Описание строения группы двумерных матриц из модифицированной модулярной криптосистемы

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 [2], для создания ключей шифрования используются матрицы 2×2 специального вида:

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

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 минимальном числе её образующих. Настоящая статья отвечает на вопрос В. А. Романькова.

§1 Введение

Здесь и далее будем считать, что все кольца, рассматриваемые в статье, являются ассоциативно-коммутативными кольцами с единицей. Группа мультипликативно обратимых элементов кольца R обозначается R^*. Напомним, что кольцо вычетов по модулю n обозначается $\mathbb{Z}_n$.

Пусть R — некоторое коммутативно-ассоциативное кольцо с единицей. Обозначим через $RM(R)$ множество матриц 2×2:

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

$RM(R)$ замкнуто относительно сложения и умножения матриц, поэтому $RM(R)$ является кольцом. Рассмотрим группу мильтипликативно обратимых элементов этого кольца $RM(R)^*$.

Определитель матрицы $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ равен $a^2 - b^2$. Поэтому

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

В некоторых системах шифрования, предложенных С. К. Росошеком, в частности, в системе шифрования с открытым ключом MMMC1 [2], для создания ключей используются элементы $RM(\mathbb{Z}_n)^*$:

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

На школе-конференции по теории групп, посвящённой 85-летию В. А. Белоногова (2020), В. А. Романьковым был поставлен вопрос об описании строения этой группы матриц и минимальном числе образующих этой группы.

Следующие три теоремы позволяют описать мультипликативную группу кольца $RM(\mathbb{Z}_n)$.

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

$$RM(\mathbb{Z}_{m_1 m_2})^* \simeq RM(\mathbb{Z}_{m_1})^* \times RM(\mathbb{Z}_{m_2})^*.$$

Теорема 2. *Если n — нечётное натуральное число, то*

$$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_n^* \times \mathbb{Z}_n^*.$$

Теорема 3. *Если $n = 2^k$, где k — натуральное, то*

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

Таким образом, теоремы 1-3 сводят описание $RM(\mathbb{Z}_n)^*$ к группам $\mathbb{Z}^*_n$, описание которых в свою очередь даётся в следующей известной теореме.

Теорема 4 ([3])**.** *Пусть $n = p_1^{a_1} \dots p_m^{a_m}$ — разложение в произведение положительных степеней простых чисел. Тогда*

$$\mathbb{Z}^*_n \simeq \mathbb{Z}^*_{p_1^{a_1}} \times \dots \times \mathbb{Z}^*_{p_m^{a_m}}.$$

При этом, если $p \neq 2$, то для натурального a

$$\mathbb{Z}^*_{p^a} \simeq \mathbb{Z}_{p^a - p^{a-1}}.$$

Иначе для натурального $a > 2$

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

и для $a = 1$ и $a = 2$

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

И, наконец, следующая теорема устанавливает минимальное количество образующих группы $RM(\mathbb{Z}_n)^*$.

Теорема 5. *Пусть $n > 1$ — натуральное и $n = 2^k p_1^{a_1} \dots p_m^{a_m}$ — разложение на простые множители, где всякое $a_i > 0$. Тогда минимальная мощность системы образующих группы $RM(\mathbb{Z}_n)^*$ равна*

$2m$ *при* $k = 0$,
$2m + 1$ *при* $k = 1$,
$2m + 3$ *при* $k = 2$,
$2m + 4$ *при* $k > 2$.

§2 Доказательство основных результатов

Докажем общую теорему, из которой будет следовать утверждение теоремы 1.

Теорема 6. *Пусть R, S, T — кольца и $R \simeq S \times T$. Тогда*

$$RM(R) \simeq RM(S) \times RM(T).$$

Доказательство теоремы 6. Пусть f — отображение из R в $S \times T$, являющееся изоморфизмом. Пусть $f\colon a \mapsto (\bar{a}, \bar{\bar{a}})$.

Рассмотрим отображение $g : RM(R) \longrightarrow RM(S) \times RM(T)$, задающееся соотношением $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right) \mapsto \left(\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{smallmatrix}\right), \left(\begin{smallmatrix} \bar{\bar{a}} & \bar{\bar{b}} \\ \bar{\bar{b}} & \bar{\bar{a}} \end{smallmatrix}\right)\right)$. Покажем, что g является гомоморфизмом:

$$\begin{array}{ccccc} \begin{pmatrix} a & b \\ b & a \end{pmatrix} & + & \begin{pmatrix} c & d \\ d & c \end{pmatrix} & = & \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix} \\ \downarrow g & & \downarrow g & & \downarrow g \\ \left(\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{smallmatrix}\right), \left(\begin{smallmatrix} \bar{\bar{a}} & \bar{\bar{b}} \\ \bar{\bar{b}} & \bar{\bar{a}} \end{smallmatrix}\right)\right) & + & \left(\left(\begin{smallmatrix} \bar{c} & \bar{d} \\ \bar{d} & \bar{c} \end{smallmatrix}\right), \left(\begin{smallmatrix} \bar{\bar{c}} & \bar{\bar{d}} \\ \bar{\bar{d}} & \bar{\bar{c}} \end{smallmatrix}\right)\right) & = & \left(\left(\begin{smallmatrix} \bar{a}+\bar{c} & \bar{b}+\bar{d} \\ \bar{b}+\bar{d} & \bar{a}+\bar{c} \end{smallmatrix}\right), \left(\begin{smallmatrix} \bar{\bar{a}}+\bar{\bar{c}} & \bar{\bar{b}}+\bar{\bar{d}} \\ \bar{\bar{b}}+\bar{\bar{d}} & \bar{\bar{a}}+\bar{\bar{c}} \end{smallmatrix}\right)\right). \end{array}$$

$$\begin{array}{ccccc}
\begin{pmatrix} a & b \\ b & a \end{pmatrix} & \times & \begin{pmatrix} c & d \\ d & c \end{pmatrix} & = & \begin{pmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{pmatrix} \\
\downarrow g & & \downarrow g & & \downarrow g \\
\left(\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{b} & \bar{a} \end{smallmatrix} \right), \left(\begin{smallmatrix} \bar{\bar{a}} & \bar{\bar{b}} \\ \bar{\bar{b}} & \bar{\bar{a}} \end{smallmatrix} \right) \right) & \times & \left(\left(\begin{smallmatrix} \bar{c} & \bar{d} \\ \bar{d} & \bar{c} \end{smallmatrix} \right), \left(\begin{smallmatrix} \bar{\bar{c}} & \bar{\bar{d}} \\ \bar{\bar{d}} & \bar{\bar{c}} \end{smallmatrix} \right) \right) & = & \left(\left(\begin{smallmatrix} \bar{a}\bar{c}+\bar{b}\bar{d} & \bar{a}\bar{d}+\bar{b}\bar{c} \\ \bar{a}\bar{d}+\bar{b}\bar{c} & \bar{a}\bar{c}+\bar{b}\bar{d} \end{smallmatrix} \right), \left(\begin{smallmatrix} \bar{\bar{a}}\bar{\bar{c}}+\bar{\bar{b}}\bar{\bar{d}} & \bar{\bar{a}}\bar{\bar{d}}+\bar{\bar{b}}\bar{\bar{c}} \\ \bar{\bar{a}}\bar{\bar{d}}+\bar{\bar{b}}\bar{\bar{c}} & \bar{\bar{a}}\bar{\bar{c}}+\bar{\bar{b}}\bar{\bar{d}} \end{smallmatrix} \right) \right).
\end{array}$$

Поскольку f является биекцией, g также биективно. Таким образом, g — изоморфизм и теорема доказана. □

Доказательство теоремы 1.
Числа m_1 и m_2 взаимно просты, следовательно выполнен изоморфизм $\mathbb{Z}_{m_1 m_2} \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$[3]. Тогда по теореме 6 имеем:

$$RM(\mathbb{Z}_{m_1 m_2}) \simeq RM(\mathbb{Z}_{m_1}) \times RM(\mathbb{Z}_{m_2})$$

и

$$RM(\mathbb{Z}_{m_1 m_2})^* \simeq RM(\mathbb{Z}_{m_1})^* \times RM(\mathbb{Z}_{m_2})^*. \square$$

Докажем общую теорему, следствием которой является теорема 2.

Теорема 7. *Пусть R — кольцо, в котором 2 является обратимым элементом. Тогда*

$$RM(R) \simeq R \times R.$$

Доказательство теоремы 7. Рассмотрим отображение $f\colon RM(R) \longrightarrow R \times R$, задающееся по правилу $f\colon \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix} \right) \mapsto (a+b, a-b)$. Покажем, что f является гомоморфизмом:

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

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

Докажем, что гомоморфизм f инъективен. Пусть $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix} \right), \left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix} \right) \in RM(R)$. Докажем, что из равенства $f\left(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix} \right) \right) = f\left(\left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix} \right) \right)$ следует равенство $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix} \right)$ и $\left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix} \right)$. Пусть $f\left(\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix} \right) \right) = f\left(\left(\begin{smallmatrix} c & d \\ d & c \end{smallmatrix} \right) \right)$. Тогда по построению f имеем $a+b = c+d$ и $a-b = c-d$. Сложив два равенства получаем $2a = 2c$. Элемент 2 имеет обратный элемент 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.

Докажем сюръективность f. Пусть $(x, y) \in R \times R$. Построим его прообраз в $RM(R)$. Рассмотрим матрицу $\left(\begin{smallmatrix} 2^{-1}(x+y) & 2^{-1}(x-y) \\ 2^{-1}(x-y) & 2^{-1}(x+y) \end{smallmatrix} \right) \in RM(R)$. Гомоморфизм f ставит ей в соответствие элемент

$$(2^{-1}(x+y) + 2^{-1}(x-y), 2^{-1}(x+y) - 2^{-1}(x-y)) \in R \times R.$$

Имеем:

$$2^{-1}(x+y) + 2^{-1}(x-y) = 2^{-1}x + 2^{-1}y + 2^{-1}x - 2^{-1}y = 2 \cdot 2^{-1}x = x$$

и

$$2^{-1}(x+y) - 2^{-1}(x-y) = 2^{-1}x + 2^{-1}y - 2^{-1}x + 2^{-1}y = 2 \cdot 2^{-1}y = y.$$

Таким образом, $\begin{pmatrix} 2^{-1}(x+y) & 2^{-1}(x-y) \\ 2^{-1}(x-y) & 2^{-1}(x+y) \end{pmatrix}$ является прообразом (x, y).

Гомоморфизм f инъективен и сюръективен, а следовательно является изоморфизмом. □

Доказательство теоремы 2.

Если n — нечётно, то двойка обратима в $\mathbb{Z}_n$, поэтому по теореме 7 для этого кольца будет выполнен изоморфизм

$$RM(\mathbb{Z}_n) \simeq \mathbb{Z}_n \times \mathbb{Z}_n.$$

Тогда будет выполнен и изоморфизм, требуемый в теореме 2:

$$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_n^* \times \mathbb{Z}_n^*. \square$$

Для удобства рассмотрения случая 2^k введём кольцо $R[j]$. Пусть R — некоторое кольцо. Обозначим $R[j]$ расширение этого кольца новым элементом j, таким что $j \notin R$ и $j^2 = 1$. Все элементы $R[j]$ будут иметь вид $a + bj$ со сложением и умножением по следующим правилам:

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

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

Ясно, что $R[j] \simeq R[x] \,/\, \langle x^2 - 1 \rangle$.

Теорема 8. *Пусть R — некоторое кольцо. Тогда кольцо $RM(R)$ изоморфно кольцу R, расширенному элементом j таким, что $j^2 = 1,\ j \notin R$:*

$$RM(R) \simeq R[j]$$

Доказательство теоремы 8.

Рассмотрим, что отображение $f\colon RM(R) \longrightarrow R[j]$, задающееся по правилу: $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right) \mapsto a + bj$.

Проверим, что f является гомоморфизмом:

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

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

Ясно, что f является биекцией и, следовательно, изоморфизмом. □

Из теоремы следует изоморфизм колец $RM(\mathbb{Z}_n)$ и $\mathbb{Z}_n[j]$:

$$RM(\mathbb{Z}_n) \simeq \mathbb{Z}_n[j],$$

а также изоморфизм их мультипликативных групп:

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

Последний изоморфизм позволяет определить является ли элемент $a + bj \in \mathbb{Z}_n[j]$ обратимым: этот элемент обратим в $\mathbb{Z}_n[j]$ тогда и только тогда, когда элемент $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ обратим в $RM(\mathbb{Z}_n)$, то есть определитель этой матрицы $a^2 - b^2 \in \mathbb{Z}_n^*$.

Перейдём к доказательству теоремы 3.

Доказательство теоремы 3.

Если $k = 1$, то группа $RM(\mathbb{Z}_2)^*$ изоморфна $\mathbb{Z}_2$, что в свою очередь изоморфно $\mathbb{Z}_2^* \times \mathbb{Z}_4^*$.

При $k \geqslant 2$ по теореме 4 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 $\mathbb{Z}_{2^k}[j]^*$.

Далее, подгруппа $\{1, j\}$ изоморфна группе $\mathbb{Z}_2$. Ясно, что эти две подгруппы пересекаются только по 1.

Покажем, что существует подгруппа $\mathbb{Z}_{2^k}[j]^*$, изоморфная $\mathbb{Z}_{2^{k-1}}$ и не имеющая элементов, представимых в виде произведения элементов подгрупп $\mathbb{Z}_{2^k}^*$ и $\{1, j\}$, кроме 1.

Рассмотрим элемент $1 + 2j$ и покажем, что он обратим в кольце $\mathbb{Z}_{2^k}[j]$ и имеет порядок 2^{k-1}. Поскольку $1^2 - 2^2 = -3$, а -3 обратимо в $\mathbb{Z}_{2^k}$, элемент $1 + 2j \in \mathbb{Z}_{2^k}[j]^*$.

Рассмотрим элементы вида $1 + a + aj$, где $a \in \mathbb{Z}_{2^k}$ и a имеет вид $2s$. Докажем, что множество элементов такого вида замкнуто относительно умножения. Действительно, $(1 + a + aj)(1 + b + bj) = 1 + (a + b + 2ab) + (a + b + 2ab)j$. Если $a = 2s_a$ и $b = 2s_b$, то $2s_a + 2s_b + 8s_a s_b = 2(s_a + s_b + 4s_a s_b)$.

Заметим, что любой ненулевой элемент $c \in \mathbb{Z}_{2^k}$ можно представить в виде $c = 2^t m$, где $t < k$ и m — нечётное. 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. Но $2^{t_1 - t_2} m_1 - m_2$ обратимо в $\mathbb{Z}_{2^k}$. Противоречие.

Квадрат $(1+a+aj)^2$ имеет вид $1+2a(a+1)+2a(a+1)j$. Таким образом, при возведении в квадрат элемента $(1+a+aj)$, где $a = 2^t m$, m обратимо и $t > 0$, будет получен элемент $1+b+bj$, где $b = 2^{t+1} l$ и l обратимо.

Имеем

$$(1 + 2j)^{2^{k-1}} = (1 + 4 + 4j)^{2^{k-2}} = \ldots = 1 + b + bj,$$

где $b = 2^k l = 0$. Порядок группы равен степени двойки, поэтому порядок элемента $1 + 2j$ равен степени двойки. Можно заметить, что для меньших степеней двойки $(1 + 2j)^{2^t} \neq 1$. Таким образом, порядок элемента $1 + 2j$ равен 2^{k-1}. Кроме того, для каждой степени $x < 2^{k-1}$ выражение $(1 + 2j)^x$ принимает различные значения $1 + b + bj$, где b имеет вид $2s$, и по 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 $2s$. Также обратим $a^2 - b^2$, следовательно, $a - b$ 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 числа из $\mathbb{Z}_{2^k}^*$, степени элемента j и степени элемента $1 + 2j$.

Покажем, что такое представление единственно. Пусть $z_1(1+2j)^{k_1} = z_2(1+2j)^{k_2}$, $k_1 \geqslant k_2$. Тогда $(1+2j)^{k_1-k_2} = z_1^{-1}z_2$, следовательно $(1+2j)^{k_1-k_2} = 1$, $(1+2j)^{k_1} = (1+2j)^{k_2}$ и $z_1 = z_2$. Если же $z_1(1+2j)^{k_1} = jz_2(1+2j)^{k_2}$, то $(1+2j)^{k_1-k_2} = jz_1^{-1}z_2$. Тогда $(1+2j)^{k_1-k_2} = 1$, но $jz_1^{-1}z_2 \neq 1$. Противоречие.

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

Для доказательства теоремы о минимальном количестве образующих группы $RM(\mathbb{Z}_n)^*$, потребуется следующая

Теорема 9 (Theorem 3.1[1]). *Пусть $C = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$, где всякое $n_i > 1$. Для каждого простого p определим $d_p = |\{i \leqslant k : p \mid n_i\}|$ и*

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

Тогда минимальное число образующих группы C равно μ_C.

Перейдём к доказательству теоремы 5.

Доказательство теоремы 5.

По условию теоремы $n = 2^k p_1^{a_1} \ldots p_m^{a_m}$. Тогда по теореме 1 имеем

$$RM(\mathbb{Z}_n)^* \simeq RM(\mathbb{Z}_{2^k})^* \times RM(\mathbb{Z}_{p_1^{a_1}})^* \times \ldots \times RM(\mathbb{Z}_{p_m^{a_m}})^*.$$

По теоремам 2 и 3 имеем:

$RM(\mathbb{Z}_n)^* \simeq (\mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \ldots \times \mathbb{Z}_{p_m^{a_m}}^*)^2$, если $k = 0$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times (\mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \ldots \times \mathbb{Z}_{p_m^{a_m}}^*)^2$, если $k = 1$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \ldots \times \mathbb{Z}_{p_m^{a_m}}^*)^2$, если $k = 2$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^k} \times (\mathbb{Z}_{p_1^{a_1}}^* \times \mathbb{Z}_{p_2^{a_2}}^* \times \ldots \times \mathbb{Z}_{p_m^{a_m}}^*)^2$, если $k > 2$.

По теореме 4 группа $\mathbb{Z}_{p_i^{a_i}}^*$ является циклической. Таким образом, $RM(\mathbb{Z}_n)^*$ представляется в виде прямого произведения $2m$, $2m+1$, $2m+3$ и $2m+4$ циклических групп при $k = 0$, $k = 1$, $k = 2$ и $k > 1$, соответственно. Следовательно, минимальная мощность системы образующих $RM(\mathbb{Z}_n)^*$ не больше $2m$, $2m+1$, $2m+3$ и $2m+4$ при $k = 0$, $k = 1$, $k = 2$ и $k > 1$, соответственно.

По теореме 4 группа $\mathbb{Z}_{p_i^{a_i}}^* \simeq \mathbb{Z}_{p^{a_i}-p^{a_i-1}}$, что в свою очередь, в силу нечётности p_i, изоморфно $\mathbb{Z}_{2^{x_i}} \times \mathbb{Z}_{t_i}$, где $p^{a_i} - p^{a_i-1} = 2^{x_i}t_i$ и t_i нечётно.

Таким образом,

$RM(\mathbb{Z}_n)^* \simeq (\mathbb{Z}_{2^{x_1}} \times \mathbb{Z}_{2^{x_2}} \times \ldots \times \mathbb{Z}_{2^{x_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 0$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times (\mathbb{Z}_{2^{x_1}} \times \mathbb{Z}_{2^{x_2}} \times \ldots \times \mathbb{Z}_{2^{x_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 1$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_{2^{x_1}} \times \mathbb{Z}_{2^{x_2}} \times \ldots \times \mathbb{Z}_{2^{x_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k = 2$,

$RM(\mathbb{Z}_n)^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^k} \times (\mathbb{Z}_{2^{x_1}} \times \mathbb{Z}_{2^{x_2}} \times \ldots \times \mathbb{Z}_{2^{x_m}})^2 \times (\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \ldots \times \mathbb{Z}_{t_m})^2$ при $k > 2$.

Тогда по теореме 9 минимальное число образующих не меньше d_2 — количества сомножителей, отвечающих степеням двойки в разложении группы $RM(\mathbb{Z}_n)^*$ в прямое произведение циклических групп порядка степени простого числа, то есть не меньше, чем $2m$, $2m+1$, $2m+3$ и $2m+4$ при $k = 0$, $k = 1$, $k = 2$ и $k > 2$, соответственно. Теорема доказана. □

Список литературы

[1] Halbeisen L., Hamilton M., Růžička P., *Minimal generating sets of groups, rings, and fields*, Quaestiones Mathematicae, 2007, 30 (3), 355–363.

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

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

[4] 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.