Сибирский математический журнал
Март—апрель, 2002. Том 43, № 2

УДК 512.542

О КОМПОЗИЦИОННЫХ ФАКТОРАХ КОНЕЧНЫХ ГРУПП С МНОЖЕСТВОМ ПОРЯДКОВ ЭЛЕМЕНТОВ, КАК У ГРУППЫ $U_3(q)$

М. Р. Алеева

Аннотация: Изучены композиционные факторы конечной неразрешимой группы с множеством порядков элементов, как у простой унитарной группы $U_3(q)$ для нечетного q. В частности, доказано, что при $q > 5$ (единственный) неабелев композиционный фактор такой группы изоморфен $U_3(q)$. Библиогр. 21.

Введение

Пусть G — конечная группа. Обозначим через $\omega(G)$ множество всех порядков элементов группы G. Это множество частично упорядочено относительно делимости и потому вполне определяется подмножеством $\mu(G)$ своих максимальных по делимости элементов. Для натурального числа n через $\pi(n)$ обозначим множество всех простых делителей числа n и положим $\pi(G) = \pi(|G|)$. Множество $\omega(G)$ определяет граф Грюнберга — Кегеля, или граф простых чисел $\mathrm{GK}(G)$ группы G, множеством вершин которого служит $\pi(G)$ и две вершины p, q из $\pi(G)$ соединены ребром, если G содержит элемент порядка pq. Обозначим через $\pi_i = \pi_i(G)$, где $i = 1, \dots, s(G)$, i-ю связную компоненту графа $\mathrm{GK}(G)$. Для группы G четного порядка положим $2 \in \pi_1$. Обозначим через $\mu_i = \mu_i(G)$ множество тех $n \in \mu(G)$, для которых $\pi(n) \subseteq \pi_i$.

Грюнберг и Кегель доказали следующую структурную теорему для конечных групп с несвязным графом простых чисел.

Теорема Грюнберга — Кегеля [1, теорема A]. *Если G — конечная группа с несвязным графом Грюнберга — Кегеля, то верно одно из следующих утверждений:*

(а) *G — группа Фробениуса;*

(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 $P \leq A \leq \mathrm{Aut}(P)$, P — простая неабелева группа с несвязным графом $\mathrm{GK}(P)$, A/P — $\pi_1(G)$-группа.*

Обозначим через $U_3(q)$ простую унитарную группу размерности 3 над полем порядка q^2. В. Д. Мазуров в [2] доказал распознаваемость (с точностью до изоморфизма) групп $U_3(q)$ по множеству порядков ее элементов для четного q. Мы рассматриваем аналогичную задачу для нечетного q.

Пусть далее $\omega(G) = \omega(U_3(q))$, где q нечетно. Тогда $\mathrm{GK}(G)$ имеет две компоненты связности: $\pi_1(G) = \pi(q(q^2-1))$, $\pi_2(G) = \pi((q^3+1)/(q+1)(3, q+1))$.

Используя классификацию конечных простых групп с несвязным графом Грюнберга — Кегеля (см. [1, 3]), мы доказываем следующие две теоремы.

Теорема 1. *Пусть G — конечная неразрешимая группа, $\omega(G) = \omega(U_3(q))$, где q нечетно. Тогда*

1) *выполняется случай* (в) *теоремы Грюнберга — Кегеля;*

2) *если $q > 5$, то группа P изоморфна группе $U_3(q)$;*

3) $\pi(N) \subseteq \pi(q+1)$;

4) *если все компоненты связности подграфа $\pi_1(G) \setminus \{2\}$ графа $\mathrm{GK}(G)$ одноэлементны, то группа N является 2-группой;*

5) $|A/P| \leq 2$.

Теорема 2. *Пусть выполняются условия теоремы* 1 *и $q \leq 11$. Тогда*

1) *если $q = 3$, то группа $G/O_2(G)$ изоморфна $L_3(2)$, $L_3(2).2$, $U_3(3)$ или $U_3(3).2$ при $O_2(G) \neq 1$, G изоморфна $U_3(3)$ или $U_3(3).2$ при $O_2(G) = 1$;*

2) *если $q = 5$, то $G/O_2(G)$ изоморфна $L_3(4)$, $L_3(4).2_1$, $L_3(4).2_3$ или A_7 при $O_2(G) \neq 1$, G изоморфна $L_3(4).2_3$ или $U_3(5)$ при $O_2(G) = 1$;*

3) *если $q = 7$, то $G/O_2(G)$ изоморфна $U_3(7)$ или $U_3(7).2$;*

4) *если $q = 9$, то G изоморфна $U_3(9)$;*

5) *если $q = 11$, то G изоморфна $U_3(11)$.*

Замечание. Имеются примеры расширений нетривиальных 2-групп при помощи групп $U_3(3)$, $L_3(4)$, $U_3(7)$ с такими же множествами порядков элементов, как у групп $U_3(3)$, $U_3(5)$, $U_3(7)$ соответственно (см. [4]).

Основные определения и обозначения, принятые в работе, стандартны, их можно найти в [5] или [6].

Автор выражает глубокую признательность своему научному руководителю А. С. Кондратьеву и А. Н. Фомину за ценные обсуждения.

1. Предварительные результаты

Напомним, что *группой Фробениуса с ядром N и дополнением H* называется полупрямое произведение $G = NH$ нетривиальных групп, где N — нормальная в G подгруппа и $C_N(h) = 1$ для любого неединичного элемента h из H.

Лемма 1 [5, 7, 8]. *Пусть $G = NH$ — группа Фробениуса с ядром N и дополнением H. Тогда верны следующие утверждения.*

1) *N — нильпотентная группа.*

2) *Если U — подгруппа порядка pq из H, где p и q — простые числа* (*не обязательно различные*), *то U — циклическая группа. В частности, силовские p-подгруппы группы H для нечетных простых чисел p циклические.*

3) *Если порядок H четен, то в H есть единственный элемент z порядка* 2, *в частности, силовская 2-подгруппа группы H является циклической группой или* (*обобщенной*) *группой кватернионов, подгруппа N коммутативна и $n^z = n^{-1}$ для любого элемента n из N.*

Лемма 2 (теорема Цассенхауза, см. [9]). *Пусть C — неразрешимое дополнение Фробениуса. Тогда C имеет подгруппу C_0 индекса, не превосходящего* 2, *$C_0 \cong SL(2,5) \times M$, где M — группа с циклическими силовскими подгруппами и $|M|$ не делится на* 2, 3, 5.

Лемма 3 [10, леммы 4.29, 4.30]. *Пусть $q = p^{2n}$, p — нечетное простое число, n — натуральное число, $P = U_3(q)$, $A = \mathrm{Aut}(P)$. Тогда*

(а) *$A \cong PGU_3(q)$, $A = CF$, $C \lhd A$, где $C \cong PU_3(q)$, $C/P \cong Z_{(3,q+1)}$, F — группа полевых автоморфизмов, $F \cong Z_{2n}$;*

(б) *если φ — единственная инволюция из F, то все инволюции из $C\varphi$ сопряжены относительно C, $C_P(\varphi) \cong SO_3(q) \cong PGL_2(q)$.*

Лемма 4 [11, лемма 1]. *Пусть G — конечная группа, $N \lhd G$, G/N — группа Фробениуса с ядром F и циклическим дополнением H. Если $(|F|, |N|) = 1$ и F не содержится в $NC_G(N)/N$, то $p|H| \in \omega(G)$ для некоторого простого делителя p порядка N. Если дополнительно полный прообраз F в G — группа Фробениуса с ядром N, то $|H| \cdot \prod_{p\in\pi(N)} p \in \omega(G)$.*

Лемма 5 (теорема Жигмонди, см. [12]). *Пусть q и n — целые числа, $q \geq 2$, $n \geq 3$. Если $(q, n) \neq (2, 6)$, то существует простое число, делящее $q^n - 1$ и взаимно простое с $q^i - 1$ для всех i, $1 \leq i < n$.*

Лемма 6. *Пусть натуральные числа r и s удовлетворяют уравнению $r^2 - r + 1 = (s^2 + \varepsilon s + 1)/3$, где $\varepsilon = \pm 1$ и $(s - \varepsilon, 3) = 3$. Тогда*

1) *если $\varepsilon = -1$ и r — степень простого числа, то $r = 3$, $s = 5$;*

2) *если $\varepsilon = -1$ и $r - 1$ — степень простого числа, то $r = 3$, $s = 5$ или $r = 10$, $s = 17$;*

3) *если $\varepsilon = 1$ и r — степень простого числа, то $r = 3$, $s = 4$;*

4) *если $\varepsilon = 1$ и $r - 1$ — степень простого числа, то $r = 3$, $s = 4$ или $r = 10$, $s = 16$.*

Доказательство. Пусть $\varepsilon = -1$. Тогда $3r(r - 1) = (s - 2)(s + 1)$. Если $s = 2$, то $r = 0, 1$. Можно считать, что $s > 2$. Утверждения 1 и 2 доказываются аналогично. Докажем утверждение 1. Если r — степень простого числа, не равного 3, то либо $r \mid (s - 2)$, либо $r \mid (s + 1)$.

Пусть $r \mid (s - 2)$. Тогда $r = (s - 2)/t$, $3(r - 1) = (s + 1)t$. Пусть $t = 1$. Тогда $r = s - 2$, $s = r + 2$, $3r - 3 = s + 1 = r + 3$, $r = 3$, $s = 5$. Пусть $t \geq 2$. Тогда $r = (s-2)/t \leq s/2-1$, $3(r-1) = (s+1)t \geq 2(s+1)$. Отсюда $2s+5 \leq 3r \leq 3s/2-3$, $s \leq -16$; противоречие.

Остальные случаи рассматриваются аналогично.

Пусть $\varepsilon = 1$. Положим $x = s + 1$. Тогда $r^2 - r + 1 = (x^2 - x + 1)/3$. Если r — степень простого числа, то по утверждению 1 имеем $x = 5$, т. е. $s = 4$. Если $r - 1$ — степень простого числа, то по утверждению 2 будет $x = 5$ или $x = 17$, т. е. $s = 4$ или $s = 16$.

Лемма 7. *Пусть x, y, z, u — натуральные числа, $x \mid u$, $y \mid u$, $z \mid u$, $d = (x, y) = (x, z) = (y, z)$. Тогда*

(а) $\frac{xy}{d} \mid u$;

(б) $\frac{xyz}{d^2} \mid u$.

Доказательство. (а) Имеем $x = x_1 d$, $y = y_1 d$, где $(x_1, y_1) = 1$. Так как $x \mid u$, то $x_1 \mid \frac{u}{d}$. Поскольку $y \mid u$, то $y_1 \mid \frac{u}{d}$. Так как $(x_1, y_1) = 1$, то $x_1 y_1 \mid \frac{u}{d}$, $x_1 y_1 d \mid u$, т. е. $\frac{xy}{d} \mid u$.

(б) Имеем $x = x_1 d$, $y = y_1 d$, $z = z_1 d$, где $(x_1, y_1) = (x_1, z_1) = (y_1, z_1) = 1$. По п. (а) $\frac{xy}{d} \mid u$, $x_1 y_1 \mid \frac{u}{d}$. Так как $z_1 \mid \frac{u}{d}$ и $(x_1 y_1, z_1) = 1$, то $x_1 y_1 z_1 \mid \frac{u}{d}$, т. е. $\frac{xyz}{d^2} \mid u$.

Лемма 8 [13, лемма 4]. *Пусть H — конечная простая группа с несвязным графом $\mathrm{GK}(H)$. Тогда $|\mu_i(H)| = 1$ для $2 \leq i \leq s(H)$. Пусть n_i означает единственный элемент из $\mu_i(H)$ для $i > 1$. Тогда H, $\pi_1(H)$, n_i для $2 \leq i \leq s(H)$ такие, как в табл. 1–3 из [13].*

Введем ряд обозначений: $d = (3, q + 1)$, $r = q + 1$, $r' = r/d$, $s = q - 1$, $t = q^2-q+1$, $t' = t/d$, $A_1 = \{0, 1, \dots, r-1\}$, $A_2 = \{1, \dots, rs\} \setminus \{s, 2s, \dots, rs\}$ ($|A_2| = r(s - 1)$), $A_3 = \{1, \dots, t - 1\} \setminus \{t', 2t'\}$ ($|A_3| = t - d$).

Зафиксируем элементы: ω_1, ρ, σ, τ мультипликативных порядков d, r, $rs(= q^2 - 1)$, $rt(= q^3 + 1)$ соответственно из $GF(q^6)$ такие, что $\rho = \sigma^s = \tau^t$, $\omega_1 = \rho^{r'}$, и элемент β из $GF(q^2)$, равный 1 при $d=1$ и не являющийся кубом в $GF(q^2)$ при $d=3$.

Рассмотрим следующие матрицы из $SU_3(q)$:

$$c_1^{(j)}=\begin{pmatrix}\omega_1^j&0&0\\0&\omega_1^j&0\\0&0&\omega_1^j\end{pmatrix},\quad c_2^{(j)}=\begin{pmatrix}\omega_1^j&0&0\\1&\omega_1^j&0\\0&0&\omega_1^j\end{pmatrix},\quad c_3^{(h,j)}=\begin{pmatrix}\omega_1^j&0&0\\\beta^h&\omega_1^j&0\\0&\beta^h&\omega_1^j\end{pmatrix},$$

где $\{h,j\}\subseteq\{0,1,\dots,d-1\}$;

$$c_4^{(a)}=\begin{pmatrix}\rho^a&0&0\\0&\rho^a&0\\0&0&\rho^{-2a}\end{pmatrix},\ c_5^{(a)}=\begin{pmatrix}\rho^a&0&0\\1&\rho^a&0\\0&0&\rho^{-2a}\end{pmatrix},\ c_6^{(a,b,c)}=\begin{pmatrix}\rho^a&0&0\\0&\rho^b&0\\0&0&\rho^c\end{pmatrix},$$

где $a,b,c\in A_1$, $a\neq b\neq c\neq a$, $r\mid a+b+c$;

$$c_6^{(0,r',2r')}=\begin{pmatrix}1&0&0\\0&\omega_1&0\\0&0&\omega_1^2\end{pmatrix};$$

$c_7^{(1)}$ и $c_8^{(1)}$ — элементы, сопряженные в $SU(3,q^6)$ с

$$h_1^{(a)}=\begin{pmatrix}\rho^{-1}&0&0\\0&\sigma^{-1}&0\\0&0&\sigma^q\end{pmatrix}\quad\text{и}\quad h_2^{(a)}=\begin{pmatrix}\tau^r&0&0\\0&\tau^{-rq}&0\\0&0&\tau^{rq^2}\end{pmatrix}$$

соответственно; $c_7^{(e)}=\big(c_7^{(1)}\big)^e$, где $e\in A_2$, и $c_8^{(f)}=\big(c_8^{(1)}\big)^f$, где $f\in A_3$.

Пусть $Cl(G)$ — множество всех классов сопряженных элементов группы G. Условимся, что

1) обозначение класса сопряженных элементов группы $SU_3(q)$, содержащего какой-либо из обозначенных выше элементов, получается из обозначения этого элемента заменой c на C;

2) если в обозначении класса C сопряженных элементов группы $SU_3(q)$, поставить черту над буквой C, то получится обозначение образа этого класса при естественном гомоморфизме $SU_3(q)$ на $U_3(q)$.

Лемма 9 [14, лемма E4]. *Пусть $G=U_3(q)$. Тогда $Cl(G)=\bigcup\limits_{i=1}^{8}K_i$, где*

1) $K_i=\big\{K_i^{(0)}\big\}$ *при* $i\in\{1,2\}$ *с* $K_i^{(0)}=\overline{C}_i^{(0)}$;

2) $K_3=\big\{K_3^{(h)}\mid h\in\{0,\dots,d-1\}\big\}$ *с* $K_3^{(h)}=\overline{C}_3^{(h,0)}$;

3) $K_i=\big\{K_i^{(a)}\mid a\in\{1,\dots,r'-1\}\big\}$ *с* $K_i^{(a)}=\overline{C}_i^{(a)}$ *при* $i\in\{4,5\}$;

4) $K_6=\big\{K_6^{(a,b,c)}\mid 0\le a<b<c\le r-1, r\mid a+b+c, (a,b,c)\neq(0,r',2r')\big\}\cup\{K_6'\}$ *с* $K_6^{(a,b,c)}=\overline{C}_6^{(a,b,c)}$ *и* $K_6'=\overline{C}_6^{(0,r',2r')}$ (K_6' *существует лишь при* $d=3$);

5) $K_7=\big\{K_7^{(e)}\mid 1\le e\le r's, s$ *не делит* $e\big\}$ *с* $K_7^{(e)}=\overline{C}_7^{(e)}$;

6) $K_8=\big\{K_8^{(f)}\mid 1\le f\le t'-1\big\}$ *с* $K_8^{(f)}=\overline{C}_8^{(f)}$.

Лемма 10. *Пусть $q=p^f$, p — нечетное простое число. Тогда*
$\mu(G)=\{p(q+1),q^2-1,q^2-q+1\}$ *при* $(3,q+1)=1$,
$\mu(G)=\{p(q+1)/3,(q^2-1)/3,(q+1),(q^2-q+1)/3\}$ *при* $(3,q+1)=3$.

Доказательство. Для вычисления порядков элементов группы $U_3(q)$ используем матричные представления элементов группы $SU_3(q)$ из [14]. Рассмотрим представителей классов сопряженных элементов группы $SU_3(q)$.

Матрицы

$$c_1^{(j)} = \begin{pmatrix} \omega_1^j & 0 & 0 \\ 0 & \omega_1^j & 0 \\ 0 & 0 & \omega_1^j \end{pmatrix}$$

имеют порядок $d = (3, q+1)$.

Вычислим порядки матриц

$$c_2^{(j)} = \begin{pmatrix} \omega_1^j & 0 & 0 \\ 1 & \omega_1^j & 0 \\ 0 & 0 & \omega_1^j \end{pmatrix}.$$

Индукцией по n получаем

$$\left(c_2^{(j)}\right)^n = \begin{pmatrix} \omega_1^{nj} & 0 & 0 \\ n\omega_1^{(n-1)j} & \omega_1^{nj} & 0 \\ 0 & 0 & \omega_1^{nj} \end{pmatrix}.$$

Значит, порядок $c_2^{(j)}$ равен pd, откуда $p \in \omega(G)$.

Рассмотрим матрицы

$$c_3^{(h,j)} = \begin{pmatrix} \omega_1^j & 0 & 0 \\ \beta^h & \omega_1^j & 0 \\ 0 & \beta^h & \omega_1^j \end{pmatrix},$$

где $\{h, j\} \subseteq \{0, 1, \ldots, d-1\}$. Индукцией по n находим

$$\left(c_3^{(h,j)}\right)^n = \begin{pmatrix} \omega_1^{nj} & 0 & 0 \\ n\beta^h\omega_1^{(n-1)j} & \omega_1^{nj} & 0 \\ \frac{n(n-1)}{2}\beta^{2h}\omega_1^{(n-2)j} & n\beta^h\omega_1^{(n-1)j} & \omega_1^{nj} \end{pmatrix}.$$

Следовательно, порядок $c_3^{(h,j)}$ равен pd.

Вычислим порядки матриц

$$c_4^{(a)} = \begin{pmatrix} \rho^a & 0 & 0 \\ 0 & \rho^a & 0 \\ 0 & 0 & \rho^{-2a} \end{pmatrix},$$

где $a \in A_1$. Индукцией по n получаем

$$\left(c_4^{(a)}\right)^n = \begin{pmatrix} \rho^{na} & 0 & 0 \\ 0 & \rho^{na} & 0 \\ 0 & 0 & \rho^{-2na} \end{pmatrix}.$$

Тем самым порядок $c_4^{(a)}$ равен $(q+1)/(a, q+1)$, откуда $(q+1)/d \in \omega(G)$.

Рассмотрим матрицы

$$c_5^{(a)} = \begin{pmatrix} \rho^a & 0 & 0 \\ 1 & \rho^a & 0 \\ 0 & 0 & \rho^{-2a} \end{pmatrix},$$

где $a \in A_1$. Индукцией по n получаем

$$\left(c_5^{(a)}\right)^n = \begin{pmatrix} \rho^{na} & 0 & 0 \\ n\rho^{(n-1)a} & \rho^{na} & 0 \\ 0 & 0 & \rho^{-2na} \end{pmatrix}.$$

Значит, порядок $c_5^{(a)}$ равен $p(q+1)/(a,q+1)$. Максимальный порядок элемента $c_5^{(a)}$ равен $p(q+1)$, поэтому $p(q+1)/d \in \omega(U_3(q))$.

Вычислим максимальный порядок матриц

$$c_6^{(a,b,c)} = \begin{pmatrix} \rho^a & 0 & 0 \\ 0 & \rho^b & 0 \\ 0 & 0 & \rho^c \end{pmatrix},$$

где $a,b,c \in A_1$, $a \neq b \neq c \neq a$, $r \mid a+b+c$. Порядок элемента $c_6^{(a,b,c)}$ делит $q+1$. Порядок элемента $c_6^{(0,1,q)}$ равен $q+1$. Значит, $q+1 \in \omega(G)$.

При $d=3$ рассмотрим матрицу

$$c_6^{(0,r',2r')} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega_1 & 0 \\ 0 & 0 & \omega_1^2 \end{pmatrix}.$$

Порядок элемента $c_6^{(0,r',2r')}$ равен $d=3$. Значит, $3 \in \omega(G)$ при $d=3$.

Элементы $c_7^{(1)}$ сопряжены в $SU(3,q^6)$ с

$$h_1^{(a)} = \begin{pmatrix} \rho^{-1} & 0 & 0 \\ 0 & \sigma^{-1} & 0 \\ 0 & 0 & \sigma^q \end{pmatrix}.$$

Порядок элемента $h_1^{(a)}$ равен q^2-1, откуда $(q^2-1)/d \in \omega(G)$.

Элементы $c_8^{(1)}$ сопряжены в $SU(3,q^6)$ с

$$h_2^{(a)} = \begin{pmatrix} \tau^r & 0 & 0 \\ 0 & \tau^{-rq} & 0 \\ 0 & 0 & \tau^{rq^2} \end{pmatrix}.$$

Порядок элемента $h_2^{(a)}$ равен q^2-q+1, откуда $(q^2-q+1)/d \in \omega(G)$.

Наконец, $c_7^{(e)} = (c_7^{(1)})^e$, где $e \in A_2$, и $c_8^{(f)} = (c_8^{(1)})^f$, где $f \in A_3$.

По лемме 9 получаем заключение леммы 10.

Лемма 11 [15, лемма 2]. *Пусть $d=(n,q-1)$. Тогда числа $(q^n-1)/d(q-1)$, $(q^{n-1}-1)/d$ лежат в $\mu(L_n(q))$.*

Лемма 12 [16]. *Пусть G — конечная группа с $\omega(G)=\omega(L_2(q))$, где $3<q\neq 9$. Тогда G изоморфна $L_2(q)$.*

2. Доказательство теорем

Пусть G — конечная неразрешимая группа с $\omega(G)=\omega(U_3(q))$, $q=p^f$ — степень нечетного простого числа p.

Докажем сначала теорему 1. Везде далее q' обозначает некоторую степень простого числа, а p' — некоторое нечетное простое число.

Лемма 13. *Утверждение 1 теоремы 1 справедливо.*

Доказательство. Предположим противное. Тогда выполняется случай (а) или (б) теоремы Грюнберга — Кегеля.

Пусть выполняется случай (а). Тогда $G=FC$ — группа Фробениуса с ядром F и дополнением C. Так как F нильпотентна, то C неразрешима. Применим лемму 2. Поскольку $8 \mid q^2-1$, то $|C : C_0 \times M| = 2$, т. е. в C есть элемент порядка 12. Пусть $p = 3$. Тогда существует $x \in C_0$, $|x| = 3$, $Z_4 \times M \leq C_C(x)$. Отсюда $4|M|$ делит $q+1$. Следовательно, $\pi(q-1) = \{2, 5\}$. Тем самым $q-1 = 10$, $q = 11$; противоречие. Пусть $p = 5$. Тогда существует $x \in C_0$, $|x| = 5$, $Z_{10} \times M \leq C_C(x)$, откуда $2|M|$ делит $q + 1$, причем 4 не делит $q + 1$. Значит, $\pi(q - 1) = \{2, 3\}$ и $4 \,|\, (q - 1)$. Отсюда $q - 1 = 12$, $q = 13$; противоречие. Пусть $p > 5$. Тогда существует $x \in M$, $|x| = p$ и 15 делит $\frac{q+1}{d}$. По лемме 10 в G есть элемент порядка $\frac{q+1}{d}$, следовательно, есть элемент порядка 15. Но в C нет элемента порядка 15; противоречие.

Пусть выполняется случай (б). Тогда $G = ABC$ и по лемме 1 A, B нильпотентны, откуда C неразрешима. По лемме 1 B — циклическая группа. Следовательно, C абелева; противоречие.

Мы будем придерживаться в дальнейшем обозначений утверждения (в) теоремы Грюнберга — Кегеля. Пользуясь таблицами 1–3 из [13] и применяя лемму 8, рассмотрим различные случаи для P.

Лемма 14. *Группа P не изоморфна спорадической группе.*

Доказательство. Пусть $P \cong J_2$. Так как $((q^3 + 1)/(q + 1)(3, q + 1)) \in \mu(G)$, по лемме 8 $(q^3 + 1)/(q + 1)(3, q + 1) = 7$, т. е. $q = 3, 5$. Если $q = 3$, то $\pi_1(G) = \pi(q(q^2 - 1)) = \{2, 3\}$ и $5 \notin \pi(G)$; противоречие. Если $q = 5$, то ввиду [6] $15 \in \omega(G)$; противоречие.

Остальные спорадические группы рассматриваются аналогично.

Лемма 15. *Если $P \cong A_n$, то $n = 7$ и $q = 5$.*

Доказательство. Пусть $P \cong A_n$. Тогда по лемме 8

$$\frac{q^2 - q + 1}{(3, q + 1)} \in \{n - 2, n - 1, n, n + 2\}.$$

Пусть $n = (q^2 - q + 1)/(3, q + 1)$. Если $(3, q + 1) = 1$, то $n = q^2 - q + 1$,

$$\pi(n - 2) = \pi(q^2 - q - 1) \subseteq \pi_1(P) \subseteq \pi_1(G) = \pi(q(q^2 - 1)),$$

но тогда $(q^2 - q - 1, q(q^2 - 1)) \neq 1$; противоречие.

Пусть $(3, q + 1) = 3$. Тогда $n = (q^2 - q + 1)/3$, $\pi(n - 3) = \pi((q^2 - q - 8)/3) \subseteq \pi(q(q^2 - 1))$. Отсюда $\pi(q^2 - q - 8) \subseteq \{2, 3\}$, т. е. $q^2 - q - 8 = 3 \cdot 2^m$. Если $m = 1$, то q не целое; противоречие. Пусть $m > 1$. Тогда

$$\pi(n - 5) = \pi((q^2 - q - 14)/3) = \pi(2(2^{m-1} - 1)),$$
$$\pi(q^2 - q - 14) \subseteq \pi(q(q^2 - 1)),\ \pi(q^2 - q - 14) \subseteq \{2, 3, 7\},\ \pi(2^{m-1} - 1) \subseteq \{3, 7\}.$$

Если $m = 3, 7$, то q не целое; противоречие. Если $m = 2$, то $q = 5$, $n = 7$. Если $m = 4$, то $q = 8$; противоречие. По лемме 5 при $5 \leq m \neq 7$ существует простой делитель s числа $2^{m-1} - 1$, взаимно простой с $2^2 - 1 = 3$, $2^3 - 1 = 7$, т. е. $s \neq 3, 7$; противоречие.

Пусть $n - 2 = (q^2 - q + 1)/(3, q + 1)$. Тогда $q = 5$, $n = 9$. Если $P \cong A_9$, то $9 \in \omega(G) = \omega(U_3(5))$; противоречие.

Пусть $n - 1 = (q^2 - q + 1)/(3, q + 1)$. Тогда $q = 5$, $n = 8$. Если $P \cong A_8$, то $15 \in \omega(G) = \omega(U_3(5))$; противоречие.

Пусть $n + 2 = (q^2 - q + 1)/(3, q + 1)$, $n > 6$. Тогда $q = 5$, $n = 5$, но $n > 6$; противоречие.

Лемма 16. *Группа P не изоморфна ни одной из следующих групп:* $^2A_3(2)$, $^2F_4(2)$, $^2A_5(2)$, $E_7(2)$, $E_7(3)$, $^2E_6(2)$.

Доказательство аналогично доказательству леммы 14.

Лемма 17. *Группа P не изоморфна ни одной из следующих групп:* $G_2(q')$, $q' \neq 2$; $^3D_4(q')$; $E_6(q')$; $F_4(q')$, q' *нечетно;* $^2E_6(q')$, $q' > 2$.

Доказательство. Пусть $P \cong E_6(q')$. Тогда по лемме 8

$$({q'}^6 + {q'}^3 + 1)/(3, q' - 1) = (q^2 - q + 1)/(3, q + 1).$$

Пусть $(3, q' - 1) = (3, q + 1)$. Тогда $q = {q'}^3 + 1$, следовательно, ${q'}^3 = 2^m$. Но $q = 2^m + 1$ — степень простого числа тогда и только тогда, когда $q = 2^{2^n} + 1$ — простое число Ферма или $q = 9$. Если $q = 9$, то $q' = 2$ и $\pi(2^5 - 1) = \{31\} \subseteq \pi(q(q^2-1)) = \{2, 3, 5\}$; противоречие. Таким образом, m делится на 3, 2^n делится на 3; противоречие.

Пусть $(3, q' - 1) = 1$, $(3, q + 1) = 3$. Тогда ${q'}^6 + {q'}^3 + 1 = (q^2 - q + 1)/3$. По лемме 6 ${q'}^3 = 2$ или ${q'}^3 = 9$, т. е. q' не целое; противоречие.

Пусть $(3, q' - 1) = 3$, $(3, q + 1) = 1$. Тогда $q^2 - q + 1 = ({q'}^6 + {q'}^3 + 1)/3$. По лемме 6 ${q'}^3 = 4$, q' не целое; противоречие.

Остальные случаи рассматриваются аналогично.

Лемма 18. *Группа P не изоморфна ни одной из следующих групп:* $C_n(q')$, $n = 2^m \geq 2$; $C_{p'}(q')$, $q' = 2, 3$; $B_{p'}(3)$; $B_n(q')$, $n = 2^m \geq 4$, q' *нечетно;* $D_{p'}(q')$, $p' \geq 5$, $q' = 2, 3, 5$; $D_{p'+1}(q')$, $q' = 2, 3$; $^2D_n(q')$, $n = 2^m \geq 4$; $^2D_n(2)$, $n = 2^m + 1$, $m \geq 2$; $^2D_{p'}(3)$, $5 \leq p' \neq 2^m + 1$; $^2D_n(3)$, $n = 2^m + 1 \neq p'$, $m \geq 2$; $^2D_{p'}(3)$, $p' = 2^m + 1$, $m \geq 1$; $F_4(q')$, $q' > 2$, q' *четно.*

Доказательство. Пусть $P \cong C_n(q')$, $n = 2^m \geq 2$. Тогда по лемме 8

$$(q^2 - q + 1)/(3, q + 1) = ({q'}^n + 1)/(2, q' - 1).$$

Пусть $(q^2 - q + 1)/(3, q + 1) = ({q'}^n + 1)/2$, q' нечетно. Если $(3, q + 1) = 1$, то

$$2q(q - 1) = {q'}^n - 1, \quad n = 2t, \quad 2q(q - 1) = ({q'}^t - 1)({q'}^t + 1).$$

Так как q — степень нечетного простого числа, то q делит ${q'}^t - 1$ или ${q'}^t + 1$.

Если q делит ${q'}^t - 1$, то $q = ({q'}^t - 1)/r$, $2(q - 1) = ({q'}^t + 1)r$, где r натуральное. Если $r = 1$, то $q = {q'}^t - 1$, т. е. q четно; противоречие. Если $r \geq 2$, то

$$q = \frac{{q'}^t - 1}{r} \leq \frac{1}{2}({q'}^t - 1), \quad 2(q - 1) = ({q'}^t + 1)r \geq 2({q'}^t + 1),$$
$${q'}^t + 2 \leq q \leq \frac{1}{2}{q'}^t - \frac{1}{2}, \quad {q'}^t \leq -5;$$

противоречие.

Если q делит ${q'}^t + 1$, то $q = ({q'}^t + 1)/r$, $2(q - 1) = ({q'}^t - 1)r$, где r натуральное. Если $r = 1$, то $q = {q'}^t + 1$, т. е. q четно; противоречие. Если $r \geq 2$, то

$$q = \frac{{q'}^t + 1}{r} \leq \frac{1}{2}({q'}^t + 1), \quad 2(q - 1) = ({q'}^t - 1)r \geq 2({q'}^t - 1).$$

Отсюда ${q'}^t \leq q \leq \frac{1}{2}{q'}^t + \frac{1}{2}$, ${q'}^t \leq 2$, но $q' \geq 3$, $t \geq 1$, т. е. ${q'}^t \geq 3$; противоречие.

Если $(3, q + 1) = 3$, то $(q^2 - q + 1)/3 = ({q'}^n + 1)/2$. Множество простых делителей чисел q', ${q'}^{2i} - 1$, $1 \leq i \leq n - 1$, содержится в $\pi(q(q^2 - 1))$. Поэтому

$\pi({q'}^n-1)\subseteq\pi(q(q^2-1))$, $\pi(({q'}^n-1)/2)=\pi((q^2-q-2)/3)\subseteq\pi(q(q^2-1))$, $\pi(q-2)\subseteq\pi(q+1)$, т. е. $q=2+3^m$. Таким образом, $2\cdot3^m(3^{m-1}+1)=({q'}^t-1)({q'}^t+1)$. Так как $({q'}^t-1,{q'}^t+1)=2$, то 3^m делит ${q'}^t-1$ или ${q'}^t+1$.

Если 3^m делит ${q'}^t-1$, то $3^m=({q'}^t-1)/r$, $2(3^{m-1}+1)=({q'}^t+1)r$. Если $r=1$, то $3^m={q'}^t-1$, т. е. 3^m четное; противоречие. Если $r\geq2$, то

$$3^m=\frac{{q'}^t-1}{r}\leq\frac{1}{2}({q'}^t-1),\quad 2(3^{m-1}+1)=({q'}^t+1)r\geq2({q'}^t+1),$$
$$3{q'}^t\leq3^m\leq\frac{1}{2}({q'}^t-1),\quad {q'}^t\leq-\frac{1}{5};$$

противоречие.

Если 3^m делит ${q'}^t+1$, то $3^m=({q'}^t+1)/r$, $2(3^{m-1}+1)=({q'}^t-1)r$. Если $r=1$, то $3^m={q'}^t-1$, т. е. 3^m четное; противоречие. Если $r\geq2$, то

$$3^m=\frac{{q'}^t+1}{r}\leq\frac{1}{2}({q'}^t+1),\quad 2(3^{m-1}+1)=({q'}^t-1)r\geq2({q'}^t-1),$$
$$3({q'}^t-2)\leq3^m\leq\frac{1}{2}({q'}^t+1),\quad {q'}^t\leq\frac{13}{5},\quad q'=2,$$

но q' нечетное; противоречие.

Пусть $(q^2-q+1)/(3,q+1)={q'}^n+1$, q' — степень 2. Если $(3,q+1)=1$, то ${q'}^n=q(q-1)$. При $q\geq3$ число $q(q-1)$ имеет по меньшей мере 2 простых делителя, но ${q'}^n$ имеет только один простой делитель; противоречие. Если $(3,q+1)=3$, то ${q'}^n=(q+1)(q-2)/3$. Левая часть не делится на 3, правая часть делится на 3 при $q\geq5$; противоречие.

Остальные случаи рассматриваются аналогично. В результате получим только следующие две возможности: $q=5$, $p=3$, $P\cong C_3(2),D_4(2)$, откуда ввиду [6] $\mu(P)=\{15,12,10,9,8,7\}$, но $15\notin\omega(G)$; противоречие.

Лемма 19. *Группа P не изоморфна ни одной из следующих групп: ${}^2G_2(q')$, $q'=3^{2m+1}>3$; ${}^2F_4(q')$, $q'=2^{2m+1}>2$; ${}^2B_2(q')$, $q'=2^{2m+1}>2$.*

Доказательство. Пусть $P\cong{}^2B_2(q')$, $q'=2^{2m+1}>2$. Тогда по лемме 8

$$\frac{q^2-q+1}{(3,q+1)}\in\{q'-1,q'-\sqrt{2q'}+1,q'+\sqrt{2q'}+1\}.$$

Пусть $q'-1=(q^2-q+1)/(3,q+1)$. Если $(3,q+1)=1$, то $q'=q^2-q+2$, $q(q-1)=2(2^{2m}-1)=2(2^m-1)(2^m+1)$.

Если q делит 2^m-1, то $q=(2^m-1)/r$, $q-1=2(2^m+1)r$, где r натуральное. Тогда

$$q=\frac{2^m-1}{r}\leq2^m-1,\quad q-1=2(2^m+1)r\geq2(2^m+1).$$

Значит, $2\cdot2^m+3\leq q\leq2^m-1$, $2^m\leq-4$; противоречие.

Если q делит 2^m+1, то $q=(2^m+1)/r$, $q-1=2(2^m-1)r$, где r натуральное. Если $r=1$, то $q=2^m+1$, $q-1=2\cdot2^m-2$, $m=1$, $q=3$, $q'=8$. Так как 2 не делит 2^m+1, то r нечетное. Если $r\geq3$, то

$$q=\frac{2^m+1}{r}\leq\frac{1}{3}(2^m+1),\quad q-1=2(2^m-1)r\geq6(2^m-1),$$
$$6\cdot2^m-5\leq q\leq\frac{1}{3}2^m+\frac{1}{3},\quad 2^m<1;$$

противоречие.

Пусть $(3,q+1)=3$. Тогда $q'=(q^2-q+4)/3$,

$$\pi((q'-\sqrt{2q'}+1)(q'+\sqrt{2q'}+1))=\pi((q'+1)^2-2q')=\pi({q'}^2+1).$$

Так как $q'=(q^2-q+4)/3$, то $\pi(((q^2-q+4)^2+9)/9)\subseteq\pi(q(q^2-1))$. Отсюда

$$\pi((q^2-q+4)^2+9)\subseteq\pi(q(q^2-1)),\quad ((q^2-q+4)^2+9),q(q^2-1))\text{ делит }225,$$
$$\pi((q^2-q+4)^2+9)\subseteq\{3,5\},\quad \pi(9{q'}^2+9)\subseteq\{3,5\},\quad \pi(2^{4m+2}+1)\subseteq\{3,5\}.$$

По лемме 5 при $m\geq 1$ существует простой делитель s числа $2^{2(4m+2)}-1$, взаимно простой с $2^{4m+2}-1$, $2^4-1=15$, т. е. $s\,|\,(2^{4m+2}+1)$ и $s\neq 3,5$; противоречие.

Пусть ${q'}^2-\sqrt{2q'}+1=(q^2-q+1)/(3,q+1)$. Если $(3,q+1)=1$, то $2^{4m+2}-2^{m+1}=q^2-q$. Положим $q=2^{2m+1}+b$, где b целое. При $b=1$ получим $2\cdot 2^{2m}+2\cdot 2^m=0$. Значит, $b\neq 1$. Имеем

$$q(q-1)=2^{m+1}(2^{3m+1}-1)>2^{2m+1}(2^{2m+1}-1)=(q-b)(q-b-1).$$

Так как $(q-b)(q-b-1)=q(q-1)+b(b-2q+1)$, то $b(b-2q+1)<0$ и $b>0$. Поскольку $b\neq 1$, то $b\geq 2$. Далее,

$$q^2-q=2^{4m+2}+4b\cdot 2^{2m}+b^2-2\cdot 2^{2m}-b,$$
$$(4b-2)2^{2m}+2\cdot 2^m+b^2-b=0,\quad D=-4[4b^3-6b^2+2b-1]\geq 0.$$

Положим $f(b)=4b^3-6b^2+2b-1$. Тогда $f(b)\leq 0$ при $b\geq 2$. Но при $b\geq 2$ будет $2b^2-3b+1=b(2b-3)+1\geq 3$, поэтому

$$f(b)=2b(2b^2-3b+1)-1\geq 11>0\quad\text{при } b\geq 2;$$

противоречие.

Если $(3,q+1)=3$, то $3\cdot 2^{m+1}(2^{3m+1}-1)=(q-2)(q+1)$. Имеем $q+1=3\cdot 2^n\cdot r$, где $(r,2)=1$. Тогда $3\cdot 2^{m+1}(2^{3m+1}-1)=3\cdot 2^n r\cdot 3(2^n r-1)$, $n=m+1$, $2^{m+1}(3r^2-2^{2m})=3r-1$, $3r=1+2^{m+1}t$, где $(2,t)=1$, $t\geq 1$. Отсюда

$$2^{2m+2}t^2+(2\cdot 2^{m+1}-3)t+(1-3\cdot 2^{2m})=0,$$
$$t=\frac{-(4\cdot 2^m-3)+\sqrt{48\cdot 2^{4m}-24\cdot 2^m+9}}{8\cdot 2^{2m}}.$$

Так как $m>0$, то $t<1$; противоречие.

Остальные случаи разбираются аналогично.

Лемма 20. *Если P изоморфна $A_1(q')$, где $q'\geq 2$, то $q'=7$ и $q=3,5$.*

Доказательство. Пусть $P\cong A_1(q')$, $q'=s^t$. Тогда по лемме 8

$$\frac{q^2-q+1}{(3,q+1)}\in\{q'-1,q'+1,(q'-1)/2,(q'+1)/2,s\}.$$

Пусть $q'-1=(q^2-q+1)/(3,q+1)$ нечетно, $q'=2^t$.

Пусть $(3,q+1)=1$. Тогда $q'=q^2-q+2$. Если $q^2-q+2=2^{2m}$, то $(2q-1)^2+7=2^{2(m+1)}$. Отсюда $2^{m+1}=4$, $2q-1=3$, $q=2$; противоречие. Если $q^2-q+2=2^{2m+1}$, то $q(q-1)=2(2^m-1)(2^m+1)$. Если q делит 2^m-1, то

$$q=\frac{2^m-1}{r}\leq 2^m-1,\quad q-1=2(2^m+1)r\geq 2(2^m+1),$$
$$2\cdot 2^m+3\leq q\leq 2^m-1,\quad 2^m\leq -4;$$

противоречие. Если q делит 2^m+1, то

$$q=\frac{2^m+1}{r}\le 2^m+1,\quad q-1=2(2^m-1)r\ge 2(2^m-1),$$
$$2\cdot 2^m-1\le q\le 2^m+1,\quad 2^m\le 2,\ m=0,1,\ q'=2,8.$$

Получили $q=3$, $q'=8$, $\mu(P)=\{9,7,2\}$, $9\in\omega(G)$; противоречие.

Пусть $(3,q+1)=3$. Тогда $q'-1=(q^2-q+1)/3$, $\pi(q'+1)=\pi((q^2-q+7)/3)\subseteq\pi(q(q^2-1))$, $\pi(q^2-q+7)\subseteq\{3,7\}$, $\pi(2^t+1)\subseteq\{3,7\}$. При $t=1$ будет $q'=2$, но $q'>2$. Если $t=2$, то $q'=4$, $\pi(2^t+1)=5\subseteq\{3,7\}$; противоречие. При $t=3$ имеем $q'=8$, $q=5$, $P\cong L_2(8)$, $9\in\omega(G)$; противоречие. По лемме 5 при $t\ge 4$ существует простой делитель r числа $2^{2t}-1$, взаимно простой с 2^t-1, $2^2-1=3$, $2^3-1=7$, т. е. $r\,|\,(2^t+1)$, $r\ne 3,7$, что противоречит включению $\pi(2^t+1)\subseteq\{3,7\}$.

Пусть $q'+1=(q^2-q+1)/(3,q+1)$. Допустим сначала, что $(3,q+1)=1$. Тогда $q'=q(q-1)$. При $q\ge 3$ число $q(q-1)$ имеет по меньшей мере два простых делителя, но q' — только один простой делитель; противоречие. Если $(3,q+1)=3$, то $q'=(q+1)(q-2)/3$. При $q\ge 5$ левая часть не делится на 3, правая часть делится на 3; противоречие.

Пусть $s=(q^2-q+1)/(3,q+1)$. Если $(3,q+1)=1$, то $s=q^2-q+1$. Имеем

$$\pi({q'}^2-1)=\pi(s^{2t}-1)\subseteq\pi(q(q^2-1)),\quad \pi(s+1)\subseteq\pi(q(q^2-1)),$$
$$\pi(q^2-q+2)\subseteq\pi(q(q^2-1)).$$

Отсюда (q^2-q+2) — степень 2. Тогда $q=3$, $q'=7$, $P\cong L_2(7)$. Если $(3,q+1)=3$, то $s=(q^2-q+1)/3$, откуда $\pi(s-1)=\pi((q+1)(q-2)/3)\subseteq\pi(q(q^2-1))$, т. е. $q=2+3^m$. Следовательно,

$$\pi(s+1)=\pi(3^{2m-1}+3^m+2)\subseteq\pi(3(2+3^m)(1+3^m)(1+3^{m-1})),$$

$(3^{2m-1}+3^m+2)$ — степень 2. Положим $d=3^{m-1}$. Тогда $3d(d+1)=2^k-2$. Так как 2^k-2 делится на 3, то $k=2l+1$. Имеем $3d(d+1)=2(2^l-1)(2^l+1)$. Поскольку d — степень 3, то d делит 2^l-1 или d делит 2^l+1.

Если d делит 2^l-1, то $d=(2^l-1)/r$, $3(d+1)=2(2^l+1)r$. Если $r=1$, то $d=2^l-1$, $3(d+1)=2(2^l+1)$. Отсюда $l=1$, $k=3$, $d=1$, $m=1$, $q=5$. Если $r\ge 3$, то

$$d=\frac{2^l-1}{r}\le\frac{1}{3}(2^l-1),\quad 3(d+1)=2(2^l+1)r\ge 6(2^l+1),$$

откуда $2\cdot 2^l+1\le d\le\frac{1}{3}\cdot 2^l-\frac{1}{3}$, $2^l\le-\frac{4}{5}$; противоречие.

Если d делит 2^l+1, то $d=(2^l+1)/r$, $3(d+1)=2(2^l-1)r$. Если $r=1$, то $d=2^l+1$, $2^l=-8$; противоречие. Если $r\ge 3$, то

$$d=\frac{2^l+1}{r}\le\frac{1}{3}(2^l+1),\quad 3(d+1)=2(2^l-1)r\ge 6(2^l-1).$$

Отсюда

$$2\cdot 2^l-3\le d\le\frac{1}{3}\cdot 2^l+\frac{1}{3},\quad 2^l\le 2,\quad l=1,\quad q=5.$$

Следовательно, $q=5$, $s=7$. Пусть $t\ge 2$. Тогда $\frac{1}{2}(q-1)=\frac{1}{2}(7^t-1)\in\omega(P)$, но $\frac{1}{2}(7^t-1)\ge 24>10$. Так как $\mu(G)=\mu(U_3(5))=\{10,8,7,6\}$, то $t=1$ и $q'=7$.

Если $(q'+1)/2=(q^2-q+1)/(3,q+1)$ или $(q'-1)/2=(q^2-q+1)/(3,q+1)$, то приходим к противоречию, рассуждая, как в предыдущих абзацах.

Лемма 21. *Группа P не изоморфна ни одной из следующих групп:* $A_{p'}(r)$, $(r-1)\,|\,(p'+1)$; ${}^2A_{p'}(r)$, $(r+1)\,|\,(p'+1)$, $(p',r)\neq(3,3),(5,2)$.

Доказательство. Пусть $P\cong {}^2A_{p'}(r)$, где $(r+1)\,|\,(p'+1)$. Тогда по лемме 8 $(q^2-q+1)/(3,q+1)=(r^{p'}+1)/(r+1)$. Обозначим $p'=2t+1$.

Пусть $(3,q+1)=1$. В таком случае

$$q(q-1)=\frac{r^{p'}-r}{r+1}=r\frac{r^{p'-1}-1}{r+1}.$$

Если $p'\equiv 3\pmod 4$, то t нечетно. Теперь $r+1$ делит r^t+1. Имеем

$$q(q-1)=r(r^t-1)\frac{r^t+1}{r+1}.$$

Если $t=1$, то $q=r$. Так как $r+1\,|\,p'+1=4$, то $r=3$, $P\cong U_4(3)$, т. е. $9\in\omega(G)=\omega(U_3(3))$; противоречие. Значит, $t\geq 3$, и либо $q\,|\,r$, либо $q\,|\,(r^t-1)/(r+1)$, либо $q\,|\,(r^t+1)$. Если q делит r, то $q=s^k$, $r=s^f$, $k\leq f$. Получим

$$s^k-1=s^{f-k}(s^{ft}-1)\frac{s^{ft}+1}{s^f+1}.$$

Если $f>k$, то правая часть делится на s, а левая нет. Поэтому $f=k$. Отсюда

$$(s^f-1)(s^f+1)=(s^{ft}-1)(s^{ft}+1),\quad s^{2f}=s^{2ft},\quad t=1,$$

но $t\geq 3$; противоречие. Если q делит r^t-1, то

$$q=\frac{r^t-1}{s},\quad q-1=r\frac{r^t+1}{r+1}s,$$

где s натуральное. Если $s=1$, то

$$q=r^t-1,\quad q-1=r\frac{r^t+1}{r+1},\quad r^t-3r-2=0.$$

Если $t=3$, то $r=2$, но $r+1\,|\,p'+1=4$; противоречие. Если $(t,r)\neq(3,2)$, то $r^{t-1}\geq 8$ и $r^t-3r-2=r(r^{t-1}-3)-2\leq 8$. Значит, $s\geq 2$. Имеем

$$q=\frac{r^t-1}{s}\leq\frac{1}{2}(r^t-1),\quad q-1=r\frac{r^t+1}{r+1}s\geq 2r\frac{r^t+1}{r+1},$$

$$2r\frac{r^t+1}{r+1}+1\leq q\leq\frac{1}{2}(r^t-1),\quad 3r^{t+1}-r^t+7r+3\leq 0,$$

но $r^t(3r-1)+7r+3>0$; противоречие.

Случай, когда q делит $(r^t+1)/(r+1)$, рассматривается аналогично случаю, когда q делит r^t-1. Получаем противоречие.

Если $p'\equiv 1\pmod 4$, то t четно. Отсюда $r+1$ делит r^t-1. Имеем

$$q(q-1)=r(r^t+1)\frac{r^t-1}{r+1},$$

и либо $q\,|\,r$, либо $q\,|\,(r^t-1)/(r+1)$, либо $q\,|\,(r^t+1)$. Дальше рассуждаем, как в случае нечетного t.

Пусть $(3,q+1)=3$. Тогда $(q^2-q+1)/3=(r^{p'}+1)/(r+1)$. Имеем

$$\pi((q^2-q-2)/3)=\pi(r(r^{p'-1}-1)/(r+1))\subseteq\pi(q(q^2-1)).$$

Следовательно, $q=2+3^m$ и

$$3^m(3^{m-1}+1)=r\frac{r^{p'-1}-1}{r+1}=r\frac{r^{2t}-1}{r+1}.$$

Дальше рассуждаем, как в случае $(3,q+1)=1$.

Случай $P\cong A_{p'}(r)$ разбирается аналогично.

Лемма 22. *Группа P не изоморфна $E_8(r)$; $A_{p'-1}(r), (p',r) \neq (3,2), (3,4)$.*

Доказательство. Пусть $P \cong A_{p'-1}(r)$. По лемме 11 в P есть элементы порядков $(r^{p'}-1)/(r-1)d$ и $(r^{p'-1}-1)/d$, где $d=(p',r-1)$. По леммам 8, 10 имеем $(q^2-q+1)/(3,q+1)=(r^{p'}-1)/(r-1)d$.

Пусть $p(q+1)/(3,q+1)=(r^{p'-1}-1)t/d$, t натуральное. Проверим, что

$$1 < \frac{r^{p'}-1}{(r^{p'-1}-1)(r-1)} < \frac{3}{2} \quad \text{при} \quad r \geq 4. \tag{$*$}$$

Действительно, так как $r(r^{p'-2}+1)-2>0$, то

$$\frac{r^{p'}-1}{(r^{p'-1}-1)(r-1)} > 1.$$

Поскольку $r[r^{p'-2}(r-3)-3]+5>0$ при $r \geq 4$, то

$$\frac{r^{p'}-1}{(r^{p'-1}-1)(r-1)} < \frac{3}{2} \quad \text{при} \quad r \geq 4.$$

Итак, $(*)$ выполняется.

Предположим, что $p<q$. Так как $p(p^{f-1}[p(p^{f-1}-1)-1]-1)+1>0$ при $f>1$, то $p^{2f}-p^{f+1}-p^f-p+1>0$ при $f>1$. Следовательно,

$$\frac{q^2-q+1}{q+1} = \frac{p^{2f}-p^f+1}{p^f+1} > p \quad \text{при } f>1.$$

Отсюда $p(q+1) < q^2-q+1 < q^2-1$. Если $(3,q+1)=3$, то $p \geq 5$. Значит, $q+1 < p(q+1)/3 < (q^2-q+1)/3 < (q^2-1)/3$. Имеем

$$\frac{(r^{p'-1}-1)t}{d} = \frac{p(q+1)}{(3,q+1)} < \frac{q^2-q+1}{(3,q+1)} = \frac{r^{p'}-1}{(r-1)d}.$$

Отсюда

$$t < \frac{r^{p'}-1}{(r^{p'-1}-1)(r-1)} < \frac{3}{2}, \quad \text{т. е. } t=1.$$

Поэтому

$$\frac{q^2-q+1}{p(q+1)} = \frac{r^{p'}-1}{(r-1)(r^{p'-1}-1)} < \frac{3}{2},$$

т. е. $2(p^{2f}-p^f+1) < 3(p^{f+1}+p)$. Но $p(p^{f-1}[p(2p^{f-1}-3)-2]-3)+2>0$; противоречие.

Предположим, что $p=q$. Тогда $q+1 < (q^2-q+1)/3 < (q^2-1)/3 < p(q+1)/3$. Имеем

$$\frac{r^{p'}-1}{(r-1)d} = \frac{q^2-q+1}{(3,q+1)} < \frac{p(q+1)}{(3,q+1)} = \frac{(r^{p'-1}-1)t}{d},$$

$$t > \frac{r^{p'}-1}{(r-1)(r^{p'-1}-1)} > 1, \quad \text{т. е.} \quad t \geq 2.$$

Следовательно,

$$\frac{q^2-q+1}{q(q+1)} = \frac{r^{p'}-1}{(r-1)(r^{p'-1}-1)t} \leq \frac{r^{p'}-1}{2(r-1)(r^{p'-1}-1)} < \frac{3}{4}.$$

Отсюда $q^2-7q+4<0$. Но $q^2-7q+4>0$ при $q\geq 7$. Значит, $q=3,5$, $(q^2-q+1)/(3,q+1)=7$ и $(r^{p'}-1)/(r-1)d=7$. Так как $1\leq d=(p',r-1)\leq r-1$, то

$$\frac{r^{p'}-1}{(r-1)^2}\leq\frac{r^{p'}-1}{(r-1)d}=7,\quad r[r(r^{p'-2}-7)+14]-8\leq 0.$$

Но $r[r(r^{p'-2}-7)+14]-8>0$ при $r\geq 4$ и $(p',r)\neq(3,4)$. Значит, $r\leq 3$.

Пусть $r=2$. Тогда $d=1$ и $(q^2-q+1)/(3,q+1)=2^{p'}-1$. Если $(3,q+1)=1$, то

$$q(q-1)=2(2^{p'-1}-1)=2(2^{(p'-1)/2}-1)(2^{(p'-1)/2}+1).$$

Дальше рассуждаем, как в лемме 20. Получим противоречие. Если $(3,q+1)=3$, то $(q^2-q-2)/3=2^{p'}-2=2(2^{p'-1}-1)$, $\pi((q^2-q-2)/3)=\pi(2(2^{p'-1}-1))\subseteq\pi(q(q^2-1))$. Отсюда $\pi(q-2)\subseteq\pi(q+1)$, т. е. $q=2+3^n$. Следовательно, $3^n(3^{n-1}+1)=2(2^{(p'-1)/2}-1)(2^{(p'-1)/2}+1)$. Дальше рассуждаем, как в лемме 20. Получим противоречие. Аналогично разбирается случай $r=3$.

Случаи $(q^2-1)/(3,q+1)=(r^{p'-1}-1)t/d$ и $q+1=(r^{p'-1}-1)t/d$, где t натуральное, рассматриваются аналогично.

Пусть $P\cong E_8(q')$. По лемме 8

$$\frac{q^2-q+1}{(3,q+1)}\in\left\{\frac{r^{10}-r^5+1}{r^2-r+1},\frac{r^{10}+r^5+1}{r^2+r+1},r^8-r^4+1,\frac{r^{10}+1}{r^2+1}\right\}.$$

Если $(q^2-q+1)/(3,q+1)=(r^{10}-r^5+1)/(r^2-r+1)$ или $(q^2-q+1)/(3,q+1)=(r^{10}+r^5+1)/(r^2+r+1)$, то рассуждаем, как для группы $A_{p'-1}(r)$.

Если $(q^2-q+1)/(3,q+1)=r^8-r^4+1$, то, используя лемму 6, получаем противоречие.

Уравнение $(q^2-q+1)/(3,q+1)=(r^{10}+1)/(r^2+1)$ не имеет решений при заданных условиях на q и r по лемме 21.

Лемма 23. *Группа P не изоморфна ${}^2A_{p'-1}(r)$ при $(p',r)\neq(3,q)$.*

Доказательство. Пусть $P\cong{}^2A_{p'-1}(r)$. Предположим сначала, что $p'\geq 5$. Рассмотрим в $SU_n(r)$ подгруппу, состоящую из всех матриц вида

$$\left(\begin{array}{c|cc} & 0 & 0\\ M & \vdots & \vdots\\ & 0 & 0\\ \hline 0\dots 0 & s^{-1} & 0\\ 0\dots 0 & 0 & 1\end{array}\right),$$

где $M\in GU(n-2,r)$, $s=\det M$. Эта группа изоморфна $GU(n-2,r)$, поэтому группа $GU(n-2,r)$ изоморфно вкладывается в $U_n(r)$. В $GU(n,r)$ при n нечетном есть элемент порядка r^n+1. Так как группа $GU(p'-2,r)$ изоморфно вкладывается в $U_{p'}(r)$, то в $U_{p'}(r)$ есть элемент порядка $r^{p'-2}+1$. Поскольку $GU(p'-4,r)$ изоморфно вкладывается в $U_{p'}(r)$, то в $U_{p'}(r)$ есть элемент порядка $r^{p'-4}+1$.

Так как $r^{p'-2}+1=r^2(r^{p'-4}+1)-(r^2-1)$ и $r^{p'-4}+1=(r^{p'-6}+r^{p'-8}+\dots+r)(r^2-1)+r+1$, то $(r^{p'-2}+1,r^{p'-4}+1)=r+1$.

По лемме 7(a) число $(r^{p'-2}+1)(r^{p'-4}+1)/(r+1)$ делит $q(q^2-1)$. Имеем $(r^{p'-2}+1)(r^{p'-4}+1)/(r+1)>r^{2p'-6}/r^2=r^{2p'-8}$, $r^{(2p'-8)/3}<q$. При $r\geq 3$ получаем $q^2/4<(q^2-q+1)/(3,q+1)=(r^{p'}+1)/(r+1)(p',r+1)\leq(r^{p'}+1)/4$. Следовательно, $r^{(4p'-16)/3}/4<q^2/4<(r^{p'}+1)/4$, $r^{(p'-16)/3}\leq 1$, $p'\leq 13$.

Если $r=2$, то $(p',r+1)=1$ и $(q^2-q+1)/(3,q+1)=(r^{p'}+1)/(r+1)$. Получили уравнение из леммы 21. Оно не имеет решений при заданных условиях на q, r, p'. Значит, $r\geq 3$ и $5\leq p'\leq 13$.

Пусть $p'=5$. Если $(p',r+1)=1$, то получим уравнение из леммы 21. Если $(p',r+1)=5$, то $(r^5+1)/5(r+1)=(q^2-q+1)/(3,q+1)$. Если $(3,q+1)=1$, то $(r^5+1)/(r+1)=5(q^2-q+1)$. Так как $(r-1)\in\omega(U_3(r))$, по лемме 7(а) $(r^3+1)(r-1)$ делит $2q(q^2-1)$, $(r-1)$ делит $2q(q^2-1)$. Так как $r(r-1)(r^2+1)=5q^2-5q+4$, то $r-1$ делит $5q^2-5q+4$. Таким образом, $(r-1)\,|\,(5q^2-5q+4,\,2q(q^2-1))\,|\,112$, $(r-1)\,|\,112$. Поскольку $(5,r+1)=5$, то $r=9$ или 29 и q не целое; противоречие.

Если $(3,q+1)=3$, то $(r^5+1)/(r+1)=5(q^2-q+1)/3$. Отсюда $3(r-1)\,|\,5q^2-5q+2$, $r-1\,|\,2q(q^2-1)$, $r-1\,|\,48$. Так как $(r+1,5)=5$, то $r=4,9,29$ или 49. В каждом из последних случаев q не целое; противоречие.

Пусть $p'=7$. Тогда $(r^7+1)/7(r+1)=(q^2-q+1)/(3,q+1)$. Если $(3,q+1)=1$, то

$$r(r^3-1)\frac{r^3+1}{r+1}=7q^2-7q+6.$$

Отсюда $(r^3+1)/(r+1)$ делит $(7q^2-7q+6)$. По лемме 7(а) $(r^5+1)(r^3+1)/(r+1)$ делит $q(q^2-1)$. Так как $(r^3+1)/(r+1)$ делит $q(q^2-1)$, то

$$\frac{r^3+1}{r+1}\,|\,(7q^2-7q+6,q(q^2-1))\,|\,120,\quad (r^2-r+1)\,|\,120.$$

Отсюда $r=2$, но $(7,r+1)=7$; противоречие. Если $(3,q+1)=3$, то $(r^3+1)/(r+1)$ делит 72, $r=2$, $(r+1,7)=1$; противоречие.

Пусть $p'=11$. В $U_{11}(r)$ есть элементы порядков r^9+1, r^7+1, r^5+1. Так как $r^9+1=r^4(r^5+1)-(r^4-1)$, $r^5+1=r(r^4-1)+(r+1)$, то $(r^5+1,r^9+1)=r+1$, $(r^5+1,r^7+1)=r+1$. Таким образом, по лемме 7(б) число $z=(r^9+1)(r^7+1)(r^5+1)/(r+1)^2$ делит $q(q^2-1)$. Имеем

$$\frac{(r^9+1)(r^7+1)(r^5+1)}{(r+1)^2}>\frac{4r^{19}}{9},\quad \frac{4r^{19}}{9}<z<q^3,\quad \sqrt[3]{\frac{4}{9}}r^{19/3}<q.$$

Положим $m=(q^2-q+1)/(3,q+1)$. Тогда

$$m>\frac{1}{4}q^2>\frac{1}{4}\sqrt[3]{\frac{16}{81}}r^{38/3}.$$

С другой стороны, $m=(r^{11}+1)/(11(r+1))<2r^{11}/33$. Отсюда

$$\frac{1}{4}\sqrt[3]{\frac{16}{81}}r^{38/3}<\frac{2r^{11}}{33},\quad r^{5/3}<\frac{8}{33}\sqrt[3]{\frac{81}{16}}<\frac{16}{33}<1;$$

противоречие.

Подслучай $p'=13$ рассматривается аналогично подслучаю $p'=11$.

Пусть $p'=3$. Тогда $(q^2-q+1)/(3,q+1)=(r^2-r+1)/(3,r+1)$ Если $(3,q+1)=(3,r+1)$, то $q=r$ и $P\cong U_3(q)$. Если $(3,q+1)=1$ и $(3,r+1)=3$, то $q^2-q+1=(r^2-r+1)/3$. По лемме 6 $q=3$, $r=5$. Если $P\cong U_3(5)$, то $5\in\omega(G)=\omega(U_3(3))$; противоречие. Если $(3,q+1)=3$ и $(3,r+1)=1$, $r^2-r+1=(q^2-q+1)/3$. По лемме 6 имеем $r=3$, $q=5$. Если $P\cong U_3(3)$, то $12\in\omega(G)=\omega(U_3(5))$; противоречие.

Из лемм 14–23 следует утверждение 2 теоремы 1.

Лемма 24. *Пусть r — простое число и $E \cong Z_r \times U_3(q)$. Тогда $\omega(E) \not\subseteq \omega(U_3(q))$.*

Доказательство. Допустим противное. Если $r \in \pi_2(G)$, то $pr \in \omega(G)$, что противоречит лемме 10. Если $r \in \pi_1(G)$, то $r \cdot (q^2 - q + 1)/(3, q+1) \in \omega(G)$, что также противоречит лемме 10.

Лемма 25. *Утверждение* 3 *теоремы* 1 *справедливо.*

Доказательство. Предположим противное. Пусть сначала $q \geq 7$. Пусть $r \in \pi(N)$, $r \neq 2$, $r \mid (q-1)$. В $U_3(q)$ существует подгруппа Фробениуса с ядром порядка q и циклическим дополнением порядка $(q-1)/2$. По лемме 4 $r(q-1)/2 \in \omega(G)$. По лемме 10 $r(q-1)/2 \notin \omega(G)$ при $r \neq 2$; противоречие.

Пусть $p \in \pi(N)$, и пусть $(3, q+1) = 3$. Ввиду [17] $L_2(q) \leq U_3(q)$. Так как группа $L_2(q)$ по лемме 12 распознаваема (с точностью до изоморфизма) по множеству порядков элементов, то в G есть элемент одного из следующих порядков: $p(q-1)/2$, $p(q+1)/2$, p^2, что противоречит лемме 10. Если $(3, q+1) = 1$, то в $U_3(q)$ есть подгруппа, изоморфная группе Фробениуса $Z_{q^2-q+1}.3$. По лемме 3 имеем $3p \in \omega(G)$, по лемме 10 — $3p \mid p(q+1)$, откуда $(3, q+1) = 3$; противоречие.

Пусть $q = 3$ и $3 \in \pi(N)$. В $U_3(3)$ существует подгруппа Фробениуса порядка $7 \cdot 3$. По лемме 3 будет $3 \cdot 3 = 9 \in \omega(G) = \omega(U_3(3))$, но $\mu(U_3(3)) = \{12, 8, 7\}$; противоречие.

Пусть $q = 5$ и $5 \in \pi(N)$. В $U_3(5)$ существует подгруппа Фробениуса порядка $7 \cdot 3$. По лемме 3 имеем $5 \cdot 3 = 15 \in \omega(G) = \omega(U_3(5))$, но $\mu(U_3(5)) = \{10, 8, 7, 6\}$; противоречие.

Лемма 26. *Если $q > 7$ и выполняется условие утверждения* 4 *теоремы* 1*, то $q = p$, $q + 1 = 3 \cdot 2^m$, $q - 1 = 2r$, r — нечетное простое число.*

Доказательство. Предположим, что $(3, q+1) = 1$. Тогда по лемме 10 $\mu(G) = \{p(q+1), q^2-1, q^2-q+1\}$. Если $q + 1 \neq 2^m$, то существует нечетное простое число s такое, что $s \mid (q+1)$ и $ps \in \omega(U_3(q))$ в противоречии с условием. Значит, $q + 1 = 2^m$ для $m \geq 3$. Следовательно, $q = p$, m — простое число. Так как $q > 7$, то $q = p \not\equiv 0 \pmod 3$, $q + 1 \not\equiv 0 \pmod 3$ и $q - 1 \equiv 0 \pmod 3$, $q - 1 = 2^t \cdot 3^l \cdot r$. По условию $r = 1$. Имеем $q + 1 \equiv 0 \pmod 4$, поэтому $q - 1 \not\equiv 0 \pmod 4$. Тем самым $t = 1$ и $q - 1 = 2 \cdot 3^l$. Имеем $q + 1 = 2^m$, $q - 1 = 2 \cdot 3^l$. Отсюда $3^l + 1 = 2^{m-1}$, поэтому либо $(l, m) = (1, 3)$ и $q = 7$, либо $(l, m) = (0, 2)$ и $q = 3$, что противоречит условию.

Итак, $(3, q+1) = 3$. Отсюда $\mu(G) = \{p(q+1)/3, (q^2-1)/3, q+1, (q^2-q+1)/3\}$. По условию $q + 1 = 3 \cdot 2^m$, $m > 3$, $q + 1 \equiv 0 \pmod 4$. Если $q - 1 \equiv 0 \pmod 4$, то $2 \equiv 0 \pmod 4$, поэтому $q - 1 = 2t$, t нечетно. По условию $t = r^n$. Таким образом, $q + 1 = 3 \cdot 2^m$, $q - 1 = 2 \cdot r^n$, $q + 1 = 2(r^n + 1) = 3 \cdot 2^m$, $r^n + 1 = 3 \cdot 2^{m-1}$, $m - 1 \geq 2$. Пусть $n > 1$. По лемме 5 существует простой делитель s_1 числа $r^{2n} - 1$, взаимно простой с $r^n - 1$, $r^2 - 1$, т. е. $s_1 \mid (r^n + 1)$ и $s_1 \neq 2, 3$. Тогда $n = 1$ и $q - 1 = 2r$. Так как $q = p^f$, то $q^2 - 1 = p^{2f} - 1 = 3 \cdot 2^{m+1} r$. Пусть $f > 1$. По лемме 5 существует простой делитель s_2 числа $q^2 - 1 = p^{2f} - 1$, взаимно простой с $p^f - 1 = q - 1 = 2r$, $p^2 - 1$, т. е. с $2 \cdot 3r$; противоречие. Значит, $f = 1$.

Лемма 27. *Утверждение* 4 *теоремы* 1 *выполняется.*

Доказательство. Ввиду лемм 25 и 26 группа N является $\{2, 3\}$-группой, а при $q = 3, 7$ даже 2-группой.

Пусть $q = 5$ и $O_3(N) \neq 1$. В $U_3(5)$ существует подгруппа Фробениуса порядка $7 \cdot 3$. По лемме 4 имеем $3 \cdot 3 = 9 \in \omega(G) = \omega(U_3(5))$, но $\mu(U_3(5)) = \{10, 8, 7, 6\}$; противоречие.

Пусть $q > 7$ и $O_3(N) \neq 1$. Тогда $\mu(G) = \{p \cdot 2^m, 2^{m+1}r, 3 \cdot 2^m, q^2 - q + 1\}$. В $U_3(q)$ есть подгруппа Фробениуса порядка $p \cdot r$. По лемме 4 $3r \in \omega(G)$; противоречие. Значит, N является 2-группой.

Лемма 28. *Если группа A содержит элемент, индуцирующий внешний диагональный автоморфизм группы P, то $\omega(G) \neq \omega(P)$.*

Доказательство. Предположим противное. Тогда $|PGU_3(q) : U_3(q)| = 3$ и группа A содержит подгруппу, изоморфную $PGU_3(q)$. По теореме 4(a) из [18] в $PGU_3(q)$ есть циклическая подгруппа порядка $\frac{q^3+1}{q+1}$, которой по лемме 10 нет в $U_3(q)$; противоречие.

Лемма 29. *Утверждение* 5 *теоремы* 1 *выполняется.*

Доказательство. По лемме 3 $P \leq A \leq PGU_3(q)F$, где $F = \langle x \rangle$ — группа полевых автоморфизмов группы P. Предположим, что $|A/P| > 2$. Допустим, что $A \nleq PF$. Тогда $3 \mid (q+1)$ и по лемме 28 в F есть элемент x_1 порядка 3 и A/P содержит произведение $x_1 zP$, где zP — элемент порядка 3, порождающий группу $PGU_3(q)/P$. По (9-1) из [19] $C_P(x_1)$ содержит подгруппу P_1, изоморфную $U_3(q_1)$, где $q_1 = \sqrt[3]{q}$. Ввиду леммы 10 в P_1 существует неединичный элемент y порядка, делящего $\frac{q_1^3+1}{(q_1+1)(3,q_1+1)}$. Тогда из доказательства леммы 28 видно, что централизатор элемента y накрывает фактор-группу $PGU_3(q)\langle x_1 \rangle/P$; противоречие с тем, что $\pi(A/P) \subseteq \pi_1(G)$, а $\pi(|y|) \subseteq \pi_2(G)$. Значит, $A \leq PF$. Пусть φ — инволюция из F. Предположим, что $|x| > 2$. Тогда F содержит элемент y порядка 4 или нечетного простого порядка $s \in \pi_1(G)$. Пусть $L = C_P(\varphi)$. По лемме 3 $L \cong PGL_2(q)$. Если $|y| = s$, то по (9-1) из [19] $U_3(\sqrt[s]{q}) \leq C_P(y)$, поэтому по лемме 10 $\frac{\sqrt[s]{q}^3+1}{(\sqrt[s]{q}+1)(3,\sqrt[s]{q}+1)} \in \omega(C_P(y))$, т. е. в группе G π_1-элемент централизует π_2-элемент; противоречие. Если $|y| = 4$, то $y^2 = \varphi$. Ясно, что $C_P(y) \leq L$. Если $C_P(y) = L$, то элемент порядка 4 централизует элемент порядка p. По лемме 10 $q+1 \equiv 0 (\mathrm{mod}\, 4)$. Так как $4 \in \omega(A/P)$, то $q = q_1^2$, $q_1^2 \equiv 1 (\mathrm{mod}\, 4)$, $q+1 \equiv 2 (\mathrm{mod}\, 4)$; противоречие. Если y не централизует L, то y индуцирует на $L' = L_2(q)$ полевой автоморфизм порядка 2 и, значит, $C_{L'}(y) \cong PGL_2(\sqrt{q})$, поэтому снова элемент порядка 4 централизует элемент порядка p; противоречие.

Доказательство теоремы 1. Теорема 1 следует из лемм 13–29.

Доказательство теоремы 2. По теореме 1 $P \cong U_3(q)$ при $q > 5$. Ввиду лемм 14–23 P изоморфна $L_3(2)$ или $U_3(3)$ при $q = 3$ и изоморфна $L_3(2)$, $L_3(4)$, $U_3(5)$ или A_7 при $q = 5$. По теореме 1 N является 2-группой при $q \leq 7$.

Пусть $q = 3$. Предположим, что $N = 1$. Тогда $G \leq \mathrm{Aut}(P)$. Если $P \cong L_3(2)$, то $\mathrm{Aut}(P) \cong L_3(2).2$, $\mu(L_3(2).2) = \{8, 7, 6\}$, что противоречит включению $12 \in \omega(G)$. Если $P \cong U_3(3)$, то $\mathrm{Aut}(P) \cong U_3(3).2$, $\mu(U_3(3).2) = \mu(U_3(3)) = \mu(G)$ и G изоморфна $U_3(3)$ или $U_3(3).2$. Пусть $N \neq 1$. Тогда $G/N \cong L_3(2)$, $L_3(2).2$, $U_3(3)$, $U_3(3).2$.

Пусть $q = 5$. Предположим, что $N = 1$. Тогда $G \leq \mathrm{Aut}(P)$. Как и в предыдущем абзаце, получаем, что $G \cong L_3(4).2_3$ или $G \cong U_3(5)$. Предположим, что $N \neq 1$. Пусть $P \cong U_3(5)$. Докажем, что не существует расширения E нетривиальной 2-группы при помощи $U_3(5)$ со свойством $\omega(E) \subseteq \omega(U_3(5))$. Пусть

g — элемент порядка 7 из $U_3(5)$, U — неприводимый $U_3(5)$-модуль над алгебраически замкнутым полем характеристики 2, β — характер Брауэра модуля U. Тогда размерность подпространства $C_U(g)$, состоящего из неподвижных точек элемента g в пространстве U, выражается формулой (см. [11])

$$\dim C_U(g) = \sum_{x \in \langle g \rangle} \beta(x)/|\langle g \rangle|.$$

Теперь таблица 2-характеров Брауэра для $U_3(5)$ (см. [20]) показывает, что $\dim C_U(g) \geq 1$ для любого $U_3(5)$-модуля U над алгебраически замкнутым полем характеристики 2. Таким образом, $\omega(E) \not\subseteq \omega(U_3(5))$ и $P \not\cong U_3(5)$. Пусть $P \cong L_3(2)$. Тогда $10 \notin \omega(G)$; противоречие. Ввиду [6] имеем $G/N \cong L_3(4)$, $L_3(4).2_1$, $L_3(4).2_3$, A_7.

Пусть $q = 7$. В силу [6] G/N изоморфна $U_3(7)$ или $U_3(7).2$.

Пусть $q = 9$. Вследствие [21] G изоморфна $U_3(9)$.

Пусть $q = 11$. Тогда $P \cong U_3(11)$. Предположим, что $N \neq 1$. Докажем, что не существует расширения E нетривиальной 2-группы при помощи $U_3(11)$ со свойством $\omega(E) \subseteq \omega(U_3(11))$. Пусть g — элемент порядка 37 из $U_3(11)$, U — неприводимый $U_3(11)$-модуль над алгебраически замкнутым полем характеристики 2, β — характер Брауэра модуля U. Таблица 2-характеров Брауэра для $U_3(11)$ (см. [20]) показывает, что $\dim C_U(g) \geq 1$ для любого $U_3(11)$-модуля U над алгебраически замкнутым полем характеристики 2. Таким образом, $\omega(E) \not\subseteq \omega(U_3(11))$. Следовательно, $N = 1$, $G \leq \mathrm{Aut}(U_3(11))$. Имеем $|\mathrm{Out}(G)| = 6$. Так как $\mu(U_3(11)) = \{44, 40, 37, 12\}$, $\mu(U_3(11).2) = \{44, 40, 37, 24\}$ и $\mu(U_3(11).3) = \{132, 120, 111\}$, то $G \cong U_3(11)$.

ЛИТЕРАТУРА

1. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
2. *Мазуров В. Д., Су М. Ч., Чао Ч. П.* Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов // Алгебра и логика. 2000. Т. 39, № 5. С. 567–586.
3. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
4. *Мазуров В. Д.* Распознавание конечных групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651–666.
5. *Aschbacher M.* Finite group theory. Cambridge: Cambridge Univ. Press, 1986.
6. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* An atlas of finite groups. Oxford: Clarendon Press, 1985.
7. *Feit W.* Characters of finite groups. New York; Amsterdam: W. A. Benjamin Inc., 1967.
8. *Бусаркин В. М., Горчаков Ю. М.* Конечные расщепляемые группы. М.: Наука, 1968.
9. *Passman D. S.* Permutation groups. New York: Benjamin, 1968.
10. *Harris M. E.* Finite groups containing an intrinsic 2–component of Chevalley type over a field of odd order // Trans. Amer. Math. Soc. 1982. V. 272, N 1. P. 1–65.
11. *Мазуров В. Д.* Характеризации конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 36–53.
12. *Zsigmondi H.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
13. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–370.
14. *Белоногов В. А.* Малые взаимодействия в группах $SL_3(q)$, $SU_3(q)$, $PSL_3(q)$ и $PSU_3(q)$ // Тр. Ин-та математики и механики УрО РАН. 1998. Т. 5. С. 3–27.
15. *Заварницин А. В.* Порядки элементов в накрытиях групп $L_n(q)$ и распознаваемость знакопеременной группы A_{16}. Новосибирск, 2000 (Препринт / НИИ дискретной математики и информатики; N 48).
16. *Brandl R., Shi W.* The characterization of $PSL(2, q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.

17. *Mitchell H. H.* Determination of the ordinary and modular ternary linear groups // Trans. Amer. Math. Soc. 1911. V. 12. P. 207–272.

18. *Huppert B.* Singer-Zyklen in klassischen Gruppen // Math. Z. 1970. Bd 117, N 1–4. S. 141–150.

19. *Gorenstein D., Lyons R.* The local structure of finite groups of characteristic 2 type. Providence, RI: Amer. Math. Soc., 1983. (Mem. Amer. Math. Soc. V. 42, N 276).

20. *Jansen C., Lux K., Parker R., Wilson R.* An atlas of Brauer characters. Oxford: Clarendon Press, 1985.

21. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по их множеству порядков элементов // Алгебра и логика (в печати).

Статья поступила 12 марта 2001 г.

Алеева Марианна Рифхатовна
Институт математики и механики УрО РАН
ул. С. Ковалевской, 16, Екатеринбург 620219
aleeva@imm.uran.ru