УДК 519.61+512.552.7 DOI: 10.14529/cmse150107

ВЫЧИСЛЕНИЕ РАНГОВ ГРУПП ЦЕНТРАЛЬНЫХ ЕДИНИЦ ЦЕЛОЧИСЛЕННЫХ ГРУППОВЫХ КОЛЕЦ КОНЕЧНЫХ ГРУПП

Р.Ж. Алеев, Н.А. Цыбина

Изучение центральных единиц (центральных обратимых элементов) целочисленных групповых колец конечных групп почти всегда приводит к трудоемким вычислениям, как в случае нахождения отдельных центральных единиц, так и при описании групп центральных единиц. В силу того, что периодическая часть групп тривиальна (с точностью до знака это элементы центра группы), более интересно нахождение сведений о части без кручения, которая является прямым произведением бесконечных циклических групп. Число таких бесконечных прямых сомножителей — ранг группы центральных единиц. Поэтому ранги групп центральных единиц целочисленных групповых колец конечных групп — одна из важнейших характеристик таких групп. Поэтому вычисление рангов групп центральных единиц представляет большой интерес при изучении групп центральных единиц. В работе приведены формулы для вычисления рангов в общем случае и в нескольких важнейших частных случаях. На основании этих формул произведены вычисления рангов в достаточно широких диапазонах. Для вычислений использовалась система компьютерной алгебры GAP. Результаты вычислений показываются в таблицах и на графике.

Ключевые слова: характер группы, центральная единица, ранг абелевой группы, система GAP.

Введение

В России (и ранее в СССР) работы по вычислительным аспектам алгебры и теории чисел не часты. Авторы не могут надеяться, что данная статья заполнит образовавшуюся лакуну, но могут надеяться, что возникнет интерес к подобным направлениям исследований.

В 2014 г. исполнилось ровно 25 лет, как первый из авторов начал заниматься центральными единицами целочисленных групповых колец. Почти с самого начала стало ясно, что это направление исследований часто приводит к таким вычислениям, которые невозможно проделать вручную, и приходилось их выполнять на компьютерах. В дальнейшем неоднократно производились различные вычисления по данной тематике, некоторые из которых вошли, как существенная часть в [2].

Далее под *центральной единицей* будет всегда (если не оговорено противное) пониматься *центральная единица (центральный обратимый элемент)* целочисленного группового кольца конечной группы. Среди задач, связанных с центральными единицами выделим задачу об нахождении рангов групп центральных единиц. Напомним, что под *рангом* конечнопорожденной абелевой группы понимается число бесконечных прямых сомножителей при разложении группы в прямое произведение циклических подгрупп. Группы центральных единиц конечнопорождены, поэтому ранг является важной необходимой характеристикой группы центральных единиц, так как периодическая часть всегда тривиальна (равна $\langle -1 \rangle \times Z(G)$) [10].

В этой работе будем рассматривать вопросы, связанные с вычислениями рангов групп центральных единиц. Статья организована следующим образом. В первом разделе приводятся формулы для вычисления рангов групп центральных единиц, как общие так и для

отдельных классов конечных групп. Во втором разделе приводятся результаты вычислений рангов в виде таблиц и графика и их анализ. Следует отметить, что невозможно привести полные результаты вычислений в связи с их экстремально большим объемами. В заключении приведена краткая сводка полученных результатов и указаны направления будущих исследований.

1. Формулы для вычисления рангов групп центральных единиц

Обозначения. *Будем придерживаться следующих обозначений.*

1) *Зафиксируем конечную группу* G.
2) *Пусть* χ — *характер группы* G. *Тогда:*
   а) $\deg\chi$ — *его степень,*
   б) $\mathbb{Q}(\chi)$ — *поле характера* χ,
   в) $d_\chi = [\mathbb{Q}(\chi):\mathbb{Q}]$ — *степень* $\mathbb{Q}(\chi)$ *над* $\mathbb{Q}$,
   г) I_χ — *множество всех характеров алгебраически сопряженных с* χ.
3) I_G — *множество представителей классов алгебраически сопряженных неприводимых характеров.*
4) $I_{\mathbb{R}} = \{\chi \in I_G \mid \mathbb{Q}(\chi) \subset \mathbb{R}\}$.
5) $I_{\mathbb{C}} = \{\chi \in I_G \mid \mathbb{Q}(\chi) \not\subseteq \mathbb{R}\}$.

Отсюда

$$I_G = I_{\mathbb{R}} \cup I_{\mathbb{C}},\ I_{\mathbb{R}} \cap I_{\mathbb{C}} = \varnothing.$$

Следующий результат получен в [10].

Лемма 1. При введенных выше обозначениях для конечной группы G:

1) группа единиц кольца целых центра рациональной групповой алгебры изоморфна прямому произведению групп единиц колец целых полей $\mathbb{Q}(\chi)$ для всех $\chi \in I_G$;
2) группа центральных единиц целочисленного группового кольца и группа единиц кольца целых центра рациональной групповой алгебры имеют одинаковые ранги.

Как следствие, из этой леммы легко получается следующий результат.

Лемма 2. [формула для рангов] Ранг центральных единиц целочисленного группового кольца равен

$$\sum_{\chi\in I_{\mathbb{R}}} d_\chi + \frac{1}{2}\sum_{\chi\in I_{\mathbb{C}}} d_\chi - |I_G|.$$

Это утверждение приведено в [2, с. 152, следствие 3.1] и нигде не опубликовано, поскольку считалось тривиальным.

На основе этой формулы были проведены вычисления рангов для всех групп, представленных в GAP [14] таблицами характеров (на 2000 г.), и это было в [2, Приложение Г.1, с. 323–336], но нигде не анонсировалось и не публиковалось.

1) Число таблиц характеров — 998.
2) Полученные значения рангов (записаны списком в виде пар, где первый элемент — значение ранга, а второй — число групп с данным значением ранга):

```
[ [ 0, 336 ], [ 1, 135 ], [ 2, 108 ], [ 3, 69 ],  [ 4, 65 ],
  [ 5, 40 ], [ 6, 42 ], [ 7, 20 ], [ 8, 27 ],  [ 9, 20 ],
```

```
[ 10, 11 ], [ 11, 14 ], [ 12, 4 ],  [ 13, 12 ], [ 14, 11 ],
[ 15, 11 ], [ 16, 8 ],  [ 17, 2 ], [ 18, 3 ], [ 19, 10 ],
[ 20, 7 ], [ 21, 1 ],  [ 22, 1 ], [ 23, 3 ], [ 24, 1 ],
[ 25, 1 ], [ 27, 6 ],  [ 28, 2 ], [ 29, 2 ], [ 31, 1 ],
[ 32, 4 ], [ 34, 2 ],  [ 35, 3 ], [ 36, 2 ], [ 40, 3 ],
[ 42, 2 ], [ 43, 1 ],  [ 45, 1 ], [ 59, 1 ], [ 69, 2 ],
[ 79, 1 ], [ 94, 1 ],  [ 126, 1 ], [ 146, 1 ] ]
```

Позднее были найдены (с помощью В.Д. Мазурова) статьи [11] и [13], в которых были другие формулы для рангов.

Лемма 3. Пусть G — конечная группа и r — число классов сопряженности группы G (равносильно число неприводимых комплексных характеров). Тогда

$$r = \sum_{\chi \in I_G} d_\chi.$$

Доказательство. Так как сопряженных с χ точно d_χ, то $r = \sum_{\chi \in I_G} d_\chi$. □

Определение 1. Элементы $a, b \in G$ называются $\mathbb{Q}$-*сопряженными,* если существует такой $x \in G$, что $x^{-1}bx = a^s$, где $(s, |G|) = 1$.

Определение 2. $\mathbb{Q}$-*класс* с представителем a назовем множество $\{a^G\}_\mathbb{Q}$ всех $\mathbb{Q}$-сопряженных с a, то есть

$$\{a^G\}_\mathbb{Q} = \bigcup_{s=1(s,|G|)=1}^{|a|-1} \left\{(a^s)^G\right\}.$$

Обозначение. *Число $\mathbb{Q}$-классов группы G обозначим через $n_\mathbb{Q}$.*

Лемма 4. Пусть G — конечная группа. Тогда $n_\mathbb{Q} = |I_G|$.

Доказательство. Так каждая орбита при действии $\mathrm{Gal}(\mathbb{Q}(\chi))$ дает одну простую компоненту $Z(\mathbb{Q}G)$, то из теоремы Бермана–Витта [8, с. 265, 287] сразу следует $n_\mathbb{Q} = |I_G|$. □

Определение 3. Элементы $a, b \in G$ называются $\mathbb{R}$-*сопряженными,* если существует такой $x \in G$, что $x^{-1}bx = a^{\pm 1}$.

Определение 4. $\mathbb{R}$-*класс* с представителем a назовем множество $\{a^G\}_\mathbb{R}$ всех $\mathbb{R}$-сопряженных с a, то есть

$$\{a^G\}_\mathbb{R} = \{a^G\} \cup \{(a^{-1})^G\}.$$

Обозначение. *Число $\mathbb{R}$-классов группы G обозначим через $n_\mathbb{R}$.*

Определение 5. Класс сопряженности a^G называется *действительным = вещественным* классом, если $a^{-1} \in \{a^G\}$.

Обозначение. *Число действительных классов группы G обозначим через $h_\mathbb{R}$.*

Определение 6. Характер χ называется *действительным = вещественным*, если поле характера $\mathbb{Q}(\chi) \subset \mathbb{R}$.

Лемма 5.

1) $h_{\mathbb{R}} = \sum_{\chi \in I_{\mathbb{R}}} d_\chi$,
2) если c число классов сопряженности $\{a^G\}$ с условием $\{a^G\} \neq \{(a^{-1})^G\}$, то

$$\begin{cases} r = h_{\mathbb{R}} + 2c \\ n_{\mathbb{R}} = h_{\mathbb{R}} + c \end{cases}.$$

Доказательство. Так как сопряженных с χ точно d_χ, то $h_{\mathbb{R}} = \sum_{\chi \in I_{\mathbb{R}}} d_\chi$.

Используя лемму 3 и первое утверждение, получим второе. □

Обозначение. *Обозначим через $r_{\mathbb{Z}}$ ранг группы центральных единиц целочисленного группового кольца группы G.*

Теперь по лемме 2

$$r_{\mathbb{Z}} = \sum_{\chi \in I_{\mathbb{R}}} d_\chi + \frac{1}{2} \sum_{\chi \in I_{\mathbb{C}}} d_\chi - |I_G|.$$

Отсюда, очевидно, имеем:

$$r_{\mathbb{Z}} = \frac{1}{2} \sum_{\chi \in I_G} d_\chi + \frac{1}{2} \sum_{\chi \in I_{\mathbb{R}}} d_\chi - |I_G|.$$

Подставляя в приведенную выше формулу значения

$$\sum_{\chi \in I_G} d_\chi, \ \sum_{\chi \in I_{\mathbb{R}}} d_\chi, \ |I_G|$$

из лемм 3, 4 и 5, мы получим

$$r_{\mathbb{Z}} = \frac{1}{2} r + \frac{1}{2} h_{\mathbb{R}} - n_{\mathbb{Q}} = \frac{1}{2} \left(r + h_{\mathbb{R}} - 2n_{\mathbb{Q}} \right).$$

Это и есть формула Риттера и Сегала из [13].

Из системы в лемме 5 имеем

$$c = r - n_{\mathbb{R}}, \ h_{\mathbb{R}} = n_{\mathbb{R}} - c = n_{\mathbb{R}} - r + n_{\mathbb{R}} = 2n_{\mathbb{R}} - r.$$

Подставим выражение для $h_{\mathbb{R}}$ в формулу Риттера и Сегала и получим

$$r_{\mathbb{Z}} = \frac{1}{2} \left(r + 2n_{\mathbb{R}} - r - 2n_{\mathbb{Q}} \right) = n_{\mathbb{R}} - n_{\mathbb{Q}}.$$

Это и есть формула Ферраза [11].

Замечание 1. Таким образом, формулы из [11] и [13] достаточно просто выводятся из леммы 2.

Подведем итог в виде теоремы.

Теорема. *Пусть G — конечная группа. При сохранении введенных ранее обозначений ранг группы центральных единиц целочисленного группового кольца группы G может вычислен по одной из следующих формул:*

1) $\sum\limits_{\chi\in I_{\mathbb{R}}} d_\chi + \frac{1}{2}\sum\limits_{\chi\in I_{\mathbb{C}}} d_\chi - |I_G| = \frac{1}{2}\sum\limits_{\chi\in I_G} d_\chi + \frac{1}{2}\sum\limits_{\chi\in I_{\mathbb{R}}} d_\chi - |I_G|,$ (формула из [2])

2) $n_{\mathbb{R}} - n_{\mathbb{Q}},$ (формула из [11])

3) $\frac{1}{2}\left(r + h_{\mathbb{R}} - 2n_{\mathbb{Q}}\right).$ (формула из [13])

Приведем, как следствия, формулы для рангов для некоторых классов групп. Однако следует отметить, что в действительности следствия 1–5 каждый раз получались без применения каких-либо общих формул. Исключение составляет последнее следствие 6, полученное по формуле из [11].

Обозначение. *Для натурального числа n пусть $\tau(n)$ — количество его натуральных делителей.*

Следствие 1. [Алеев, [1]] Ранг группы центральных единиц целочисленного группового кольца группы $L_2(2^n)$ равен

$$2^n + 1 - \tau(2^n - 1) - \tau(2^n + 1).$$

Следствие 2. [Алеев—Ишечкина, [3]] Пусть $q = 2^{2n+1}$, $n \geqslant 1$, $m_+ = q+1+2r$, $m_- = q+1-2r$, где $r = 2^n = \sqrt{\frac{q}{2}}$. Тогда ранг группы центральных единиц целочисленного группового кольца группы $Sz(q)$ равен

$$q + 2 - \tau(m_+) - \tau(m_-) - \tau(q - 1).$$

Следствие 3. [Алеев—Митина, [4]] Ранг группы центральных единиц целочисленного группового кольца группы $PGL_2(q)$, q нечетно, равен

$$q + 2 - \tau(q - 1) - \tau(q + 1).$$

Следствие 4. [Алеев—Перавина, [5]] Ранг группы центральных единиц целочисленного группового кольца группы $L_2(q)$, q нечетно, равен

$$\frac{q+3}{2} - \tau\left(\frac{q-1}{2}\right) - \tau\left(\frac{q+1}{2}\right) + 1,$$

при $q \equiv 1 \pmod 4$ и q — не квадрат,

$$\frac{q+3}{2} - \tau\left(\frac{q-1}{2}\right) - \tau\left(\frac{q+1}{2}\right),$$

в остальных случаях.

Следствие 5. [Алеев, [10]] Пусть G — циклическая группа порядка n. Тогда ранг группы центральных целочисленного группового кольца группы G равен

$$\left[\frac{n}{2}\right] - \tau(n) + 1 = \begin{cases} \frac{n+1}{2} - \tau(n) & \text{для нечетного } n, \\ \frac{n}{2} - \tau(n) + 1 & \text{для четного } n. \end{cases}$$

Следствие 6. [Шумакова, [9]] Пусть G — метациклическая группа Фробениуса с циклическим ядром порядка m и циклическим дополнением порядка n (n делит n). Тогда ранг группы центральных единиц целочисленного группового кольца группы G равен

$$\left(1+\left[\frac{n}{2}\right]-\frac{n}{2}\right)\frac{m-1}{n}-\left[\frac{n}{2}\right]+2-\tau(m)-\tau(n)=$$
$$=\begin{cases}\frac{m-1}{2n}+\frac{n-1}{2}+2-\tau(m)-\tau(n) & \text{для нечетного } n,\\ \frac{m-1}{n}+\frac{n}{2}+2-\tau(m)-\tau(n)+1 & \text{для четного } n.\end{cases}$$

2. Вычисления рангов

В этом разделе приведем результаты вычислений рангов для случаев, описанных в следствиях 1–6. Вычисления производились в системе GAP [12] с привлечением дополнительных средств для анализа полученных результатов.

Во всех следствиях 1–6 есть «неинтересная» часть, вычисляемая легко (как правило, это линейная функция) по параметрам группы (например, для следствия 3 это $q+2$), и «интересная» часть, связанная с нахождением количества делителей некоторых чисел. Интерес ко второй части побуждается тем, что количество делителей числа напрямую не связано с данным числом. А именно, если $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ — разложение числа в произведение степеней различных простых чисел (каноническое разложение), то количество делителей

$$\tau(n)=(\alpha_1+1)\cdots(\alpha_k+1).$$

Однако следует отметить, что этот подход приводит к задаче факторизации натуральных чисел, которая наряду с задачей дискретного логарифма, является (как общепризнано) очень трудной[1].

Соглашение. *Мы сосредоточимся на вычислениях, связанных с количеством делителей.*

2.1. Степени 2

В этом пункте мы рассмотрим случаи для групп $L_2(2^n)$ и $Sz(2^{2n+1})$. Так как согласно леммам 1 и 2 вычисления зависят от 2^n, то вполне понятно, что здесь можно вычислить небольшое число возможностей для n.

2.1.1. Группы $L_2(2^n)$

Согласно следствию 1 нужно вычислить сумму $s(n)=\tau(2^n-1)+\tau(2^n+1)$ для натуральных n, что было проделано для n от 1 до 102. Приведем код программы при интерактивном вводе в GAPe на рис. 1.

Последнее сообщение в программе

```
gap> Tau(2^103+1);
#I  FactorsInt: used the following factor(s) which are probably primes:
#I        8142767081771726171
```

означает, что появляется трудность с факторизацией $2^{103}+1$.

Табл. 1 показывает зависимость между n и $s(n)$.

[1] Трудность задач факторизации и дискретного логарифма широко используется для целей защиты информации, например, [6] и [7]

```
# Задание списка
gap> t:=[];
[  ]
# Заполнение списка
# Tau - встроенная функция GAP для подсчета числа делителей
gap> for n in [1..102] do
> i:=2^n;
> tm1:=Tau(i-1);
> tp1:=Tau(i+1);
> Add(t,[tm1+tp1,n]);
> od;
# Сортировка
gap> Sort(t);
gap> for i in [1..Length(t)] do
# Запись списка в файл
> AppendTo("Tau2p.txt",t[i],"\n");
> od;
# Возникновение трудности для 103
gap> Tau(2^103+1);
#I  FactorsInt: used the following factor(s) which are probably primes:
#I        8142767081771726171
gap> quit;
```

Рис. 1. Нахождение $s(n)$

Таблица 1

Зависимость между n и $s(n)$

$s(n)$	n	$s(n)$	n	$s(n)$	n	$s(n)$	n	$s(n)$	n
3	1	24	21, 22, 25, 26, 34, 38, 85	88	87	196	40	960	78
4	2	28	12, 27, 39	96	91, 98	208	42	1040	88
5	3	32	93	104	24	224	54, 75	2048	102
6	4, 5, 7, 13, 17, 19, 31, 61	36	32, 97	112	55	256	81	4624	60
8	11, 23, 101	40	33, 57, 62, 69	128	45	264	56	5632	90
10	6, 8	48	18, 35, 46	132	64	448	66	6152	96
12	9, 37, 41, 43, 49, 67, 79	52	20	136	44, 52	512	99	8284	72
14	10	64	74, 82, 86, 95	140	68	516	92	8256	100
16	14, 29, 47, 53, 71, 73	68	28, 83	144	30, 76	528	36	9248	84
18	16, 18	72	58, 65	160	63	608	70		
20	15, 59	80	51, 77, 94	192	50	776	48, 80		

2.1.2. *Группы* $Sz(2^{2n+1})$

По следствию 2 нужно вычислить сумму

$$s_1(n) = \tau(2^{2n+1} - 2^{n+1} + 1) + \tau(2^{2n+1} + 2^{n+1} + 1) + \tau(2^{2n+1} + 1)$$

для натуральных n, что было проделано для таких n от 1 до 75, а при $n > 75$ возникают трудности с факторизацией.

На рис. 2 изображены точки с координатами $(2n + 1, s_1(n))$, и становится ясно, что распределение этих точек весьма хаотично.

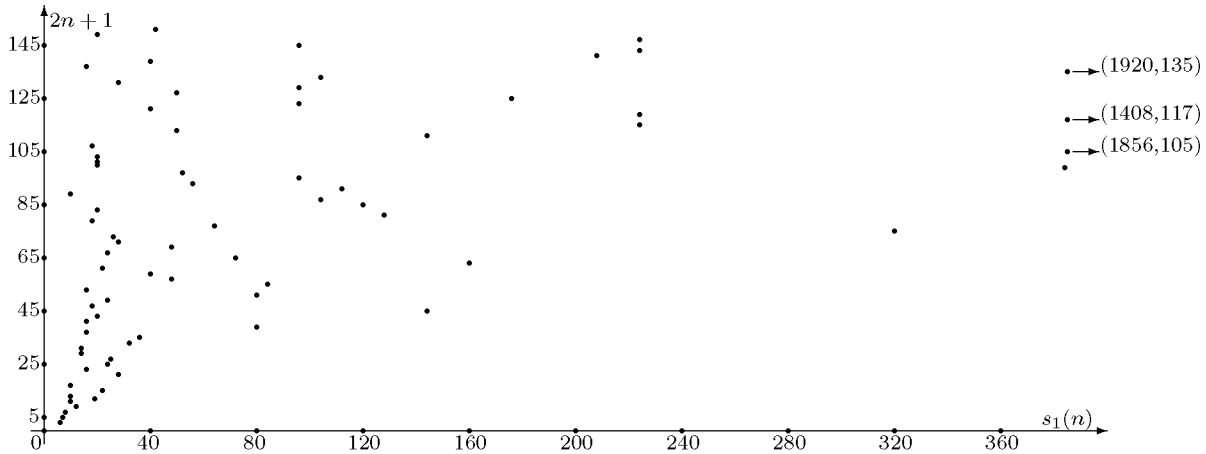

Рис. 2. Распределение $2n + 1$ и $s_1(n)$

Табл. 2 показывает зависимость между n и $s_1(n)$.

Таблица 2

Зависимость между n и $s_1(n)$

$s_1(n)$	$2n+1$	$s_1(n)$	$2n+1$	$s_1(n)$	$2n+1$	$s_1(n)$	$2n+1$
6	3	24	25, 27, 49, 67	56	93	160	63
7	5	26	73	64	77	208	141
8	7	28	21, 71, 131	80	39, 51	224	115, 119, 143, 147
10	11, 13, 17, 89	32	33	84	55	320	75
12	9, 19	36	35	96	95, 129, 145	384	99
14	29, 31	40	59, 121, 139	104	87, 133	1408	117
16	23,37,41, 53,137	42	151	112	91	1856	105
18	47, 79, 107	48	57, 79	120	85	1920	135
20	43,83,101, 103,109,149	50	113	128	81		
22	15, 61	52	97	144	45, 111		

2.2. Группы $PGL_2(q)$ и $PSL_2(q)$, q нечетно

Для построения таблиц в этом пункте 2.2. были найдены все нечетные примарные q, от 3 до $2^{26}+1 = 67\,108\,865$. Отметим, что таких q в указанном диапазоне будет 3 958 973.

2.2.1. Группы $PGL_2(q)$, q нечетно

По следствию 3 нужно вычислить сумму $s_2(q) = \tau(q-1) + \tau(q+1)$.

Таблица 3

Все значения $s_2(q)$

$3 \leqslant s_2(q) \leqslant 140$	$5, 7, 8, [10..14], [16..18], [20..118], [120..124], 126, 128, [129..134], [136..140],$
$142 \leqslant s_2(q) \leqslant 176$	$[142..146], [148..156], [158..160], 162, 164, [166..168], 170, [172..174], 176,$
$178 \leqslant s_2(q) \leqslant 206$	$178, [180..184], [186..190]_2, [192..194], [196..198], 200, 202, [204..206],$
$208 \leqslant s_2(q) \leqslant 236$	$[208..212]_2, [214..216], 218, [220..222], 224, 226, [228..230], [232..234], 236,$
$238 \leqslant s_2(q) \leqslant 298$	$238, [240..242], 244, [246..248], [250..252], [254..272]_2, [274..276], [278..298]_2,$
$300 \leqslant s_2(q) \leqslant 332$	$[300..302], [304..306], [308..316]_2, [318..320], [324..328]_2, [330..332],$
$334 \leqslant s_2(q) \leqslant 452$	$[334..404_2], [408..410], [412..416]_2, [420..432]_4, [436..440]_2, [444..452]_4,$
$454 \leqslant s_2(q) \leqslant 556$	$[454..466]_2, 472, 480, [484..488]_2, [492..498]_2, [504..528]_4, 536, 544, 548, 556,$
$564 \leqslant s_2(q) \leqslant 602$	$564, 568, 576, [580..584]_2, 588, 592, 600, 608, 644, 648, 656, 664, 680, 688, 724.$

Таблица 4

Наиболее часто встречающиеся значения $s_2(q)$

$s_2(q)$	n	m	$s_2(q)$	n	m	$s_2(q)$	n	m	$s_2(q)$	n	m
14	16310	29	40	308403	1429	72	155576	7561	124	13317	92399
16	24914	41	42	17644	2351	76	78813	10079	128	43542	55439
18	10376	97	44	191279	1259	80	182475	13441	132	12119	379^2
20	93166	71	46	13364	1681	84	39349	13859	136	32259	65519
22	49578	179	48	222011	2161	88	118659	21839	144	26015	225721
24	85598	169	50	13790	4049	92	19624	20161	152	28784	180181
26	30585	181	52	137856	3079	96	81653	22679	160	22230	151201
28	211019	239	54	19996	3361	100	36320	30241	168	13041	166319
30	23038	883	56	305278	2521	104	92798	42841	176	14319	262079
32	231756	419	60	80262	4159	108	23665	45361	200	13471	332641
34	28133	701	64	218627	5041	112	82275	78121			
36	131798	839	68	71811	5039	116	14719	81901			
38	45983	881	70	18305	20789	120	31025	87359			

В рассматриваемом диапазоне $s_2(q)$ изменяется от 5 для 3 до 724 для 61261199 и 64864799, и принимает 339 различных значений. Мы ограничились двумя таблицами, в первой из которых (табл. 3) указаны все возможные значения $s_2(q)$ (использованы обозначения $[i..j]$ для идущих подряд чисел, $[2k..2l]_2$ для идущих подряд *четных* чисел и $[4m..4n]_4$

для идущих подряд чисел, *делящихся на* 4), а во второй (табл. 4) указаны значения $s_2(q)$, которые встречаются $n > 10\,000$ раз и m — наименьшее значение q с данным $s_2(q)$..

2.2.2. Группы $PSL_2(q)$, q нечетно

По следствию 4 нужно вычислить сумму $s_3(q) = \tau((q-1)/2) + \tau((q+1)/2)$. Оказалось, что $s_3(q)$ изменяется от 3 для 3 до 602 для 64864799.

В табл. 5 будем использовать обозначения, указанные перед табл. 3.

Таблица 5

Все значения $s_3(q)$

$3 \leqslant s_3(q) \leqslant 230$	$[3..164], [166..178], [180..184], [186..210], [212..218]_2, [219..222], [224..230],$
$232 \leqslant s_3(q) \leqslant 266$	$232, 233, [234..240]_2, [241..252], [254..256], 255, 256, [258..262], [264..266],$
$268 \leqslant s_3(q) \leqslant 316$	$268, [272..290]_2, 291, [292..296]_2, 297, 298, [300..304], 306, 308, [312..316],$
$319 \leqslant s_3(q) \leqslant 360$	$319, 320, [322..324], [326..332]_2, 333, [334..344], 348, [352..356], 360,$
$362 \leqslant s_3(q) \leqslant 411$	$[362..366]_2, [368..380]_4, [382..392]_2, 393, [394..402]_2, 403, 404, 408, 409, 411,$
$412 \leqslant s_3(q) \leqslant 504$	$412, 416, 422, 424, 428, 434, 436, [440..448]_4, [450..456]_2, 482, 484, 488, 504,$
$506 \leqslant s_3(q) \leqslant 602$	$506, 508, 512, [514..516], 520, 548, 578, 580, 584, 602.$

В табл. 6 укажем значения $s_3(q)$, которые встречаются $n > 10\,000$ раз и m — наименьшее значение q с данным $s_3(q)$.

Таблица 6

Наиболее часто встречающиеся значения $s_3(q)$

$s_3(q)$	n	m	$s_3(q)$	n	m	$s_3(q)$	n	m	$s_3(q)$	n	m
8	16310	23	30	33043	43^2	54	15938	13859	88	31424	63361
10	30821	41	32	297813	1439	56	155300	12601	96	13464	122401
12	127433	79	34	63696	2399	60	39323	21121	98	19449	92399
14	57706	11^2	36	219546	2161	64	80045	13441	100	41143	55439
16	217966	13^2	38	39161	2879	66	26062	15121	104	33946	65519
18	74281	421	40	299168	2521	68	70806	21839	112	14997	100799
20	326442	239	42	20454	6047	72	71257	36721	132	11599	166319
22	63282	479	44	115823	3359	74	13455	181^2	148	10679	262079
24	333303	769	48	146398	5279	76	43984	20161			
26	66910	719	50	45882	71^2	80	54321	35281			
28	274405	31^2	52	139916	5039	84	22888	45361			

Замечание 2. Возникает обманчивое впечатление, что $s_2(q)$ и $s_3(q)$ очень просто между собой связаны, например, пропорциональны. Однако на самом деле все сложнее. Пусть

$\varepsilon = (-1)^{\frac{q-1}{2}}$. Тогда

$$q - \varepsilon \equiv 0 \pmod 4 \quad \text{и} \quad q + \varepsilon \equiv 2 \pmod 4.$$ Отсюда

$q - \varepsilon = 2^\alpha \beta$ и $q + \varepsilon = 2\gamma$, где $\alpha \geqslant 2$, а β и γ нечетны.

Таблица 7

Значения $\tau(n)$

$\tau(n)$	$o(\tau(n))$	$m(\tau(n))$	$\tau(n)$	$o(\tau(n))$	$m(\tau(n))$	$\tau(n)$	$o(\tau(n))$	$m(\tau(n))$	$\tau(n)$	$o(\tau(n))$	$m(\tau(n))$
2	2063689	2	49	4	46656	125	4	810000	245	1	29160000
3	760	4	50	3715	6480	126	1557	100800	250	12	5670000
4	6090743	6	51	7	589824	128	63439	83160	252	750	1108800
5	21	16	52	1618	61440	130	29	1658880	256	3327	1081080
6	1093224	12	54	21339	6300	132	1006	322560	260	7	11612160
7	7	128	55	6	82944	135	155	176400	264	175	3548160
8	7417249	24	56	72561	6720	136	22	6881280	270	240	1940400
9	1553	36	57	4	2359296	140	1589	181440	280	303	1995840
10	198403	48	60	99135	5040	144	61851	110880	288	4740	1441440
11	3	2^{10}	63	205	14400	147	8	1166400	294	10	8164800
12	2679516	60	64	481777	7560	150	661	226800	297	2	11289600
13	2	2^{12}	65	4	331776	152	1	27525120	300	235	2494800
14	48545	384	66	1118	46080	153	2	14745600	308	1	26127360
15	479	144	68	99	983040	154	14	3732480	312	13	14192640
16	4963136	120	70	1532	25920	156	215	1290240	315	6	6350400
17	1	2^{16}	72	247434	10080	160	22594	1166400	320	1117	2162160
18	213193	180	75	85	32400	162	1005	352800	324	244	3880800
19	1	2^{18}	76	22	3932160	165	10	2073600	330	4	14515200
20	444480	240	77	3	746496	168	7437	221760	336	610	2882880
21	195	576	78	321	184320	170	1	26542080	350	1	22680000
22	3616	3072	80	134694	15120	175	5	3240000	352	21	10644480
23	1	2^{22}	81	292	44100	176	680	967680	360	558	3603600
24	2511201	360	84	20053	20160	180	5406	277200	378	24	7761600
25	22	1296	85	1	5308416	182	3	14929920	384	757	4324320
26	1045	12288	88	3465	107520	189	42	705600	392	5	17962560
27	1083	900	90	7272	25200	192	30885	332640	396	7	17740800
28	100471	960	91	1	2985984	195	3	8294400	400	72	6486480
30	61943	720	95	1	21233664	196	94	1632960	405	3	21344400
32	1996343	840	96	284560	27720	198	86	1612800	420	26	9979200
33	49	9216	98	138	233280	200	1565	498960	432	186	7207200
34	96	196608	99	34	230400	204	2	20643840	440	1	31933440
35	18	5184	100	4916	45360	208	94	3870720	448	47	86486400
36	395896	1260	102	25	2949120	210	223	907200	450	5	17463600
38	30	786432	104	727	430080	216	6094	554400	480	97	10810800
39	26	36864	105	57	129600	220	52	2903040	486	1	31046400
40	360258	1680	108	23187	50400	224	2671	665280	504	17	14414400
42	14591	2880	110	105	414720	225	24	1587600	512	17	17297280
44	6315	15350	112	22538	60480	231	1	18662400	540	2	25225200
45	569	3600	114	5	11796480	234	17	6451200	560	1	25945920
46	3	12582912	117	14	921600	240	7070	720720	576	10	21621600
48	1174467	2520	120	47554	55440	243	17	2822400	600	1	32432400

Поэтому

$$s_2(q) = \tau(q-1) + \tau(q+1) = (\alpha+1)\tau(\beta) + 2\tau(\beta),$$
$$s_3(q) = \tau((q-1)/2) + \tau((q+1)/2) = \alpha\tau(\beta) + \tau(\beta).$$

2.3. Циклические группы и метациклические группы Фробениуса

По следствию 5 для циклических групп нужно подсчитать число делителей натуральных чисел, что было проделано в диапазоне от 2 до $2^{25} = 33\,554\,432$. Отметим, что число делителей изменяется от 2 (это в точности простые числа) до 600 для 32 432 400. В табл. 7 указаны возможные $\tau(n)$, количество $o(\tau(n))$ таких $\tau(n)$ в рассматриваемом диапазоне для n и минимальное значение $n = m(\tau(n))$ с данным $\tau(n)$.

Для метациклических групп Фробениуса можно из вычислений $\tau(n)$ можно получить по следствию 6 нужные значения $\tau(m) + \tau(n)$, где n делит $m-1$. Однако тут возникает слишком много возможностей для m и n, что приведет к огромным таблицам, которые просто невозможно разместить в рамках одной статьи.

Заключение

Результаты, приведенные в данной работе, дают удобные для вычислений формулы рангов групп центральных единиц, что позволяет анализировать поведение рангов при возрастании параметров, таких как порядок конечного поля для линейных групп или порядок группы для циклических или метациклических групп Фробениуса. Таблицы и график, приведенные во втором разделе, показывают характер изменений параметров рангов групп центральных единиц, связанных с числом делителей чисел, которые входят в формулы для рангов.

В дальнейшем на основе полученных данных планируется изучить асимптотическое поведение рангов групп центральных единиц.

Первый автор и его ученики получали существенную техподдержку от коллективов, возглавляемых Л.Б. Соколинским, что позволяет, наконец, выразить большую признательность ему за содействие.

Литература

1. Алеев, Р.Ж. Теория центральных единиц целочисленных групповых колец групп $PSL_2(2^n)$ / Р.Ж. Алеев // Сб. научн. трудов «Комбинат. и вычислит. методы в матем.». — Омск: ОмГУ , 1999. — С. 1–19.
2. Алеев, Р.Ж. Центральные единицы целочисленных групповых колец конечных групп: дисс. ...д-ра физ.-мат. наук. / Р.Ж. Алеев — Челябинск, 2000. — 355 с.
3. Алеев, Р.Ж. Теория групп центральных единиц целочисленных групповых колец групп $Sz(q)$ / Р.Ж. Алеев, Н.Б. Ишечкина // Труды Института математики и механики УрО РАН. — 2001. — Т.7, № 2. — С. 3–16.
4. Алеев, Р.Ж. Теорема разложения и ранги групп центральных единиц целочисленных групповых колец групп $PGL(2,q)$, q нечетно / Р.Ж. Алеев, О.В. Митина // Сибирские Электронные Математические Известия. — 2008. — Т. 5. — С. 652–672.

5. Алеев, Р.Ж. Ранги групп центральных единиц целочисленных групповых колец групп $PSL(2, q)$, q нечетно / Р.Ж. Алеев, О.В. Перавина // Вестник ЧелГУ, сер. «Математика. Механика». — 1999, № 1(4). — С. 5–15.
6. Василенко, О.Н. Теоретико–числовые алгоритмы в криптографии. / О.Н. Василенко — М.: МЦНМО, 2006. — 336 с.
7. Глухов, М.М. Введение в теоретико–числовые методы в криптографии. / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин — СПб.: Изд-во «Лань», 2011. — 400 с.
8. Кэртис, Ч. Теория представлений конечных групп и ассоциативных алгебр: Пер. с англ. / Ч. Кэртис, И. Райнер — М.: Наука, 1969. — 668 с.
9. Шумакова, Е.О. Группы центральных единиц целочисленных групповых колец метациклических групп Фробениуса / Е.О. Шумакова // Сибирские Электронные Математические Известия. — 2008. — Т. 5. — С. 691–698.
10. Aleev, R. Ž. Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers / R. Ž. Aleev // Intern. Journ. Algebra and Computations. — 1994. — Vol. 4. — P. 309–358.
11. Ferraz, R. A. Simple components and central units in group rings / R.A. Ferraz // Journal of Algebra. — 2004. — Vol. 279, No. 1. — P. 91–203.
12. The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.7.4. — 2014. URL: `http://www.gap-system.org` (дата обращения: 04.05.2014).
13. Ritter, J. Trivial units in RG / J. Ritter, S.K. Sehgal // Mathematical Proceedings of the Royal Irish Academy. — 2005. — Vol. 105A, No. 1. — P. 25–39.
14. Schönert, M. GAP – Groups, Algorithms, and Programming / M. Schönert et al. — Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, sixth edition, 1997. URL: `http://www.gap-system.org/Gap3` (дата обращения: 14.06.2012).

Алеев Рифхат Жалялович, д.ф.-м.н., профессор кафедры системного программирования, Южно-Уральский государственный университет (Челябинск, Российская Федерация), aleevrz@susu.ac.ru.

Цыбина Наталья Андреевна, магистр кафедры системного программирования, Южно-Уральский государственный университет (Челябинск, Российская Федерация), tsybinanatasha@gmail.com.

Поступила в редакцию 20 декабря 2014 г.

Bulletin of the South Ural State University
Series "Computational Mathematics and Software Engineering"
2015, vol. 4, no. 1, pp. 71–85

DOI: 10.14529/cmse150107

THE COMPUTATION OF RANKS OF UNIT GROUPS OF INTEGRAL GROUP RINGS OF FINITE GROUPS

R.Zh. Aleev, South Ural State University (Chelyabinsk, Russian Federation)
aleevrz@susu.ac.ru,
N.A. Tsybina, South Ural State University (Chelyabinsk, Russian Federation)
tsybinanatasha@gmail.com

The study of central units (central invertible elements) of integral group rings is encountered to difficult calculations almost everywhere, both in the case of finding of individual central unit and in the case of describing of group of central elements. By virtue of torsion part of central unit group is trivial (up to sign those are elements of center group) it is more interesting to find data about torsion free part that is direct product infinite cyclic groups. The number of such infinite factors is the rank of central unit group. Therefore the ranks of central unit groups of integral group rings of finite groups are the very important characteristic those groups. So that the computation ranks of central unit groups has big interest for study of central unit groups. In the paper we point out the formulas for computation of ranks in general case and some important particular cases. On the base of those formulas we compute the ranks in quite large ranges. We used computer algebra system GAP. The results are shown on tables and graph.

Keywords: group character, central unit, rank of Abelian group, system GAP.

References

1. Aleev R.Zh. Teoriya central'nyh edinic celochislennyh gruppovyh kolec grupp $PSL_2(2^n)$ [The theory of central units of integral goup rings of groups $PSL_2(2^n)$] // Sb. nauchn. trudov «Combinat. i vychislit. metody v matem.». Omsk: OmGU , 1999. P. 1–19.
2. Aleev R.Zh. Central'nye edinicy celochislennyh gruppovyh kolec konechnyh grupp [Central units of integral group rings of finite groups]: diss. . . . d-ra fis.-mat. nauk. Chelyabinsk, 2000. 355 p.
3. Aleev R.Zh., Ishechkina N.B. A Theory of Central Unit Groups of Integral Group Rings of Groups $Sz(q)$ // Proccedings of the Steklov Institute of Mathematics, Suppl. 2. MAIK «Nauka/Interperiodica». 2001. P. 1–15.
4. Aleev R. Zh., Mitina O. V. Teorema razlozheniya and rangi central'nyh edinic celochislennyh gruppovyh kolec grupp $PSL(2, q)$, q nechetno [The decomposition theorem and ranks of central unit groups of integer group rings of groups $PGL2(q)$, q odd] // Siberian Electonic Mathematcal Reports. 2008. Vol. 5. P. 652–672
5. Aleev R.Zh., Peravina O.V. Rangi grupp central'nyh edinic celochislennyh gruppovyh kolec grupp $PSL(2, q)$, q nechetno [The ranks central units of integral group rings of finite groups $PSL(2, q)$, q odd] // Vest. ChelSU. ser. Mat. Mekh., 1999, No 1(4). P. 5–15.
6. Vasilenko O.N. Number-theoretic Algorithms in Cryptography. AMS, 2007. 243 p.

7. Glukhov M.M., Kruglov I.A., Pichkur A.B., Cheremushkin A.V. Vvedenie v teoretiko-chislovye metody kriptografii [Introduction to theoretical and numerical methods in cryptography]. Sankt-Peterburg: Lan', 2011. 400 p.
8. Curtis, Charles W.; Reiner, Irving, Representation theory of finite groups and associative algebras, Pure and Applied Mathematics, Vol. XI, New York-London, Interscience Publishers, a division of John Wiley & Sons, 1962. 703 p.
9. Shumakova E.O. Gruppy central'nyh edinic celochislennyh gruppovyh kolec metaciklicheskih grupp Frobeniusa [Central units in integral group rings for Frobenius metacyclic groups] // Siberian Electonic Mathematcal Reports. 2008. Vol. 5. C. 691–698.
10. Aleev R. Ž. Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers // Intern. Journ. Algebra and Computations. 1994. Vol. 4. P. 309–358.
11. Ferraz R. A. Simple components and central units in group rings // Journal of Algebra. 2004. Vol. 279, No. 1. P. 91–203.
12. The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.7.4. — 2014. URL: `http://www.gap-system.org` (accessed: 04.05.2014).
13. Ritter J., Sehgal S.K. Trivial units in *RG* // Mathematical Proceedings of the Royal Irish Academy. 2005. Vol. 105A, No 1. P. 25–39.
14. Schönert M. et al. GAP – Groups, Algorithms, and Programming // Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, sixth edition, 1997. URL: `http://www.gap-system.org/Gap3` (accessed: 14.06.2012).

Received December 20, 2014.