Описание строения группы обратимых центросимметричных двумерных матриц над $\mathbb{Z}_{2^k}$

К. Зюбин
Томск, МАОУ СОШ № 32, 10Б, 2021

Аннотация

В системе шифрования с открытым ключом MMMC1, предложенной С. К. Росошеком в статье Modified Matrix Modular Cryptosystems [1], для создания ключей шифрования используются обратимые центросимметричные матрицы 2×2 над кольцом вычетов:

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

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. Настоящая статья показывает, что такая группа матриц изоморфна мультипликативной группе факторкольца $\mathbb{Z}_n[x] \,/\, \langle x^2 - 1 \rangle$, описывает её строение при $n = 2^k$.

1 Введение

Напомним, что кольцо вычетов по модулю n обозначается $\mathbb{Z}_n$. Группа мультипликативно обратимых элементов этого кольца обозначается $\mathbb{Z}_n^*$.

Пусть n — некоторое натуральное число. Обозначим через $SM_2(\mathbb{Z}_n)$ множество центросимметричных матриц 2×2 над кольцом $\mathbb{Z}_n$:

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

$SM_2(\mathbb{Z}_n)$ замкнуто относительно сложения и умножения матриц, поэтому $SM_2(\mathbb{Z}_n)$ является кольцом. Рассмотрим группу $SGL_2(\mathbb{Z}_n)$ мультипликативно обратимых элементов этого кольца. Определитель матрицы $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ равен $a^2 - b^2$. Поэтому

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

В некоторых системах шифрования, предложенных С. К. Росошеком, в частности, в системе шифрования с открытым ключом MMMC1 [1], для создания ключей используются элементы группы $SGL_2(\mathbb{Z}_n)$. 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 образующих этой группы.

Следующая теорема позволяет представить группу $SGL_2(\mathbb{Z}_{2^k})$ в виде прямого произведения циклических групп.

Теорема 1. *Пусть k — натуральное число. Тогда*
при $k = 1$

$$SGL_2(\mathbb{Z}_2) \simeq \mathbb{Z}_2,$$

при $k = 2$

$$SGL_2(\mathbb{Z}_4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

и при $k > 2$

$$SGL_2(\mathbb{Z}_{2^k}) \simeq \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_2.$$

2 Факторкольцо $\mathbb{Z}_n[x]/\langle x^2-1\rangle$

Рассмотрим факторкольцо $\mathbb{Z}_n[x]/\langle x^2-1\rangle$. Элементы этого факторкольца могут быть представлены в виде $a+bj$, где $a,b\in\mathbb{Z}_n$ и j такой элемент, что $j\notin\mathbb{Z}_n$ и $j^2=1$. При этом сложение и умножение этих элементов будет определяться следующим образом:

$$(a+bj)+(c+dj)=(a+c)+(b+d)j;$$

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

Здесь и далее мы будем обозначать это факторкольцо через $\mathbb{Z}_n[j]$.

Следующая теорема устанавливает изоморфизм между кольцом $SM_2(\mathbb{Z}_n)$ и факторкольцом $\mathbb{Z}_n[j]$. Утверждения о группе $SGL_2(\mathbb{Z}_n)$ удобнее доказывать в терминах мультипликативной группы факторкольца $\mathbb{Z}_n[j]$.

Теорема 2.

$$SM_2(\mathbb{Z}_n)\simeq\mathbb{Z}_n[j].$$

Доказательство теоремы 2.
Искомый изоморфизм устанавливается отображением $f\colon \left(\begin{smallmatrix}a & b\\ b & a\end{smallmatrix}\right)\mapsto a+bj$.
Ясно, что f является биекцией. Проверим, что f является гомоморфизмом:

$$\begin{array}{ccccc}
\begin{pmatrix}a & b\\ b & a\end{pmatrix} & + & \begin{pmatrix}c & d\\ d & c\end{pmatrix} & = & \begin{pmatrix}a+c & b+d\\ b+d & a+c\end{pmatrix}\\
\downarrow f & & \downarrow f & & \downarrow f\\
(a+bj) & + & (c+dj) & = & (a+c)+(b+d)j.
\end{array}$$

$$\begin{array}{ccccc}
\begin{pmatrix}a & b\\ b & a\end{pmatrix} & \times & \begin{pmatrix}c & d\\ d & c\end{pmatrix} & = & \begin{pmatrix}ac+bd & ad+bc\\ ad+bc & ac+bd\end{pmatrix}\\
\downarrow f & & \downarrow f & & \downarrow f\\
(a+bj) & \times & (c+dj) & = & (ac+bd)+(ad+bc)j.
\end{array}$$

Таким образом, f — изоморфизм и

$$SM_2(\mathbb{Z}_n)\simeq\mathbb{Z}_n[j].\ \square$$

Замечание. Отметим, что теорема 2 верна для произвольных ассоциативно-коммутативных колец R с единицей:

$$SM_2(R)\simeq R[x]/\langle x^2-1\rangle.$$

Из теоремы 2 имеем

$$SGL_2(\mathbb{Z}_n)\simeq\mathbb{Z}_n[j]^*.$$

Отсюда следует, что элемент $a+bj$ обратим в $\mathbb{Z}_n[j]$ тогда и только тогда, когда матрица $\left(\begin{smallmatrix}a & b\\ b & a\end{smallmatrix}\right)$ обратима в $SM_2(\mathbb{Z}_n)$, то есть когда определитель этой матрицы обратим: $a^2-b^2\in\mathbb{Z}_n^*$.

3 Доказательство теоремы 1

В доказательстве мы будет использоваться следующая

Теорема 3 ([2]). *Пусть a — натуральное. Тогда для натурального $a>2$*

$$\mathbb{Z}_{2^a}^*\simeq\mathbb{Z}_{2^{a-2}}\times\mathbb{Z}_2$$

и для $a=1$ и $a=2$

$$\mathbb{Z}_2^*\simeq\mathbb{Z}_1,\ \mathbb{Z}_4^*\simeq\mathbb{Z}_2.$$

Доказательство теоремы 1.
Если $k = 1$, то группа $SGL_2(\mathbb{Z}_2)$ изоморфна группе $\mathbb{Z}_2[j]^* = \{1, j\} \simeq \mathbb{Z}_2$.
Если $k = 2$, то группа $SGL_2(\mathbb{Z}_4)$ изоморфна группе

$$\mathbb{Z}_4[j]^* = \{\pm 1, \pm j, \pm 1 + 2j, 2 \pm j\} \simeq \langle -1 \rangle \times \langle j \rangle \times \langle 1 + 2j \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

При $k > 2$ по теореме 3 выполняется следующий изоморфизм:

$$\mathbb{Z}_{2^k}^* \simeq \mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2.$$

Докажем изоморфизм, равносильный требуемому в теореме:

$$\mathbb{Z}_{2^k}[j]^* \simeq \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_2.$$

Для этого укажем в $\mathbb{Z}_{2^k}[j]^*$ три подгруппы, прямым произведением которых она является.

Заметим, что группа $\mathbb{Z}_{2^k}^* = \left\{ a + 0j \middle| \, a \in \mathbb{Z}_{2^k}^* \right\}$ является подгруппой группы $\mathbb{Z}_{2^k}[j]^*$.
Далее, подгруппа $\{1, j\}$ группы $\mathbb{Z}_{2^k}[j]^*$ изоморфна группе $\mathbb{Z}_2$. Ясно, что эти две подгруппы пересекаются только по 1.
Рассмотрим подгруппу, порождённую элементом $1 + 2j$. Покажем, что её порядок равен 2^{k-1}, и она не содержит элементов, кроме 1, представимых в виде произведения элементов подгрупп $\mathbb{Z}_{2^k}^*$ и $\{1, j\}$.
Рассмотрим элементы вида $1 + 2s + 2sj$, где $s \in \mathbb{Z}_{2^k}$. Докажем, что множество элементов такого вида замкнуто относительно умножения. Действительно,

$$(1 + 2s_1 + 2s_1 j)(1 + 2s_2 + 2s_2 j) = 1 + 2(s_1 + s_2 + 2s_1 s_2) + 2(s_1 + s_2 + 2s_1 s_2)j.$$

Заметим, что любой ненулевой элемент $c \in \mathbb{Z}_{2^k}$ можно представить в виде $c = 2^t m$, где $t < k$ и m обратим. Докажем, что в таком представлении t определяется однозначно. Пусть $2^{t_1} m_1 = 2^{t_2} m_2$ и $t_1 < t_2$. Тогда $2^{t_2}(2^{t_1 - t_2} m_1 - m_2) = 0$. Степень $t_2 < k$, поэтому $2^{t_1 - t_2} m_1 - m_2$ является делителем 0. Однако $2^{t_1 - t_2} m_1 - m_2$ обратим в $\mathbb{Z}_{2^k}$. Противоречие.
Квадрат $(1 + 2^t m + 2^t mj)^2$, где элемент m обратим, имеет вид

$$1 + 2 \cdot 2^t m(2^t m + 1) + 2 \cdot 2^t m(2^t m + 1)j = 1 + 2^{t+1} m(2^t m + 1) + 2^{t+1} m(2^t m + 1)j.$$

При этом, если $t > 0$, то элемент $m(2^t m + 1)$ обратим.
Элемент $(1 + 2j)^2$ равен $1 + 2^2 + 2^2 j$. Тогда по доказанному ранее

$$(1 + 2j)^{2^t} = (1 + 2^2 + 2^2 j)^{2^{t-1}} = \ldots (1 + 2^{t-1+2} m + 2^{t-1+2} mj) = (1 + 2^{t+1} m + 2^{t+1} mj)$$

для некоторого обратимого m. Поэтому $(1 + 2j)^{2^{k-1}} = 1 + 2^k m + 2^k mj = 1$. Порядок элемента $1 + 2j$ делит степень двойки, следовательно, он сам является степенью 2. Так как $2^t m \neq 0$ при $t < k$, то для степеней двойки меньших чем $(k-1)$-я элемент $(1+2j)^{2^t} \neq 1$. Таким образом, порядок элемента $1+2j$ и порождённой им подгруппы равен 2^{k-1}. Кроме того, для каждой степени $v < 2^{k-1}$ выражение $(1+2j)^v$ принимает различные значения вида $1+2s+2sj$, и согласно принципу Дирихле пробегает их все ровно по одному разу. Таким образом, подгруппа, порождённая элементом $(1+2j)$, пересекается с произведением подгрупп $\mathbb{Z}_{2^k}^*$ и $\{1, j\}$ только по 1.

Докажем, что любой элемент $a + bj$ можно представить как произведение элемента $z \in \mathbb{Z}_{2^k}^*$, степени j (то есть j или $j^2 = 1$) и степени $1 + 2j$. Заметим, что так как $a + bj$ обратим, то ровно один из элементов a и b обратим, при этом второй имеет вид $2s$. Далее, $a^2 - b^2$ обратим, и, значит, элемент $a - b$ также обратим. Пусть $z = (a - b)^{-1}$. Тогда если b имеет вид $2s$, то

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

и если a имеет вид $2s$, то

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

Элемент $1+bz+bzj$ в первом случае и элемент $1+az+azj$ во втором случае по доказанному ранее являются некоторыми степенями элемента $1+2j$. Таким образом, любой элемент $\mathbb{Z}_{2^k}[j]^*$ представим в виде произведения элемента из $\mathbb{Z}_{2^k}^*$, степени элемента j и степени элемента $1+2j$.

Покажем, что такое представление единственно. Пусть $z_1(1+2j)^v = z_2(1+2j)^u$, $v \geqslant u$. Тогда $(1+2j)^{v-u} = z_1^{-1}z_2$, следовательно, $(1+2j)^{v-u} = 1$, $(1+2j)^v = (1+2j)^u$ и $z_1 = z_2$. Если же $z_1(1+2j)^v = jz_2(1+2j)^u$, то $(1+2j)^{v-u} = jz_1^{-1}z_2$. Тогда $(1+2j)^{v-u} = 1$, но $jz_1^{-1}z_2 \neq 1$. Противоречие.

Таким образом, $\mathbb{Z}_{2^k}[j]^* \simeq \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_2$. Теорема доказана.

Список литературы

[1] Rososhek S. K., *Modified matrix modular cryptosystems*, British Journal of Mathematics & Computer Science, 2015, 5 (5), 613–636.

[2] Арнольд В. И., *Группы Эйлера и арифметика геометрических прогрессий*, МЦНМО, 2003, 44 с.5

[3] Маслова Н. В., Белоусов И. Н., Минигулов Н. А., *Открытые проблемы, сформулированные на XIII Школе-конференции по теории групп, посвященной 85-летию В.А. Белоногова*, Труды Института математики и механики УрО РАН, 2020, 26 (3), 275–285.