S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Том 20, № 2, стр. 144–144 (2023) УДК 512.54
https://doi.org/10.33048/semi.2023.20.??? MSC 20H25

ОПИСАНИЕ СТРОЕНИЯ ГРУППЫ ОБРАТИМЫХ ЦЕНТРОСИММЕТРИЧНЫХ ДВУМЕРНЫХ МАТРИЦ НАД $\mathbb{Z}_n$

К.С. Зюбин

Представлено П.П. Петровым *(заполняется редактором)*

Abstract: The public-key cryptosystem MMMC1 proposed by S. Rososhek creates keys using invertible centrosymmetric 2-by-2 matrices over the modulo ring:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ where } a, b \in \mathbb{Z}_n \text{ and } a^2 - b^2 \in \mathbb{Z}_n^*.$$

On the 13th School-Conference on Group Theory (2020) dedicated to V. A. Belonogov's 85th birthday, V. Romankov asked to describe the structure of this matrix group and find the minimal number of its generators. This paper gives the required description and minimal number of generators.

Keywords: centrosymmetric 2-by-2 matrices, split complex numbers.

1 Введение

Всюду в статье R обозначает ассоциативно-коммутативное кольцо с единицей, а R^* — его мультипликативную группу. Кольцо вычетов по модулю n обозначается $\mathbb{Z}_n$.

Zyubin, K.S., The Description of the Group of Invertible Centrosymmetric 2-by-2 Martices over $\mathbb{Z}_n$.

Поступила 16 июля 2023 г., опубликована . . . . . 2023 г.

Для кольца R обозначим через $SM_2(R)$ множество центросимметричных 2×2 матриц:

$$SM_2(R) = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| \, a, b \in R \right\}.$$

Множество $SM_2(R)$ является кольцом относительно сложения и умножения матриц. Обозначим группу мультипликативно обратимых элементов этого кольца через $SGL_2(R)$. Тогда

$$SGL_2(R) = SM_2(R)^* = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| \, a, b \in R,\ a^2 - b^2 \in R^* \right\}.$$

Элементы группы $SGL_2(\mathbb{Z}_n)$ используются для создания ключей в системе шифрования с открытым ключом MMMC1 из статьи С. К. Росошека [4]. На школе-конференции по теории групп (2020), посвящённой 85-летию В. А. Белоногова, В. А. Романьковым был поставлен вопрос об описании строения этой группы матриц и нахождении минимального числа её образующих [3, Вопрос 14].

Следующая теорема даёт представление группы $SGL_2(\mathbb{Z}_n)$ в виде прямого произведения мультипликативных групп вида $\mathbb{Z}^*_{p^k}$.

Теорема 1. *Пусть* $n = 2^k p_1^{k_1} \dots p_m^{k_m}$ $(k \geqslant 0, k_i \geqslant 1)$ — *разложение натурального числа* $n > 1$ *в произведение целых степеней различных простых чисел. Тогда*

Если $k = 0$, *то*

$$SGL_2(\mathbb{Z}_n) \cong (\mathbb{Z}^*_{p_1^{k_1}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2.$$

Если $k \geqslant 1$, *то*

$$SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}^*_{2^k} \times \mathbb{Z}^*_{2^{k+1}} \times (\mathbb{Z}^*_{p_1^{k_1}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2.$$

В свою очередь, группы $\mathbb{Z}^*_{p^k}$ описывает известная

Теорема 2. [2, Chapter 9, §2] *Справедливы изоморфизмы*

$$\mathbb{Z}^*_2 \cong \mathbb{Z}_1; \quad \mathbb{Z}^*_4 \cong \mathbb{Z}_2; \quad \mathbb{Z}^*_{2^{k+2}} \cong \mathbb{Z}_{2^k} \times \mathbb{Z}_2; \quad \mathbb{Z}^*_{p^k} \cong \mathbb{Z}_{p^k - p^{k-1}},$$

где $p > 2$ — *простое,* k — *натуральное.*

Таким образом, в совокупности теоремы 1 и 2 позволяют описать группу $SGL_2(\mathbb{Z}_n)$ как прямое произведение циклических групп.

Минимальное число образующих группы $SGL_2(\mathbb{Z}_n)$ устанавливает

Теорема 3. *Пусть* $n = 2^k p_1^{k_1} \dots p_m^{k_m}$ $(k \geqslant 0, k_i \geqslant 1)$ — *разложение натурального числа* $n > 1$ *в произведение целых степеней различных простых чисел. Тогда минимальное число образующих группы* $SGL_2(\mathbb{Z}_n)$ *равно*

$2m$ *при* $k = 0$,

$2m+1$ *при* $k=1$,
$2m+3$ *при* $k=2$,
$2m+4$ *при* $k>2$.

Параграф 2 позволяет свести доказательство теоремы 1 к рассмотрению двух случаев, когда n — степень нечётного простого и когда n — степень двойки. Эти случаи разбираются в параграфах 3 и 4, соответственно. Доказательство теоремы 1 приведено в параграфе 5, а доказательство теоремы 3 — в параграфе 6.

2 Предварительные результаты

Теорема 4. *Пусть* R, S, T *— кольца и* $R \cong S \times T$. *Тогда*

$$SM_2(R) \cong SM_2(S) \times SM_2(T).$$

Доказательство. Пусть f — изоморфизм из R в $S \times T$ и $f(a) = (\bar{a}, \bar{\bar{a}})$. Отображение g, задающееся по правилу $g(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)) = \left(\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{smallmatrix}\right), \left(\begin{smallmatrix} \bar{\bar{a}} & \bar{\bar{b}} \\ \bar{\bar{b}} & \bar{\bar{a}} \end{smallmatrix}\right)\right)$ даёт искомый изоморфизм из $SM_2(R)$ в $SM_2(S) \times SM_2(T)$. □

Следствие 1. *Если* $n = m_1 m_2$, *где* m_1, m_2 *— натуральные большие 1 и* $(m_1, m_2) = 1$, *то*

$$SGL_2(\mathbb{Z}_{m_1 m_2}) \cong SGL_2(\mathbb{Z}_{m_1}) \times SGL_2(\mathbb{Z}_{m_2}).$$

Доказательство. Поскольку числа m_1 и m_2 взаимно просты, то [2, Chapter 9, §2] имеет место изоморфизм $\mathbb{Z}_{m_1 m_2} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Тогда по теореме 4 имеем изоморфизм колец:

$$SM_2(\mathbb{Z}_{m_1 m_2}) \cong SM_2(\mathbb{Z}_{m_1}) \times SM_2(\mathbb{Z}_{m_2}).$$

Отсюда следует изоморфизм для соответствующих мультипликативных групп:

$$SGL_2(\mathbb{Z}_{m_1 m_2}) \cong SGL_2(\mathbb{Z}_{m_1}) \times SGL_2(\mathbb{Z}_{m_2}).$$

□

Следствие 1 позволяет свести изучение строения группы $SGL_2(\mathbb{Z}_n)$ к рассмотрению случая, когда $n = p^k$ является степенью нечётного простого числа и когда $n = 2^k$ — степень двойки. Описание строения группы $SGL_2(\mathbb{Z}_n)$ для степени нечётного простого даётся в параграфе 3. Случай степени двойки будет разобран в параграфе 4.

3 Строение $SGL_2(\mathbb{Z}_{p^k})$ для нечётного простого p

Теорема 5. *Пусть* R *— кольцо, в котором 2 является обратимым элементом. Тогда*

$$SM_2(R) \cong R \times R.$$

Доказательство. Искомый изоморфизм задаётся отображением $f\colon \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right) \mapsto (a+b, a-b)$. Гомоморфность отображения f проверяется непосредственными выкладками. Проверим, что f инъективно и сюръективно.

Пусть $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right), \left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix}\right) \in SM_2(R)$ и $f\left(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix}\right)\right)$. Тогда по построению f имеем $a+b = c+d$ и $a-b = c-d$. Сложив оба равенства, получаем $2a = 2c$. По условию элемент 2 обратим в кольце R. Следовательно, $a = c$. Аналогично, $b = d$. Таким образом, $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix}\right)$ и инъективность f доказана.

Пусть $(x, y) \in R \times R$. Его прообразом в $SM_2(R)$ является матрица $\left(\begin{smallmatrix} 2^{-1}(x+y) & 2^{-1}(x-y) \\ 2^{-1}(x-y) & 2^{-1}(x+y) \end{smallmatrix}\right) \in SM_2(R)$. Таким образом, f сюръективно.

Итак, отображение f является изоморфизмом. □

Из теоремы 5 вытекает

Следствие 2. *Если p — нечётное простое число, то*

$$SGL_2(\mathbb{Z}_{p^k}) \cong \mathbb{Z}^*_{p^k} \times \mathbb{Z}^*_{p^k}.$$

4 Строение $SGL_2(\mathbb{Z}_{2^k})$

Основным результатом параграфа является

Теорема 6. *Пусть k — натуральное. Тогда*

$$SGL_2(\mathbb{Z}_{2^k}) \cong \mathbb{Z}^*_{2^k} \times \mathbb{Z}^*_{2^{k+1}}.$$

Разбор этого случая будет удобнее вести в терминах двойных чисел определяемых ниже.

Рассмотрим классы смежности многочленов с коэффициентами из R по модулю многочлена $x^2 - 1$, то есть факторкольцо $R[x]/\langle x^2 - 1\rangle$. Множество таких классов также называется двойными числами над R и обозначается $R[j]$, где j — это класс сравнимости многочлена x. Каждый элемент $R[j]$ может быть представлен в виде $a + bj$, где $a, b \in R$. При этом $j^2 = 1$, а сложение и умножение двойных чисел выполняются по формулам:

$$(a + bj) + (c + dj) = (a + c) + (b + d)j,$$
$$(a + bj) \times (c + dj) = (ac + bd) + (ad + bc)j.$$

Из данных определений вытекает

Теорема 7. *Отображение $f\colon SM_2(R) \longrightarrow R[j]$ заданное формулой $f(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)) = a + bj$, где $a, b \in R$, является изоморфизмом колец.*

Следствие 3. *Группы $SGL_2(\mathbb{Z}_n)$ и $\mathbb{Z}_n[j]^*$ изоморфны.*

Следствие 4. *Элемент $a + bj$ обратим в $\mathbb{Z}_n[j]$ тогда и только тогда, когда элемент $a^2 - b^2$ обратим в $\mathbb{Z}_n$.*

Для доказательства теоремы 6 установим следующие утверждения.

Лемма 1. *Порядок элемента* $3+2j$ *из группы* $\mathbb{Z}_{2^k}[j]^*$ *равен* 2^{k-1}.

Доказательство. Докажем индукцией по t, что $(3+2j)^{2^t} = (1+2+2j)^{2^t} = 1+2^{t+1}m+2^{t+1}mj$ для некоторых обратимых m (вообще говоря, различных для различных t).

База индукции: $(1+2+2j)^{2^0} = 1+2^1\cdot 1+2^1\cdot 1\cdot j$.

Шаг индукции: пусть $(1+2+2j)^{2^t} = 1+2^{t+1}m+2^{t+1}mj$. Тогда

$$(1+2+2j)^{2^{t+1}} = (1+2^{t+1}m+2^{t+1}mj)^2 =$$
$$= 1+2^{2t+2}m^2+2^{2t+2}m^2+2^{t+2}m+2^{t+2}mj+2^{2t+3}m^2j =$$
$$= 1+2^{t+2}(m+2^{t+1}m^2)+2^{t+2}(m+2^{t+1}m^2)j.$$

Элемент $m+2^{t+1}m^2$ обратим в $\mathbb{Z}_{2^k}$ как сумма обратимого и нильпотентного.

Таким образом, $(1+2+2j)^{2^{k-1}} = 1+2^km+2^kmj = 1$. Следовательно, порядок элемента $1+2+2j$ делит 2^{k-1}. При $t<k-1$ элемент $(1+2+2j)^{2^t} \neq 1$. Значит, порядок элемента $1+2+2j$ равен 2^{k-1}. □

Лемма 2. *Подгруппа* $\langle 3+2j\rangle$ *группы* $\mathbb{Z}_{2^k}[j]^*$ *состоит из всех элементов вида* $1+2s+2sj$, *где* $s\in\mathbb{Z}_{2^k}$ *и только из них.*

Доказательство. Ясно, что множество $Y = \{1+2s+2sj \mid s\in\mathbb{Z}_{2^k}\}$ является подгруппой группы $\mathbb{Z}_{2^k}[j]^*$.

Если $1+2s_1+2s_1j = 1+2s_2+2s_2j$, то $2s_1 = 2s_2$ и $2(s_1-s_2)=0$. Это возможно, только если s_1 сравнимо с s_2 по модулю 2^{k-1}. Поэтому множество Y состоит ровно из 2^{k-1} различных элементов.

Элемент $3+2j = 1+2+2j$ принадлежит Y. Поэтому подгруппа $\langle 3+2j\rangle$ лежит в Y. Поскольку порядок элемента $3+2j$ равен 2^{k-1}, то порядок порождённой им подгруппы также равен 2^{k-1}. Однако, порядок подгруппы Y тоже равен 2^{k-1}. Следовательно, $\langle 3+2j\rangle$ совпадает с Y. □

Лемма 3. *Справедлив следующий изоморфизм*

$$\mathbb{Z}_{2^k}[j]^* \cong \mathbb{Z}_{2^k}^* \times \langle 3+2j\rangle \times \langle j\rangle.$$

Доказательство. Убедимся, что любой элемент $a+bj\in\mathbb{Z}_{2^k}[j]^*$ может быть единственным образом представлен в виде произведения zyx, где $z\in\mathbb{Z}_{2^k}^*$, $y\in\langle 3+2j\rangle$ и $x\in\langle j\rangle$.

Покажем, что такое представление существует. Если элемент $a+bj$ обратим, то a^2-b^2 также обратим и, значит, обратимы $a+b$ и $a-b$. Поэтому ровно один из элементов a и b обратим, при этом второй имеет вид $2s$. Если $a=2s$, то возьмём $z=(b-a)^{-1}$. Тогда

$$a+bj = jz^{-1}z(b+aj) = j(bz+azj)z^{-1} = z^{-1}(1+az+azj)j.$$

В случае, когда $b=2s$, возьмём $z=(a-b)^{-1}$. Тогда

$$a+bj = z^{-1}z(a+bj) = (az+bzj)z^{-1} = z^{-1}(1+bz+bzj)\cdot 1.$$

Согласно лемме 2 элемент $1 + az + azj$ в первом случае и элемент $1 + bz + bzj$ во втором являются элементами подгруппы $\langle 3 + 2j \rangle$. Таким образом, любой элемент $\mathbb{Z}_{2^k}[j]^*$ представим в виде необходимого произведения zyx.

Проверим, что такое представление единственно. Пусть $z_1, z_2 \in \mathbb{Z}_{2^k}^*$, $y_1, y_2 \in \langle 3 + 2j \rangle$, $x_1, x_2 \in \langle j \rangle$ и при этом $z_1 y_1 x_1 = z_2 y_2 x_2$. Тогда $y_1 y_2^{-1} = z_1^{-1} x_1^{-1} z_2 x_2 = (z_1^{-1} z_2)(x_1^{-1} x_2)$. Любой элемент подгруппы $\langle 3 + 2j \rangle$, кроме 1 имеет вид $a + bj$, где $a \neq 0, b \neq 0$ и, значит, непредставим в виде произведения элемента из $\mathbb{Z}_{2^k}^*$ и элемента из $\langle j \rangle$. Тогда $y_1 y_2^{-1} = 1$ и $(z_1^{-1} z_2)(x_1^{-1} x_2) = 1$. Отсюда $y_1 = y_2$ и $z_1^{-1} z_2 = x_1 x_2^{-1}$. Подгруппы $\mathbb{Z}_{2^k}^*$ и $\langle j \rangle$ пересекаются только по 1. Имеем $y_1 = y_2$, $z_1^{-1} z_2 = 1$ и $x_1 x_2^{-1} = 1$. Таким образом, $z_1 = z_2$, $y_1 = y_2$ и $x_1 = x_2$. □

Доказательство теоремы 6. Справедлива следующая цепочка изоморфизмов, из которой вытекает искомый:

$$SGL_2(\mathbb{Z}_{2^k}) \cong \mathbb{Z}_{2^k}[j]^* \cong \mathbb{Z}_{2^k}^* \times \langle 3 + 2j \rangle \times \langle j \rangle \cong$$

$$\cong \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k-1}} \times \langle j \rangle \cong \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_2 \cong \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k+1}}^*,$$

где первый изоморфизм справедлив в силу следствия 3, второй верен по лемме 3, третий — в силу леммы 1 и так как $\langle j \rangle = \{1, j\} \cong \mathbb{Z}_2$ и, наконец, четвёртый выполняется по теореме 2. □

5 Доказательство теоремы 1

Пусть $n = 2^k p_1^{k_1} \dots p_m^{k_m}$ $(k \geqslant 0, k_i \geqslant 1)$ — разложение натурального числа n в произведение целых степеней различных простых чисел.

Если $k = 0$, то справедливы следующие изоморфизмы:

$$SGL_2(\mathbb{Z}_n) \cong SGL_2(\mathbb{Z}_{p_1^{k_1}}) \times \dots \times SGL_2(\mathbb{Z}_{p_m^{k_m}}) \cong$$

$$\cong (\mathbb{Z}_{p_1^{k_1}}^* \times \mathbb{Z}_{p_1^{k_1}}^*) \times \dots \times (\mathbb{Z}_{p_m^{k_m}}^* \times \mathbb{Z}_{p_m^{k_m}}^*) =$$

$$= (\mathbb{Z}_{p_1^{k_1}}^* \times \dots \times \mathbb{Z}_{p_m^{k_m}}^*)^2,$$

где первый изоморфизм верен по следствию 1, второй — по следствию 2.

Если $k > 0$, то справедливы следующие изоморфизмы:

$$SGL_2(\mathbb{Z}_n) \cong SGL_2(\mathbb{Z}_{2^k}) \times SGL_2(\mathbb{Z}_{p_1^{k_1}}) \times \dots \times SGL_2(\mathbb{Z}_{p_m^{k_m}}) \cong$$

$$\cong (\mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k+1}}^*) \times (\mathbb{Z}_{p_1^{k_1}}^* \times \mathbb{Z}_{p_1^{k_1}}^*) \times \dots \times (\mathbb{Z}_{p_m^{k_m}}^* \times \mathbb{Z}_{p_m^{k_m}}^*) =$$

$$= \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k+1}}^* \times (\mathbb{Z}_{p_1^{k_1}}^* \times \dots \times \mathbb{Z}_{p_m^{k_m}}^*)^2,$$

где первый изоморфизм верен по следствию 1, второй — по следствию 2 и теореме 6.

Теорема 1 доказана. □

6 Доказательство теоремы 3

Для доказательства теоремы о минимальном количестве образующих группы $SGL_2(\mathbb{Z}_n)$ потребуется следующая

Теорема 8. [1, Theorem 3.1] *Пусть* $C = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$, *где всякое* $n_i > 1$. *Для каждого простого* p *определим* $d_p = |\{i \leqslant m : p \mid n_i\}|$ *и*

$$\mu_C = \max\{d_p : p \text{ — простое}\}.$$

Тогда минимальное число образующих группы C *равно* μ_C.

Доказательство теоремы 3. По условию теоремы $n = 2^k p_1^{k_1} \ldots p_m^{k_m}$, где p_i — различные нечётные простые. Тогда по теореме 1 имеем:

если $k = 0$, то $SGL_2(\mathbb{Z}_n) \cong (\mathbb{Z}^*_{p_1^{k_1}} \times \mathbb{Z}^*_{p_2^{k_2}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2$;

если $k = 1$, то $SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times (\mathbb{Z}^*_{p_1^{k_1}} \times \mathbb{Z}^*_{p_2^{k_2}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2$;

если $k = 2$, то $SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}^*_{p_1^{k_1}} \times \mathbb{Z}^*_{p_2^{k_2}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2$;

если $k > 2$, то $SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^k} \times (\mathbb{Z}^*_{p_1^{k_1}} \times \mathbb{Z}^*_{p_2^{k_2}} \times \ldots \times \mathbb{Z}^*_{p_m^{k_m}})^2$.

По теореме 2 группа $\mathbb{Z}^*_{p_i^{k_i}}$ является циклической. Поэтому $SGL_2(\mathbb{Z}_n)$ представляется в виде прямого произведения $2m$, $2m+1$, $2m+3$ и $2m+4$ циклических групп при $k = 0$, $k = 1$, $k = 2$ и $k > 2$, соответственно. Следовательно, минимальное число образующих группы $SGL_2(\mathbb{Z}_n)$ не больше $2m$, $2m + 1$, $2m + 3$ и $2m + 4$ при $k = 0$, $k = 1$, $k = 2$ и $k > 2$, соответственно.

Вновь по теореме 2 имеем $\mathbb{Z}^*_{p_i^{k_i}} \cong \mathbb{Z}_{p^{k_i} - p^{k_i - 1}}$, что в свою очередь, в силу нечётности p_i, изоморфно $\mathbb{Z}_{2^{v_i}} \times \mathbb{Z}_{t_i}$, где $p^{k_i} - p^{k_i - 1} = 2^{v_i} t_i$ и t_i нечётно.

Таким образом,

$SGL_2(\mathbb{Z}_n) \cong (\mathbb{Z}_{2^{v_1}} \times \mathbb{Z}_{2^{v_2}} \times \ldots \times \mathbb{Z}_{2^{v_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 0$,

$SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times (\mathbb{Z}_{2^{x_1}} \times \mathbb{Z}_{2^{v_2}} \times \ldots \times \mathbb{Z}_{2^{v_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 1$,

$SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_{2^{v_1}} \times \mathbb{Z}_{2^{v_2}} \times \ldots \times \mathbb{Z}_{2^{v_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 2$,

$SGL_2(\mathbb{Z}_n) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^k} \times (\mathbb{Z}_{2^{v_1}} \times \mathbb{Z}_{2^{v_2}} \times \ldots \times \mathbb{Z}_{2^{v_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k > 2$.

По теореме 8 минимальное число образующих группы $SGL_2(\mathbb{Z}_n)$ не меньше d_2 — количества сомножителей чётного порядка в её разложении в прямое произведение циклических групп. Другими словами, оно не меньше, чем $2m$, $2m+1$, $2m+3$ и $2m+4$ при $k = 0$, $k = 1$, $k = 2$ и $k > 2$, соответственно. Теорема доказана. □

References

[1] Halbeisen L., Hamilton M., Růžička P., *Minimal generating sets of groups, rings, and fields*, Quaestiones Mathematicae, 2007, 30 (3), 355–363.
[2] Kostrikin A. I., *Introduction to Algebra*, Springer-Verlag, 1982, xiv+575 c.
[3] Maslova N. V., Belousov I. N., Minigulov N. A., *Open questions formulated at the 13th School-Conference on Group Theory Dedicated to V. A. Belonogov's 85th Birthday*, Trudy Instituta Matematiki i Mekhaniki, 2020, 26 (3), 275–285.
[4] Rososhek S. K., *Modified matrix modular cryptosystems*, British Journal of Mathematics & Computer Science, 2015, 5 (5), 613–636.

Konstantin Sergeevich Zyubin
Prostorny, Luchistaya, 5,
634045, Tomsk, Russia
Email address: konstantin.zyubin@gmail.com