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, для создания ключей шифрования используются обратимые центросимметричные матрицы 2×2 с элементами — вычетами по модулю n:

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

Настоящая статья показывает, что такая группа матриц изоморфна группе обратимых многочленов с коэффициентами из $\mathbb{Z}_n$ по модулю многочлена $x^2 - 1$. Затем доказывается, что при $n = 2^k$ $(k > 1)$ последняя группа изоморфна прямой сумме групп $\mathbb{Z}_{2^{k-1}}$, $\mathbb{Z}_{2^{k-2}}$ и двух экземпляров $\mathbb{Z}_2$.

1 Введение

Пусть n — некоторое целое положительное число. Напомним, что множество вычетов по модулю n с операциями сложения и умножения по модулю n обозначается $\mathbb{Z}_n$. Группа обратимых по умножению элементов этого множества обозначается $\mathbb{Z}_n^*$.

Обозначим через $SGL_2(\mathbb{Z}_n)$ группу обратимых по умножению матриц вида $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$, где $a, b \in \mathbb{Z}_n$. 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.

Теорема 1. *Пусть k — целое $\geqslant 2$. Тогда*

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

Замечание. Группа $SGL_2(\mathbb{Z}_{2^1})$ состоит всего из двух матриц $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ и изоморфна $\mathbb{Z}_2$.

2 Двойные числа над $\mathbb{Z}_n$

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

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

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

Обозначим через $SM_2(\mathbb{Z}_n)$ множество всех центросимметричных матриц 2×2 с элементами из $\mathbb{Z}_n$:

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

Множество $SM_2(\mathbb{Z}_n)$ замкнуто относительно сложения и умножения матриц.

Теорема 2. *Отображение $f\colon SM_2(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n[j]$ заданное формулой $f(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)) = a + bj$, где $a, b \in \mathbb{Z}_n$, является изоморфизмом колец.*

Доказательство.
Ясно, что f является биекцией. Проверим, что f сохраняет сложение и умножение:

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

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

Таким образом, f — изоморфизм $\square$.

Замечание. Аналог теоремы 2 верен для произвольных ассоциативно-коммутативных колец R с единицей:

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

Обозначим через $\mathbb{Z}_n[j]^*$ группу обратимых по умножению двойных чисел.

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 $\mathbb{Z}_n$.*

3 Доказательство теоремы 1

Благодаря следствию 3 для доказательства теоремы 1 достаточно установить изоморфизм:

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

Поскольку $\mathbb{Z}_{2^k}[j]^*$ является группой по умножению, требуемый изоморфизм будет удобнее доказывать в мультипликативной формулировке:

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

Последний изоморфизм, в свою очередь, будет вытекать из следующих лемм 5–7.

Лемма 5.

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

.

Лемма 6. *Порядок элемента $3 + 2j$ из группы $\mathbb{Z}_{2^k}[j]^*$ равен 2^{k-1}.*

Лемма 7. [2, Теорема 4] *Пусть a — целое $\geqslant 2$. Тогда*

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

Действительно, как только леммы 5 и 6 будут доказаны, будет справедлива следующая цепочка изоморфизмов:

$$\begin{gathered}\mathbb{Z}_{2^k}[j]^* \cong \mathbb{Z}_{2^k}^* \times \langle 3+2j\rangle \times \langle j\rangle \cong \\ \cong \mathbb{Z}_{2^k}^* \times \mathbb{Z}_{2^{a-2}} \times \langle j\rangle \cong \\ \cong \mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}} \times \langle j\rangle \cong \\ \cong \mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}} \times \mathbb{Z}_2,\end{gathered}$$

где первый изоморфизм верен в силу леммы 5, второй — в силу леммы 6, третий — по лемме 7 и, наконец, четвёртый выполняется так как $\langle j\rangle = \{1, j\} \cong \mathbb{Z}_2$.

Доказательство леммы 6.

Докажем по индукции, что $(3+2j)^{2^t} = (1+2+2j)^{2^t} = 1 + 2^{t+1}m + 2^{t+1}mj$ для некоторого обратимого m.

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

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

Элемент $m + 2^{t+1}m^2$ обратим в $\mathbb{Z}_{2^k}$.

Таким образом, $(1+2+2j)^{2^{k-1}} = 1 + 2^k m + 2^k mj = 1$. 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}. $\square$

Для доказательства леммы 5 потребуется описывать все элементы подгруппы $\langle 3+2j\rangle$.

Лемма 8. *Подгруппа $\langle 3+2j\rangle$ состоит из всех элементов вида $1+2s+2sj$, где $s \in \mathbb{Z}_{2^k}$ и только из них.*

Доказательство леммы 8.

Убедимся, что множество $Y = \{1+2s+2sj \mid s \in \mathbb{Z}_{2^k}\}$ является подгруппой группы $\mathbb{Z}_{2^k}[j]^*$, то есть содержит 1 и замкнуто относительно умножения и взятия обратного.

Действительно, $1 = 1 + 2\cdot 0 + 2\cdot 0\cdot j \in Y$.

Далее,

$$(1+2s_1+2s_1j)(1+2s_2+2s_2j) = 1 + 2(s_1+s_2+4s_1s_2) + 2(s_1+s_2+4s_1s_2)j \in Y.$$

Обратным к $1+2s+2sj$ будет элемент $1 + 2\cdot\frac{-s}{1+4s} + 2\cdot\frac{-s}{1+4s}\cdot j \in Y$.

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. $\square$

Доказательство леммы 5.

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. Согласно следствию 4, если элемент $a+bj$ обратим, то a^2-b^2 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 8 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 $z_1y_1x_1 = z_2y_2x_2$. Тогда $y_1y_2^{-1} = z_1^{-1}x_1^{-1}z_2x_2 = (z_1^{-1}z_2)(x_1^{-1}x_2)$. 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 $y_1y_2^{-1} = 1$ и $(z_1^{-1}z_2)(x_1^{-1}x_2) = 1$. Отсюда $y_1 = y_2$ и $z_1^{-1}z_2 = x_1x_2^{-1}$. 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 $x_1x_2^{-1} = 1$. Таким образом, $z_1 = z_2$, $y_1 = y_2$ и $x_1 = x_2$. $\square$

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.