]. *За исключением соотношений $(239)^2 - 2(13)^4 = -1$ и $(3)^5 - 2(11)^2 = 1$, каждое решение уравнения*

$$p^m - 2q^n = \pm 1, \quad p, q \text{ простые},\ m, n > 1,$$

имеет показатели $m = n = 2$, т. е. оно получается из единицы $p - q.2^{\frac{1}{2}}$ поля $Q(2^{\frac{1}{2}})$, для которого коэффициенты p, q простые.

Лемма 2.9 (теорема Жигмонди [18]). *Пусть p простое и n положительное целое. Тогда выполнено одно из следующих утверждений:*

(i) *существует примитивное простое p' для $p^n - 1$, т. е. $p' \mid (p^n - 1)$, но $p' \nmid (p^m - 1)$ для любого $1 \leq m < n$,*

(ii) $p = 2$, *n равно 1 или 6,*

(iii) p — *простое число Мерсенна и* $n = 2$.

Напомним понятия квадратичного вычета и символа Лежандра из теории чисел.

Замечание 2.2 [15]. Пусть $(k,n) = 1$. Если есть такое целое x, что $x^2 \equiv k \pmod n$, то k называют *квадратичным вычетом* $\pmod n$. В ином случае k называют *квадратичным невычетом* $\pmod n$.

Пусть p простое нечетное. Символ (a/p) принимает значение 1, если a — квадратичный вычет $\pmod p$, -1, если a — квадратичный невычет $\pmod p$, и 0, если $p \mid a$. Символ (a/p) называют *символом Лежандра*.

Пусть p простое и $(a,p) = 1$. Пусть $k \geq 1$ — наименьшее положительное целое число такое, что $a^k \equiv 1 \pmod p$. Тогда k называют *порядком* a *относительно* p и обозначают через $\mathrm{ord}_p(a)$. Из малой теоремы Ферма очевидно следует, что $\mathrm{ord}_p(a) \mid (p-1)$. Кроме того, если $a^n \equiv 1 \pmod p$, то $\mathrm{ord}_p(a) \mid n$.

Лемма 2.10 (квадратичный закон взаимности). *Пусть* p *и* q — *простые нечетные числа. Тогда*

(i) $(-1/p) = (-1)^{(p-1)/2}$,

(ii) $(2/p) = (-1)^{(p^2-1)/8}$,

(iii) $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$.

Лемма 2.11. *Не существуют такие* $\alpha > 0$ *и простые числа* p *и* p_0, *что* $\pi((p^2+1)/2) = \{p_0\}$ *и* $\pi((p_0^\alpha - 1)/2) = \{p\}$.

Доказательство. Если $\pi((p_0^\alpha - 1)/2) = \{p\}$, то $p_0^\alpha = 2p^k + 1$ для некоторого $k > 0$. Кроме того, $p^2 + 1 = 2p_0^t$ для какого-то $t > 0$. Используя лемму 2.8, заключаем, что $t = 1$ или $t = 2$, или $(p, p_0, t) = (239, 13, 4)$. Из леммы 2.8 вытекает, что $\alpha = 1$ или $k = 1$, или $(\alpha, k) = (2, 2)$, или $(p, p_0, \alpha, k) = (11, 3, 5, 2)$. Рассмотрим все случаи по отдельности.

Если $\alpha = t = 1$, то $p^2 + 1 = 4p^k + 2$, поэтому $p \mid 1$; противоречие.

Если $\alpha = k = 2$ и $t = 1$, то $4p_0^2 = (p^2+1)^2 = 8p^2 + 4$, откуда $p^2 \mid 3$; противоречие.

Обоснования в остальных случаях аналогичны, и мы опустим детали. □

Подобным образом можно доказать следующее утверждение.

Лемма 2.12. *Если существуют* $\alpha > 0$ *и простые числа* p *и* p_0 *такие, что* $\pi((p^2+1)/2) = \{p_0\}$ *и* $\pi((p_0^\alpha + 1)/2) = \{p\}$, *то* $(p, p_0, \alpha) = (3, 5, 1)$.

3. Основные результаты

В этом разделе в качестве основного результата мы определим конечные группы G такие, что $\Gamma(G) = \Gamma(PSL(2,p^2))$, где p простое.

Теорема 3.1. *Пусть* p *простое. Если* G — *конечная группа и* $\Gamma(G) = \Gamma(PSL(2,p^2))$, *то в обозначениях из* [10]

(i) *если* $p = 2$ *или* $p = 3$, *то* $G \cong PSL(2,9)$ *или* $G \cong PSL(2,9).2_3$, *где* $PSL(2,9).2_3$ — *нерасщепляемое расширение* $PSL(2,9)$ *посредством* $\mathbb{Z}_2$, *или* $G/O_2(G) \cong PSL(2,4)$;

(ii) *если* $p = 7$, *то* G *изоморфно* $PSL(2,49)$ *или* $PSL(2,49).2_3$, *нерасщепляемому расширению* $PSL(2,49)$ *посредством* $\mathbb{Z}_2$, *или* $G/O_{\{2,3\}}(G)$ *изоморфно* $PSL(3,4)$, $PSL(3,4).2_1$, $PSU(4,3)$ *или* A_7;

(iii) *если* $p \neq 2, 3, 7$, *то* $G \cong PSL(2, p^2)$ *или* G *изоморфно* $PSL(2, p^2).2_3$, *нерасщепляемому расширению* $PSL(2, p^2)$ *посредством* $\mathbb{Z}_2$; *отсюда* $PSL(2, p^2)$ *2-распознаваема по ее графу простых чисел.*

Доказательство. Известно, что $\mu(PSL(2, 4)) = \mu(A_5) = \{2, 3, 5\}$. Из результатов Диксона [13, с. 213] вытекает, что если $p \neq 2$, то

$$\mu(PSL(2, p^2)) = \left\{p, \frac{p^2 - 1}{2}, \frac{p^2 + 1}{2}\right\}.$$

Поэтому $t(G) = 3$, $\pi_1 = \pi((p^2 - 1)/2)$ и нечетные компоненты $\Gamma(G)$ суть $\pi_2 = \pi((p^2 + 1)/2)$ и $\pi_3 = \{p\}$. Из леммы 2.3 следует, что G не является ни фробениусовой группой, ни 2-фробениусовой группой. По лемме 2.4 в G есть нормальный ряд $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ такой, что G/K — π_1-группа, H — нильпотентная π_1-группа и K/H — неабелева простая группа. Кроме того, $t(K/H) \geq 3$. Рассмотрим все случаи для K/H по отдельности.

Заметим, что $PSL(2, 4) \cong PSL(2, 5) \cong A_5$ и $\Gamma(PSL(2, 4)) = \Gamma(PSL(2, 9))$. Тем самым достаточно доказать теорему для p простого нечетного, и в дальнейшем p будем считать таковым.

Случай 1. Пусть $K/H \cong A_{p'}$, где p' и $p' - 2$ простые. Нечетные компоненты $A_{p'}$ суть $\{p'\}$ и $\{p' - 2\}$. Рассмотрим эти два подслучая.

Если $p = p'$ и $\pi((p^2 + 1)/2) = \{p' - 2\}$, то $(p^2 + 1)/2 = (p - 2)^k$ для некоторого $k \in \mathbb{N}$. Отсюда $p^2 + 1 = 2(p - 2)^k$ и по лемме 2.8 $k = 1$ или $k = 2$. Поэтому $p = 7$ является единственным решением. Значит, если $p = 7$, то $K/H \cong A_7$. Так как $\mathrm{Out}(A_7) \cong \mathbb{Z}_2$ и в $A_7.2$ есть элемент порядка 10, то $\Gamma(A_7.2)$ не является подграфом в $\Gamma(G)$, так что $G = K$. Отсюда $G/O_{\{2,3\}}(G) \cong A_7$.

Если $p = p' - 2$ и $\pi((p^2 + 1)/2) = \{p'\}$, то $(p^2 + 1)/2 = p'^k$ для некоторого $k \in \mathbb{N}$. Тогда $(p^2 + 1)/2 = (p + 2)^k$ и поскольку $(p^2 + 1)/2 < (p + 2)^2$, то $(p^2 + 1)/2 = p + 2$ и $p = 3$. Поэтому если $p = 3$, то $K/H \cong A_5 \cong PSL(2, 4)$. Отметим, что $\mathrm{Out}(PSL(2, 4)) \cong \mathbb{Z}_2$ (см. [10]). Следовательно, по лемме 2.4 $G/K \leq \mathrm{Out}(PSL(2, 4)) \cong \mathbb{Z}_2$. Если $G/K \cong \mathbb{Z}_2$, то из того, что $PSL(2, 4).2$ имеет элемент порядка 6, вытекает, что $\Gamma(PSL(2, 4).2)$ не является подграфом в $\Gamma(G)$. Итак, $G = K$ и $G/O_2(G) \cong PSL(2, 4)$.

Случай 2. Пусть $K/H \cong PSL(2, q)$, где $4 \mid (q + 1)$. Тогда нечетными компонентами будут $\{\pi((p^2 + 1)/2), \pi(p)\} = \{\pi(q), \pi((q - 1)/2)\}$. Рассмотрим два подслучая.

(2.1) Если $\pi(q) = \{p\}$ и $\pi((p^2 + 1)/2) = \pi((q - 1)/2)$, то $q = p^\alpha$ для некоторого $\alpha \in \mathbb{N}$. Известно, что $((p^2 + 1)/2, p^2 - 1) = 1$ и $(p - 1) \mid (p^\alpha - 1)$. Поэтому если $\pi((p^\alpha - 1)/2) = \pi((p^2 + 1)/2)$, то $\pi((p - 1)/2) = \varnothing$. Отсюда $(p - 1)/2 = 1$ и тем самым $p = 3$. Имеем $\pi((3^\alpha - 1)/2) = \{5\}$, откуда $3^\alpha - 1 = 2 \times 5^\beta$ для некоторого $\beta > 0$. Из леммы 2.8 вытекает, что это диофантово уравнение не имеет решения.

(2.2) Пусть $q = p_0^\alpha$, где p_0 — простое число и $\alpha \in \mathbb{N}$. Если $\pi((q - 1)/2) = \{p\}$ и $\pi((p^2 + 1)/2) = \pi(q)$, то $(p_0^\alpha - 1)/2 = p^k$ для некоторого $k > 0$ и $(p^2 + 1)/2 = p_0^t$ для какого-то $t > 0$. По лемме 2.11 приходим к противоречию.

Случай 3. Пусть $K/H \cong PSL(2, q)$, где $4 \mid (q - 1)$. Тогда $\{\pi(p), \pi((p^2 + 1)/2)\} = \{\pi((q + 1)/2), \pi(q)\}$. Вновь рассмотрим два случая.

(3.1) Если $\pi(q) = \{p\}$ и $\pi((p^2 + 1)/2) = \pi((q + 1)/2)$, то $q = p^\alpha$ для некоторого $\alpha \in \mathbb{N}$ и $\pi((p^\alpha + 1)/2) = \pi((p^2 + 1)/2)$.

Если $\alpha = 1$, то $\pi((p+1)/2) = \pi((p^2+1)/2)$. Если p_0 — первичное простое в p^4-1, то p_0 делит p^2+1, так как $p^4-1 = (p^2-1)(p^2+1)$. Очевидно, $p_0 \notin \pi(p+1)$ ввиду того, что $(p+1) \mid (p^2-1)$; противоречие.

Если $\alpha > 2$, то пусть p_0 — первичное простое в $p^{2\alpha}-1$. Поскольку $p^{2\alpha}-1 = (p^\alpha-1)(p^\alpha+1)$, то $p_0 \in \pi(p^\alpha+1)$ и $p_0 \notin \pi(p^2+1)$, ибо $(p^2+1) \mid (p^4-1)$ и $2\alpha > 4$.

Если $\alpha = 2$, то $K/H \cong PSL(2,p^2)$. По лемме 2.4 $G/K \leq \mathrm{Out}(PSL(2,p^2))$, а как известно, каждый элемент из $\mathrm{Out}(PSL(2,p^2))$ является произведением изоморфизма полей и диагонального изоморфизма. Поэтому $\mathrm{Out}(PSL(2,p^2)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, так что в $\mathbb{Z}_2 \times \mathbb{Z}_2$ есть три инволюции. Следуя [10], обозначим их через 2_1, 2_2, 2_3. Каждый автоморфизм поля централизует простое подполе, тем самым вершина p не может быть изолированной в $\Gamma(G)$. Известно также, что $\mathrm{Aut}(PSL(2,p^n)) = PGL(2,p^n).\mathbb{Z}_n$ и $\mu(PGL(2,p^n)) = \{p, p^n-1, p^n+1\}$. Кроме того, $PSL(2,p^2).2_1$ и $PSL(2,p^2).2_2$ содержат элементы порядков p^2+1 и $2p$ соответственно. Поэтому $\Gamma(PSL(2,p^2).2_1)$ и $\Gamma(PSL(2,p^2).2_2)$ не будут подграфами в $\Gamma(G)$. Если через $PSL(2,p^2).2_3$ обозначить нерасщепляемое расширение $PSL(2,p^2)$ посредством $\mathbb{Z}_2$, то $\Gamma(PSL(2,p^2)) = \Gamma(PSL(2,p^2).2_3)$. Отсюда $G/H \cong PSL(2,p^2)$ или $G/H \cong PSL(2,p^2).2_3$. Если $H \neq 1$, то пусть $p_0 \in \pi(H)$ и Q — силовская p_0-подгруппа в H. Так как H нильпотентна, $Q \,\mathrm{char}\, H$ и $H \trianglelefteq G$, заключаем, что $Q \trianglelefteq G$. Пусть P — силовская p-подгруппа в G. Поскольку $p \not\sim p_0$ в $\Gamma(G)$, то P действует на Q без неподвижных точек. Отсюда PQ — группа Фробениуса с ядром Q и фробениусовым дополнением P. Тем самым P циклическая. Получили противоречие, поскольку $PSL(2,p^2)$ не имеет элементов порядка p^2. Следовательно, $H = 1$ и $G \cong PSL(2,p^2)$ или $G \cong PSL(2,p^2).2_3$.

(3.2) Если $\pi(q) = \pi((p^2+1)/2)$ и $\pi((q+1)/2) = \{p\}$, то по лемме 2.12 $p = 3$ и $K/H \cong PSL(2,5)$. Но известно, что $PSL(2,5) \cong A_5$, а мы рассмотрели это в случае 1.

Случай 4. Пусть $K/H \cong PSL(2,q)$, где $4 \mid q$. Тогда нечетные компоненты в K/H суть $\pi(q-1)$ и $\pi(q+1)$. Пусть $q = 2^\alpha$.

(4.1) Если $\pi(q-1) = \{p\}$ и $\pi(q+1) = \pi((p^2+1)/2)$, то $2^\alpha - 1 = p^\beta$ для некоторого $\beta > 0$. Из леммы 2.7 вытекает, что $\beta = 1$ и $p = 2^\alpha - 1$. Кроме того, $\pi(q+1) = \pi((p^2+1)/2)$, откуда следует, что $\pi(2^\alpha+1) = \pi(2^{2\alpha-1} - 2^\alpha + 1)$. Пусть $x \in \pi(2^\alpha+1)$. Тогда $x \mid (2^{2\alpha-1} - 2^\alpha + 1)$, так что $x \mid (2^{2\alpha-1} + 2)$. Отсюда

$$x \mid (2^{\alpha-1}(2^\alpha+1) - 2^{\alpha-1} + 2) \Rightarrow x \mid (2^{\alpha-1} - 2) \Rightarrow x \mid (2^\alpha - 4).$$

Поскольку $x \mid (2^\alpha+1)$, имеем $x \mid 5$. Поэтому $\pi(2^\alpha+1) = \pi(2^{2\alpha-1} - 2^\alpha + 1) = \{5\}$, значит, $\alpha = 2$, $p = 3$ и $K/H \cong PSL(2,4)$. Но $PSL(2,4) \cong A_5$, а это мы обсудили в случае 1.

(4.2) Если $\pi(q+1) = \{p\}$ и $\pi((p^2+1)/2) = \pi(q-1)$, то $2^\alpha + 1 = p^\beta$ для некоторого $\beta > 0$. Из леммы 2.7 вытекает, что $\beta = 1$ или $(\alpha,\beta) = (3,2)$. Если $(\alpha,\beta) = (3,2)$, то $p = 3$; противоречие с тем, что $\pi(q-1) = \{7\} \neq \{5\}$. Если $\beta = 1$, то $p = 2^\alpha + 1$. Кроме того, $\pi(2^\alpha - 1) = \pi((p^2+1)/2) = \pi(2^{2\alpha-1} + 2^\alpha + 1)$. Если $x \in \pi(2^\alpha - 1)$, то

$$x \mid (2^{2\alpha-1} + 2^\alpha + 1) = 2^{\alpha-1}(2^\alpha - 1) + 2^{\alpha-1} + 2^\alpha + 1 \Rightarrow x \mid (2^\alpha + 2^{\alpha-1} + 1).$$

Поэтому $x \mid (2^\alpha - 1)$ и $x \mid (2^{\alpha-1} + 2)$, откуда $x \mid 5$. Тем самым $\pi(2^\alpha - 1) = \{5\}$ и $2^\alpha - 1 = 5^s$ для какого-то $s \in \mathbb{N}$; противоречие согласно лемме 2.7. Проведенные рассуждения показывают, что если $p \neq 3$, то $K/H \ncong PSL(2,2^m)$ при $m \geq 2$.

Случай 5. Пусть $K/H \cong {}^2B_2(q)$, где $q = 2^{2n+1} > 2$. Тогда компоненты связности в K/H суть $\{2\}$, $\pi(q-1)$, $\pi(q+\sqrt{2q}+1)$ и $\pi(q-\sqrt{2q}+1)$. Поскольку $\{p\}$ — нечетная компонента в G, рассмотрим три подслучая.

(5.1) Если $\pi(q-1) = \{p\}$, то для некоторого $\alpha > 0$ по лемме 2.7 имеем

$$q - 1 = p^\alpha \Rightarrow 2^{2n+1} - 1 = p^\alpha \Rightarrow p = 2^{2n+1} - 1.$$

Кроме того, $\pi(q+\sqrt{2q}+1)$ и $\pi(q-\sqrt{2q}+1)$ суть нечетные компоненты в K/H. Тем самым $\pi((p^2+1)/2) \subseteq \pi(q+\sqrt{2q}+1) \cup \pi(q-\sqrt{2q}+1)$. Так как $(q+\sqrt{2q}+1)(q-\sqrt{2q}+1) = q^2+1$, имеем $\pi((p^2+1)/2) \subseteq \pi(q^2+1)$. Поэтому

$$\pi(2^{4n+1} - 2^{2n+1} + 1) \subseteq \pi(2^{2(2n+1)} + 1).$$

Аналогично последним случаям если $x \in \pi(2^{4n+1} - 2^{2n+1} + 1)$, то $x \mid (2^{2(n+1)} - 1)$, и мы заключаем, что $x \mid (2^{4n+4} - 1)$. Значит, $x \mid 5$ и $\pi((p^2+1)/2) = \{5\}$. Отсюда $p^2 + 1 = 2 \times 5^k$ и из леммы 2.8 следует, что $p = 3$ или $p = 7$. Если $p = 3$, то $\pi(q-1) = \{3\}$, а это влечет, что $q = 4$; противоречие, ибо $q = 2^{2n+1}$. Если $p = 7$, то $q = 8$. Однако $13 \mid |{}^2B_2(8)|$ и $13 \nmid |L_2(49)|$; противоречие.

(5.2) Если $\pi(q+\sqrt{2q}+1) = \{p\}$, то $2^{2n+1} + 2^{n+1} + 1 = p^\alpha$ для некоторого $\alpha > 0$. Отсюда

$$2^{n+1}(2^n + 1) = p^\alpha - 1 = (p-1)(p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1).$$

Поэтому $\pi(p-1) \subseteq \pi(2^n+1) \cup \{2\}$. Из свойств нечетных компонент вытекает, что $\pi((p^2+1)/2)$ равно либо $\pi(q-1)$, либо $\pi(q-\sqrt{2q}+1)$. Рассмотрим два случая.

(a) Пусть $\pi((p^2+1)/2) = \pi(q-1) = \pi(2^{2n+1}-1)$. Если $p_0 \in \pi((p^2+1)/2)$, то $p^2 \equiv -1 \pmod{p_0}$. Поэтому $(-1/p_0) = 1$ и из леммы 2.10 следует, что $p_0 \equiv 1 \pmod 4$. Значит, каждый простой делитель $2^{2n+1}-1$ имеет вид $4k+1$, откуда $2^{2n+1} - 1 \equiv 1 \pmod 4$; противоречие.

(b) Пусть $\pi((p^2+1)/2) = \pi(q-\sqrt{2q}+1)$. Согласно предположению $\pi(p) = \pi(q+\sqrt{2q}+1)$ и тем самым $\pi(q-1) \subseteq \pi((p^2-1)/2)$.

Как отмечено выше, существует такое $\alpha > 0$, что $2^{2n+1} + 2^{n+1} + 1 = p^\alpha$. Покажем, во-первых, что α не является четным. Если α четно, то $(p^2-1) \mid (p^\alpha - 1)$. Если $x \in \pi(q-1)$ простое нечетное, то $x \mid (2^{2n+1}-1)$. Кроме того, $\pi(q-1) \subseteq \pi((p^2-1)/2)$, и тем самым $x \mid (p^2-1)$. Отсюда

$$x \mid (p^\alpha - 1) \Rightarrow x \mid (2^{2n+1} + 2^{n+1}), \quad x \mid (2^{2n+1}-1) \Rightarrow x \mid (2^{n+1}+1) \Rightarrow x \mid (2^{2n+2}-1).$$

Поэтому $x \mid (2^{2n+2}-1)$ и $x \mid (2^{2n+1}-1)$, откуда вытекает, что $x = 1$; противоречие. Следовательно, α нечетно. Докажем теперь, что $\alpha \neq 1$ невозможно. Пусть $\alpha > 1$ нечетно. По предположению

$$2^{n+1}(2^n+1) = (p-1)\left(\frac{p^\alpha - 1}{p-1}\right),$$

а согласно лемме 2.6 нам известно, что $\left(p-1, \frac{p^\alpha-1}{p-1}\right) = (p-1, \alpha)$. Поскольку $2 \mid (p-1)$ и α нечетно, имеем $2^{n+1} \mid (p-1)$. Поэтому

$$\frac{p^\alpha - 1}{p-1} \leq 2^n + 1 < 2^{n+1} \leq p - 1 \Rightarrow p^\alpha - 1 \leq p^2 - 1;$$

противоречие, ибо $\alpha \geq 3$. Итак, $\alpha = 1$ и $p = 2^{2n+1}+2^{n+1}+1$. Если $x \in \pi(p-1)$ и x нечетно, то $x \in \pi(2^n+1)$. В этом случае имеем также, что $\pi(q-1) \subseteq \pi((p^2-1)/2)$. Несложными вычислениями можно показать, что

$$\pi(q-1) \cap \pi(p-1) = \pi(2^{2n+1}-1) \cap (\pi(2^n+1) \cup \{2\}) = \varnothing.$$

Поэтому если x — нечетный простой делитель $q-1 = 2^{2n+1}-1$, то $x \in \pi(p+1) = \pi(2^{2n+1}+2^{n+1}+2)$ и путем простых вычислений получаем $x = 7$. Отсюда $n = 1$ и $q = 8$, следовательно, $p = 13$. Пришли к противоречию, так как $\pi(q-\sqrt{2q}+1) = \{5\} \neq \pi((p^2+1)/2)$.

(5.3) Если $\pi(q-\sqrt{2q}+1) = \{p\}$, то $2^{2n+1}-2^{n+1}+1 = p^\beta$ для некоторого $\beta > 0$. Вновь аналогично (5.2) приходим к противоречию. Детали мы опустим.

Случай 6. Пусть $K/H \cong {}^2D_{p'}(3)$, где $p' = 2^n+1$ $(n \geq 2)$. Тогда нечетные компоненты K/H суть $\pi((3^{p'-1}+1)/2)$ и $\pi((3^{p'}+1)/4)$.

(6.1) Если $\pi((3^{p'-1}+1)/2) = \{p\}$ и $\pi((3^{p'}+1)/4) = \pi((p^2+1)/2)$, то $(3^{p'-1}+1)/2 = p^k$ для некоторого $k > 0$. По лемме 2.8 заключаем, что $k = 1$ и $p = (3^{p'-1}+1)/2$. Кроме того, согласно предположениям

$$\pi((3^{p'}+1)/4) = \pi((p^2+1)/2) = \pi((3^{2p'-2}+2\times 3^{p'-1}+5)/8).$$

Если x — нечетный элемент из $\pi(3^{p'}+1)$, то ввиду того, что $x \mid (3^{2p'}-1+1+2\times 3(3^{p'}+1)-6+45)$, имеем $x \mid 40$. Поэтому $x \mid 5$ и $(3^{p'}+1)/4 = 5^k$ при каком-то $k > 0$. Поскольку $p' = 2^n+1$, то

$$3^{p'} = 3^{2^n+1} = 3\times 3^{2^n} \equiv 3(-1)^{2^{n-1}} \equiv 3 \not\equiv -1 \pmod 5;$$

противоречие.

(6.2) Если $\pi((3^{p'-1}+1)/2) = \pi((p^2+1)/2)$ и $\pi((3^{p'}+1)/4) = \{p\}$, то $(3^{p'}+1)/4 = p^k$ для некоторого $k > 0$. Тем самым $(3^{p'-1}+1)/2 = (2p^k+1)/3$. Отсюда $\pi((p^2+1)/2) = \pi((2p^k+1)/3)$. Если k нечетно и $x \in \pi((p^2+1)/2)$, то $x \mid (p^{2k}+1)$. К тому же $x \mid (2p^k+1)$, откуда $x \mid (4p^{2k}-1)$. Значит, $x \mid 5$ и $(p^2+1)/2 = 5^k$. По лемме 2.8 ввиду нечетности k имеем $k = 1$ и $p = 3$; противоречие, ибо $(3^{p'}+1)/4 \neq 3^k$. Если k четно и $x \in \pi((p^2+1)/2) = \pi((3^{p'-1}+1)/2)$, то $x \neq 3$ и $p^2 \equiv -1 \pmod x$. Отсюда

$$p^k \equiv (-1)^{k/2} \pmod x \Rightarrow 2p^k+1 \equiv 2(-1)^{k/2}+1 \not\equiv 0 \pmod x;$$

противоречие.

Случай 7. Пусть $K/H \cong F_4(q)$, где $q = 2^n > 2$. Тогда нечетные компоненты K/H суть q^4+1 и q^4-q^2+1. Вновь рассмотрим два подслучая.

(7.1) Если $\pi(2^{4n}+1) = \{p\}$ и $\pi(2^{4n}-2^{2n}+1) = \pi((p^2+1)/2)$, то $p = 2^{4n}+1$ по лемме 2.7. Отсюда $\pi(2^{4n}-2^{2n}+1) = \pi(2^{8n-1}+2^{4n}+1)$. Аналогично последним случаям можно показать, что $(2^{4n}-2^{2n}+1, 2^{8n-1}+2^{4n}+1) = 1$; противоречие.

(7.2) Если $\pi(2^{4n}-2^{2n}+1) = \{p\}$ и $\pi(2^{4n}+1) = \pi((p^2+1)/2)$, то $2^{4n}-2^{2n}+1 = p^k$ для некоторого $k > 0$. Если $4 \mid k$, то $(p^2+1) \mid (p^k-1)$, тем самым $\pi(2^{4n}+1) \subseteq \pi(2^{4n}-2^{2n})$, а это противоречит тому, что $\pi(2^{4n}+1) \cap \pi(2^{2n}-1) = \varnothing$. Если $2 \| k$, то $(p^2+1) \mid (p^k+1)$, так что $\pi(2^{4n}+1) \subseteq \pi(2^{4n}-2^{2n}+2)$; противоречие. Следовательно, k нечетно и $2 \nmid (p-1,k)$. Отсюда по лемме 2.6 вытекает, что $(p-1,(p^k-1)/(p-1))$ нечетно и $2 \mid (p-1)$, откуда

$$2^{2n}(2^{2n}-1) = (p-1)\cdot\frac{p^k-1}{p-1} \Rightarrow\ 2^{2n} \mid (p-1),\quad \frac{p^k-1}{p-1} \leq 2^{2n}-1.$$

Поэтому $p^k-1\le p^2-1$ и тем самым $k=1$. Тогда $p=2^{4n}-2^{2n}+1$ и $(p^2+1)/2=(2^{4n-1}-2^{2n}+1)(2^{4n}+1)$. Согласно предположению $\pi((p^2+1)/2)=\pi(2^{4n}+1)$, следовательно, $\pi(2^{4n-1}-2^{2n}+1)\subseteq\pi(2^{4n}+1)$. Если $x\in\pi(2^{4n-1}-2^{2n}+1)$, то $x\mid(2^{4n}+1)$ и мы заключаем, что $x\mid 5$. Значит, $\pi(2^{4n-1}-2^{2n}+1)=\{5\}$, поэтому $2^{4n-1}-2^{2n}+1=5^\alpha$ при каком-то $\alpha\in\mathbb{N}$. Тогда $2^{2n}(2^{2n-1}-1)=5^\alpha-1$.

Пусть $\alpha=2^rs$, где $r,s\in\mathbb{N}$ и s нечетно. Заметим, что $2^{r+2}\|(5^{2^r}-1)$, ибо

$$5^{2^r}-1=4\prod_{i=0}^{r-1}(5^{2^i}+1)$$

и $2\|(5^{2^i}+1)$ для любого $i\in\mathbb{N}$. По лемме 2.6 имеем

$$\left(\frac{5^\alpha-1}{5^{2^r}-1},5^{2^r}-1\right)=\left(\frac{5^{2^rs}-1}{5^{2^r}-1},5^{2^r}-1\right)=(s,5^{2^r}-1).$$

Отсюда $(5^\alpha-1)/(5^{2^r}-1)$ нечетно, так как s нечетно. Поэтому $2^{r+2}\|(5^\alpha-1)$, откуда вытекает, что $2n=r+2$, ибо $2^{2n}(2^{2n-1}-1)=5^\alpha-1$. Если $r\ge2$, то

$$2^{2n-1}-1<2^{r+1}<\frac{5^{2^{r-1}}+1}{2}\Rightarrow 2^{2n}(2^{2n-1}-1)=2^{r+2}(2^{r+1}-1)<5^{2^r}-1\le5^\alpha-1;$$

противоречие. Если $r=0$, то $n=1$ и $p=13$. Но в таком случае $\pi((p^2+1)/2)\ne\pi(2^{4n}+1)$; противоречие.

Случай 8. Если $K/H\cong E_8(q)$, ${}^2F_4(q)$, где $q=2^{2n+1}>2$, или если $K/H\cong{}^2G_2(q)$, где $q=3^{2n+1}$, то подобно случаю 7 приходим к противоречию, поэтому опустим детали.

Случай 9. Если $K/H\cong G_2(q)$, где $q=3^n$, то надо рассмотреть два случая.

(9.1) Если $\pi(q^2+q+1)=\{p\}$ и $\pi(q^2-q+1)=\pi((p^2+1)/2)$, то $\pi(p-1)\subseteq\pi(3^{2n}+3^n)$. Если $x\in\pi(q^2-q+1)$, то $p^2\equiv-1\pmod{x}$. Поэтому $(-1/x)=1$, а значит, $x=4k+1$. Следовательно, каждый простой делитель $q^2-q+1=3^{2n}-3^n+1$ имеет вид $4k+1$, так что q^2-q+1 вида $4k+1$. Но n четно. Пусть $n=2m$. Тогда

$$q^2+q+1=3^{4m}+3^{2m}+1=(3^{2m}+1+3^m)(3^{2m}+1-3^m);$$

противоречие, потому что $\pi(q^2+q+1)=\{p\}$ и $\pi(3^{2m}+1+3^m)\cap\pi(3^{2m}+1-3^m)=\varnothing$.

(9.2) Если $\pi(q^2-q+1)=\{p\}$ и $\pi(q^2+q+1)=\pi((p^2+1)/2)$, то $3^{2n}+3^n+1$ вида $4k+1$, откуда n нечетно. И вновь приходим к противоречию аналогично последним случаям.

Случай 10. Если $p\ne7$ и K/H — простая спорадическая группа, $PSL(3,4)$, $PSU(6,2)$, $PSU(4,3)$, $E_7(2)$, $E_7(3)$, ${}^2E_6(2)$ или $F_4(2)$, то легко прийти к противоречию, используя порядок группы и нечетность компоненты. Например, если $K/H\cong F_4(2)$, то $p=13$ или $p=17$. Если $p=13$, $\pi((p^2+1)/2)\ne\{17\}$ и если $p=17$, то $\pi((p^2+1)/2)\ne\{13\}$; противоречие.

Если $p=7$, то $K/H\cong PSL(3,4)$ или $PSU(4,3)$.

Пусть $K/H\cong PSL(3,4)$. Известно, что $\mathrm{Out}(PSL(3,4))\cong\mathbb{Z}_2\times S_3$. Из атласа конечных групп известно, что $PSL(3,4).2_2\cong PSL(3,4).2_2'\cong PSL(3,4).2_2''$ имеет элемент порядка 14 и $PSL(3,4).2_3\cong PSL(3,4).2_3'\cong PSL(3,4).2_3''$ включает элемент порядка 10. Но $2\nsim5$ и $2\nsim7$ в $\Gamma(PSL(2,49))$. Отсюда подобно последним случаям следует, что $G/O_{\{2,3\}}(G)\cong PSL(3,4)$ или $PSL(3,4).2_1$.

Пусть $K/H \cong PSU(4,3)$. Заметим, что $\mathrm{Out}(PSU(4,3)) \cong D_8$. Тогда аналогично заключаем, что $G/O_{\{2,3\}}(G) \cong PSU(4,3)$, так как в обозначениях из атласа конечных групп $2 \nsim 5$ в $\Gamma(G)$ и $PSU(4,3).2_1$, $PSU(4,3).2_2$, $PSU(4,3).2_3$ и $PSU(4,3).4$ имеют элементы порядка 10 и, следовательно, $\Gamma(PSU(4,3).2_1)$, $\Gamma(PSU(4,3).2_2)$, $\Gamma(PSU(4,3).2_3)$ и $\Gamma(PSU(4,3).4)$ не подграфы $\Gamma(G)$.

Теорема доказана. □

Теорема 3.2. *Пусть G — конечная группа. Если G — конечная группа такая, что $|G| = |PSL(2,p^2)|$ и $\Gamma(G) = \Gamma(PSL(2,p^2))$, то $G \cong PSL(2,p^2)$.*

Доказательство. Если $p \neq 2,3,7$, то из теоремы 3.1 следует, что $G \cong PSL(2,p^2)$.

Если $p = 3$, то из теоремы 3.1 вытекает, что $G \cong PSL(2,9)$, $PSL(2,9).2_3$ или $G/O_2(G) \cong PSL(2,5)$. Но $G/O_2(G) \ncong PSL(2,5)$, так как $3 \| |PSL(2,5)|$ и $3^2 \mid |PSL(2,9)|$. Теперь $|G| = |PSL(2,9)|$ влечет, что $G \cong PSL(2,9)$.

Если $p = 7$, то $G \cong PSL(2,49)$, $PSL(2,49).2_3$ или $G/O_{\{2,3\}}(G)$ изоморфна $PSL(3,4)$, $PSL(3,4).2_1$, $PSU(4,3)$ или A_7. Известно, что $7^2 \mid |PSL(2,49)|$, но 7^2 не делит порядки $PSL(3,4)$, $PSL(3,4).2_1$, $PSU(4,3)$ и A_7. Поэтому $G \cong PSL(2,49)$ или $PSL(2,49).2_3$. Используя порядок G, получаем требуемое.

Аналогично приходим к результату при $p = 2$. □

Замечание 3.1. Ши и Би в [19] сделали следующее

Предположение. *Пусть G — конечная группа и M — конечная простая группа. Тогда $G \cong M$ в том и только в том случае, если* (i) $|G| = |M|$, (ii) $\pi_e(G) = \pi_e(M)$.

Это предположение справедливо для простых спорадических групп [20], альтернированных групп и некоторых простых групп лиева типа [19–21]. В качестве следствия предыдущих теорем дадим новое доказательство этого предположения для рассматриваемых групп.

Следствие 3.1. *Пусть G — конечная группа. Если $|G| = |PSL(2,p^2)|$ и $\pi_e(G) = \pi_e(PSL(2,p^2))$, то $G \cong PSL(2,p^2)$.*

Благодарности

Авторы признательны рецензенту за внимательное прочтение и многочисленные пожелания, которые помогли улучшить первоначальную версию статьи. Второй автор выражает благодарность Исследовательскому институту теоретической физики и математики (IPM), Тегеран, Иран, за финансовую поддержку. Мы посвящаем эту статью нашей семье — Зорайе, Бахману и Бехнаму за из бесконечную любовь и поддержку.

ЛИТЕРАТУРА

1. *Васильев А. В., Гречкосеева М. А.* О распознаваемости конечных простых ортогональных групп размерности 2^m, 2^m+1 и 2^m+2 над полем характеристики 2 // Сиб. мат. журн. 2004. Т. 45, № 3. С. 420–432.
2. *Iiyori N., Yamaki H.* Prime graph components of the simple groups of Lie type over the field of even characteristic // J. Algebra. 1993. V. 155, N 2. P. 335–343.
3. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
4. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
5. *Lucido M. S.* The diameter of the prime graph of a finite group // J. Group Theory. 1999. V. 2, N 2. P. 157–172.

6. *Hagie M.* The prime graph of a sporadic simple group // Comm. Algebra. 2003. V. 31, N 9. P. 4405–4424.
7. *Хосрави А., Хосрави Б.* Квазираспознавание простой группы $^2G_2(q)$ по графу простых чисел // Сиб. мат. журн. 2007. Т. 48, № 3. С. 707–716.
8. *Заварницин А. В.* О распознавании конечных групп по графу простых чисел // Алгебра и логика. 2006. Т. 45, № 4. С. 390–408.
9. *Khosravi B., Khosravi B., Khosravi B.* On the prime graph of $PSL(2,p)$ where $p > 3$ is a prime number // Acta. Math. Hung. 2007. V. 116, N 4. P. 295–307.
10. *Conway J., Curtis R., Norton S., Parker R., Wilson R.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
11. *Lucido M. S.* Prime graph components of finite almost simple groups // Rend. Sem. Mat. Univ. Padova. 1999. V. 102. P. 1–22.
12. *Gruenberg K. W., Roggenkamp K. W.* Decomposition of the augmentation ideal and of the relation modules of a finite group // Proc. London Math. Soc. 1975. V. 31, N 2. P. 148–166.
13. *Huppert B.* Endliche Gruppen I. New York: Springer-Verl., 1967. (Grundlehren der Math. Wiss.; N 134).
14. *Gorenstein D.* Finite groups. New York: Harper and Row, 1968.
15. *Sierpiński W.* Elementary theory of numbers. Warsaw: Panstwowe Wydawnictwo Nauk., 1964.
16. *Khosravi A., Khosravi B.* A new characterization of some alternating and symmetric groups (II) // Houston J. Math. 2004. V. 30, N 4. P. 465–478.
17. *Crescenzo P.* A Diophantine equation which arises in the theory of finite groups // Adv. Math. 1975. V. 17, N 1. P. 25–29.
18. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.
19. *Shi W. Bi J.* A characteristic property for each finite projective special linear group // Lecture Notes in Math. 1990. V. 1456. P. 171–180.
20. *Shi W.* A new characterization of the sporadic simple groups // Group theory: Proc. of the 1987 Singapore group theory conference. Berlin; New York: Walter de Gruyter, 1989. P. 531–540.
21. *Shi W.* Pure quantitative characterization of finite simple groups (I) // Progr. Natur. Sci. 1994. V. 4, N 3. P. 316–326.
22. *Shi W.* A new characterization of some simple groups of Lie type // Contemp. Math. 1989. V. 82. P. 171–180.

Статья поступила 5 июня 2006 г., окончательный вариант — 16 октября 2007 г.

Amir Khosravi (Хосрави Амир)
Faculty of Mathematical Sciences and Computer Engineering,
University For Teacher Education,
599 Taleghani Ave., Tehran 15614, IRAN

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,
Institute for Studies in Theoretical Physics and Mathematics (IPM)
khosravibbb@yahoo.com