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:

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

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. Настоящая статья показывает, что такая группа матриц изоморфна группе обратимых многочленов с коэффициентами из $\mathbb{Z}_n$ по модулю многочлена $x^2 - 1$ и описывает её строение при $n = 2^k$.

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 $SM_2(\mathbb{Z}_n)$ множество 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. Обозначим через $SGL_2(\mathbb{Z}_n)$ группу обратимых по умножению матриц из $SM_2(\mathbb{Z}_n)$. 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.

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

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 смежные классы 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 смежных классов также называется двойными числами над $\mathbb{Z}_n$ и обозначается $\mathbb{Z}_n[j]$, где j — это смежный класс 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:

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

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

Следующая теорема устанавливает изоморфизм между матрицами $SM_2(\mathbb{Z}_n)$ и двойными числами $\mathbb{Z}_n[j]$.

Теорема 2. *Отображение* $f\colon \left(\begin{smallmatrix} a & b\\ b & a\end{smallmatrix}\right) \mapsto a+bj$ $(a,b\in\mathbb{Z}_n)$ *является изоморфизмом между* $SM_2(\mathbb{Z}_n)$ *и* $\mathbb{Z}_n[j]$.

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

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

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

Таким образом, f — изоморфизм $\square$.

Замечание. Отметим, что 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. Для этой группы из теоремы 2 немедленно вытекает

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

При изоморфизме, заданном в теореме 2, элемент $a+bj$ является обратимым 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 будет использоваться следующая

Лемма 3. [2, Теорема 4] *Пусть* a *— целое* $\geqslant 2$. *Тогда*

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

Групповой операцией группы $\mathbb{Z}_{2^k}[j]^*$ является умножение, поэтому будем доказывать теорему 1 в мультипликативной терминологии. В силу леммы 3 и следствия из теоремы 2 достаточно доказать изоморфизм

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

Для этого вначале укажем в $\mathbb{Z}_{2^k}[j]^*$ три подгруппы, изоморфные соответственно $\mathbb{Z}_{2^k}^*$, $\mathbb{Z}_{2^{k-1}}$ и $\mathbb{Z}_2$, а затем убедимся, что $\mathbb{Z}_{2^k}[j]^*$ является их прямым произведением.

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 $\mathbb{Z}_2$.

Оставшуюся из искомых подгрупп образуют двойные числа вида $1 + 2s + 2sj$, где $s \in \mathbb{Z}_{2^k}$, что вытекает из следующих далее лемм 4–6. Множество двойных чисел такого вида будем обозначать $Y = \{1 + 2s + 2sj \mid s \in \mathbb{Z}_{2^k}\}$.

Лемма 4. *Элементы множества Y образуют подгруппу группы $\mathbb{Z}_{2^k}[j]^*$. Эта подгруппа имеет порядок 2^{k-1}.*

Доказательство.

Убедимся, что множество Y содержит 1 и замкнуто относительно умножения и взятия обратного. Действительно, $1 = 1 + 2 \cdot 0 + 2 \cdot 0 \cdot j \in Y$.

Далее,

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

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 $1+2s_1+2s_1 j = 1+2s_2+2s_2 j$, 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. □

Лемма 5. *Порядок элемента $1 + 2 + 2j$ из группы $\mathbb{Z}_{2^k}[j]^*$ равен 2^{k-1}.*

Доказательство.

Докажем по индукции, что $(1 + 2 + 2j)^{2^t} = 1 + 2^{t+1}m + 2^{t+1}mj$ 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

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

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

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

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}. □

Лемма 6. *Подгруппа Y изоморфна циклической группе $\mathbb{Z}_{2^{k-1}}$.*

Доказательство.

Элемент $1 + 2 + 2j$ принадлежит подгруппе Y. Поэтому подгруппа $\langle 1 + 2 + 2j \rangle$, порождённая элементом $1 + 2 + 2j$, лежит в Y. Поскольку порядок элемента $1 + 2 + 2j$ равен 2^{k-1}, то порядок порождённой им группы также равен 2^{k-1}. Однако, порядок подгруппы Y тоже равен 2^{k-1}. Следовательно, она порождается элементом $1 + 2 + 2j$ и является циклической группой порядка 2^{k-1}, то есть изоморфна $\mathbb{Z}_{2^{k-1}}$. □

Следующая лемма позволяет завершить доказательство теоремы 1.

Лемма 7. *Группа $\mathbb{Z}_{2^k}[j]^*$ является прямым произведением подгрупп $\{1, j\}$, Y и $\mathbb{Z}_{2^k}^*$.*

Доказательство.

Убедимся, что любой элемент $a + bj \in \mathbb{Z}_{2^k}[j]^*$ может быть единственным образом представлен в виде произведения xyz, где $x \in \{1, j\}$, $y \in Y$ и $z \in \mathbb{Z}_{2^k}^*$.

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

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

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

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

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

Проверим, что такое представление единственно. Пусть $x_1, x_2 \in \{1, j\}$, $y_1, y_2 \in Y$, $z_1, z_2 \in \mathbb{Z}_{2^k}^*$ и при этом $x_1y_1z_1 = x_2y_2z_2$. 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 Y, 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 $\{1, j\}$. 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 $\{1, j\}$ пересекаются только по 1. Имеем $y_1 = y_2$, $z_1^{-1}z_2 = 1$ и $x_1x_2^{-1} = 1$. Таким образом, $x_1 = x_2$, $y_1 = y_2$ и $z_1 = z_2$. □

Согласно лемме 7 группа $\mathbb{Z}_{2^k}[j]^*$ является прямым произведением подгрупп, изоморфных соответственно $\mathbb{Z}_{2^k}^*$, $\mathbb{Z}_{2^{k-1}}$, $\mathbb{Z}_2$. Переходя к аддитивной формулировке и учитывая лемму 3, получаем

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

Теорема 1 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.