Сибирский математический журнал
Январь—февраль, 2013. Том 54, № 1

УДК 512.542

НАИБОЛЬШИЕ ПОРЯДКИ ЭЛЕМЕНТОВ И ХАРАКТЕРИСТИКА КОНЕЧНЫХ ПРОСТЫХ СИМПЛЕКТИЧЕСКИХ ГРУПП

Д. В. Лыткин

Аннотация. *Характеристикой простой группы лиева типа* называется характеристика поля, над которым она определена. Пусть $G = \mathrm{Sp}_{2n}(q)$, где $q = 2^k$. Показано, что любая конечная группа лиева типа с такими же двумя наибольшими порядками элементов, как у G, имеет характеристику 2.

Ключевые слова: простая симплектическая группа, наибольшие порядки элементов.

Введение

Задача о связи между характеристикой поля определения группы лиева типа и наибольшими порядками ее элементов возникла в [1] при анализе алгоритмических проблем вычислительной теории групп. Следуя обозначениям этой работы, для конечной простой группы лиева типа G обозначим через $ch(G)$ характеристику поля, над которым она определена, и через $m_1(G)$, $m_2(G)$ и $m_3(G)$ — три наибольших числа в множестве порядков ее элементов, расположенных по убыванию. В [1, теорема 1.2] показано, что если G и H — конечные простые группы лиева типа над полями нечетных характеристик и $m_i(G) = m_i(H)$ для $1 \leq i \leq 3$, то $\mathrm{ch}(G) = \mathrm{ch}(H)$. Иными словами, три наибольших порядка элементов однозначно задают характеристику простой группы лиева типа при условии, что эта характеристика нечетна.

Естественным образом возникает вопрос о том, может ли конечная простая группа лиева типа над полем характеристики 2 иметь общие три наибольших порядка элементов с какой-либо простой группой лиева типа над полем нечетной характеристики. Для групп небольших порядков отрицательный ответ получен прямыми вычислениями [1, факт 1.1]. Методами из [1] можно получить ответ и для всех остальных групп, кроме $\mathrm{Sp}_{2n}(2^k)$, $\Omega^+_{2n}(2^k)$ и $\Omega^-_{2n}(2^k)$. Для указанных же симплектических и ортогональных групп нахождение наибольших порядков элементов представляет существенно более сложную задачу, чем для остальных простых групп лиева типа.

В настоящей работе найдены явные формулы для двух наибольших порядков элементов в группах $\mathrm{Sp}_{2n}(2^k)$ (табл. 1, 2), и доказано, что эти группы можно отличить от групп лиева типа нечетной характеристики по двум наибольшим порядкам элементов.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 12–01–31221, 12–01–33102).

Теорема 1. *Пусть $G = \mathrm{Sp}_{2n}(q)$, где $q = 2^k$, и H — простая группа лиева типа такая, что $m_1(G) = m_1(H)$ и $m_2(G) = m_2(H)$. Тогда $\mathrm{ch}(H) = 2$.*

§ 1. Предварительные результаты и числовые леммы

Для простого числа p через $n_{\{p\}}$ обозначается p-часть числа n, т. е. наибольшая степень числа p, делящая n. Наибольший общий делитель и наименьшее общее кратное чисел $n_1, \dots, n_s$ обозначаются через $(n_1, \dots, n_s)$ и $[n_1, \dots, n_s]$ соответственно. Через $\lfloor x \rfloor$ обозначается целая часть числа x.

Лемма 1 [2, следствие 3]. *Пусть q — степень числа 2 и $G = \mathrm{Sp}_{2n}(q)$, $n \geq 2$. Тогда множество порядков элементов группы G состоит из всех делителей следующих чисел:*

1) $[q^{n_1}+\varepsilon_1, \dots, q^{n_s}+\varepsilon_s]$ *для любых* $s \geq 1$, $\varepsilon_i = \pm 1$, $1 \leq i \leq s$, $n_1, n_2, \dots, n_s > 0$ *таких, что* $n_1 + n_2 + \dots + n_s = n$;

2) $2[q^{n_1}+\varepsilon_1, \dots, q^{n_s}+\varepsilon_s]$ *для любых* $s \geq 1$, $\varepsilon_i = \pm 1$, $1 \leq i \leq s$, *и* $n_1, n_2, \dots, n_s > 0$ *таких, что* $n_1 + n_2 + \dots + n_s = n - 1$;

3) $2^k[q^{n_1} + \varepsilon_1, \dots, q^{n_s} + \varepsilon_s]$ *для любых* $s \geq 1$, $k \geq 2$, $\varepsilon_i = \pm 1$, $1 \leq i \leq s$, *и* $n_1, n_2, \dots, n_s > 0$ *таких, что* $2^{k-2} + 1 + n_1 + n_2 + \dots + n_s = n$;

4) 2^k, *если* $2^{k-2} + 1 = n$ *для некоторого* $k \geq 2$.

Лемма 2 [3, лемма 6(iii)]. *Пусть a, b, q — натуральные числа, $q > 1$. Тогда*

1) $(q^a - 1, q^b - 1) = q^{(a,b)} - 1$;

2) $(q^a + 1, q^b + 1) = \begin{cases} q^{(a,b)} + 1, & \text{если } a_{\{2\}} = b_{\{2\}}, \\ (2, q-1) & \text{иначе;} \end{cases}$

3) $(q^a - 1, q^b + 1) = \begin{cases} q^{(a,b)} + 1, & \text{если } a_{\{2\}} > b_{\{2\}}, \\ (2, q-1) & \text{иначе.} \end{cases}$

Лемма 3 [4]. *Пусть $p^a - q^b = 1$, где p и q — простые, $a, b \geq 1$ — натуральные числа. Тогда выполняется одно из следующих утверждений:*

1) $p^a = 3^2$, $q^b = 2^3$;

2) $a = 1$, $q = 2$, $p = 2^b + 1$;

3) $b = 1$, $p = 2$, $q = 2^a - 1$.

Лемма 4. *Пусть a, b, q — натуральные числа, $b > a$, $q > 1$, и пусть $c = \left\lfloor \frac{q^{a+b}-1}{q^b-q^a} \right\rfloor$. Тогда $c \equiv 1 \pmod q$, если $(b-a) \mid b$, и $c \equiv 0 \pmod q$ иначе.*

Доказательство. Пусть i — натуральное число такое, что $a+b-i(b-a) < b \leq a + b - (i-1)(b-a)$. Тогда

$$\left\lfloor \frac{q^{a+b}-1}{q^b-q^a} \right\rfloor = \left\lfloor \frac{q^{a+b} - q^{a+b-i(b-a)}}{q^b - q^a} + \frac{q^{a+b-i(b-a)} - 1}{q^b - q^a} \right\rfloor = \frac{q^{a+b-i(b-a)}(q^{i(b-a)} - 1)}{q^a(q^{b-a} - 1)}.$$

Осталось заметить, что условие $(b-a) \mid b$ эквивалентно равенству $a = a + b - i(b-a)$.

§ 2. Два наибольших порядка элементов

Пусть $m_1(n, q)$ и $m_2(n, q)$ — два наибольших числа вида $[q^{n_1} \pm 1, \dots, q^{n_k} \pm 1]$, где знаки выбираются независимо, $k, n_1, \dots, n_k \geq 1$ и $n_1 + \dots + n_k = n$, причем $m_1(n, q) > m_2(n, q)$. Для неотрицательного числа n через $p(n)$ будем обозначать наибольшее целое число p такое, что $2^p \leq n$.

Лемма 5. *Пусть q — четное натуральное число, $n_1, \dots, n_s \geq 1$ — нечетные числа, $s \geq 2$ и $n_1 + \dots + n_s = n$. Тогда $[q^{n_1}+1, \dots, q^{n_s}+1] \leq q^n - 1$.*

Доказательство. Проведем индукцию по s. Пусть $s = 2$. Пользуясь леммой 2, получим, что

$$[q^{n_1}+1, q^{n_2}+1] = \frac{(q^{n_1}+1)(q^{n_2}+1)}{q^{(n_1,n_2)}+1} \leq \frac{(q^{n_1}+1)(q^{n_2}+1)}{q+1} \leq q^{n_1+n_2} - 1.$$

Пусть теперь $s > 2$. Используя предположение индукции, получаем, что

$$[q^{n_1}+1, \dots, q^{n_s}+1] \leq \frac{[q^{n_1}+1, \dots, q^{n_{s-1}}+1](q^{n_s}+1)}{q+1} \leq \frac{(q^{n-n_s}-1)(q^{n_s}+1)}{q+1} \leq q^n - 1.$$

Лемма 6. *Пусть n, q — натуральные числа, n нечетно, q четно, $n = n_1 + \dots + n_s$ — разбиение числа n, не являющееся двоичным разложением, и $u = (q^{n_1}+1)\dots(q^{n_s}+1)$. Если числа $q^{n_1}+1, \dots, q^{n_s}+1$ попарно взаимно просты, то*

$$u \leq (q^{n'_1}+1)\dots(q^{n'_k}+1)(q^{3\cdot 2^r}+1)(q^{2^{r+1}}+1)\dots(q^{2^{p-1}}+1),$$

где $n'_1 + n'_2 + \dots + n'_k + 2^r + 2^p$ — двоичное разложение числа n в порядке возрастания. В частности,

$$u < (q^{n'_1}+1)\dots(q^{n'_k}+1)(q^{2^r}+1)(q^{2^p}+1).$$

Замечание. Здесь и далее при $b < a$ будем считать значение выражения $(q^a+1)\dots(q^b+1)$ равным единице.

Доказательство. По лемме 2 числа q^a+1 и q^b+1 взаимно просты в том и только том случае, когда a и b имеют различные 2-части. Поэтому все $n_1, \dots, n_s$ имеют различные 2-части. Будем также считать, что числа n_i упорядочены по возрастанию 2-части.

Пусть n_i — наибольший по 2-части элемент разбиения, отличный от степени двойки. Тогда $n_i = 2^j \cdot t$, где $t \geq 3$. Допустим, что последовательные степени $2^{j+p(t)}, \dots, 2^{j+p(t)+h}$ содержатся в разбиении $n_1 + \dots + n_s$, а $2^{j+p(t)+h+1}$ нет. Верны неравенства

$$\begin{aligned}
&(q^{2^j\cdot t}+1)(q^{2^j\cdot 2^{p(t)}}+1)\dots(q^{2^j\cdot 2^{p(t)+h}}+1)\\
&\qquad \leq (q^{2^j\cdot(t-2^{p(t)})}+1)(q^{2^j\cdot 2^{p(t)}}-1)(q^{2^j\cdot 2^{p(t)}}+1)\dots(q^{2^j\cdot 2^{p(t)+h}}+1)\\
&\qquad = (q^{2^j\cdot(t-2^{p(t)})}+1)(q^{2^j\cdot 2^{p(t)+h+1}}-1) < (q^{2^j\cdot(t-2^{p(t)})}+1)(q^{2^j\cdot 2^{p(t)+h+1}}+1).
\end{aligned}$$

Если же число $2^{j+p(t)}$ не содержится в разбиении, то

$$q^{2^j\cdot t}+1 < (q^{2^j\cdot(t-2^{p(t)})}+1)(q^{2^j\cdot 2^{p(t)}}+1).$$

Таким образом, получили новое разбиение числа n, элементы которого имеют различные 2-части, при этом уменьшив наибольший элемент, отличный от степени двойки. Будем продолжать такие преобразования до тех пор, пока в разбиении не останется единственный элемент n_i, отличный от степени двойки, причем $n_i = 2^j \cdot (1+2^k)$, $k \geq 1$. Предположим, что последовательные степени $2^{j+k}, \dots, 2^{j+k+h-1}$ содержатся в разбиении, а 2^{j+k+h} нет, $h \geq 0$. Легко понять, что все элементы разбиения, кроме этих степеней и числа n_i, являются элементами двоичного разложения числа n. Поэтому для доказательства утверждения достаточно проверить неравенство

$$\frac{(q^{2^j\cdot(1+2^k)}+1)(q^{2^j\cdot 2^k}+1)\dots(q^{2^j\cdot 2^{k+h-1}}+1)}{(q^{2^j}+1)(q^{2^j\cdot 2^{k+h}}+1)} \le \frac{(q^{3\cdot 2^r}+1)(q^{2^{r+1}}+1)\dots(q^{2^{p-1}}+1)}{(q^{2^r}+1)(q^{2^p}+1)}.$$

Преобразуем обе части этого неравенства:

$$\frac{(q^{2^j\cdot(1+2^k)}+1)(q^{2^j\cdot 2^{k+h}}-1)}{(q^{2^j}+1)(q^{2^j\cdot 2^k}-1)(q^{2^j\cdot 2^{k+h}}+1)} \le \frac{(q^{3\cdot 2^r}+1)(q^{2^p}-1)}{(q^{2^r}+1)(q^{2^{r+1}}-1)(q^{2^p}+1)}.$$

Функция $(ax+1)/(x-1)$ убывает по x при $a>0$, $x>1$, поэтому верно неравенство

$$\frac{q^{2^j\cdot(1+2^k)}+1}{(q^{2^j}+1)(q^{2^j\cdot 2^k}-1)} \le \frac{q^{3\cdot 2^j}+1}{(q^{2^j}+1)(q^{2^{j+1}}-1)}.$$

Функция $(x^2-x+1)/(x-1)$ возрастает при $x\ge 4$. Следовательно,

$$\frac{q^{3\cdot 2^j}+1}{(q^{2^j}+1)(q^{2^{j+1}}-1)} \le \frac{q^{3\cdot 2^r}+1}{(q^{2^r}+1)(q^{2^{r+1}}-1)}.$$

Функция $(x-1)/(x+1)$ возрастает при $x>0$, значит,

$$\frac{q^{2^{k+j+h}}-1}{q^{2^{k+j+h}}+1} \le \frac{q^{2^p}-1}{q^{2^p}+1}.$$

Последнее утверждение леммы следует из неравенства

$$(q^{3\cdot 2^r}+1)(q^{2^{r+1}}+1)\dots(q^{2^{p-1}}+1) = (q^{3\cdot 2^r}+1)(q^{2^p}-1)/(q^{2^{r+1}}-1) < (q^{2^r}+1)(q^{2^p}+1).$$

Предложение 1. *Пусть n — нечетное натуральное число, $n\ge 3$, $q>2$ четно, и пусть $n_1+n_2+\dots+n_k+2^r+2^p$ — двоичное разложение числа n в порядке возрастания. Тогда*

$$m_1(n,q) = [q^{n_1}+1,\dots,q^{n_k}+1,q^{2^r}+1,q^{2^p}+1],$$

$$m_2(n,q) = [q^{n_1}+1,\dots,q^{n_k}+1,q^{3\cdot 2^r}+1,q^{2^{r+1}}+1\dots q^{2^{p-1}}+1].$$

Доказательство. Для краткости записи далее в доказательстве будем обозначать через $m_1(n,q)$ и $m_2(n,q)$ числа в правых частях равенств в утверждении предложения. Необходимо показать, что $m_1(n,q)>m_2(n,q)$ и $m_2(n,q)\ge u$ для любого $u=[q^{n_1}+\varepsilon_1,\dots,q^{n_s}+\varepsilon_s]$, отличного от $m_1(n,q)$, где $n_1+\dots+n_s$ — некоторе разбиение числа n и $\varepsilon_i=\pm 1$ для $i=1,\dots,s$.

Заметим, что $q^{2x}-1=(q^x-1)(q^x+1)=[q^x-1,q^x+1]$. Поэтому можем считать, что у всех элементов $q^{n_i}+\varepsilon_i$ с $\varepsilon_i=-1$ показатель n_i нечетен.

Разобьем множество $\{q^{n_i}+\varepsilon_i\}_{i=1}^s$ на классы: элементы с $\varepsilon_i=-1$ отнесем к классу M_-, а остальные разобьем на классы по 2-части показателя: $M_j=\{q^{n_i}+1 \mid (n_i)_{\{2\}}=2^j\}$. Тогда по лемме 2 любые два элемента из разных классов взаимно просты. Таким образом, число $[q^{n_1}+\varepsilon_1,\dots,q^{n_s}+\varepsilon_s]$ можно записать в виде

$$[q^{m_1}-1,\dots,q^{m_k}-1][q^{n_1^0}+1,\dots,q^{n_{k_0}^0}+1]\dots[q^{n_1^l}+1,\dots,q^{n_{k_l}^l}+1],$$

где n_i^j — показатели с 2-частью 2^j, а k и k_j — число элементов классов M_- и M_j соответственно. Положим $n^j = n_1^j + \dots + n_{k_j}^j$, $m = m_1 + \dots + m_k$.

Пусть $u = [q^{n_1} + \varepsilon_1, \dots, q^{n_s} + \varepsilon_s]$ отлично от $m_1(n,q)$. Так как все n^j при $j > 0$ четны, возможны два случая.

Случай 1: m нечетно, n^0 четно. Применяя неравенства $[q^{n_1^j}+1, \dots, q^{n_{k_j}^j}+1] \le q^{n^j} - 1$ при $k_j > 1$ и $[q^{m_1} - 1, \dots, q^{m_k} - 1] \le q^m - 1$, получим $u \le (q^m - 1)(q^{n^0} \pm 1)\dots(q^{n^l} \pm 1)$, где в $q^{n^j} \pm 1$ стоит минус в том и только в том случае, когда $k_j > 1$. Стало быть, $u \le (q^{\widetilde{m}} - 1) \prod\limits_{j:k_j=1} (q^{n^j} + 1)$, где $\widetilde{m} = m + \sum\limits_{j:k_j>1} n^j$.

Предположим, что $\widetilde{m} = 1$. Тогда $u \le (q^{n^t+1} + 1) \prod\limits_{j\ne t:k_j=1} (q^{n^j} + 1)$, где n^t — какой-нибудь четный элемент разбиения. При этом $(n^t + 1) + \sum\limits_{j\ne t:k_j=1} n^j$ не является двоичным разложением, а все слагаемые имеют разные 2-части.

Если же $\widetilde{m} > 1$, то $u \le (q^{\widetilde{m}} + 1) \prod\limits_{j:k_j=1} (q^{n^j} + 1)$. При этом $\widetilde{m} + \sum\limits_{j:k_j=1} n^j$ — не двоичное разложение и все слагаемые имеют разные 2-части.

Случай 2: m четно, n^0 нечетно. Если $m \ne 0$, то $k > 1$, потому что все m_i нечетны. Следовательно, $[q^{m_1} - 1, \dots, q^{m_k} - 1] \le \frac{q^m-1}{q-1}$. Получим

$$u \le \frac{q^m - 1}{q - 1}(q^{n^0} \pm 1)\dots(q^{n^l} \pm 1) \le (q^{\widetilde{m}} + 1) \prod_{j\ne 0\,:\,k_j=1} (q^{n^j} + 1),$$

где $\widetilde{m} = m + n^0 + \sum\limits_{j\ne 0\,:\,k_j>1} n^j$. Заметим, что $\widetilde{m} \ge 3$, поэтому $\widetilde{m} + \sum\limits_{j:k_j=1} n^j$ не является двоичным разложением числа n.

Если $m = 0$, то $u \le (q^{\widetilde{m}} + 1) \prod\limits_{j\ne 0\,:\,k_j=1} (q^{n^j} + 1)$, где $\widetilde{m} = n^0 + \sum\limits_{j\ne 0\,:\,k_j>1} n^j$. В силу выбора числа u, отличного от $m_1(n,q)$, имеем $\widetilde{m} > 1$.

Значит, в обоих случаях можем считать, что $u = (q^{n_1} + 1)\dots(q^{n_s} + 1)$, где все $n_1, \dots, n_s$ имеют различные 2-части и $n = n_1 + \dots + n_s$ — не двоичное разложение. Осталось применить лемму 6.

Предложение 2. *Пусть n и q — четные натуральные числа и $p = p(n/3)$.*
1. *Если $n = 2$, то $m_1(n,q) = q^2 + 1$, $m_2(n,q) = q^2 - 1$.*
2. *Если $n = 4$, то $m_1(n,q) = [q + 1, q^3 - 1]$, $m_2(n,q) = q^4 + 1$.*
3. *Если $n > 4$, то*

$$m_1(n,q) = [q+1, q^2+1, q^4+1, \dots, q^{2^p}+1, q^{n-2^{p+1}+1} - 1] = \frac{(q^{2^{p+1}} - 1)(q^{n-2^{p+1}+1} - 1)}{q - 1},$$

$$m_2(n,q) = [q+1, q^2+1, q^4+1, \dots, q^{2^{p+1}}+1, q^{n-2^{p+2}+1} - 1] = \frac{(q^{2^{p+2}} - 1)(q^{n-2^{p+2}+1} - 1)}{q - 1}$$

при $5 \cdot 2^p \le n$ и

$$m_2(n,q) = [q+1, q^2+1, q^4+1, \dots, q^{2^{p-1}}+1, q^{n-2^p+1} - 1] = \frac{(q^{2^p} - 1)(q^{n-2^p+1} - 1)}{q - 1}$$

иначе.

Доказательство. Как и раньше, считаем, что

$$u = [q^{m_1} - 1, \dots, q^{m_k} - 1][q^{n_1^0} + 1, \dots, q^{n_{k_0}^0} + 1] \dots [q^{n_1^l} + 1, \dots, q^{n_{k_l}^l} + 1],$$

где m_i нечетны, n_i^j имеют 2-часть 2^j, а k и k_j — число элементов классов M_- и M_j соответственно, и u отлично от $m_1(n,q)$. Положим $n^j = n_1^j + \dots + n_{k_j}^j$, $m = m_1 + \dots + m_k$.

Для $n \le 4$ утверждение очевидно либо легко проверяется. Пусть $n \ge 6$, тогда $p \ge 1$.

Покажем, что $u \le (q^{m'} - 1)(q^{n'_1} + 1) \dots (q^{n'_t} + 1)$, где m' — некоторое нечетное число, отличное от $n - 2^{p+1} + 1$, $n'_1 + \dots + n'_t = n - m'$ и все множители в правой части попарно взаимно просты.

Случай 1: m и n^0 нечетны. Положим $\widetilde{m} = m + \sum\limits_{j \ne 0\,:\,k_j > 1} n^j$. Если $\widetilde{m} \ne n - 2^{p+1} + 1$, то, пользуясь леммой 5, получим, что

$$u \le (q^{m'} - 1)(q^{n^0} + 1) \prod_{j \ne 0\,:\,k_j = 1} (q^{n^j} + 1),$$

где $m' = \widetilde{m}$ — нечетное число и все множители в правой части попарно взаимно просты.

Предположим теперь, что $\widetilde{m} = n - 2^{p+1} + 1$. Если в множестве $N = \{n^0\} \cup \{n^j \mid j > 0,\ k_j = 1\}$ найдется число $n^{j'}$, отличное от степени двойки, т. е. $n^{j'} = t \cdot 2^{j'} > 2^{j'}$, то

$$u \le (q^{m'} - 1)(q^{2^{j'}} + 1) \prod_{j \in N, j \ne j'} (q^{n^j} + 1),$$

где $m' = \widetilde{m} + (t-1) \cdot 2^{j'}$ — нечетное число и все множители в правой части попарно взаимно просты.

Пусть все числа из N являются степенями двойки. В силу того, что $\sum\limits_{j \in N} n^j = 2^{p+1} - 1$, имеем $N = \{n^j \mid 0 \le j \le p\}$. Тогда M_j для $0 \le j \le p$ — в точности все классы с плюсами, состоящие из единственного элемента. Если существует непустой класс $M_{j'}$ для $j' > p$, то $k_{j'} \ge 2$ и $n^j \ge 2 \cdot 2^{j'}$. Но тогда

$$n = m + \sum_{j=0}^{p} n^j + \sum_{j:k_j>1} n^j \ge 1 + 2^{p+1} - 1 + 2^{p+2} = 3 \cdot 2^{p+1},$$

чего не может быть. Поэтому классы с плюсами исчерпываются классами M_j для $0 \le j \le p$. В силу того, что $u \ne m_1(n,q)$, класс M_- не может состоять из одного элемента, поэтому $k \ge 3$. Если $m_i \le 2^p$ хотя бы для одного i, то $(q^{m_i} - 1)(q^{2^p} + 1) \le q^{m_i + 2^p} - 1$ и $u \le (q^{n - 2^p + 1} - 1)(q+1)(q^2+1) \dots (q^{2^{p-1}} + 1)$. Если же $m_i > 2^p$ для всех i, то

$$m_1 < m - (k-1)2^p \le m - 2^{p+1} = n - 2^{p+2} + 1 < 2^{p+1},$$

и выполнены неравенства

$$[q^{m_1} - 1, \dots, q^{m_k} - 1] \le (q^{m_1} - 1)(q^{m - m_1} - 1) < (q^{2^{p+1}} - 1)(q^{n - 2^{p+2} + 1} - 1),$$

откуда $u \le (q^{n - 2^{p+2} + 1} - 1)(q+1)(q^2+1) \dots (q^{2^{p+1}} + 1)$.

Случай 2: m и n^0 четны. Если хотя бы одно из k, k_0 не равно нулю, то

$$[q^{m_1}-1,\dots,q^{m_k}-1][q^{n_1^0}+1,\dots,q^{n_{k_0}^0}+1] \le q^{m+n^0}-1 \le (q^{m+n^0-1}-1)(q+1),$$

и можем перейти к предыдущему случаю.

Допустим, что $k = k_0 = 0$. Для самого большого по 2-части класса M_l имеем $n^l > 2$, откуда $[q^{n_1^l}+1,\dots,q^{n_{k_l}^l}+1] \le q^{n^l}+1 \le (q^{n^l-1}-1)(q+1)$, и можем перейти к предыдущему случаю.

Итак, во всех возможных случаях получили, что $u \le (q^{m'}-1)(q^{n'_1}+1)\dots(q^{n'_t}+1)$, где $m' \ne n-2^{p+1}+1$. Значит, $n-m'$ нечетно, и в силу леммы 6 можем считать, что $n'_1+\dots+n'_t$ — двоичное разложение числа $n-m'$.

Теперь можем доказать, что $u \le m_2(n,q)$. Будем считать, что n'_i упорядочены по возрастанию. Предположим, что среди них некоторые степени младше n'_t отсутствуют. Пусть наибольшей из таких степеней является 2^h и $2^{h+1} = n'_i$ для некоторого i. Заметим, что $(q^{m'}-1)(q^{2^{h+1}}+1) \le (q^{m'+2^h}-1)(q^{2^h}+1)$. Таким образом, можем сдвинуть все степени старше 2^h на одну вниз.

Предположим, что $t \ne p+1$. Тогда, повторяя описанный прием, получим $u \le (q^{n-2^t+1}-1)(q+1)(q^2+1)\dots(q^{2^{t-1}}+1)$. Если $t < p+1$, то $q^{n-2^t+1}-1 \le (q^{n-2^{t+1}+1}-1)(q^{2^t}+1)$. Если $t > p+1$, то $(q^{n-2^t+1}-1)(q^{2^{t-1}}+1) \le q^{n-2^{t-1}+1}-1$. Таким образом, если $t < p+1$, то $u \le (q^{n-2^p+1}-1)(q+1)(q^2+1)\dots(q^{2^{p-1}}+1)$, а если $t > p+1$, то $u \le (q^{n-2^{p+2}+1}-1)(q+1)(q^2+1)\dots(q^{2^{p+1}}+1)$. Осталось заметить, что при $n \ge 5\cdot 2^p$ выполнено неравенство $q^{n-2^p+1}-1 < (q^{n-2^{p+2}+1}-1)(q^{2^p}+1)(q^{2^{p+1}}+1)$, а при $n < 5\cdot 2^p$ — обратное неравенство.

Предположим теперь, что $t = p+1$. Тогда будем повторять описанный прием до тех пор, пока не получим $u \le (q^{n-3\cdot 2^p+1}-1)(q+1)(q^2+1)\dots(q^{2^{p-1}}+1)(q^{2^{p+1}}+1)$. При $n < 5\cdot 2^p$ выполнено неравенство $(q^{n-3\cdot 2^p+1}-1)(q^{2^{p+1}}+1) \le q^{n-2^p+1}-1$, а при $n \ge 5\cdot 2^p$ — неравенство $q^{n-3\cdot 2^p+1}-1 < (q^{n-2^{p+2}+1}-1)(q^{2^p}+1)$.

Наконец, для доказательства того, что $m_2(n,q) < m_1(n,q)$, достаточно проверить неравенства

$$(q^{2^{p+1}}+1)(q^{n-2^{p+2}+1}-1) < q^{n-2^{p+1}+1}-1,$$

$$q^{n-2^p+1}-1 < (q^{2^p}+1)(q^{n-2^{p+1}+1}-1).$$

Предложение 3. *Пусть n — нечетное натуральное число.*

1. *Если $n \in \{9, 2^l-1, 3\cdot 2^l-1\}$, $l \ge 1$, то*

$$m_1(n,2) = [2^{n_1}+1, 2^{n_2}+1, \dots, 2^{n_s}+1],$$

где $n_1+n_2+\dots+n_s$ — двоичное разложение числа n. Таким образом,

a) $m_1(9,2) = 771 = 3\cdot 257$;

b) $m_1(n,2) = 2^{2^l}-1 = 2^{n+1}-1$ *при* $n = 2^l-1$, $l \ge 1$;

c) $m_1(n,2) = (2^{2^l}-1)(2^{2^{l+1}}+1) = (2^{\frac{n+1}{3}}-1)(2^{\frac{2n+2}{3}}+1)$ *при* $n = 3\cdot 2^l-1$, $l \ge 1$.

Кроме того,

d) $m_2(n,2) = (2^{\frac{n+1}{4}}-1)(2^{\frac{3n+3}{4}}+1)$ *при* $n = 2^l-1$, $l \ge 3$;

e) $m_2(n,2) = (2^{\frac{n+1}{3}}-1)(2^{\frac{n-2}{3}}-1)(2^{\frac{n+4}{3}}-1)$ *при* $n = 3\cdot 2^l-1$, $l \ge 3$.

2. *Если $n \notin \{9, 2^l-1, 3\cdot 2^l-1\}$, $l \ge 1$, то*

$$m_1(n,2) = [2+1, 2^2+1, 2^4+1, \dots, 2^{2^p}+1, 2^a-1, 2^b-1] = (2^{2^{p+1}}-1)(2^a-1)(2^b-1),$$

где $p = p(n-3) - 2$, *и*

a) *при* $n \equiv 3 \pmod 4$

$$a = \frac{n-1}{2} - 2^p, \quad b = \frac{n+3}{2} - 2^p;$$

b) *при* $n \equiv 1 \pmod 4$

$$a = \frac{n-3}{2} - 2^p, \quad b = \frac{n+5}{2} - 2^p.$$

Доказательство. Как и раньше, считаем, что

$$u = [2^{m_1} - 1, \dots, 2^{m_k} - 1][2^{n_1^0} + 1, \dots, 2^{n_{k_0}^0} + 1] \dots [2^{n_1^l} + 1, \dots, 2^{n_{k_l}^l} + 1],$$

где m_i нечетны, n_i^j имеют 2-часть 2^j, а k и k_j — число элементов классов M_- и M_j соответственно. Положим $n^j = n_1^j + \dots + n_{k_j}^j$, $m = m_1 + \dots + m_k$.

Для $n \leq 5$ утверждение легко проверяется. Пусть $n \geq 7$. Рассмотрим три случая.

Случай 1: k_0 четно, тогда m нечетно. Если $m = n$, то $u = 2^n - 1 < (2+1)(2^3-1)(2^{n-4}-1)$. Если $m \neq n$, то по предложению 2 выполнено $u \leq (2+1)\dots(2^{2^t}+1)(2^{n-m-2^{t+1}+1}-1)(2^m-1)$, где $t = p\left(\frac{n-m}{3}\right)$. Поэтому верна оценка $u \leq (2+1)\dots(2^{2^t}+1)(2^a-1)(2^b-1)$, где $t \geq 0$, a и b — различные нечетные числа и $a + b = n - 2^{t+1} + 1$

Если $a < 2^t$, то $(2^{2^t}+1)(2^a-1) < (2^{a+2^t}-1)$. Поэтому можем считать, что $a, b > 2^t$.

Далее, если $a + b \equiv 0 \pmod 4$, то

$$(2^a-1)(2^b-1) \leq (2^{\frac{a+b}{2}+1}-1)(2^{\frac{a+b}{2}-1}-1),$$

и в этом случае считаем, что $a = b + 2$. При $t \geq 1$ это эквивалентно тому, что

$$n \equiv 3 \pmod 4, \quad a = \frac{n+3}{2} - 2^t, \quad b = \frac{n-1}{2} - 2^t.$$

Если же $a + b \equiv 2 \pmod 4$, то

$$(2^a-1)(2^b-1) \leq (2^{\frac{a+b}{2}+2}-1)(2^{\frac{a+b}{2}-2}-1),$$

и в этом случае считаем $a = b + 4$. При $t \geq 1$ это эквивалентно тому, что

$$n \equiv 1 \pmod 4, \quad a = \frac{n+5}{2} - 2^t, \quad b = \frac{n-3}{2} - 2^t.$$

В обоих случаях новые a и b взаимно просты.

Допустим, что $t < p(n-3) - 2$, тогда $2^{t+3} \leq n - 3$. В этом случае

$$(2^a-1)(2^b-1) \leq (2^{2^{t+1}}+1)(2^{a-2^t}-1)(2^{b-2^t}-1),$$

поэтому считаем, что $t = p(n-3) - 2$. Таким образом, получили окончательную оценку из п. 2 предложения. Осталось рассмотреть случай $n \in \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$.

Пусть $n = 2^l - 1$. Тогда $t = l - 3$, $m_1 + m_2 = 2^{t+1} + 2^{t+2}$ и $(2^{m_1}-1)(2^{m_2}-1) < 2^{3 \cdot 2^{t+1}} + 1$, где правая часть взаимно проста со всеми остальными $2^{2^i} + 1$. Тем же свойством обладают множители $2^{2^{t+1}} + 1$, $2^{2^{t+2}} + 1$. Очевидно, что $2^{3 \cdot 2^{t+1}} + 1 < (2^{2^{t+1}}+1)(2^{2^{t+2}}+1)$, откуда следуют доказываемые утверждения.

Пусть $n = 3 \cdot 2^l - 1$. Тогда при $l \geq 3$ полученная оценка в точности $u \leq m_2(n, 2)$. Далее, $t = l - 1$, $m_1 + m_2 = 2^{t+2}$ и $(2^{m_1} - 1)(2^{m_2} - 1) < 2^{2^{t+2}} + 1$, где правая часть взаимно проста со всеми $2^{2^i} + 1$.

Пусть, наконец, $n = 9$. Тогда $(2 + 1)(2^3 - 1)(2^5 - 1) < (2 + 1)(2^8 + 1)$.

Случай 2: k_0 нечетно и $k > 0$. Тогда $[2^{m_1} - 1, \ldots, 2^{m_k} - 1] \leq (2^{m_1} - 1)(2^{m-m_1} - 1)$ и по предложению 2 выполнено $u \leq (2+1) \ldots (2^{2^t}+1)(2^{n-m_1-2^{t+1}+1} - 1)(2^{m_1} - 1)$, где $t = p\big(\frac{n-m_1}{3}\big)$. Дальнейшее доказательство повторяет предыдущий случай.

Случай 3: k_0 нечетно и $k = 0$. Если $k_j > 1$ нечетно для некоторого j, то число n^j имеет 2-часть 2^j. Далее, $[2^{n_1^j} + 1, \ldots, 2^{n_{k_j}^j} + 1] < 2^{n^j} + 1$, где число в правой части взаимно просто с остальными $2^{n_i^{j'}} + 1$. Если $k_j > 1$ четно, то $[2^{n_1^j} + 1, \ldots, 2^{n_{k_j}^j} + 1] < \frac{(2^{n^j - n_1^j}+1)(2^{n_1^j}+1)}{2^{2^j}+1}$. Далее,

$$[2^{n_1^0} + 1, \ldots, 2^{n_{k_0}^0} + 1][2^{n_1^j} + 1, \ldots, 2^{n_{k_j}^j} + 1] \\ < (2^{n^0} + 1)\frac{(2^{n^j - n_1^j} + 1)(2^{n_1^j} + 1)}{2^{2^j} + 1} \leq (2^{n^j - n_1^j} + 1)(2^{n_0 + n_1^j} + 1),$$

где $n_0 + n_1^j$ нечетно, а $2^{n^j - n_1^j} + 1$ и $2^{n_0 + n_1^j} + 1$ взаимно просты со всеми остальными множителями. Поэтому считаем, что все $k_j = 1$.

Предположим, что $n = 2^l - 1$, $l \geq 3$. Тогда если исходное разложение не являлось двоичным, то по лемме 6

$$u \leq (2 + 1)(2^2 + 1) \ldots (2^{2^{l-3}} + 1)(2^{3 \cdot 2^{l-2}} + 1) = (2^{2^{l-2}} - 1)(2^{3 \cdot 2^{l-2}} + 1) \\ = (2^{\frac{n+1}{4}} - 1)(2^{\frac{3n+3}{4}} + 1).$$

Пусть теперь $n = 3 \cdot 2^l - 1$, $l \geq 3$. Тогда если исходное разложение не являлось двоичным, то по лемме 6

$$u \leq (2 + 1)(2^2 + 1) \ldots (2^{2^{l-2}} + 1)(2^{3 \cdot 2^{l-1}} + 1)(2^{2^l} + 1).$$

Необходимо показать, что

$$(2 + 1)(2^2 + 1) \ldots (2^{2^{l-2}} + 1)(2^{3 \cdot 2^{l-1}} + 1)(2^{2^l} + 1) \\ < (2 + 1)(2^2 + 1) \ldots (2^{2^{l-1}} + 1)(2^{2^l - 1} - 1)(2^{2^l + 1} - 1). \quad (1)$$

После раскрытия скобок и приведения подобных получим неравенство $2^{2^l+2} + 2^{2^l-1} < 2^{3 \cdot 2^{l-1}} + 2^{2^{l-1}}$, которое выполнено при $l \geq 3$. Осталось заметить, что правая часть неравенства (1) равна $(2^{\frac{n+1}{3}} - 1)(2^{\frac{n-2}{3}} - 1)(2^{\frac{n+4}{3}} - 1)$.

Если $n \notin \{2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 3$, то по лемме 6 выполнено $u \leq (2^{n_1'} + 1) \ldots (2^{n_t'} + 1)$, где $n_1' + \cdots + n_t' = n$ — двоичное разложение числа n.

Пусть старшая степень разложения n равна 2^h, а самая младшая отсутствующая степень двойки — 2^i. Если $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$, то $i < h - 1$ и $h \geq 3$.

Если $n = 13$, то $(2 + 1)(2^4 + 1)(2^8 + 1) < (2 + 1)(2^2 + 1)(2^3 - 1)(2^7 - 1)$. Пусть $n \notin \{9, 13, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$. Тогда $h \geq 4$. Возможны следующие случаи.

(a) $i = 1$. Тогда $2^{2^h} + 1 \leq (2^2 + 1)(2^{2^{h-1}-3} - 1)(2^{2^{h-1}+1} - 1)$.

(b) $i > 1$. Тогда $2^{2^h} + 1 \leq (2^{2^i} + 1)(2^{2^{h-1}-2^{i-1}-1} - 1)(2^{2^{h-1}-2^{i-1}+1} - 1)$.

Значит, если $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$, то

$$u \leq (2+1)\dots(2^{\tilde{n}_1}+1)(2^{\widetilde{m}_1}-1)(2^{\widetilde{m}_2}-1),$$

где $\widetilde{m}_1, \widetilde{m}_2$ — взаимно простые и нечетные, $\tilde{n}_i$ — различные степени двойки. Все множители попарно взаимно просты, поэтому число $(2+1)\dots(2^{\tilde{n}_1}+1)(2^{\widetilde{m}_2}-1)$ является числом вида $[2^{n_1} \pm 1, \dots, 2^{n_s} \pm 1]$ и можем применить предложение 2.

Итак, доказали, что для любого $n \in \{2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 3$, верны доказываемые оценки $u \leq m_2(n, 2)$, если $u \neq m_1(n, 2)$. Нетрудно получить неравенство $m_2(n, 2) < m_1(n, 2)$. При $n = 9$ и $n \in \{2^l - 1, 3 \cdot 2^l - 1\}$, $l = 1, 2$, по лемме 6 получили доказываемую оценку $u \leq m_1(n, 2)$.

Также мы доказали, что для любого $n \notin \{9, 2^l-1, 3\cdot 2^l-1\}$, $l \geq 1$, выполнено

$$u \leq (2+1)\dots(2^{2^{t-1}}+1)(2^{2^t}+1)(2^a-1)(2^b-1),$$

где a и b — различные нечетные числа и $a + b = n - 2^{t+1} + 1$. Дальнейшее доказательство повторяет случай 1.

Теперь можем найти числа $m_1(G)$ и $m_2(G)$ для $G = \mathrm{Sp}_{2n}(q)$. Покажем сначала, что при $q > 2$ числа $m_1(G)$ и $m_2(G)$ в точности $m_1(n, q)$ и $m_2(n, q)$. Нам понадобится следующая

Лемма 7. *Пусть $q \geq 4$ четно. Тогда $m_2(n, q)/m_1(n, q) \geq (q - 1)/q \geq 3/4$.*

Доказательство. При $n = 2$ и $n = 4$ оценка легко проверяется, поэтому пусть $n \geq 6$ четно. При $q \geq 2$, $a > b \geq 1$ выполнено неравенство $(q^a - q^b)/(q^{a+b} - 1) < 1/q$. Пусть $p = p(n/3)$. Если $n \geq 5 \cdot 2^p$, то

$$\frac{m_2}{m_1} = \frac{(q^a+1)(q^b-1)}{q^{a+b}-1} = 1 - \frac{q^a - q^b}{q^{a+b}-1} > 1 - \frac{1}{q} = \frac{q-1}{q},$$

где $a = 2^{p+1} > b = n - 2^{p+2} + 1$. Аналогично при $n < 5 \cdot 2^p$

$$\frac{m_1}{m_2} = \frac{(q^a+1)(q^b-1)}{q^{a+b}-1} = 1 - \frac{q^a - q^b}{q^{a+b}-1} < 1 + \frac{1}{q} = \frac{q+1}{q} < \frac{q}{q-1},$$

где $a = 2^p < b = n - 2^{p+1} + 1$.

Пусть $n \geq 3$ нечетно. При $q \geq 4$, $a \geq 1$ выполнено неравенство $(q^{2a} - q^a + 1)/(q^{2a} - 1) \geq (q^2 - q + 1)/(q^2 - 1)$. Следовательно,

$$\frac{m_2}{m_1} = \frac{(q^{2a}-q^a+1)(q^b-1)}{(q^{2a}-1)(q^b+1)} \geq \frac{q^2-q+1}{q^2-1} \cdot \frac{q^2-1}{q^2+1} = \frac{q^2-q+1}{q^2+1} > \frac{q-1}{q},$$

где a и b — две старшие степени в двоичном разложении числа n, причем $1 \leq a < b$.

Предложение 4. *Пусть $G = \mathrm{Sp}_{2n}(q)$, где $q \geq 4$ четно. Тогда $m_1(G) = m_1(n, q)$ и $m_2(G) = m_2(n, q)$, т. е. табл. 1 верна.*

Доказательство. Для $n \leq 4$ утверждение доказывается прямой проверкой. Пусть $n \geq 5$. Покажем, что все четные порядки элементов не превосходят $2m_1(n, q)/3$. Тогда по лемме 7 они будут меньше, чем $m_2(n, q)$, и утверждение будет доказано.

Пусть $u = 2[q^{n_1} \pm 1, \dots, q^{n_k} \pm 1]$, где $n_1 + \dots + n_k = n - 1 \geq 4$. Тогда $u \leq 2m_1(n - 1, q)$. Если n четно, то в $m_1(n - 1, q)$ нет членов с минусами, поэтому верна цепочка неравенств

$$2m_1(n-1, q) \leq \frac{2}{3}(q-1)m_1(n-1, q) \leq \frac{2}{3}m_1(n, q).$$

Таблица 1. Наибольшие порядки элементов групп $G = \mathrm{Sp}_{2n}(q)$, где $q > 2$

Условия на G	$m_1(G)$	$m_2(G)$	Обозначения
$n = 2$	q^2+1	q^2-1	
$n = 4$	$(q+1)(q^3-1)$	q^4+1	
$n \geq 6$ четно, $n \geq 5 \cdot 2^p$	$\frac{(q^{2^{p+1}}-1)(q^{n-2^{p+1}+1}-1)}{q-1}$	$\frac{(q^{2^{p+2}}-1)(q^{n-2^{p+2}+1}-1)}{q-1}$	$p = p(\frac{n}{3})$
$n \geq 6$ четно, $n < 5 \cdot 2^p$	$\frac{(q^{2^{p+1}}-1)(q^{n-2^{p+1}+1}-1)}{q-1}$	$\frac{(q^{2^{p}}-1)(q^{n-2^{p}+1}-1)}{q-1}$	$p = p(\frac{n}{3})$
n нечетно	$(q^{2^r}+1)(q^{2^p}+1) \times \prod_{i=1}^{k}(q^{n_i}+1)$	$\frac{(q^{3\cdot 2^r}+1)(q^{2^p}-1)\prod_{i=1}^{k}(q^{n_i}+1)}{q^{2^{r+1}}-1}$	$\sum_{i=1}^{k} n_i + 2^r + 2^p$ — двоичное разложение n в порядке возрастания

Если n нечетно, то $m_1(n-1,q) = (q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$, где b нечетно. Тогда

$$2m_1(n-1,q) \leq \frac{2}{3}(q-1)m_1(n-1,q) = \frac{2}{3}(q-1)(q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$$
$$\leq \frac{2}{3}(q^{b+2}+1)(q^2+1)\dots(q^{2^a}+1) \leq \frac{2}{3}m_1(n,q).$$

Пусть $u = 4[q^{n_1} \pm 1, \dots, q^{n_k} \pm 1]$, где $n_1 + \dots + n_k = n - 2 \geq 3$. Тогда $u \leq 4m_1(n-2,q)$. Если n нечетно, то

$$4m_1(n-2,q) = 4(q+1)(q^{n'_2}+1)\dots(q^{n'_l}+1)$$
$$\leq \frac{4}{13}(q^3+1)(q^{n'_2}+1)\dots(q^{n'_l}+1) < \frac{2}{3}m_1(n,q),$$

где $1 + n'_2 + \dots + n'_l$ — двоичное разложение числа $n-2$. Если n четно, то $m_1(n-2,q) = (q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$, где b нечетно. Тогда

$$4m_1(n-2,q) = 4(q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$$
$$\leq \frac{4}{15}(q^2-1)(q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$$
$$< \frac{2}{3}(q^{b+2}-1)(q+1)(q^2+1)\dots(q^{2^a}+1) \leq \frac{2}{3}m_1(n,q).$$

Пусть $u = 2^k[q^{n_1} \pm 1, \dots, q^{n_k} \pm 1]$, где $k \geq 3$. Тогда $u \leq 2^k m_1(n-1-2^{k-2},q)$. Отметим, что

$$2^k \leq \frac{2}{3}(q-1)\cdot 2^{k-1} \leq \frac{2}{3}(q-1)(q^{2^{k-2}}-1) < \frac{2}{3}(q^{2^{k-2}+1}-1).$$

Если n четно, то $n-1-2^{k-2}$ нечетно и в $m_1(n-1-2^{k-2},q)$ нет членов с минусами, поэтому верна цепочка неравенств

$$2^k m_1(n-1-2^{k-2},q) \leq \frac{2}{3}(q^{2^{k-2}+1}-1)m_1(n-1-2^{k-2},q) \leq \frac{2}{3}m_1(n,q).$$

Если n нечетно, то $n-1-2^{k-2}$ четно и $m_1(n-1-2^{k-2},q) = (q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1)$ при $n-1-2^{k-2} \neq 2$ и $m_1(n-1-2^{k-2},q) = q^2+1$ в противном случае. В первом случае

$$\begin{aligned} 2^k m_1(n-1-2^{k-2},q) &\leq \frac{2}{3}(q-1)(q^{2^{k-2}}-1)(q+1)(q^2+1)\dots(q^{2^a}+1)(q^b-1) \\ &\leq \frac{2}{3}(q^{b+2^{k-2}+2}-1)(q^2+1)\dots(q^{2^a}+1) \leq \frac{2}{3}m_1(n,q). \end{aligned}$$

Во втором случае $n = 3+2^{k-2}$ и

$$2^k m_1(2,q) = 2^k(q^2+1) \leq \frac{2}{3}(q^{2^{k-2}+1}-1)(q^2+1) \leq \frac{2}{3}m_1(n,q).$$

Пусть, наконец, $n = 1+2^{k-2}$ и $u = 2^k$. Тогда $m_2(n,q) = (q^3+1)(q^2+1)\dots(q^{2^{k-3}}+1) > 2^3 \cdot 2^{k-3} = u$.

Заключение предложения 4 неверно в общем случае для $q = 2$. Как мы покажем далее, в этом случае два наибольших порядка элементов группы G лежат среди чисел $m_1(n,2)$, $2 \cdot m_1(n-1,2)$, $4 \cdot m_1(n-2,2)$, $8 \cdot m_1(n-3,2)$. Докажем сначала несколько лемм.

Лемма 8. *Пусть $n \geq 4$ и $\mathrm{mix}(n,2)$ — наибольший элемент вида $2^k[2^{n_1}\pm 1,\dots,2^{n_s}\pm 1]$, где $k \geq 3$, $s \geq 1$, $n_1+\dots+n_s = n-2^{k-2}-1$. Тогда $\mathrm{mix}(n,2) = 2^3 m_1(n-3,2)$.*

Доказательство. Очевидно, что $\mathrm{mix}(n,2) = 2^k m_1(n-2^{k-2}-1,2)$ для некоторого k.

Нетрудно проверить, что для любого n выполнены неравенства (см. предложения 2, 3) $2^n < m_1(n,2) \leq 2^{n+1}-1$, из которых следует, что при $k \geq 4$ верна цепочка неравенств

$$2^k m_1(n-2^{k-2}-1,2) \leq 2^k(2^{n-2^{k-2}}-1) \leq 2^n < 2^3 m_1(n-3,2).$$

Лемма 9. *Пусть $n \geq 4$ четно. Тогда $4 \cdot m_1(n-2,2) < m_1(n,2)$.*

Доказательство. В силу предложения 2

$$m_1(n,2) = (2^{2^{p+1}}-1)(2^{n+1-2^{p+1}}-1),$$

$$4 \cdot m_1(n-2,2) = 4(2^{2^{p'+1}}-1)(2^{n-1-2^{p'+1}}-1),$$

где $p = p\big(\frac{n}{3}\big)$, $p' = p\big(\frac{n-2}{3}\big)$. Нетрудно понять, что $p' \leq p \leq p'+1$.

Пусть $p = p'$. Тогда неравенство $4 \cdot m_1(n-2,2) < m_1(n,2)$ эквивалентно неравенству $4(2^{n-1-2^{p'+1}}-1) < 2^{n+1-2^{p+1}}-1$, которое очевидно.

Пусть $p = p'+1$. В силу того, что $3 \cdot 2^p < n+1$, выполнена цепочка неравенств

$$4(2^{n-1-2^p}-1) < 2^{n+1-2^p}-2^2+2^{n+1-2^{p+1}}-2^p < (2^{2^p}+1)(2^{n+1-2^{p+1}}-1),$$

откуда следует доказываемое неравенство.

Лемма 10. *Пусть n нечетно и $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$. Тогда $m_1(n, 2) < 2 \cdot m_1(n-1, 2)$.*

Доказательство. В силу предложений 2 и 3

$$m_1(n, 2) = (2^{2^{t+1}} - 1)(2^a - 1)(2^b - 1),$$

где $t = p(n-3) - 2$, и $a + b = n + 1 - 2^{t+1}$;

$$m_1(n-1, 2) = (2^{2^{p+1}} - 1)(2^{n-2^{p+1}} - 1),$$

где $p = p\left(\frac{n-1}{3}\right)$.

Из условия $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$, следует, что $n \geq 13$ и, значит, $p \geq 2$. Поэтому

$$2^{p+1} < 3 \cdot 2^p - 2 \leq n - 3 < 3 \cdot 2^{p+1} - 2 < 2^{p+3},$$

откуда либо $p = t$, либо $p = t + 1$.

Пусть $p = t$. Необходимо показать, что $(2^a - 1)(2^b - 1) < 2(2^{n-2^{p+1}} - 1)$. Так как $a + b = n + 1 - 2^{t+1}$, то это неравенство эквивалентно неравенству $2^a + 2^b > 3$, которое выполнено в силу того, что $a, b > 1$.

Пусть $p = t + 1$. Необходимо показать, что $(2^a - 1)(2^b - 1) < 2(2^{2^p} + 1)(2^{n-2^{p+1}} - 1)$. В силу того, что $3 \cdot 2^p \leq n - 1$, верна цепочка неравенств

$$2^{2^p+1} + 1 < 2^{2^p+2} \leq 2^{n+1-2^{p+1}},$$

откуда следует, что

$$\begin{aligned} 2(2^{2^p} + 1)(2^{n-2^{p+1}} - 1) &= 2^{n+1-2^p} + 2^{n+1-2^{p+1}} - 2^{2^p+1} - 2 \\ &> 2^{n+1-2^p} - 1 = 2^{a+b} - 1 > (2^a - 1)(2^b - 1). \end{aligned}$$

Лемма 11. *Пусть n нечетно и $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$. Тогда $2 \cdot m_1(n, 2) < m_1(n+1, 2)$.*

Доказательство. В силу предложений 2 и 3

$$m_1(n, 2) = (2^{2^{t+1}} - 1)(2^a - 1)(2^b - 1),$$

где $t = p(n-3) - 2$, и $a + b = n + 1 - 2^{t+1}$;

$$m_1(n+1, 2) = (2^{2^{p+1}} - 1)(2^{n+2-2^{p+1}} - 1),$$

где $p = p\left(\frac{n+1}{3}\right)$.

Из условия $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$, следует, что $n \geq 13$ и, значит, $p \geq 2$. Поэтому

$$2^{p+1} < 3 \cdot 2^p - 4 \leq n - 3 < 3 \cdot 2^{p+1} - 4 < 2^{p+3},$$

откуда либо $p = t$, либо $p = t + 1$.

Пусть $p = t$. Тогда доказываемое неравенство следует из того, что $2(2^a - 1)(2^b - 1) < 2(2^{n+1-2^{t+1}} - 1) < 2^{n+2-2^{p+1}} - 1$.

Пусть $p = t + 1$. Необходимо показать, что $2(2^a - 1)(2^b - 1) < (2^{2^p} + 1)(2^{n+1-2^{p+1}} - 1)$. В силу того, что $3 \cdot 2^p \leq n + 1$, выполнено неравенство $2^{n+2-2^{p+1}} > 2^{2^p}$, откуда

$$\begin{aligned} 2(2^a - 1)(2^b - 1) &< 2(2^{n+1-2^p} - 1) = 2^{n+2-2^p} - 2 \\ &< 2^{n+2-2^p} - 1 + 2^{n+2-2^{p+1}} - 2^{2^p} = (2^{2^p} + 1)(2^{n+2-2^{p+1}} - 1). \end{aligned}$$

Таблица 2. Наибольшие порядки элементов групп $G = \mathrm{Sp}_{2n}(2)$

Условия на G	$m_1(G)$	$m_2(G)$	Обознач․
$n = 3$	15	12	
$n = 4$	30	24	
$n = 5$	60	51	
$n = 6$	120	105	
$n = 2^l - 1 \geq 7$	$2^{n+1} - 1$	$2(2^{\frac{n+1}{2}} - 1)(2^{\frac{n-1}{2}} - 1)$	
$n = 2^l \geq 8$	$2(2^n - 1)$	$(2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}+1} - 1)$	
$n = 2^l + 1 \geq 9$	$4(2^{n-1} - 1)$	$2(2^{\frac{n+1}{2}} - 1)(2^{\frac{n-1}{2}} - 1)$	
$n = 2^l + 2 \geq 10$	$8(2^{n-2} - 1)$	$(2^{\frac{n}{2}-1} - 1)(2^{\frac{n}{2}+2} - 1)$	
$n = 3 \cdot 2^l - 1 \geq 11$	$(2^{\frac{2n+2}{3}} + 1)(2^{\frac{n+1}{3}} - 1)$	$2(2^{\frac{n+1}{3}} - 1)(2^{\frac{2n-1}{3}} - 1)$	
$n = 3 \cdot 2^l \geq 12$	$(2^{\frac{2n}{3}} - 1)(2^{\frac{n}{3}+1} - 1)$	$2(2^{\frac{n}{3}} - 1)(2^{\frac{2n}{3}} + 1)$	
$n = 3 \cdot 2^l + 1 \geq 13$	$2(2^{\frac{2n-2}{3}} - 1)(2^{\frac{n+2}{3}} - 1)$	$4(2^{\frac{n-1}{3}} - 1)(2^{\frac{2n-2}{3}} + 1)$	
$n = 3 \cdot 2^l + 2 \geq 14$	$(2^{\frac{2n-4}{3}} - 1)(2^{\frac{n+7}{3}} - 1)$	$4(2^{\frac{2n-4}{3}} - 1)(2^{\frac{n+1}{3}} - 1)$	
n нечетно, $n \notin \{2^l \pm 1,$ $3 \cdot 2^l \pm 1\}$, $l \geq 1$	$2(2^{2^{p+1}} - 1)(2^{n-2^{p+1}} - 1)$	$8(2^{2^{p+1}} - 1)(2^{n-2^{p+1}-2} - 1)$	$p = p(\frac{n-1}{3})$
n четно, $n - 1 \notin$ $\{2^l \pm 1, 3 \cdot 2^l \pm 1\}$, $l \geq 1$	$(2^{2^{p+1}} - 1)(2^{n+1-2^{p+1}} - 1)$	$4(2^{2^{p+1}} - 1)(2^{n-1-2^{p+1}} - 1)$	$p = p(\frac{n}{3})$

Лемма 12. *Пусть n нечетно и $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$. Тогда $m_1(n,2) < 8 \cdot m_1(n-3,2)$.*

Доказательство. В силу предложений 2 и 3

$$m_1(n,2) = (2^{2^{t+1}} - 1)(2^a - 1)(2^b - 1),$$

где $t = p(n-3) - 2$, $a + b = n + 1 - 2^{t+1}$;

$$m_1(n-3,2) = (2^{2^{p+1}} - 1)(2^{n-2-2^{p+1}} - 1),$$

где $p = p\left(\frac{n-3}{3}\right)$.

В силу неравенств $2^{t+2} \leq n - 3 < 2^{t+3}$ и

$$2^{p+1} < 3 \cdot 2^p \leq n - 3 < 3 \cdot 2^{p+1} < 2^{p+3}$$

имеем два варианта: $p = t$ либо $p = t + 1$.

Пусть $p = t$. Необходимо показать, что $(2^a - 1)(2^b - 1) < 2^3(2^{n-2-2^{p+1}} - 1)$. Так как $a + b = n + 1 - 2^{t+1}$, это неравенство эквивалентно неравенству $2^a + 2^b > 2^3 + 1$. Из условия $n \notin \{9, 2^l - 1, 3 \cdot 2^l - 1\}$, $l \geq 1$, вытекает, что $n \geq 13$. Следовательно,

$$2^a + 2^b > 2^{a+1} \geq 2^{\frac{n-3}{2} - 2^t + 1} \geq 2^{\frac{n-3}{2} - \frac{n-3}{4} + 1} \geq 2^{\frac{7}{2}} > 2^3 + 1.$$

Пусть теперь $p = t + 1$. Необходимо показать, что $(2^a - 1)(2^b - 1) < 2^3(2^{2^p} + 1)(2^{n-2-2^{p+1}} - 1)$. В силу того, что $3 \cdot 2^p \leq n - 3$, выполнена цепочка неравенств

$$2^{2^p + 3} + 2^3 - 1 < 2^{2^p + 4} \leq 2^{n+1-2^{p+1}},$$

откуда следует, что

$$2^3(2^{2^p} + 1)(2^{n-2-2^{p+1}} - 1) = 2^{n+1-2^p} + 2^{n+1-2^{p+1}} - 2^{2^p+3} - 2^3$$
$$> 2^{n+1-2^p} - 1 = 2^{a+b} - 1 > (2^a - 1)(2^b - 1).$$

Предложение 5. *Таблица 2 верна.*

Доказательство. Для удобства разобъем числа из леммы 1 следующим образом.

1. $[2^{n_1} \pm 1, \ldots, 2^{n_s} \pm 1]$ для любых $s \geq 1$ и $n_1, n_2, \ldots, n_s > 0$ таких, что $n_1 + n_2 + \cdots + n_s = n$;

2. $2[2^{n_1} \pm 1, \ldots, 2^{n_s} \pm 1]$ для любых $s \geq 1$ и $n_1, n_2, \ldots, n_s > 0$ таких, что $n_1 + n_2 + \cdots + n_s = n - 1$;

3. $4[2^{n_1} \pm 1, \ldots, 2^{n_s} \pm 1]$ для любых $s \geq 1$ и $n_1, n_2, \ldots, n_s > 0$ таких, что $n_1 + n_2 + \cdots + n_s = n - 2$;

4. $2^k[2^{n_1} \pm 1, \ldots, 2^{n_s} \pm 1]$ для любых $s \geq 1$, $k \geq 3$ и $n_1, n_2, \ldots, n_s > 0$ таких, что $2^{k-2} + 1 + n_1 + n_2 + \cdots + n_s = n$;

5. 2^k, если $2^{k-2} + 1 = n$ для некоторого $k \geq 2$.

Нетрудно убедиться, что в любом пункте найдется число, большее числа из п. 5, тем самым этот пункт можно отбросить. Обозначим через $m_1^i(n,2)$ и $m_2^i(n,2)$ два наибольших элемента из i-го пункта. В силу леммы 8 элементы $m_1^i(n,2)$, $i = 1, \ldots, 4$, — это в точности числа $m_1(n,2)$, $2 \cdot m_1(n-1,2)$, $4 \cdot m_1(n-2,2)$, $8 \cdot m_1(n-3,2)$. Докажем, что $m_1(G)$ и $m_2(G)$ содержатся среди этих чисел. Для этого сначала будем искать среди них два наибольших, скажем, $m_1^i(n,2) > m_1^j(n,2)$, а затем показывать, что $m_1^j(n,2) > m_2^i(n,2)$.

1. Пусть $n = 3$. Тогда $m_1(n,2) = 15$, $2 \cdot m_1(n-1,2) = 10$, $4 \cdot m_1(n-2,2) = 12$, $8 \cdot m_1(n-3,2)$ не существует; $m_2^1(n,2) = 9$.

2. Пусть $n = 4$. Тогда $m_1(n,2) = 21$, $2 \cdot m_1(n-1,2) = 30$, $4 \cdot m_1(n-2,2) = 20$, $8 \cdot m_1(n-3,2) = 24$; $m_2^2(n,2) = 18$.

3. Пусть $n = 5$. Тогда $m_1(n,2) = 51$, $2 \cdot m_1(n-1,2) = 42$, $4 \cdot m_1(n-2,2) = 60$, $8 \cdot m_1(n-3,2) = 40$; $m_3^2(n,2) = 36$.

4. Пусть $n = 6$. Тогда $m_1(n,2) = 105$, $2 \cdot m_1(n-1,2) = 102$, $4 \cdot m_1(n-2,2) = 84$, $8 \cdot m_1(n-3,2) = 120$; $m_2^4(n,2) = 72$.

5. Пусть $n = 2^l - 1 \geq 7$. Если $n = 7$, то $m_1(n,2) = 255$, $2 \cdot m_1(n-1,2) = 210$, $4 \cdot m_1(n-2,2) = 204$, $8 \cdot m_1(n-3,2) = 168$. При этом $m_2^1(n,2) = 195$.

Пусть теперь $n \geq 15$. Из предложения 3 следует, что $m_1(n,2) = 2^{n+1} - 1$. Легко понять, что $2 \cdot m_1(n-1,2) < 2(2^n - 1) < m_1(n,2)$. По лемме 9 выполнено неравенство $8 \cdot m_1(n-3,2) < 2 \cdot m_1(n-1,2)$. Ввиду того, что $n - 2 \notin \{9, 2^k - 1, 3 \cdot 2^k - 1\}$, $k \geq 1$, применима лемма 10, и значит $4 \cdot m_1(n-2,2) < 8 \cdot m_1(n-3,2)$.

Выполнены равенства $p\left(\frac{n-1}{3}\right) = p\left(\frac{2^l-2}{3}\right) = l - 2$. В силу предложений 2 и 3

$$m_2^1(n,2) = m_2(n,2) = (2^{\frac{n+1}{4}} - 1)(2^{\frac{3n+3}{4}} + 1) < 2(2^{\frac{n+1}{2}} - 1)(2^{\frac{n-1}{2}} - 1) = 2 \cdot m_1(n-1,2).$$

6. Пусть $n = 2^l \geq 8$. Из предложения 3 следует, что $2 \cdot m_1(n-1,2) = 2(2^n - 1)$. Верны равенства $p\left(\frac{n}{3}\right) = p\left(\frac{2^l}{3}\right) = l - 2$, поэтому

$$m_1(n,2) = (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}+1} - 1) = 2^{n+1} - 3 \cdot 2^{\frac{n}{2}} + 1 < 2(2^n - 1).$$

По лемме 9 выполнено неравенство $4 \cdot m_1(n-2,2) < m_1(n,2)$. При $n \geq 16$ имеем $n - 3 \notin \{9, 2^k - 1, 3 \cdot 2^k - 1\}$, $k \geq 1$, и по лемме 11 справедливо неравенство $8 \cdot m_1(n-3,2) < 4 \cdot m_1(n-2,2)$. При $n = 8$

$$8 \cdot m_1(n-3,2) = 408 < 420 = 4 \cdot m_1(n-2,2).$$

В силу предложения 3

$$m_2^2(n,2) = 2 \cdot m_2(n-1,2) = 2(2^{\frac{n}{4}} - 1)(2^{\frac{3n}{4}} + 1) < (2^{\frac{n}{2}} - 1)(2^{\frac{n}{2}+1} - 1) = m_1(n,2).$$

7. Пусть $n = 2^l + 1 \geq 9$. Пусть сначала $n = 9$. В этом случае $m_1(n, 2) = 771$, $2 \cdot m_1(n-1, 2) = 930$, $4 \cdot m_1(n-2, 2) = 1020$, $8 \cdot m_1(n-3, 2) = 840$. При этом $m_2^3(n, 2) = 780$.

Пусть теперь $n \geq 17$. Из предложения 3 следует, что $4 \cdot m_1(n-2, 2) = 4(2^{n-1} - 1)$. Верны равенства $p\big(\frac{n-1}{3}\big) = p\big(\frac{2^l}{3}\big) = l - 2$, поэтому

$$2 \cdot m_1(n-1, 2) = 2(2^{\frac{n-1}{2}} - 1)(2^{\frac{n+1}{2}} - 1) < 4(2^{\frac{n-1}{2}} - 1)(2^{\frac{n-1}{2}} + 1) = 4 \cdot m_1(n-2, 2).$$

По лемме 9 выполнено неравенство $8 \cdot m_1(n-3, 2) < 2 \cdot m_1(n-1, 2)$. Ввиду того, что $n \notin \{9, 2^k - 1, 3 \cdot 2^k - 1\}$, $k \geq 1$, применима лемма 12 и, значит, $m_1(n, 2) < 8 \cdot m_1(n-3, 2)$.

В силу предложения 3

$$m_2^3(n, 2) = 4 \cdot m_2(n-2, 2) = 4(2^{\frac{n-1}{4}} - 1)(2^{\frac{3n-3}{4}} + 1)$$
$$< 2(2^{\frac{n-1}{2}} - 1)(2^{\frac{n+1}{2}} - 1) = 2 \cdot m_1(n-1, 2).$$

8. Пусть $n = 2^l + 2 \geq 10$. Из предложения 3 следует, что $8 \cdot m_1(n-3, 2) = 8(2^{n-2} - 1)$. Верны равенства $p\big(\frac{n}{3}\big) = p\big(\frac{2^l+2}{3}\big) = l - 2$, поэтому

$$m_1(n, 2) = (2^{\frac{n}{2}-1} - 1)(2^{\frac{n}{2}+2} - 1) = 2^{n+1} + 1 - 9 \cdot 2^{\frac{n}{2}-1} < 8(2^{n-2} - 1).$$

По лемме 9 выполнено неравенство $4 \cdot m_1(n-2, 2) < m_1(n, 2)$. При $n \geq 18$ имеем $n - 1 \notin \{9, 2^k - 1, 3 \cdot 2^k - 1\}$, $k \geq 1$, и по лемме 11 справедливо неравенство $2 \cdot m_1(n-1, 2) < m_1(n, 2)$. При $n = 10$

$$2 \cdot m_1(n-1, 2) = 1542 < 1905 = m_1(n, 2).$$

В силу предложения 3

$$m_2^4(n, 2) = 8 \cdot m_2(n-3, 2) = 8(2^{\frac{n-2}{4}} - 1)(2^{\frac{3n-6}{4}} + 1) < (2^{\frac{n}{2}-1} - 1)(2^{\frac{n}{2}+2} - 1) = m_1(n, 2).$$

9. Пусть $n = 3 \cdot 2^l - 1 \geq 11$. Тогда $m_1(n, 2) = (2^{\frac{n+1}{3}} - 1)(2^{\frac{2n+2}{3}} + 1)$. Верны равенства $p\big(\frac{n-1}{3}\big) = p\big(2^l - \frac{2}{3}\big) = l - 1$, поэтому

$$2 \cdot m_1(n-1, 2) = 2(2^{\frac{n+1}{3}} - 1)(2^{\frac{2n-1}{3}} - 1) < (2^{\frac{n+1}{3}} - 1)(2^{\frac{2n+2}{3}} + 1) = m_1(n, 2).$$

По лемме 9 выполнено неравенство $8 \cdot m_1(n-3, 2) < 2 \cdot m_1(n-1, 2)$. Ввиду того, что $n - 2 \notin \{9, 2^k - 1, 3 \cdot 2^k - 1\}$, $k \geq 1$, применима лемма 10, и значит, $4 \cdot m_1(n-2, 2) < 8 \cdot m_1(n-3, 2)$.

В силу предложения 3 при $n \geq 23$

$$m_2^1(n, 2) = m_2(n, 2) = (2^{\frac{n+1}{3}} - 1)(2^{\frac{n-2}{3}} - 1)(2^{\frac{n+4}{3}} - 1)$$
$$< 2(2^{\frac{n+1}{3}} - 1)(2^{\frac{2n-1}{3}} - 1) = 2 \cdot m_1(n-1, 2).$$

При $n = 11$

$$m_2^1(n, 2) = 3315 < 3570 = 2 \cdot m_1(n-1, 2).$$

10. Пусть $n = 3 \cdot 2^l \geq 12$. Тогда $2 \cdot m_1(n-1, 2) = 2(2^{\frac{n}{3}} - 1)(2^{\frac{2n}{3}} + 1)$. Верны равенства $p\big(\frac{n}{3}\big) = p(2^l) = l$, поэтому

$$m_1(n, 2) = (2^{\frac{2n}{3}} - 1)(2^{\frac{n}{3}+1} - 1) = (2^{\frac{n}{3}} - 1)(2^{\frac{n}{3}} + 1)(2^{\frac{n}{3}+1} - 1)$$
$$= (2^{\frac{n}{3}} - 1)(2^{\frac{2n}{3}+1} + 2^{\frac{n}{3}} - 1) > (2^{\frac{n}{3}} - 1)(2^{\frac{2n}{3}+1} + 2) = 2 \cdot m_1(n-1, 2).$$

Легко понять, что $p\left(\frac{n-2}{3}\right) = l-2$, поэтому $4 \cdot m_1(n-2,2) = 4(2^{\frac{n}{3}}-1)(2^{\frac{2n}{3}-1}-1)$. Неравенство $4 \cdot m_1(n-2,2) < 2 \cdot m_1(n-1,2)$ эквивалентно неравенству $2^{\frac{2n}{3}}-2 < 2^{\frac{2n}{3}}+1$, которое очевидно.

Пусть $n \geq 24$. Тогда $n-3 \notin \{9, 2^k-1, 3\cdot 2^k-1\}$, $k \geq 1$, поэтому $8 \cdot m_1(n-3,2) = (2^{2^{t+1}}-1)(2^a-1)(2^b-1)$, где $t = p(n-6)-2 = l-1$ и $a+b = n-2-2^{t+1}$, откуда

$$8 \cdot m_1(n-3,2) < 8(2^{\frac{n}{3}}-1)(2^{\frac{2n}{3}-2}-1) < 2(2^{\frac{n}{3}}-1)(2^{\frac{2n}{3}}+1) = 2 \cdot m_1(n-1,2).$$

При $n = 12$

$$8 \cdot m_1(n-3,2) = 6168 < 7710 = 2 \cdot m_1(n-1,2).$$

В силу предложения 2

$$m_2^1(n,2) = (2^{\frac{n}{3}}-1)(2^{\frac{2n}{3}+1}-1) < 2(2^{\frac{n}{3}}-1)(2^{\frac{2n}{3}}+1) = 2 \cdot m(n-1,2).$$

11. Пусть $n = 3 \cdot 2^l + 1 \geq 13$. Тогда $4m_1(n-2,2) = 4(2^{\frac{n-1}{3}}-1)(2^{\frac{2n-2}{3}}+1)$. Очевидно, что $p\left(\frac{n-1}{3}\right) = p(2^l) = l$, поэтому

$$2 \cdot m_1(n-1,2) = 2(2^{\frac{2n-2}{3}}-1)(2^{\frac{n+2}{3}}-1) > 4(2^{\frac{n-1}{3}}-1)(2^{\frac{2n-2}{3}}+1) = 4 \cdot m_1(n-2,2).$$

По лемме 9 выполнено неравенство $8 \cdot m_1(n-3,2) < 2 \cdot m_1(n-1,2)$. Ввиду того, что $n \notin \{9, 2^k-1, 3\cdot 2^k-1\}$, $k \geq 1$, применима лемма 12 и, значит, $m_1(n,2) < 8 \cdot m_1(n-3,2)$.

Аналогично предыдущему пункту получаем, что

$$m_2^2(n,2) = 2(2^{\frac{n-1}{3}}-1)(2^{\frac{2n+1}{3}}-1) < 4(2^{\frac{n-1}{3}}-1)(2^{\frac{2n-2}{3}}+1) = 4 \cdot m(n-2,2).$$

12. Пусть $n = 3 \cdot 2^l + 2 \geq 14$. По лемме 9 выполнено неравенство $4 \cdot m_1(n-2,2) < m_1(n,2)$. Легко понять, что $n-1 \notin \{9, 2^k-1, 3\cdot 2^k-1\}$, $k \geq 1$, поэтому по лемме 10 верно неравенство $2 \cdot m_1(n-1,2) < 4 \cdot m_1(n-2,2)$. Выполнены равенства $p\left(\frac{n-2}{3}\right) = p(2^l) = l$, поэтому $4 \cdot m_1(n-2,2) = 4(2^{\frac{2n-4}{3}}-1)(2^{\frac{n+1}{3}}-1)$. В силу предложения 3

$$8 \cdot m_1(n-3,2) = 8(2^{\frac{2n-4}{3}}+1)(2^{\frac{n-2}{3}}-1) < 4(2^{\frac{2n-4}{3}}-1)(2^{\frac{n+1}{3}}-1) = 4 \cdot m_1(n-2,2).$$

Ясно, что $p\left(\frac{n}{3}\right) = l$, поэтому ввиду предложения 2

$$m_2^1(n,2) = (2^{\frac{n-2}{3}}-1)(2^{\frac{2n+1}{3}}-1) < 4(2^{\frac{2n-4}{3}}-1)(2^{\frac{n+1}{3}}-1) = 4 \cdot m_1(n-2,2).$$

13. Пусть n нечетно и $n \notin \{2^l \pm 1, 3 \cdot 2^l \pm 1\}$, $l \geq 1$. Тогда из лемм 9, 10 и 12 следует, что наибольшие среди $m_1^i(n,2)$ суть числа $2 \cdot m_1(n-1,2) = 2(2^{2^{p+1}}-1)(2^{n-2^{p+1}}-1)$ и $8 \cdot m_1(n-3,2) = 8(2^{2^{p'+1}}-1)(2^{n-2^{p'+1}-2}-1)$, где $p = p\left(\frac{n-1}{3}\right)$ и $p' = p\left(\frac{n-3}{3}\right)$, причем первое число больше второго. Очевидно, что $p-1 \leq p' \leq p$. Предположим, что $p-1 = p'$. Но тогда $n = 3 \cdot 2^p + 1$; противоречие. Поэтому $p = p'$.

Далее, по предложению 2 имеем два случая. При $5 \cdot 2^p \leq n-1$ в силу неравенства $n - 2^{p+2} + 1 \leq 2^{p+1}$ получаем

$$\begin{aligned} m_2^2(n,2) &= 2(2^{2^{p+2}}-1)(2^{n-2^{p+2}}-1) \\ &= 2(2^{2^{p+1}}-1)(2^{n-2^{p+1}} + 2^{n-2^{p+2}} - 2^{2^{p+1}} - 1) \\ &< 8(2^{2^{p+1}}-1)(2^{n-2^{p+1}-2}-1) = 8 \cdot m_1(n-3,2). \end{aligned}$$

При $5 \cdot 2^p > n-1$ ввиду неравенства $n - 2^{p+1} \geq 2^p + 3$ имеем

$$\begin{aligned} 8 \cdot m_1(n-3,2) &= 8(2^{2^p}-1)(2^{2^p}+1)(2^{n-2^{p+1}-2}-1) \\ &= 2(2^{2^p}-1)(2^{n-2^p}+2^{n-2^{p+1}}-2^{2^p+2}-4) \\ &> 2(2^{2^p}-1)(2^{n-2^p}-1) = m_2^2(n,2). \end{aligned}$$

14. Пусть n четно и $n \notin \{2^l, 2^l+2, 3\cdot 2^l, 3\cdot 2^l+2\}$, $l \geq 1$. Тогда из лемм 9, 10 и 11 следует, что наибольшими среди $m_1^i(n,2)$ являются числа $m_1(n,2) = (2^{2^{p+1}}-1)(2^{n+1-2^{p+1}}-1)$ и $4 \cdot m_1(n-2,2) = 4(2^{2^{p'+1}}-1)(2^{n-1-2^{p'+1}}-1)$, где $p = p\big(\frac{n}{3}\big)$ и $p' = p\big(\frac{n-2}{3}\big)$. Дальнейшее доказательство повторяет предыдущий пункт с заменой $n-1$ на n.

§ 3. Доказательство теоремы 1

Для доказательства теоремы будем использовать подход, применяемый в [1], а именно разбивать множество $\mathscr{C}$ простых групп лиева типа на классы в зависимости от свойств двух максимальных порядков элементов:

$$\mathscr{C}_1 := \{G \in \mathscr{C} \mid m_1 - m_2 > (m_1,m_2)^2 > 1\},$$

$$\mathscr{C}_2 := \{G \in \mathscr{C} \mid (m_1,m_2)^2 \geq m_1 - m_2 > (m_1,m_2) > 1\},$$

$$\mathscr{C}_3 := \{G \in \mathscr{C} \mid m_1 - m_2 = (m_1,m_2) > 1\},$$

$$\mathscr{C}_4 := \{G \in \mathscr{C} \mid (m_1,m_2) = 1,\ m_1 \leq (m_1-m_2)^{3/2}\},$$

$$\mathscr{C}_5 := \{G \in \mathscr{C} \mid (m_1,m_2) = 1,\ m_1 > (m_1-m_2)^{3/2}\}.$$

Будем также использовать числа $a_0, a_1, \dots$ из разложений чисел $m_1/(m_1-m_2)$ в цепную дробь

$$\frac{m_1}{m_1-m_2} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots}}}.$$

Замечание. В [1] из рассмотрения исключено некоторое конечное множество групп $\mathscr{S}_0$, поэтому, строго говоря, $\mathscr{C}$ не является множеством всех простых групп лиева типа. Однако доказано, что для всех $G \in \mathscr{S}_0$ теорема верна, т. е. не существует простой группы лиева типа $H \not\simeq G$ (включая характеристику 2) такой, что $m_1(G) = m_1(H)$, $m_2(G) = m_2(H)$ и $\mathrm{ch}(G) \neq \mathrm{ch}(H)$. Таким образом, перечисляя группы какого-либо класса $\mathscr{C}_i$, либо его подкласса $\mathscr{C}_{ij}$, будем рассматривать лишь те группы, которые не содержатся в $\mathscr{S}_0$.

Напомним, что $G = \mathrm{Sp}_{2n}(q)$, где $q = 2^k$ и H — простая группа лиева типа такая, что $m_1(G) = m_1(H)$ и $m_2(G) = m_2(H)$. Предположим, что число $\mathrm{ch}(H)$ нечетно. Ввиду существенных различий в формулах наибольших порядков для $q=2$ и $q>2$ будем рассматривать эти два случая раздельно.

Случай 1: $q > 2$. В этом случае оба числа $m_1(G)$ и $m_2(G)$ нечетны. Простые группы лиева типа над полями нечетных характеристик с нечетными m_1 и m_2 перечислены в табл. 3. Максимальные порядки элементов, а также

Таблица 3

H	Условия на H	$m_1(H)$	$m_2(H)$	$\mathscr{C}_i$
$\mathrm{PSL}_2(u)$	u простое, $u \equiv 1 \,(\mathrm{mod}\, 4)$	u	$\frac{u+1}{2}$	$\mathscr{C}_4$
$\mathrm{PSL}_{4k}(u)$	$k \geq 1$, $(4k)_{\{2\}} = (u-1)_{\{2\}}$	$\frac{u^{4k}-1}{(u-1)(u-1,4k)}$	$\frac{(u^{2k+1}-1)(u^{2k-1}-1)}{(u-1)(u-1,4k)}$	$\mathscr{C}_5$
$\mathrm{PSU}_4(u)$	u составное, $u \equiv 3 \,(\mathrm{mod}\, 4)$	$\frac{u^3+1}{4}$	$\frac{(u-1)(u^2+1)}{4}$	$\mathscr{C}_5$
$\mathrm{PSU}_{2k}(u)$	$k \geq 4$, u сост., $u+1 \nmid 2k$ $(2k)_{\{2\}} = (u+1)_{\{2\}}$	$\frac{u^{2k-1}+1}{(u+1,2k)}$	$\frac{(u^{a(2k)}+1)(u^{2k-a(2k)}+1)}{(u+1)(u+1,2k)}$	$\mathscr{C}_1$
$\mathrm{P}\Omega^+_{2k}(u)$	$k \in \{5,7,9\}$, u сост., $u \equiv 1 \,(\mathrm{mod}\, 4)$	$\frac{(u^{k-1}+1)(u+1)}{4}$	$\frac{(u^2+1)(u^{k-2}+1)}{4}$	$\mathscr{C}_1$
$\mathrm{P}\Omega^-_{10}(u)$	$3 < u \equiv 3 \,(\mathrm{mod}\, 4)$	$\frac{(u^2+1)(u^3-1)}{4}$	$\frac{q^5+1}{4}$	$\mathscr{C}_5$
${}^2\mathrm{G}_2(3)'$		9	7	

принадлежность классам $\mathscr{C}_i$ взяты из [1]. Через $a(n)$ обозначается наименьшее нечетное целое число $a \geq 3$ такое, что $(a, n-a) = 1$.

Предположим, что $n = 2$. Очевидно, что $(m_1, m_2) = 1$ и $m_1^2 = (q^2+1)^2 \geq 17^2 > 8 = (m_1 - m_2)^3$. Значит, $G \in \mathscr{C}_5$, и, следовательно, $H \in \{\mathrm{PSL}_{4k}(u), \mathrm{PSU}_4(u), \mathrm{P}\Omega^-_{10}(u)\}$. Воспользуемся тем, что $m_1 - m_2 = 2$.

Пусть $H = \mathrm{PSL}_{4k}(u)$. Тогда

$$2 = \frac{u^{4k}-1}{(u-1)(u-1,4k)} - \frac{(u^{2k+1}-1)(u^{2k-1}-1)}{(u-1)(u-1,4k)} = \frac{u^{2k+1}+u^{2k-1}-2}{(u-1)(u-1,4k)} \geq u;$$

противоречие.

Пусть $H = \mathrm{PSU}_4(u)$. Тогда $(u^3+1)/4 - (u-1)(u^2+1)/4 = 2$, откуда $u = 3$; противоречие.

Пусть $H = \mathrm{P}\Omega^-_{10}(u)$. Тогда $(u^2+1)(u^3-1)/4 - (u^5+1)/4 = 2$, откуда $u^2(u-1) = 10$; противоречие.

Предположим, что $n = 4$. По лемме 2 имеем $(m_1, m_2) = 1$. При $q \geq 4$ верно неравенство $m_1^2 = (q+1)^2(q^3-1)^2 < (q^3-q-2)^3 = (m_1-m_2)^3$. Следовательно, $G \in \mathscr{C}_4$, и, значит, $H = \mathrm{PSL}_2(u)$. Но в этом случае $m_1(H) = u$ простое, чего не может быть, так как $m_1(G) = (q+1)(q^3-1)$.

Предположим, что $n > 4$ четно, и пусть $p = p(n/3)$.

Пусть сначала $n \geq 5 \cdot 2^p$. Тогда $(m_1, m_2) = q^{2^{p+1}} - 1$ и

$$m_1 - m_2 = (q^{2^{p+1}} - q^{n-2^{p+2}+1})(q^{2^{p+1}}-1)/(q-1) \leq (q^{2^{p+1}}-1)^2/(q-1) < (m_1, m_2)^2,$$

значит, в этом случае $G \in \mathscr{C}_2$ и подходящей группы H не существует; противоречие.

Пусть теперь $n < 5 \cdot 2^p$. Тогда $(m_1, m_2) = q^{2^p} - 1$ и

$$m_1 - m_2 = (q^{n-2^{p+1}+1} - q^{2^p})(q^{2^p}-1)/(q-1) \geq q^{2^p}(q^{2^p}-1) > (m_1, m_2)^2,$$

значит, $G \in \mathscr{C}_1$. Следовательно, $H \in \{\mathrm{PSU}_{2k}(u), \mathrm{P}\Omega^+_{2k}(u)\}$.

Рассмотрим число

$$\frac{m_1}{m_1 - m_2} = 1 + \frac{q^{n-2^p+1}-1}{q^{n-2^{p+1}+1} - q^{2^p}}.$$

Из леммы 4 следует, что $a_0 \equiv 2 \,(\mathrm{mod}\, 4)$, если $n = 3 \cdot 2^p$, и $a_0 \equiv 1 \,(\mathrm{mod}\, 4)$, если $n > 3 \cdot 2^p$.

Пусть $H = \mathrm{PSU}_{2k}(u)$. Тогда

$$\frac{m_1}{m_1 - m_2} = \frac{(u^{2k-1}+1)(u+1)}{u^{2k-1} - u^{2k-a(2k)} - u^{a(2k)} + u} = u + 1 + \frac{(u^{2k-a(2k)} + u^{a(2k)} - u + 1)(u+1)}{u^{2k-1} - u^{2k-a(2k)} - u^{a(2k)} + u}.$$

Нетрудно убедиться, что $m_1/(m_1 - m_2) - (u+1) < 1$. Значит, $a_0 = u+1$, и, в частности, a_0 четно. Следовательно, $n = 3\cdot 2^p$, откуда $(m_1 - m_2)/(m_1, m_2) = q^{2^p}$. С другой стороны, $(m_1 - m_2)/(m_1, m_2)$ делится на u; противоречие.

Пусть $H = \mathrm{P}\Omega^+_{2k}(u)$. Тогда

$$\frac{m_1}{m_1 - m_2} = \frac{u^k + u^{k-1} + u + 1}{u^{k-1} - u^{k-2} - u^2 + u} = u + 2 + \frac{2u^{k-2} + u^3 + u^2 - u + 1}{u^{k-1} - u^{k-2} - u^2 + u}.$$

При $u \geq 9$ верно неравенство $m_1/(m_1 - m_2) - (u+2) < 1$, значит, $a_0 = u + 2 \equiv 3 \pmod 4$; противоречие.

Предположим, что $n > 1$ нечетно. Тогда $(m_1, m_2) > 1$, значит, $H \in \{\mathrm{PSU}_{2k}(u), \mathrm{P}\Omega^+_{2k}(u)\}$. Более того, из предложения 1 следует, что $m_1/(m_1, m_2) = q^{2^{p(n)}} + 1$.

Пусть $H = \mathrm{PSU}_{2k}(u)$. Покажем сначала, что $(2k - a(2k), 2k-1) = 1$. Предположим, что найдется $b > 1$ такое, что $b \mid 2k-1$ и $b \mid 2k - a(2k)$. Но тогда $b \mid a(2k) - 1$ и $(b, 2k - b) = 1$; противоречие с минимальностью $a(2k)$. Теперь рассмотрим число (m_1, m_2):

$$(m_1, m_2) = \left(\frac{u^{2k-1}+1}{(u+1, 2k)}, \frac{(u^{a(2k)}+1)(u^{2k-a(2k)}+1)}{(u+1)(u+1, 2k)}\right) = \frac{(u^{2k-1}+1, u^{a(2k)}+1)}{(u+1, 2k)} = \frac{u^{(2k-1, a(2k))}+1}{(u+1, 2k)}.$$

Следовательно, $m_1/(m_1, m_2) = (u^{2k-1}+1)/(u^{(2k-1, a(2k))}+1)$, и, значит, число $\frac{m_1}{(m_1, m_2)} - 1$ делится на u. С другой стороны, оно должно быть степенью числа 2; противоречие.

Пусть $H = \mathrm{P}\Omega^+_{10}(u)$. Тогда $m_1/(m_1, m_2) = (u^4+1)/2$, откуда $u^4 - q^{2^{p(n)}+1} = 1$; противоречие с леммой 3.

Пусть $H = \mathrm{P}\Omega^+_{14}(u)$. Тогда $m_1/(m_1, m_2) = u^4 + u^2 + 1$, откуда $u^2(u^2+1) = q^{2^{p(n)}}$, чего не может быть.

Пусть $H = \mathrm{P}\Omega^+_{18}(u)$. Тогда $m_1/(m_1, m_2) = (u^8+1)/2$, откуда $u^8 - q^{2^{p(n)}+1} = 1$; противоречие.

Таким образом, закончили доказательство для случая $q > 2$.

Случай 2: $q = 2$. В [1] посчитано, что для $n \leq 18$ группы H с требуемыми свойствами не существует (см. [1, факт 1.1]), поэтому случаи $n = 3, 4, 5, 6$ из рассмотрения можно исключить. В табл. 4 приведены значения (m_1, m_2) и $(m_1 - m_2)/(m_1, m_2)$ для всех остальных простых симплектических групп над полем порядка 2.

Все эти группы лежат в классе $\mathscr{C}_2$, который разбивается на следующие подклассы:

$$\mathscr{C}_{21} := \{G \in \mathscr{C}_2 \mid a_1 > a_0\}, \quad \mathscr{C}_{22} := \{G \in \mathscr{C}_2 \mid (m_1, m_2) = 4\},$$

$$\mathscr{C}_{23} := \{G \in \mathscr{C}_2 \mid 2a_0 - r = 1\}, \quad \mathscr{C}_{24} := \{G \in \mathscr{C}_2 \mid 2a_0 - r = 3\},$$

Таблица 4. Свойства чисел $m_1(G)$ и $m_2(G)$ для групп $G = Sp_{2n}(2)$ при $n \geq 7$

n	(m_1, m_2)	$(m_1 - m_2)/(m_1, m_2)$
$2^l - 1 \geq 7$	$2^{\frac{n+1}{2}} - 1$	3
$2^l \geq 8$	$2^{\frac{n}{2}} - 1$	3
$2^l + 1 \geq 9$	$2(2^{\frac{n-1}{2}} - 1)$	3
$2^l + 2 \geq 10$	$2^{\frac{n-2}{2}} - 1$	9
$3 \cdot 2^l - 1 \geq 11$	$2^{\frac{n+1}{3}} - 1$	3
$3 \cdot 2^l \geq 12$	$2^{\frac{n}{3}} - 1$	$2^{\frac{n}{3}} - 3$
$3 \cdot 2^l + 1 \geq 13$	$2(2^{\frac{n-1}{3}} - 1)$	$2^{\frac{n-1}{3}} - 3$
$3 \cdot 2^l + 2 \geq 14$	$2^{\frac{2n-4}{3}} - 1$	3
n нечетно, $n \notin \{2^l \pm 1, 3 \cdot 2^l \pm 1\}$	$2(2^{2^{p+1}} - 1)$, $p = p(\frac{n-1}{3})$	3
n четно, $n \notin \{2^l, 2^l + 2, 3 \cdot 2^l, 3 \cdot 2^l + 2\}$	$2(2^{2^{p+1}} - 1)$, $p = p(\frac{n}{3})$	3

$$\mathscr{C}_{25} := \{G \in \mathscr{C}_2 \mid (m_1, m_2) \neq 4,\ 2 \leq a_0/a_1 < 4\}, \quad \mathscr{C}_{26} := \mathscr{C}_2 \setminus \bigcup_{i=1}^{5} \mathscr{C}_{2i},$$

где $r = 2(m_1 - m_2)/(m_1, m_2) - 1$.

Нетрудно убедиться, что для всех этих групп выполняется неравенство $a_0 > (m_1 - m_2)/(m_1, m_2) + 1$, откуда следует, что ни одна из этих групп не лежит ни в $\mathscr{C}_{23}$, ни в $\mathscr{C}_{24}$. Кроме того, очевидно, что ни одна из них не лежит в $\mathscr{C}_{22}$. Также заметим, что $(m_1, m_2) \geq 15$.

Таблица 5

H	Условия на H	$m_1(H)$	$m_2(H)$
$PSU_{15}(u)$	u сост.	$\frac{(u^7-1)(u^7+1)}{(u+1,15)}$	$\frac{(u^7+1)(u^8-1)}{(u+1)(u+1,15)}$
$P\Omega_{26}^-(u)$	u сост., $u \equiv 3 \pmod 4$	$\frac{(u+1)(u^4+1)(u^8+1)}{4}$	$\frac{(u^2+1)(u^3+1)(u^8+1)}{4}$
$P\Omega_{7\cdot 2^{l+1}+2}^-(u)$	u сост., $u \equiv 3 \pmod 4$	$\frac{(u+1)(u^{2^l}+1)(u^{3\cdot 2^{l+1}}+1)}{4}$	$\frac{(u+1)(u^{2^{l+1}}+1)(u^{5\cdot 2^l}+1)}{4}$
$F_4(u)$	u пр.	$u(u+1)(u^2+1)$	$(u^3-1)(u+1)$
$\Omega_{4k+3}(u)$	$k \geq 2$, $u \geq 5$ пр.	$\frac{(u^{2k}+1)(u+1)}{2}$	$\frac{u(u+1)(u^{2k-1}-1)}{2}$
$\Omega_{4k+1}(u)$	$k \geq 2$, $u \geq 5$ пр.	$\frac{u(u+1)(u^{2k-2}+1)}{2}$	$\frac{(u^{2k-1}-1)(u+1)}{2}$
$P\Omega_{4k+2}^+(u)$	$k \geq 2$, $u \geq 5$ пр.	$\frac{(u^{2k}+1)(u+1)}{(u-1,4)}$	$\frac{u(u+1)(u^{2k-1}-1)}{(u-1,4)}$
$P\Omega_{8k}^+(u)$	$k \geq 2$, u пр.	$\frac{u(u+1)(u^2+1)(u^{4k-4}+1)}{4}$	$\frac{(u+1)(u^2+1)(u^{4k-3}-1)}{4}$
$P\Omega_{8k}^-(u)$	$u \geq 5$ пр.	$\frac{u(u+1)(u^{4k-2}+1)}{2}$	$\frac{(u+1)(u^{4k-1}-1)}{2}$
$P\Omega_{8k+6}^-(u)$	$u \equiv 3 \pmod 4$ пр.	$\frac{(u+1)(u^2+1)(u^{4k}+1)}{4}$	$\frac{u(u+1)(u^2+1)(u^{4k-1}-1)}{4}$

Простые группы лиева типа над полями нечетных характеристик, лежащие в классах $\mathscr{C}_{21}$, $\mathscr{C}_{25}$ и $\mathscr{C}_{26}$, перечислены в табл. 5.

Пусть $H \simeq PSU_{15}(u)$. Тогда $(m_1 - m_2)/(m_1, m_2) = u(u^6 - 1)/(u - 1)$ четно; противоречие.

Пусть $H \simeq P\Omega_{26}^-(u)$. Тогда $(m_1 - m_2)/(m_1, m_2) = u(u - 1)^2/2$ четно; противоречие.

Пусть $H \simeq P\Omega^-_{7\cdot 2^{l+1}+2}(u)$. Тогда $(m_1 - m_2)/(m_1, m_2) = q^{2^l}(q^{2^l} - 1)^2$ четно; противоречие.

Все остальные группы лежат в классе $\mathscr{C}_{26}$, значит, для них $(m_1 - m_2)/(m_1, m_2) = (u + 1)/2$ (см. [1, предложение 3.3]). Это число должно быть нечетным, поэтому $u \equiv 1 \pmod 4$. Следовательно, $H \not\simeq P\Omega^-_{8k+6}(u)$.

Пусть $H \simeq F_4(u)$. Тогда $(m_1, m_2) = 2(u + 1)$ делится на 4, чего не может быть.

Пусть $H \in \{\Omega_{4k+3}(u), \Omega_{4k+1}(u), P\Omega^-_{8k}(u)\}$. Тогда $(m_1, m_2) = u + 1 = 2(m_1 - m_2)/(m_1, m_2)$, что невозможно.

Пусть $H \simeq P\Omega^+_{4k+2}(u)$. Тогда (m_1, m_2) равно $u + 1$ либо $(u + 1)/2$ и $(m_1 - m_2)/(m_1, m_2) = (u+1)/2$, откуда $(m_1, m_2) = 2(m_1 - m_2)/(m_1, m_2)$, либо $(m_1, m_2) = (m_1 - m_2)/(m_1, m_2)$. Оба случая невозможны.

Пусть $H \simeq P\Omega^+_{8k}(u)$. Тогда $(m_1, m_2) = (u + 1)(u^2 + 1)/2$ четно и $(m_1 - m_2)/(m_1, m_2) = (u + 1)/2$. Возможны следующие случаи.

1. $(m_1 - m_2)/(m_1, m_2) = 3$, откуда $u = 5$ и $(m_1, m_2) = 78$. Но число $(m_1, m_2)/2 + 1$ должно являться степенью двойки; противоречие.

2. $(m_1 - m_2)/(m_1, m_2) = (m_1, m_2)/2 - 2$, т. е. $(u+1)/2 = (u+1)(u^2+1)/4 - 2$, чего не может быть.

Теорема доказана.

ЛИТЕРАТУРА

1. *Kantor W. M., Seress A.* Large element orders and the characteristic of Lie-type simple groups // J. Algebra. 2009. V. 322, N 3. P. 802–832.
2. *Бутурлакин А. А.* Спектры конечных симплектических и ортогональных групп // Мат. тр. 2010. Т. 13, № 2. С. 33–83.
3. *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7. P. 81–97.
4. *Gerono G. C.* Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n + 1$ // Nouv. Ann. Math. (2). 1870. V. 9. P. 469–471.

Статья поступила 31 октября 2012 г.

Лыткин Даниил Всеволодович
Новосибирский гос. университет,
ул. Пирогова, 2, Новосибирск 630090
dan.lytkin@gmail.com