Национальная академия наук Беларуси
Труды Института математики НАН Беларуси. 2025. Том 33. № 2. С. 21–27

УДК 512.544.6, 512.71, 519.719.2 EDN: HQZGXB

ОБ ОДНОЙ ФУНДАМЕНТАЛЬНОЙ ОБЛАСТИ В СПЕЦИАЛЬНОЙ ЛИНЕЙНОЙ ГРУППЕ

Г. В. Матвеев[1], **А. А. Осиновская**[2]

[1]*Белорусский государственный университет, Минск, Беларусь*
[2]*Институт математики НАН Беларуси, Минск, Беларусь*
e-mail: matveev@bsu.by, anna@im.bas-net.by

Поступила: 09.09.2025 **Исправлена:** 13.10.2025 **Принята:** 15.12.2025

Ключевые слова: специальная линейная группа, конгруэнц-подгруппа, фундаментальная область.

Аннотация. Модулярное разделение секрета в группе $SL_2(\mathbb{Z})$ было предложено Янчевским, Матвеевым и Говорушко. В настоящей работе построена в явном виде вся фундаментальная область при действии левыми сдвигами главной конгруэнц-подгруппы на группе $SL_2(\mathbb{Z})$, что представляет дополнительные возможности для построения схем, так как эта область является пространством хранимых секретов схемы разделения секрета.

ON A FUNDAMENTAL DOMAIN IN A SPECIAL LINEAR GROUP

G. V. Matveev[1], **A. A. Osinovskaya**[2]

[1]*Belarusian State University, Minsk, Belarus*
[2]*Institute of Mathematics of the National Academy of Sciences of Belarus, Minsk, Belarus*
e-mail: matveev@bsu.by, anna@im.bas-net.by

Received: 09.09.2025 **Revised:** 13.10.2025 **Accepted:** 15.12.2025

Keywords: special linear group, congruence subgroup, fundamental domain.

Abstract. Modular secret sharing in the group $SL_2(\mathbb{Z})$ was recently proposed by Yanchevskiy, Matveev, and Govorushko. In this paper we have constructed in explicit form the entire fundamental domain under the action of left shifts of the principal congruence subgroup on the group $SL_2(\mathbb{Z})$, which presents additional possibilities for constructing schemes, since the domain is the space of stored secrets of the secret sharing scheme.

Модулярное разделение секрета в группе $SL_2(\mathbb{Z})$ было недавно предложено в работе [1]. Специальная линейная группа $SL_2(\mathbb{Z})$ – это матрицы над кольцом целых чисел размера 2×2 с единичным определителем. В качестве пространства ключей и хранимого ключа используется фундаментальная область при действии левыми сдвигами главной конгруэнц-подгруппы на группе $SL_2(\mathbb{Z})$. Однако построить всю фундаментальную область нам не удалось. Построена лишь часть, пригодная для реализации алгоритма разделения секрета.

Попытки построить всю фундаментальную область предпринимались и ранее [2], вне связи с разделением секрета, т. е. эта задача интересна и чисто с алгебраической точки зрения. Уместно будет напомнить, что в книге [3, §7.1, с. 438–439] отмечается нетривиальный характер задачи подъема решений уравнения по некоторой системе модулей до целочисленного решения. С нашей точки зрения задача подъема решений – это в точности алгоритм восстановления секрета. Вместе с тем в работах [1; 4] показано, что знание фундаментальной области значительно облегчает восстановление секрета.

В настоящей работе нами построена в явном виде вся фундаментальная область при действии левыми сдвигами главной конгруэнц-подгруппы на группе $SL_2(\mathbb{Z})$, что представляет дополнительные возможности для разделения секрета в этой группе.

Пусть $m \neq 1$ – целое положительное число. Напомним определения конгруэнц-подгрупп в группе $SL_2(\mathbb{Z})$:

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{m} \right\},$$

$$\Gamma(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{m} \right\}.$$

Здесь и далее сравнимость матриц по модулю m означает их поэлементную сравнимость. Известно, что $\Gamma_0(m)$ и $\Gamma(m)$ действительно подгруппы и справедливы включения

$$\Gamma(m) \subset \Gamma_0(m) \subset SL_2(\mathbb{Z}).$$

Подгруппа $\Gamma(m)$ называется главной конгруэнц-подгруппой по модулю m.

Главная конгруэнц-подгруппа $\Gamma(m)$ действует левыми сдвигами на группах $\Gamma_0(m)$ и $SL_2(\mathbb{Z})$. Система представителей орбит называется фундаментальной областью. Имеем $\Gamma(m) \lhd SL_2(\mathbb{Z})$ [5, § 2.1]. Две матрицы A и A' принадлежат одной орбите, если $A\Gamma(m) = A'\Gamma(m)$. Это равенство удобно трактовать иначе.

Лемма 1.1 [1]. *Условие $A\Gamma(m) = A'\Gamma(m)$ эквивалентно условию $A \equiv A' \pmod{m}$.*

В свою очередь группа $\Gamma_0(m)$ действует левыми сдвигами на группе $SL_2(\mathbb{Z})$.

Лемма 1.2. *Для матриц*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$$

условие $A\Gamma_0(m) = A'\Gamma_0(m)$ эквивалентно условию $ac' \equiv a'c \pmod{m}$.

Доказательство. Наше условие означает

$$A^{-1}A' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(m),$$

что равносильно сравнению $ac' \equiv a'c \pmod{m}$. □

Лемма 1.3. *Пусть число m составное и $m = aa_1$ – некоторое его разложение на нетривиальные множители. Для любого целого числа c, $0 < c \leqslant a_1$, $(c, a, a_1) = 1$, существует единственное целое число $c_1 \leqslant \frac{m}{(a,a_1)}$ такое, что $(c_1, a) = 1$ и $c_1 \equiv c \pmod{a_1}$.*

Доказательство. По китайской теореме об остатках существует единственное целое число $c_1 \leqslant \frac{m}{(a,a_1)}$, для которого $c_1 \equiv c \pmod{a_1}$ и $c_1 \equiv 1 \pmod{p}$ для любого простого числа p такого, что $p \mid a$ и $p \nmid a_1$. Возьмем теперь любое простое число p со свойствами $p \mid a$ и $p \mid a_1$. Так как $(c, a, a_1) = 1$, то $p \nmid c$. Поскольку $c_1 \equiv c \pmod{p}$, то $p \nmid c_1$. Отсюда следует, что $(c_1, a) = 1$ и c_1 является искомым. Предложение доказано. □

Следствие 1.4. *Если $m = p^k$, где p простое, то $c_1 = c$.*

Рассмотрим произвольный составной модуль m. Для любой пары (a, c), где a – нетривиальный делитель числа m, $m = aa_1$, $0 < c \leqslant a_1$, $(c, a, a_1) = 1$, определим матрицу

$$M(a, c) = \begin{pmatrix} a & b \\ c_1 & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

где c_1 такое же, как в лемме 1.3. Такие матрицы существуют (хотя и определены неоднозначно). Действительно, поскольку $(a, c_1) = 1$, то можно найти целочисленное разложение $az + c_1 w = 1$ НОДа. Положив $d := z$ и $b := -w$, получаем искомую матрицу. Для каждой пары (a, c) фиксируем одну такую матрицу.

Лемма 1.5. *Если $(a, c) \neq (a', c')$, то $M(a, c)\Gamma_0(m) \neq M(a', c')\Gamma_0(m)$.*

Доказательство. Будем доказывать от противного. По лемме 1.2 из $M(a, c)\Gamma_0(m) = M(a, c')\Gamma_0(m)$ следует, что $ac'_1 \equiv ac_1 \pmod{m}$, а значит, $c'_1 \equiv c_1 \pmod{a_1}$. По построению чисел c_1 и c'_1, $c' \equiv c \pmod{a_1}$, откуда получаем $c' = c$, поскольку $0 < c', c \leqslant a_1$.

Пусть теперь $M(a, c)\Gamma_0(m) = M(a', c')\Gamma_0(m)$ при $a \neq a'$. Тогда $ac'_1 \equiv a'c_1 \pmod{m}$. Без ограничения общности можем считать, что $a \nmid a'$. Из предыдущего сравнения получаем, что $ac'_1 = a'c_1 + mk$ для некоторого $k \in \mathbb{Z}$. Значит, $a \mid a'c_1$. Поскольку $(a, c_1) = 1$, то $a \mid a'$. Полученное противоречие доказывает лемму. □

Положим

$$M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ N(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \ 0 \leqslant c < m.$$

Для произвольного $m \neq 1$ определим множество

$$\mathcal{M} = \{M, N(c),\ 0 \leqslant c < m,\ M(a,c),\ m = aa_1,\ a, a_1 \neq 1,\ 0 < c \leqslant a_1,\ (c,a,a_1) = 1\}.$$

Заметим, что если m простое, то

$$\mathcal{M} = \{M, N(c),\ 0 \leqslant c < m\}.$$

Теорема 1.6. *Пусть m – некоторый целочисленный модуль. Тогда множество $\mathcal{M}$ составляет фундаментальную область группы $SL_2(\mathbb{Z})$ относительно подгруппы $\Gamma_0(m)$.*

Доказательство. Сначала покажем, что смежные классы для всех этих матриц различны.

Будем доказывать от противного. Воспользуемся леммой 1.2. Если $M\Gamma_0(m) = N(c)\Gamma_0(m)$, то $0 \equiv 1 \pmod{m}$ и мы получаем противоречие. Из $M\Gamma_0(m) = M(a,c)\Gamma_0(m)$ следует, что $0 \equiv a \pmod{m}$, и снова приходим к противоречию. Из $N(c)\Gamma_0(m) = N(c')\Gamma_0(m)$ вытекает $c \equiv c' \pmod{m}$, а значит, $c = c'$. Если $N(c)\Gamma_0(m) = M(a',c')\Gamma_0(m)$, то $c_1' \equiv a'c \pmod{m}$, что влечет $a' \mid c_1'$, но в то же время $(c_1', a') = 1$, получаем противоречие. Наконец, по лемме 1.5 из $M(a,c)\Gamma_0(m) = M(a',c')\Gamma_0(m)$ следует, что $(a,c) = (a',c')$.

Установим теперь, что любая матрица

$$A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$$

лежит в смежном классе для одной из этих матриц.

1) Действительно, если $a' \equiv 0 \pmod{m}$, то по лемме 1.2, $A'\Gamma_0(m) = M\Gamma_0(m)$.

2) Пусть $(a', m) = 1$. Тогда существует целочисленное разложение НОДа $a't + my = 1$. Положим $c = c't \pmod{m}$. Тогда $c < m$, $a'c \equiv a'c't \equiv c'(1 - my) \equiv c' \pmod{m}$ и по лемме 1.2, $A'\Gamma_0(m) = N(c)\Gamma_0(m)$.

3) В остальных случаях положим $a := (a', m) > 1$. Тогда существуют целые числа t и y, для которых $a't + my = a$. Отсюда следует, что $\frac{a'}{a}t + a_1 y = 1$, а значит, $(t, a_1) = 1$.

Заметим, что в данном случае $b' \neq 0$, так как иначе $|A'| = a'd' \neq 1$. Если $d' = 0$, то из $|A'| = 1$ следует, что $c' = 1$, $b' = -1$, либо $c' = -1$, $b' = 1$. В обоих случаях $(a', c') = 1$. Если же $d' \neq 0$, то $(a', c') = 1$, поскольку $|A'| = a'd' - b'c' = 1$. Значит, во всех случаях $(a', c') = 1$, откуда вытекает $(a, c') = 1$.

Определим целое число c из равенства $c := c't \bmod a_1$. Пусть $p \mid c$, a и a_1 для некоторого простого p. Тогда $p \mid c't$, а значит $p \mid c'$ либо $p \mid t$. В обоих случаях получаем противоречие. Если $p \mid c'$, то противоречие с $(a, c') = 1$, поскольку $p \mid a$. Если $p \mid t$, то противоречие с $(a_1, t) = 1$, поскольку $p \mid a_1$. Следовательно, $(c, a, a_1) = 1$ и для такой пары (a, c) можно построить матрицу $M(a,c) \in SL_2(\mathbb{Z})$.

Поскольку $c_1 = c't + a_1 k$, $k \in \mathbb{Z}$, то

$$c_1 a' = c'(a't) + mk\frac{a'}{a} = c'(a - my) + mk\frac{a'}{a} = c'a + m(k\frac{a'}{a} - yc').$$

Из леммы 1.2 вытекает, что $M(a,c)\Gamma_0(m) = A'\Gamma_0(m)$. □

Замечание 1.7. *Известно, что*

$$[SL_2(\mathbb{Z}) : \Gamma_0(m)] = m\prod_{p \mid m}\left(1 + \frac{1}{p}\right). \tag{1}$$

В [5, предложение 2.1.1] *этот индекс найден как частное индексов $[SL_2(\mathbb{Z}) : \Gamma(m)]/[\Gamma_0(m) : \Gamma(m)]$. Из теоремы* 1.6 *следует еще одно, непосредственное, доказательство этого факта.*

Доказательство. Если $m = p^k$, $k \geqslant 1$, то по теореме 1.6 и следствию 1.4

$$[SL_2(\mathbb{Z}) : \Gamma_0(p^k)] = |\mathcal{M}| = 1 + p^k + \sum_{i=1}^{k-1}(p^{k-i} - p^{k-i-1}) = p^k + p^{k-1}$$

и мы получили искомое.

Пусть теперь число m имеет следующее каноническое разложение на простые множители:

$$m = p_1^{e_1} \dots p_r^{e_r}.$$

Оно индуцирует естественное отображение множеств смежных классов

$$\psi : SL_2(\mathbb{Z})\backslash\Gamma_0(m) \to SL_2(\mathbb{Z})\backslash\Gamma_0(p_1^{e_1}) \times \ldots \times SL_2(\mathbb{Z})\backslash\Gamma_0(p_r^{e_r}),$$

задаваемое формулой $A\Gamma_0(m) \mapsto (A\Gamma_0(p_1^{e_1}), \ldots, A\Gamma_0(p_r^{e_r}))$.

Отображение ψ является биекцией. Действительно, рассмотрим две матрицы

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Если $A\Gamma_0(p_i^{e_i}) = A'\Gamma_0(p_i^{e_i})$ для любого $i, 1 \leqslant i \leqslant r$, то по лемме 1.2 $ac' \equiv a'c \pmod{p_i^{e_i}}$. Применяя китайскую теорему об остатках, получаем, что $ac' \equiv a'c \pmod{m}$. Следовательно, $A\Gamma_0(m) = A'\Gamma_0(m)$ и отображение ψ инъективно.

Докажем сюръективность ψ. Пусть

$$(A_1\Gamma_0(p_1^{e_1}), \ldots, A_r\Gamma_0(p_r^{e_r})) \in SL_2(\mathbb{Z})\backslash\Gamma_0(p_1^{e_1}) \times \ldots \times SL_2(\mathbb{Z})\backslash\Gamma_0(p_r^{e_r}).$$

Применяя китайскую теорему об остатках, можно найти матрицу A' такую, что $A'\Gamma_0(p_i^{e_i}) = A_i\Gamma_0(p_i^{e_i})$ для всех i. Заметим, что A' не обязательно принадлежит группе $SL_2(\mathbb{Z})$, однако из китайской теоремы об остатках следует, что $\det A' \equiv 1 \pmod{m}$. Поскольку отображение $f : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z})$ сюръективно [5, §2.1], существует матрица $A \in SL_2(\mathbb{Z})$ такая, что $A\Gamma_0(m) = A'\Gamma_0(m)$. Тогда $A\Gamma_0(m)$ является искомым прообразом.

Значит,

$$[SL_2(\mathbb{Z}) : \Gamma_0(m)] = [SL_2(\mathbb{Z}) : \Gamma_0(p_1^{e_1})] \cdot \ldots \cdot [SL_2(\mathbb{Z}) : \Gamma_0(p_r^{e_r})],$$

откуда получаем формулу (1). □

Укажем теперь представителей смежных классов группы $SL_2(\mathbb{Z})$ по подгруппе $\Gamma(m)$. Пусть $\varphi(m)$ – количество натуральных чисел $< m$ и взаимно простых с ним (функция Эйлера). Тогда

$$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right).$$

Обозначим все такие числа через $\varepsilon_i \in \mathbb{Z}$, $1 \leqslant i \leqslant \varphi(m)$. Тогда для любого ε_i существует число $\varepsilon_i' \in \mathbb{Z}$ такое, что

$$\varepsilon_i\varepsilon_i' = 1 + mk_i$$

и ε_i', k_i однозначно определяются выбором ε_i. Введем матрицы

$$B_{i,j} = \begin{pmatrix} \varepsilon_i + jm & k_i + j\varepsilon_i' \\ m & \varepsilon_i' \end{pmatrix},$$

где $i = 1, \ldots, \varphi(m)$, $j = 0, \ldots, m-1$,

$$C_{i,j,l} = \begin{pmatrix} \varepsilon_i + jm & k_i + j\varepsilon_i' \\ m + (\varepsilon_i + jm)l & \varepsilon_i' + (k_i + j\varepsilon_i')l \end{pmatrix},$$

где $i = 1, \ldots, \varphi(m)$, $j, l = 0, \ldots, m-1$, и

$$D_{i,j} = \begin{pmatrix} -m & -\varepsilon_i' \\ \varepsilon_i + jm & k_i + j\varepsilon_i' \end{pmatrix},$$

где $i = 1, \ldots, \varphi(m)$, $j = 0, \ldots, m-1$.

Положим

$$\mathcal{B} = \{B_{i,j} \mid i = 1, \ldots, \varphi(m),\ j = 0, \ldots, m-1\},$$
$$\mathcal{C} = \{C_{i,j,l} \mid i = 1, \ldots, \varphi(m),\ j, l = 0, \ldots, m-1\},$$
$$\mathcal{D} = \{D_{i,j} \mid i = 1, \ldots, \varphi(m),\ j = 0, \ldots, m-1\}.$$

Лемма 1.8. *Пусть m – произвольный модуль.*
(i) $\mathcal{B} \subset \Gamma_0(m)$, $\mathcal{C}$ и $\mathcal{D} \subset SL_2(\mathbb{Z})$.
(ii) Матрицы $C_{i,j,l}$ и $D_{i,j}$ попарно несравнимы по модулю m.

(*iii*) *Множество* $\mathcal{B}$ *составляет фундаментальную область группы* $\Gamma_0(m)$ *относительно подгруппы* $\Gamma(m)$.

Доказательство. (*i*) Определитель матрицы $C_{i,j,l}$ равен

$$(\varepsilon_i + jm)(\varepsilon_i' + (k_i + j\varepsilon_i')l) - (m + (\varepsilon_i + jm)l)(k_i + j\varepsilon_i') =$$

$$= (\varepsilon_i + jm)(\varepsilon_i' + (k_i + j\varepsilon_i')l - l(k_i + j\varepsilon_i')) - m(k_i + j\varepsilon_i') =$$

$$= (\varepsilon_i + jm)\varepsilon_i' - m(k_i + j\varepsilon_i') = \varepsilon_i\varepsilon_i' - mk_i = 1.$$

Поскольку $B_{i,j} = C_{i,j,0}$, отсюда получаем, что $|B_{i,j}| = 1$. Очевидно, $B_{i,j} \in \Gamma_0(m)$. Также очевидно, что $|D_{i,j}| = |C_{i,j,0}| = 1$.

(*ii*) Докажем от противного, что матрицы $C_{i,j,l}$ попарно несравнимы при различных i, j, l. Действительно, если $i_1 \neq i_2$, то

$$\varepsilon_{i_1} + j_1 m \equiv \varepsilon_{i_2} + j_2 m (\bmod\ m) \Leftrightarrow \varepsilon_{i_1} \equiv \varepsilon_{i_2} (\bmod\ m).$$

Если $i_1 = i_2 = i$, но $j_1 \neq j_2$, то

$$k_i + j_1\varepsilon_i' \equiv k_i + j_2\varepsilon_i' (\bmod\ m) \Leftrightarrow j_1\varepsilon_i' \equiv j_2\varepsilon_i' (\bmod\ m) \Leftrightarrow j_1 \equiv j_2 (\bmod\ m).$$

Если $i_1 = i_2 = i$, $j_1 = j_2 = j$, но $l_1 \neq l_2$, то

$$m + (\varepsilon_i + jm)l_1 \equiv m + (\varepsilon_i + jm)l_2 (\bmod\ m) \Leftrightarrow$$

$$\Leftrightarrow \varepsilon_i l_1 \equiv \varepsilon_i l_2 (\bmod\ m) \Leftrightarrow l_1 \equiv l_2 (\bmod\ m).$$

Во всех случаях приходим к противоречию. Аналогично получаем, что матрицы $D_{i,j}$ попарно несравнимы при различных i, j. Докажем теперь, что $C_{i_1,j_1,l_1} \neq D_{i_2,j_2}$ при любых i_1, i_2, j_1, j_2, l_1. Действительно, $\varepsilon_{i_1} + j_1 m \neq -m$, поскольку $m \nmid \varepsilon_{i_1}$.

(*iii*) Это доказано в [1]. □

Теорема 1.9. *Если* $m = p$, *то множество* $\mathcal{C} \cup \mathcal{D}$ *составляет всю фундаментальную область группы* $SL_2(\mathbb{Z})$ *относительно подгруппы* $\Gamma(p)$.

Доказательство. Действительно, согласно [5, предложение 2.1.1]

$$[SL_2(\mathbb{Z}) : \Gamma(p)] = p(p^2 - 1),$$

а это в точности число всех матриц $D_{i,j}$ и $C_{i,j,l}$. □

Тем самым для простого модуля получены представители фундаментальной области в виде, удобном для реализации в схеме разделения секрета.

Теорема 1.10. *Пусть* m *– некоторый целочисленный модуль. Тогда матрицы* AB *для* $A \in \mathcal{M}$ *и* $B \in \mathcal{B}$ *составляют фундаментальную область группы* $SL_2(\mathbb{Z})$ *по подгруппе* $\Gamma(m)$.

Доказательство. Утверждение следует из теоремы 1.6 и леммы 1.8 (*iii*). □

Пример 1.11. Приведем в явном виде пример фундаментальной области для $m = 6$. Согласно предложению 2.1.1 из [5]

$$[\Gamma_0(6) : \Gamma(6)] = 12,\ [SL_2(\mathbb{Z}) : \Gamma_0(6)] = 12.$$

Имеем

$$\mathcal{B} = \left\{ \begin{pmatrix} 1+6j & j \\ 6 & 1 \end{pmatrix}, \begin{pmatrix} 5+6j & 4+5j \\ 6 & 5 \end{pmatrix},\ j = 0, \ldots, 5 \right\};$$

$$\mathcal{M} = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},\ c = 0, \ldots, 5, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \right\}.$$

Тогда по теореме 1.10 фундаментальная область состоит из произведений матриц из этих множеств.

На основе найденной фундаментальной области можно построить схему разделения секрета с большим пространством хранимых ключей, чем в работе [1]. Для этого удобно использовать матрицы $\mathcal{C}$, имеющие хорошую параметризацию. Они занимают большую часть фундаментальной области группы $SL_2(\mathbb{Z})$ относительно подгруппы $\Gamma(m)$ поскольку их количество равно $m^2\varphi(m)$,

а при этом [5, предложение 2.1.1]

$$[SL_2(\mathbb{Z}) : \Gamma(m)] = m^2 \varphi(m) \prod_{p|m} \left(1 + \frac{1}{p}\right).$$

С помощью этих матриц построим в группе $SL_2(\mathbb{Z})$ аналог модулярной пороговой схемы разделения секрета по Миньотту [6]. Пусть у нас имеется k участников и разрешенным является всякое подмножество, если число участников в нем не меньше, чем t.

Выберем систему $m_1 < m_2 < \ldots < m_k$ попарно взаимно простых модулей, для которой выполнено условие Миньотта

$$M_1 = m_{k-t+2} m_{k-t+3} \ldots m_k < m_1 m_2 \ldots m_t = M_2.$$

Одновременно требуется, чтобы разность $M_2 - M_1$ была по возможности большой.

В качестве открытых ключей берутся главные конгруэнц-подгруппы $\Gamma(m_1), \ldots, \Gamma(m_k)$, где модули $m_1, \ldots, m_k$ те же, что и в пороговой модулярной схеме Миньотта.

Секретом является матрица $S = C_{i,j,l} \in \mathcal{C}$, где $m = m_1 \ldots m_k$, $i = 1, \ldots, \varphi(m)$, причем $M_1 < < \varepsilon_i < M_2$, $M_1 < j, l < M_2$.

Частичными секретами участников являются поэлементные вычеты этой матрицы по модулям $m_1, \ldots, m_k$. Например, частичным секретом первого участника будет образ матрицы S при каноническом эпиморфизме

$$SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z})/\Gamma(m_1) \cong SL_2(\mathbb{Z}/m_1\mathbb{Z}),$$

что является аналогом обычного частичного секрета в схеме Миньотта.

Теорема 1.12. *Секрет S однозначно восстанавливается по частичным секретам подмножества участников A, где $|A| \geqslant t$.*

Доказательство. Модуль m находится автоматически.

Поскольку нам известны $\varepsilon_i + jm \equiv \varepsilon_i (\bmod\ m_r)$, $r \in A$, по китайской теореме об остатках находим $\varepsilon_i (\bmod \prod\limits_{r \in A} m_r)$. Найденное решение в силу выбора ε_i будет одним и тем же по модулям $\prod\limits_{r \in A} m_r$ и m, так как $\varepsilon_i < \prod\limits_{r \in A} m_r \leqslant M_2$.

Решив сравнение $\varepsilon_i \varepsilon_i' \equiv 1 \ (\bmod\ m)$, находим ε_i'. Напомним, что все модули $m_1, \ldots, m_k$ известны участникам.

Число k_i однозначно восстанавливается по формуле $k_i = \frac{\varepsilon_i \varepsilon_i' - 1}{m}$.

Нам известны $k_i + j\varepsilon_i' \ (\bmod\ m_r)$, $r \in A$, Используя китайскую теорему об остатках, находим $k_i + j\varepsilon_i' (\bmod \prod\limits_{r \in A} m_r)$. Поскольку $(\varepsilon_i', m) = 1$, то значение j по модулю $\prod\limits_{r \in A} m_r$ восстанавливается однозначно. Так как $j < M_2$, отсюда получаем j.

Аналогично из $m + (\varepsilon_i + jm)l \equiv \varepsilon_i l \ (\bmod\ m_r)$, $r \in A$, находим $\varepsilon_i l \ (\bmod \prod\limits_{r \in A} m_r)$. Используя тот факт, что $(\varepsilon_i, m) = 1$ и $l < M_2$, получаем l.

Таким образом, матрица S восстановлена корректно. □

Работа выполнена при финансовой поддержке БРФФИ, договор № Ф25-012.

Литература

1. *Янчевский В. И., Говорушко И. О., Матвеев Г. В.* Разделение секрета в специальной линейной группе // Информатика. 2024. Т. 21, № 3. С. 23–31. https://doi.org/10.37661/1816-0301-2024-21-3-23-31

2. *Harcos G.* CEU lecture notes: a set of representatives for $\Gamma_0(q)\backslash SL_2(\mathbb{Z})$ [Electronic resourse]. – Mode of access: https://users.renyi.hu/g̃Harcos/CEU_Gamma0(q).pdf

3. *Платонов В. П., Рапинчук А. С.* Алгебраические группы и теория чисел. М. : Наука, 1991. 656 с.

4. *Матвеев Г. В., Осиновская А. А., Янчевский В. И.* Фундаментальная область в специальной линейной группе $SL_2(\mathbb{F}_p[x])$ и схема разделения секрета на ее основе // Труды Института математики НАН Беларуси. 2024. Т. 32, № 2. С. 7–16.

5. *Di Matteo G.* The action of $SL_2(\mathbb{Z})$ on the upper-half complex plane[Electronic resourse]. – Mode of access: https://www.dimatteo.is/Mathematics/Courses/Modular-forms/02-SL2Z.pdf

6. *Mignotte M.* How to share a secret // Lecture Notes in Computer Science. 1983. Vol. 149. P. 371–375.

References

1. Yanchevskiy V. I., Govorushko I. O., Matveev G. V. Secret sharing in the special linear group. *Informatics*, 2024, vol. 21, no. 3, pp. 23–31 (in Russian). https://doi.org/10.37661/1816-0301-2024-21-3-23-31

2. *Harcos G. CEU lecture notes: a set of representatives for* $\Gamma_0(q)\backslash SL_2(\mathbb{Z})$ [Electronic resourse]. – Mode of access: https://users.renyi.hu/g̃Harcos/CEU_Gamma0(q).pdf

3. Platonov V., Rapinchuk A. *Algebraic groups and number theory*. Pure and Applied Mathematics, 139. Boston, Academic Press Inc., 1994. xii+614 p.

4. *Di Matteo G. The action of* $SL_2(\mathbb{Z})$ *on the upper-half complex plane* [Electronic resourse]. – Mode of access: https://www.dimatteo.is/Mathematics/Courses/Modular-forms/02-SL2Z.pdf

5. Matveev G. V., Osinovskaya A. A., Yanchevskii V. I. A fundamental domain in the special linear group and secret sharing on its basis. *Proceedings of the Institute of Mathathematics of the NAS of Belarus*, 2024, vol. 32, no. 2, pp. 23–31 (in Russian).

6. Mignotte M. How to share a secret. *Lecture Notes in Computer Science*, 1983, vol. 149, pp. 371–375.