Math-Net.Ru

Общероссийский математический портал

В. Е. Фирстов, Специальная матричная полугруппа преобразований примитивных пар и генеалогия пифагоровых троек, *Матем. заметки*, 2008, том 84, выпуск 2, 281–299

DOI: <https://doi.org/10.4213/mzm4074>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.67.100

26 апреля 2023 г., 13:24:12

Специальная матричная полугруппа преобразований примитивных пар и генеалогия пифагоровых троек

В. Е. Фирстов

В работе даются построение, исследование и свойства специальной матричной полугруппы, действующей на множестве примитивных пар натуральных чисел, реализующих натуральную параметризацию некоторых диофантовых уравнений, например, при определении пифагоровых троек, с которыми связано некоторое трихотомическое дерево решений.

Библиография: 3 названия.

1. Введение: задача Пифагора и специальная матричная полугруппа примитивных пар. В знаменитой задаче Пифагора отыскиваются натуральные решения уравнения $x^2 + y^2 = z^2$, которые принято называть *пифагоровыми тройками*. Фактически, решение задачи Пифагора эквивалентно определению множества π всех примитивных пифагоровых троек, для которых $(x, y, z) = 1$. Со времен Евклида известна биекция $\pi \rightarrow P$, устанавливаемая посредством натуральной параметризации вида

$$x = 2ab, \quad y = b^2 - a^2, \quad z = b^2 + a^2, \quad (1)$$

где P – множество примитивных пар, определяемое следующим образом:

$$P = \{(b, a) : (a, b) = 1, b - a = 2k - 1, a, b, k \in \mathbb{N}\} \quad (2)$$

На P целесообразно определить следующее отношение

$$(b_1, a_1) \prec (b_2, a_2) \Leftrightarrow b_1 + a_1 < b_2 + a_2, \quad (3)$$

являющееся строгим частичным порядком с наименьшим элементом $(2, 1) \in P$.

Таким образом, решение задачи Пифагора сводится к описанию множества P всех примитивных пар, что естественным образом приводит к рассмотрению соответствующей полугруппы преобразований множества P и определяет цель данной работы.

Пусть Tg – симметрическая полугруппа преобразований множества P . В этой полугруппе выделяется специальная матричная полугруппа $\text{SP} \subset \text{Tg}$ вида

$$\forall g \in \text{SP} \quad \forall (b, a) \in P \quad g(b, a) = (B, A) \Leftrightarrow \begin{cases} B = m_1 b + n_1 a, \\ A = m_2 b + n_2 a, \end{cases} \quad (4)$$

с дополнительным условием монотонности

$$3 \leq b + a < B + A. \quad (5)$$

В существовании SP легко убедиться на примере. Полагая в (4) $m_1 = 2$, $n_1 = 1$, $m_2 = 1$, $n_2 = 0$, в результате получаем соответствующее матричное преобразование g , удовлетворяющее требованиям (4), (5). Вместе с этим данное преобразование g порождает моногенную полугруппу $\langle g \rangle$, каждый элемент которой отвечает условиям (4), (5), и, таким образом, снимаются вопросы, связанные с существованием полугруппы SP, однако встают вопросы характеристики элементов полугруппы SP и ее строения.

2. Характеризация элементов полугруппы SP. Элементы полугруппы SP – это целочисленные (2×2) -матрицы, реализующие требования (4), (5), и, следовательно, компоненты m_1 , n_1 , m_2 , n_2 и строение этих матриц должны отвечать определенным условиям.

Условия, связанные с ограничениями на компоненты матриц полугруппы SP, устанавливаются в нижеследующих утверждениях.

ПРЕДЛОЖЕНИЕ 1. Для любого преобразования $g \in \text{SP}$ и любой пары $(b, a) \in P$ степень $g^k(b, a)$ описывается следующим рекуррентным уравнением 2-го порядка:

$$g^k(u) = (m_1 + n_2)g^{k-1}(u) - \Delta g^{k-2}(u), \quad (6)$$

где $k \geq 2$, $k \in \mathbb{N}$ и формально обозначено $u \cong (b, a)$.

Уравнение (6) последовательно получается из (4) по индукции.

ПРЕДЛОЖЕНИЕ 2. Всякое преобразование (4), (5) является невырожденным, т.е. определитель

$$\Delta = m_1 n_2 - m_2 n_1 \neq 0. \quad (7)$$

Утверждение (7) является следствием (4)–(6).

ПРЕДЛОЖЕНИЕ 3. Сумма элементов главной диагонали (шпур) матрицы любого преобразования (4), (5) – всегда целое положительное число, т.е.

$$\text{Sp } g = m_1 + n_2 > 0. \quad (8)$$

Неравенство (8) следует из (6).

ТЕОРЕМА 1. Для элементов матрицы преобразования (4), (5) разности $m_1 - m_2$ и $n_1 - n_2$ всегда нечетны.

ДОКАЗАТЕЛЬСТВО этой теоремы получается с помощью (2), (4), (7).

ТЕОРЕМА 2. Определитель Δ любого преобразования (4), (5) удовлетворяет соотношению

$$|\Delta| = 2^s, \quad (9)$$

где $s \geq 0$, $s \in \mathbb{Z}$ и зависит от коэффициентов данного преобразования.

ДОКАЗАТЕЛЬСТВО (9) получается путем обращения (4) с использованием определения (2) и теоремы 1.

СЛЕДСТВИЕ 1. Если $|\Delta| = 1$, то в матрице любого преобразования (4), (5) четные и нечетные элементы располагаются в шахматном порядке, если $|\Delta| > 1$, то одна строка матрицы содержит четные числа, а другая – нечетные. Обратное также справедливо.

Доказательство получается из теорем 1 и 2.

ТЕОРЕМА 3. Справедливо неравенство

$$m_1 > m_2 \geq 0, \quad (10)$$

причем при $\Delta < 0$ обязательно $m_2 > 0$.

ДОКАЗАТЕЛЬСТВО неравенства (10) следует из рассмотрения системы

$$\begin{cases} m_1 + n_1 t > m_2 + n_2 t > 0, \\ (n_1 + n_2 - 1)t > 1 - m_1 - m_2, \end{cases} \quad (11)$$

где $0 < t < 1$, $t = a/b$, $(b, a) \in P$, которая получается из определений (2), (4), (5).

В то же время, при $m_2 = 0$ из (4) следует $n_2 > 0$ и из (10) имеем $m_1 > 0$, т.е. $\Delta = m_1 n_2 > 0$. Поэтому, учитывая (10), случай $\Delta < 0$ обязательно требует $m_2 > 0$. Теорема 3 полностью доказана.

СЛЕДСТВИЕ 2. Среди элементов матриц преобразований (4), (5) может быть не более одного нулевого элемента.

Для доказательства достаточно рассмотреть случай двух нулей, когда в (4) $n_1 = m_2 = 0$, поскольку остальные возможности исключаются неравенствами (7) и (10). В этом случае, используя теоремы 1, 2, получаем $m_1 = n_2 = 1$, что противоречит (5) и, таким образом, следствие доказано.

СЛЕДСТВИЕ 3. Справедлива эквивалентность

$$m_2 = 0 \Leftrightarrow m_1 = 1, \quad (12)$$

и в этом случае $n_2 = 2^s$, где s – целое неотрицательное число.

Для доказательства (12) замечаем, что в случае $m_2 = 0$ в (4) выполнено $(m_1, a) = 1$, откуда, с учетом (10) $m_1 = 1$. Учитывая (9), отсюда сразу следует $n_2 = 2^s$, если иметь в виду неравенства (7) и (8). Следствие 3 полностью доказано.

ТЕОРЕМА 4. Компоненты матриц преобразований (4), (5) удовлетворяют следующим неравенствам:

$$\begin{cases} m_1 + n_1 \geq m_2 + n_2 \geq 0, \\ m_1 + n_1 + m_2 + n_2 \geq 2. \end{cases} \quad (13)$$

ДОКАЗАТЕЛЬСТВО неравенств (13) получается путем исключения параметра t из системы (11).

СЛЕДСТВИЕ 4. Положим $m_1 - m_2 = k$, $n_1 - n_2 = l$, где k, l – по теореме 1 нечетные числа, причем $k > 0$ согласно (10). Тогда справедливы неравенства

$$k + l \geq 0, \quad m_1 + n_1 \geq \frac{1}{2}(k + l) + 1. \quad (14)$$

Доказательство этих неравенств прямо следует из системы (13).

Предложения 1–3, теоремы 1–4, а также следствия 1–4 определяют те необходимые ограничения, которые накладываются на компоненты m_1, m_2, n_1, n_2 целочисленных (2×2) -матриц с тем, чтобы эти матрицы отвечали требованиям (4), (5).

Далее, в нижеследующих утверждениях устанавливается общий вид этих матриц, причем сначала задача рассматривается в частных случаях, предусмотренных следствиями 1, 2.

ПРЕДЛОЖЕНИЕ 4. При $n_1 = 0$ определитель любого из преобразований (4), (5) равен $|\Delta| = 2^s$, $s \in \mathbb{N}$, а соответствующая матрица (в зависимости от знака Δ) имеет вид

$$g = \begin{pmatrix} 2^s & 0 \\ 2^s - k & \pm 1 \end{pmatrix}, \quad (15)$$

где k – нечетное положительное число, меньшее 2^s .

ПРЕДЛОЖЕНИЕ 5. При $n_2 = 0$ определитель любого из преобразований (4), (5) равен $|\Delta| = 2^s$, $s \geq 0$, $s \in \mathbb{Z}$, а соответствующая матрица (в зависимости от знака Δ) имеет вид

$$g = \begin{pmatrix} 2^s + k & \pm 1 \\ 2^s & 0 \end{pmatrix}, \quad (16)$$

где k – нечетное положительное число.

ПРЕДЛОЖЕНИЕ 6. При $m_2 = 0$ определитель любого из преобразований (4), (5) равен $\Delta = 2^s$, где $s \geq 0$, $s \in \mathbb{Z}$, а соответствующая матрица имеет вид

$$g = \begin{pmatrix} 1 & 2^s - 1 + c \\ 0 & 2^s \end{pmatrix}, \quad (17)$$

где c – четное положительное число, если $s = 0$, и c – четное неотрицательное число, если $s > 0$.

Доказательства предложений 4–6 приводятся в [1].

Переходя к общему случаю, замечаем, что первое из неравенств (14) позволяет провести полную классификацию матриц преобразований (4), (5), если ввести индекс $I(g) = k + l$ и к первому классу отнести матрицы с индексом $I(g) = 0$, а во втором классе поместить матрицы с индексом $I(g) > 0$.

ТЕОРЕМА 5. Пусть $I(g) = 0$. Тогда для преобразований (4), (5) определитель $\Delta = 2^s$, $s \geq 0$, $s \in \mathbb{Z}$, а соответствующая матрица преобразований имеет вид

$$g = \begin{pmatrix} m_1 & 2^s - m_1 \\ m_1 - 1 & 2^s - m_1 + 1 \end{pmatrix}, \quad (18)$$

где $m_1 > 1$ при $s = 0$ и $m_1 \geq 1$ при $s > 0$.

ДОКАЗАТЕЛЬСТВО. Для доказательства (18) замечаем, что условие $I(g) = 0$ эквивалентно условию $m_1 + n_1 = m_2 + n_2$, причем, $m_2 + n_2 > 0$, так как при $m_2 + n_2 = 0$ не выполняется второе неравенство в (13).

Определитель матрицы преобразования (4), (5) в данном случае оказывается равным

$$\Delta = \begin{vmatrix} m_1 & n_1 \\ m_1 - k & n_1 + k \end{vmatrix} = k(m_1 + n_1) > 0.$$

Учитывая (9), отсюда получается $k(m_1 + n_1) = 2^s$. Так как k – нечетно и положительно, то последнее равенство имеет место только при $k = 1$. Но тогда $l = -1$, $m_1 + n_1 = 2^s$, и матрица преобразований (4), (5) приобретает вид (18), что и требовалось доказать.

ТЕОРЕМА 6. Пусть $I(g) > 0$ и g – некоторое преобразование (4), (5) с матрицей

$$g = \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix}. \quad (19)$$

Обозначим $m_1 + n_1 = \lambda$, $m_2 + n_2 = \mu$, и пусть $\lambda \geq 2$. Тогда

$$g = \frac{1}{l+k} \begin{pmatrix} \lambda k - \Delta & \lambda k + \Delta \\ \mu l - \Delta & \mu l + \Delta \end{pmatrix}, \quad (20)$$

где $\mu k - \Delta \geq 0$ и λ, μ – одинаковой четности: при $|\Delta| = 1$ оба нечетны, при $|\Delta| = 2^s$, $s \in \mathbb{N}$, оба четны.

Для доказательства (20) используется очевидное равенство $k + l + \mu = \lambda$, с помощью которого получаем, что определитель преобразований (4), (5) равен

$$\Delta = \begin{vmatrix} m_1 & n_1 \\ m_2 & n_2 \end{vmatrix} = \begin{vmatrix} m_1 & n_1 \\ m_1 - k & n_1 - l \end{vmatrix} = \begin{vmatrix} m_1 & \lambda - m_1 \\ m_1 - k & \lambda - m_1 - l \end{vmatrix} = \lambda k - (l + k)m_1 \neq 0.$$

Отсюда следует

$$(\lambda k - \Delta) \div (l + k), \quad \lambda k - \Delta \geq l + k > 0,$$

и, далее, легко получается утверждение теоремы 6.

Предложения 4–6 и теоремы 5, 6 определяют общий вид матриц преобразований (4), (5) полугруппы SP.

3. Некоторые общие алгебраические свойства полугруппы SP. Результаты пп. 1, 2 позволяют установить ряд общих утверждений, касающихся полугруппы SP.

1. Полугруппа SP является полугруппой с сокращением (следствие неравенства (7)).

2. В полугруппе SP отсутствуют идемпотенты (следствие неравенства (5)), поэтому любая ее моногенная подполугруппа изоморфна $(\mathbb{N}, +)$.

3. Полугруппа SP представляется в виде разбиения $SP = SP_1 \cup SP_2$, $SP_1 \cap SP_2 = \emptyset$, где SP_1, SP_2 – подполугруппы SP, элементы которых имеют определители соответственно $|\Delta| = 1$ и $|\Delta| = 2^s$, $s \in \mathbb{N}$ (следствие равенства (9)). Поэтому имеет место представление $SP \rightarrow B_2$, где B_2 – двухэлементная булева полурешетка.

4. В SP имеет место композиционный ряд вида

$$SP \supset SP_2 \supset SP_4 \supset SP_8 \supset \dots, \quad (21)$$

где $SP_2, SP_4, SP_8, \dots$ – собственные идеалы SP, элементы которых определяются условием

$$g \in SP_{2^s}, \quad s \in \mathbb{N}, \quad \Leftrightarrow \quad |\Delta| \div 2^s,$$

ТАБЛИЦА 1

	$[q_1]$	$[q_2]$	$[q_3]$	$[q_4]$
$[q_1]$	$[q_1]$	$[q_1]$	$[q_1]$	$[q_1]$
$[q_2]$	$[q_2]$	$[q_2]$	$[q_2]$	$[q_2]$
$[q_3]$	$[q_2]$	$[q_1]$	$[q_4]$	$[q_3]$
$[q_4]$	$[q_1]$	$[q_2]$	$[q_3]$	$[q_4]$

Δ – определитель g (следствие равенства (9)).

5. Существует разбиение

$$SP = SP^0 \cup SP', \quad SP^0 \cap SP' = \emptyset,$$

где SP^0 и SP' – подполугруппы SP , элементы которых отвечают требованиям соответственно $I(g) = 0$ и $I(g) > 0$, причем, SP' является простым идеалом в SP (следствие 4, теоремы 5, 6). При этом также реализуется представление $SP \rightarrow B_2$.

6. Существует разбиение

$$SP = SP^+ \cup SP^-, \quad SP^+ \cap SP^- = \emptyset,$$

где SP^+ – подполугруппа SP с элементами, имеющими положительный определитель, SP^- – подмножество SP , содержащее элементы с отрицательным определителем. Поэтому имеется представление $SP \rightarrow Z_2$, где Z_2 – аддитивная группа классов вычетов по mod 2.

7. Пусть $\mathbb{N}_0$ – множество натуральных чисел с нулем. Имеет место гомоморфизм $SP \rightarrow (\mathbb{N}_0, +)$, определенный правилом $g \rightarrow s$, где s – целое неотрицательное число такое, что $|\Delta| = 2^s$, Δ – определитель преобразования $g \in SP$ (следствие равенства (9)).

8. Пусть преобразование $g \in SP$ описывается матрицей с элементами g_{ij} , $i, j \in \{1, 2\}$. Определим соответствие, по которому четным g_{ij} поставим в соответствие 0, а нечетным – 1. Тем самым, учитывая следствие 1, формируется сюръективное отображение $SP \rightarrow SP_q$, где SP_q – четырехэлементное множество, содержащее матрицы следующего вида:

$$[q_1] = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad [q_2] = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad [q_3] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad [q_4] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (22)$$

Рассматривая матрицы (22) над полем характеристики 2, легко убедиться, что SP_q является мультипликативной полугруппой, представляющей гомоморфный образ при отображении $SP \rightarrow SP_q$. Поэтому имеет место изоморфизм $SP_q \cong SP/q$, где SP/q – фактор-полугруппа, построенная на SP по эквивалентности q – отношению равнообразности при гомоморфизме $SP \rightarrow SP_q$ и состоящая из классов $[q_1]$, $[q_2]$, $[q_3]$, $[q_4]$ в (22) с законом умножения, представленным в табл. 1.

Из таблицы 1 видно, что SP/q представляет собой фактор-моноид с единицей $e = [q_4]$, содержащий две подполугруппы $\{[q_1], [q_2]\}$ и $\{[q_1], [q_2], [q_4]\}$, а также подгруппу $\{[q_3], [q_4]\} \cong \mathbb{Z}_2$, причем при естественном гомоморфизме $SP \rightarrow SP/q$ в силу следствия 1 получается

$$SP_1 \rightarrow \{[q_3], [q_4]\}, \quad SP_2 \rightarrow \{[q_1], [q_2]\}. \quad (23)$$

4. Строение полугруппы SP_1 . Полугруппа $SP_1 \subset SP$ является простой и в силу (23) имеет гомоморфный образ в виде аддитивной группы $\mathbb{Z}_2$. Основным результатом, полностью объясняющий строение SP_1 , представляет следующая

ТЕОРЕМА 7. *Полугруппа SP_1 (с точностью до изоморфизма) есть свободная полугруппа с тремя образующими.*

Для доказательства в SP_1 выделяются следующие три преобразования:

$$g_1 = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}, \quad g_{-1} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \quad h_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad (24)$$

степени которых определяются следующими выражениями:

$$g_1^n = \begin{pmatrix} n+1 & -n \\ n & 1-n \end{pmatrix}, \quad h_1^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, \quad g_{-1}^n = \begin{pmatrix} \alpha_n + 2\beta_n & \beta_n \\ \beta_n & \alpha_n \end{pmatrix}, \quad (25)$$

где $\alpha_1 = 0$, $\beta_1 = 1$, а при $n > 1$:

$$\alpha_n = \sum_{i=0}^{[(n-2)/2]} C_{n-1}^{2i+1} 2^i, \quad \beta_n = \sum_{i=0}^{[(n-2)/2]} C_n^{2i+1} 2^i.$$

Далее, применим утверждения теорем 5, 6 при $s = 0$, что дает полное описание элементов SP_1 , сводя его к рассмотрению двух случаев: $I(g) = 0$ и $I(g) > 0$. При этом отметим, что для $g \in SP_1$ в силу следствия 1 и неравенств (13) получается $\mu = m_2 + n_2 > 0$, где m_2 и n_2 определяются представлением (19) для g .

Тогда при $I(g) = 0$, полагая в (18) $m_1 = n + 1$, приходим к соотношению (25) для g_1^n , т.е. $g \in \langle g_1 \rangle$ и, таким образом, в данном случае утверждение теоремы доказано.

Допустим теперь $I(g) > 0$ и для определенности пока полагаем $g \in SP_1^+$. Тогда представляются следующие возможности.

1) Пусть $g = g_1 \circ x$. Тогда $x \in SP_1^+$ и с помощью (19), (20), (24) для преобразования x получается выражение

$$x = g_1^{-1} \circ g = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} = \begin{pmatrix} m_2 & n_2 \\ 2m_2 - m_1 & 2n_2 - n_1 \end{pmatrix} = \begin{pmatrix} m_2 & n_2 \\ m_2 - k & n_2 - l \end{pmatrix}. \quad (26)$$

Для соответствующих элементов матрицы x должно выполняться неравенство (10), по которому $m_2 > m_2 - k \geq 0$, что дает

$$m_2 \geq k. \quad (27)$$

Ограничения, связанные с выполнением неравенств (13), для элементов матрицы x вида (26), определяются следующими индексными соотношениями:

$$\begin{cases} \mu > I(g), \\ 2\mu - I(g) \geq 2, \end{cases} \Leftrightarrow \mu > I(g). \quad (28)$$

Представляя определитель g в виде $\Delta = kn_2 - lm_2$, получаем, что индексное неравенство (28) принимает вид

$$(m_2 - k)I(g) + \Delta > 0. \quad (29)$$

Так как в данном случае $\Delta = 1$, $I(g) > 0$, или, что эквивалентно, $I(g) \geq 2$ и $m_2 \geq k$ в силу (27), то неравенство (29), а следовательно, и неравенство (28), автоматически выполняются.

2) Пусть $g = h_1 \circ y$. Тогда $y \in \text{SP}_1^+$, и далее, действуя, как и в предыдущем случае, приходим к неравенству

$$0 \leq m_2 < \frac{k}{2}. \quad (30)$$

Ограничения, связанные с неравенствами (13), в данном случае определяются следующим индексным неравенством:

$$I(g) \geq 2\mu, \quad (31)$$

которое, как и в предыдущем случае, представляется в виде

$$(k - 2m_2)I(g) \geq 2\Delta. \quad (32)$$

Поскольку имеем $I(g) > 0$ или, что эквивалентно, $I(g) \geq 2$, $\Delta = 1$ и $k - 2m_2 > 0$ в силу (30), неравенство (32), а следовательно, и неравенство (31), автоматически выполняются.

3) Пусть $g = g_{-1} \circ z$. Тогда $z \in \text{SP}_1^-$, и тем же способом, что и выше, получаем неравенство

$$\frac{k}{2} < m_2 < k. \quad (33)$$

Ограничения, связанные с неравенствами (13), в данном случае приводят к следующему индексному неравенству:

$$\mu < I(g) \leq 2\mu, \quad (34)$$

которое тем же способом, что и выше, представляется в виде

$$\begin{cases} (k - m_2)I(g) > \Delta, \\ (2m_2 - k)I(g) + 2\Delta \geq 0. \end{cases} \quad (35)$$

Поскольку имеем $I(g) > 0$ или, что эквивалентно, $I(g) \geq 2$, $\Delta = 1$ и неравенство (33), система (35), а следовательно, и неравенство (34), автоматически выполняются.

При $I(g) > 0$, $g \in \text{SP}_1^-$, действуя аналогично трем рассмотренным выше случаям, получаем следующие ограничения:

$$\text{при } g = g_1 \circ x, \ x \in \text{SP}_1^- : \quad m_2 > k, \quad (36)$$

$$\text{при } g = h_1 \circ y, \ y \in \text{SP}_1^- : \quad 0 < m_2 < \frac{k}{2}, \quad (37)$$

$$\text{при } g = g_{-1} \circ z, \ z \in \text{SP}_1^+ : \quad \frac{k}{2} < m_2 \leq k, \quad (38)$$

Непосредственно устанавливается, что при $I(g) > 0$, $g \in \text{SP}_1^-$ и ограничениях по m_2 вида (36)–(38) соответствующие индексные ограничения (28), (29), (31), (32), (34), (35) автоматически выполняются, что обеспечивает выполнение неравенств (13).

ТАБЛИЦА 2. К разложению $g \in \text{SP}_1$

m_2	0	$\left(0, \frac{k}{2}\right)$	$\left(\frac{k}{2}, k\right)$	k	(k, ∞)
h_1					
g_{-1}					
g_1					

Проведем анализ ограничений по m_2 в рассматриваемом случае $I(g) > 0$, $g \in \text{SP}_1$, для чего полученные данные (27), (30), (33), (36)–(38) сводятся в табл. 2. В верхней строке табл. 2 приведена шкала значений m_2 и каждому преобразованию h_1 , g_{-1} , g_1 в последующих строках отведена полоска, разбитая на две части: в ее верхней части серым цветом указана область ограничений по m_2 в случае, когда это преобразование является первым (слева) членом разложения некоторого преобразования $g \in \text{SP}_1^+$, а в нижней части – цветом отмечена область ограничений по m_2 в случае, когда это преобразование указанным образом входит в разложение $g \in \text{SP}_1^-$.

Как видно из табл. 2, области ограничений по m_2 для различных представлений $g \in \text{SP}_1^+$ не пересекаются и такая же картина имеет место для представлений $g \in \text{SP}_1^-$. Поэтому, для произвольно выбранного преобразования $g \in \text{SP}_1$, реализуется только одно из представлений, указанных в табл. 2 в зависимости от значений k , m_2 и Δ . Отсюда, не вдаваясь в детали [1], получается доказательство теоремы 7.

СЛЕДСТВИЕ 5. *Справедливо равенство $\text{SP}_1(2, 1) = P \setminus \{(2, 1)\}$, где $\text{SP}_1(2, 1) = \{g(2, 1) : g \in \text{SP}_1\}$.*

Доказательство этого следствия дается в работе [1].

5. Строение полугрупп SP_2 и SP . Предварительные результаты, касающиеся полугруппы SP_2 , установлены в п. 3. В дальнейшем для изучения строения SP_2 и SP привлекается три следующих преобразования:

$$g_2 = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, \quad g_{-2} = \begin{pmatrix} 2 & 0 \\ 1 & -1 \end{pmatrix}, \quad h_2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad (39)$$

натуральные степени которых имеют следующий вид:

$$g_2^n = \begin{pmatrix} 2^n & 0 \\ 2^n - 1 & 1 - n \end{pmatrix}, \quad g_{-2}^n = \begin{pmatrix} 2^n & 0 \\ \frac{1}{3}(2^n - (-1)^n) & (-1)^n \end{pmatrix}, \quad h_2^n = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}. \quad (40)$$

Отметим, что преобразования (24) и (39) связаны следующими соотношениями:

$$\begin{aligned} g_2 &= g_1 \circ h_2, & h_1 \circ h_2 &= h_2 \circ h_1^2, & g_1 \circ g_2 &= h_2 \circ g_1 = g_1^2 \circ h_2, \\ g_1 \circ g_{-2} &= h_2 \circ g_{-1}, & g_{-1} \circ h_2 &= g_{-2} \circ h_1, & h_1 \circ g_{-2} &= g_{-2} \circ g_1, \\ h_2 \circ h_1 \circ g_1 &= g_{-1} \circ g_{-2}, & g_{-2} \circ g_{-1} &= h_1 \circ g_1 \circ h_2. \end{aligned} \quad (41)$$

Изучение строения SP_2 и SP начнем с частных случаев, обозначенных следующими утверждениями.

ПРЕДЛОЖЕНИЕ 7. *Имеет место соотношение*

$$\forall g \in SP \quad \mu = 0 \quad \Leftrightarrow \quad g \in SP_2^-, \quad (42)$$

где параметр μ определен в теореме 6.

Действительно, в случае $\mu = 0$ для определителя $g \in SP$ имеем

$$\Delta = \begin{vmatrix} m_1 & n_1 \\ m_2 & n_2 \end{vmatrix} = \begin{vmatrix} m_2 + k & l - m_2 \\ m_2 & -m_2 \end{vmatrix} = -m_2 I(g) < 0,$$

откуда $g \in SP_2^-$, так как $I(g)$ четно и случай $I(g) = 0$ исключается по теореме 5, что и требовалось доказать.

ПРЕДЛОЖЕНИЕ 8. *Матрицы (15) образуют подполугруппу $\langle g_2, g_{-2} \rangle \subset SP_2$.*

ПРЕДЛОЖЕНИЕ 9. *Пусть H^+ – множество всех матриц вида (17) и $H_2^+ \subset H^+$ – подмножество таких матриц с показателем $s \in \mathbb{N}$. Тогда $H^+ = \langle h_1, h_2 \rangle \subset SP^+$, причем, H_2^+ – идеал полугруппы H^+ .*

Доказательство предложений 8, 9 дается в [1].

Более общий результат, касающийся строения полугрупп SP_2 и SP , устанавливает

ТЕОРЕМА 8. *Всякое преобразование $g \in SP$ представляется в рамках полугруппы $\langle g_1, g_{-1}, h_1, h_2, g_{-2} \rangle$, исключая случаи*

$$g \in [q_1] \cap SP^+, \quad 0 < m_2 < k, \quad I(g) < \mu \quad \Leftrightarrow \quad (k - m_2)I(g) < \Delta, \quad (43)$$

$$g \in [q_1] \cap SP^-, \quad m_2 > k, \quad I(g) > \mu \quad \Leftrightarrow \quad (m_2 - k)I(g) < -\Delta. \quad (44)$$

ДОКАЗАТЕЛЬСТВО. При $I(g) = 0$, $m_1 = 1$ из (18), (40) получается $g \in \langle h_2 \rangle$, при $m_1 > 1$ с помощью (25), (40) находим представление $g = g_1^m \circ h_2^s$, которое соответствует рассматриваемому случаю, если в (18) положить $m_1 = m + 1$.

Следовательно, при $I(g) = 0$ условия теоремы выполнены.

При $I(g) > 0$, действуя так же, как и при доказательстве теоремы 7, приходим к результатам, представленным в табл. 3.

Проводя анализ табл. 3 так, как это сделано в [1], получаем доказательство теоремы 8.

СЛЕДСТВИЕ 6. *Пусть $g \in SP$ и в матрице g вида (24) элемент $m_2 = k$. Тогда $g \in \langle g_1, g_{-1}, h_1, h_2, g_{-2} \rangle$ и при этом*

$$1) \quad k = 1, \quad g = \begin{pmatrix} 2 & n_2 + l \\ 1 & n_2 \end{pmatrix}, \quad (45)$$

$$2) \quad \Delta = n_2 - l, \quad I(g) = 1 + l, \quad \mu = 1 + n_2. \quad (46)$$

1) При $I(g) = 0$ имеем $l = -1$, что дает

$$\begin{aligned} \text{при } \Delta = 1 & & g = g_1, \\ \text{при } \Delta = 2^s, \quad s \in \mathbb{N}, & & g = g_1 \circ h_2^s. \end{aligned} \quad (47)$$

ТАБЛИЦА 3. К разложению $g \in \text{SP}_2$

m_2	0	$\left(0, \frac{k}{2}\right)$	$\left(\frac{k}{2}, k\right)$	k	(k, ∞)	Индексные ограничения	Классы SL/q
h_2						—	$[q_2]$
g_{-2}						$I(g) \geq \mu$	$[q_1]$
						—	
h_1						$I(g) \geq 2\mu$	$[q_2]$
							$[q_1]$
						—	$[q_1]; [q_2]$
g_{-1}						$\mu \leq I(g) \leq 2\mu$	
						$\mu < I(g) \leq 2\mu$	
g_1						—	
						$I(g) \leq \mu$	

2) При $I(g) > 0$ имеем $l \geq 1$, что дает

$$\text{при } \Delta = 1 \quad g = g_1 \circ h_1^n, \quad n = (l+1)/2, \quad (48)$$

$$\text{при } \Delta = -1 \quad g = g_{-1}, \quad \text{если } l = 1 \quad (49)$$

$$\text{и } g = g_{-1} \circ h_1^n, \quad \text{если } l > 1, \quad n = (l-1)/2,$$

$$\text{при } \Delta = 2^s, \quad s \in \mathbb{N}, \quad g = g_1 \circ \langle h_1, h_2 \rangle, \quad (50)$$

$$\text{при } \Delta = -(2^s), \quad s \in \mathbb{N}, \quad g = g_{-2} \circ \langle h_1, h_2 \rangle. \quad (51)$$

Доказательство следствия 6 дается в работе [1].

6. Бесконечный “хвост” в системе образующих полугруппы SP. Пусть $SV = SV^+ \cup SV^-$, где SV^+ , SV^- – множества преобразований, отвечающих соответственно условиям (43), (44). Легко убедиться, что эти множества полугруппами не являются. Следующее утверждение показывает, что для определения элементов SV фактически достаточно указать способ определения элементов множества SV^+ .

ПРЕДЛОЖЕНИЕ 10. Множества SV^+ и SV^- связаны взаимно однозначным соответствием.

Для доказательства достаточно взять любое преобразование $g \in SV^+$ вида (19) и определить соответствие $f(g) = g'$ по правилу

$$f: \begin{pmatrix} m_1 & n_1 \\ m_2 & n_2 \end{pmatrix} \rightarrow \begin{pmatrix} m_1 & n_1 \\ k & l \end{pmatrix}, \quad (52)$$

как это сделано в работе [1].

ПРЕДЛОЖЕНИЕ 11. Преобразование f вида (52) обладает свойством

$$f(g \circ x) = g' \circ x, \quad (53)$$

где $g \in SV^+$, $x \in SP$, $g' = f(g)$.

Действительно, представляя преобразование f матрицей

$$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

в силу ассоциативности матричного умножения получаем (53).

Следующее утверждение устанавливает способ определения элементов множества SV и его мощность.

ТЕОРЕМА 9. Все элементы множества SV^+ определяются решениями системы

$$\begin{cases} (k - m_2)I(g) = 4r, \\ k\mu - m_2I(g) = 2^s, \end{cases} \quad (54)$$

где $\mu > 4$, и натуральный параметр r определяется нечетными решениями неравенства

$$1 \leq r < 2(2^{s-3} - 1). \quad (55)$$

Система (54) имеет решения при всех натуральных $s \geq 4$, причем, каждому такому значению s соответствует конечное подмножество решений (54), так что SV является бесконечным счетным множеством.

ДОКАЗАТЕЛЬСТВО. Соотношения (54), (55) получаются из условия (43), при этом решения системы (54), как показано в [1], существуют при всех $s \geq 4$. Следовательно, SV – бесконечное счетное множество и, таким образом, получается доказательство теоремы 9.

СЛЕДСТВИЕ 7. Любое преобразование $g \in SP$ с определителем $|\Delta| \leq 2^s$, $s = 3$, является элементом полугруппы $\langle g_1, g_{-1}, h_1, h_2, g_{-2} \rangle$.

Фактически, при построении множества SV по теореме 9 используется процедура разбиения

$$SV = \bigcup SV_i, \quad i \in \{2^s : s \in \mathbb{N}, s \geq 4\},$$

на классы SV_i так, что в каждом таком отдельном классе содержатся преобразования, определители которых отвечают требованию $|\Delta| = i = 2^s$ при фиксированном $s \geq 4$, причем для представителей каждого класса справедлива

ТЕОРЕМА 10. Каждый представитель класса SV_i не имеет простых делителей в этом классе.

ДОКАЗАТЕЛЬСТВО. Допустим противное: пусть некоторый представитель $g \in SV_i$ имеет простой делитель $h \in SV_i$. Тогда следует написать $g = h \circ x$, где $x \in SP_1$, откуда $h^{-1} \circ g \in SP_1$. Последнее, как показано в работе [1], оказывается невозможным, откуда следует утверждение теоремы 10.

Отсюда, кстати, сразу следует, что если $g, h \in SV_i$ и при этом h – делитель g , то h не является простым элементом в классе SV_i и имеет вид $h = g_k \circ z$, где g_k – некоторый простой элемент в классе SV_k , $16 \leq k < i$, $z \in SP_2$.

Остается в целом выяснить вопрос о простых элементах полугруппы SP . По теореме 8 простыми элементами в SP являются преобразования $g_1, g_{-1}, h_1, h_2, g_{-2}$, и, следовательно, интересующий вопрос сводится к определению простых элементов из множества $SV = SP \setminus \langle g_1, g_{-1}, h_1, h_2, g_{-2} \rangle$, причем для этого достаточно найти способ определения простых элементов в SV^+ , так как $SV = SV^+ \cup SV^-$ и в силу (52) $SV^- = f(SV^+)$ со свойством (53).

Алгоритм определения простых элементов в SV^+ в принципе напоминает реализацию известной процедуры решета Эратосфена для выделения простых чисел из натурального ряда и в данном случае осуществляется следующим образом.

1) По теореме 9 последовательно строятся подмножества

$$SV_i^+, \quad i \in \{2^s : s \in \mathbb{N}, s \geq 4\}$$

– классы разбиения SV^+ .

2) Класс SV_{16}^+ согласно вычислениям [1] содержит только одно преобразование

$$g_{16} = \begin{pmatrix} 4 & 4 \\ 1 & 5 \end{pmatrix},$$

которое, очевидно, является простым.

3) Преобразованию g_{16} согласно (52) отвечает единственное преобразование $g_{-16} \in SV_{16}^-$ и, таким образом, строится $SV_{16}^p = \{g_{16}, g_{-16}\}$ – класс простых элементов в SV с определителем $|\Delta| = 16$.

4) Класс SV_{32}^+ согласно [1] содержит 4 преобразования, и среди них имеется только одно преобразование

$$g_{32} = \begin{pmatrix} 8 & 8 \\ 3 & 7 \end{pmatrix},$$

не допускающее представление

$$g = p \circ x, \quad (56)$$

где $g \in SV_{32}^+$, $p \in SV_{16}^p$, $x \in SP$. Этот факт, если воспользоваться теоремами 8, 10 и следствием 7, доказывает простоту элемента g_{32} .

5) Преобразованию g_{32} согласно (52) отвечает единственное преобразование g_{-32} и, таким образом, строится класс $SV_{32}^p = \{g_{32}, g_{-32}\}$ простых элементов в SV с определителем $|\Delta| = 32$.

6) Класс SV_{64}^+ содержит 18 преобразований [1], и среди них содержится 5 преобразований

$$\begin{aligned} g_{64}^{(1)} &= \begin{pmatrix} 4 & 20 \\ 1 & 21 \end{pmatrix}, & g_{64}^{(2)} &= \begin{pmatrix} 10 & 2 \\ 3 & 7 \end{pmatrix}, & g_{64}^{(3)} &= \begin{pmatrix} 12 & -4 \\ 1 & 5 \end{pmatrix}, \\ g_{64}^{(4)} &= \begin{pmatrix} 6 & 14 \\ 1 & 13 \end{pmatrix}, & g_{64}^{(5)} &= \begin{pmatrix} 16 & 16 \\ 7 & 11 \end{pmatrix}, \end{aligned} \quad (57)$$

которые не представляются в виде (56), где теперь следует полагать $g \in SV_{64}^+$, $p \in SV_{16}^p \cup SV_{32}^p$. Отсюда устанавливается простота элементов (57).

7) Простые элементы SV_{64}^- получаются из (57) с помощью (52) и, таким образом, строится 10-элементное множество SV_{64}^p простых элементов в SV с определителем $|\Delta| = 64$ и т.д.; указанным образом строится множество SV_p всех простых элементов $SV \subset SP$.

В связи с этим, естественно, возникает вопрос: конечна или бесконечна описанная процедура определения простых элементов в SV ? Для ответа на данный вопрос следует явно определить строение матриц преобразований SV .

ТЕОРЕМА 11. Пусть $g \in SV$ и имеет определитель $|\Delta| = 2^s$, $s \geq 4$. Тогда

1) Если $g \in SV^+$, то

$$g = \begin{pmatrix} \alpha_1 \cdot 2^{s_1} & \beta_1 \cdot 2^{s_1} \\ m_2 & n_2 \end{pmatrix}, \quad (58)$$

где $\alpha_1, \beta_1, m_2, n_2$ – нечетные числа такие, что

$$\alpha_1 > 0, \quad \alpha_1 + \beta_1 > 0, \quad m_2 > 0, \quad \mu = m_2 + n_2 > 0, \quad m_2 \neq n_2, \quad (59)$$

показатель $s_1 \in \mathbb{N}$ удовлетворяет неравенству

$$1 \leq s_1 \leq s - 2, \quad (60)$$

причем,

$$s_1 = s - 2 \Leftrightarrow \alpha_1 = \beta_1 = 1, \quad m_2 = 2^{s-3} - 1, \quad n_2 = 2^{s-3} + 3. \quad (61)$$

В остальных случаях

$$1 \leq s_1 < s - 2 \quad (62)$$

и при $s_1 > 1$ параметры $\alpha_1, \beta_1, m_2, n_2$ матрицы (58) определяются условиями

$$0 < m_2 < 2^{s_1-1} \cdot \alpha_1 \Leftrightarrow m_2 = 1, 3, 5, \dots, 2^{s_1-1}\alpha_1 - 1, \quad (63)$$

$$\mu < (\alpha_1 + \beta_1)2^{s_1} < 2\mu. \quad (64)$$

В случае $s_1 = 1$ имеет место

$$s_1 = 1 \Leftrightarrow \alpha_1 > 1 \quad (65)$$

и параметры $\alpha_1, \beta_1, m_2, n_2$ матрицы (58) определяются условиями

$$0 < m_2 < \alpha_1 \Leftrightarrow m_2 = 1, 3, 5, \dots, \alpha_1 - 2, \quad (66)$$

$$\frac{1}{2}\mu < \alpha_1 + \beta_1 < \mu, \quad (67)$$

$$2^{s-2} \equiv \gamma\beta_1 \pmod{\alpha_1}, \quad (68)$$

где $\gamma \in \mathbb{N}$ и удовлетворяет неравенству $\alpha_1 - 2\gamma \geq 1$.

2) Если $g \in SV^-$, то

$$g = \begin{pmatrix} \alpha_1 \cdot 2^{s_1} & \beta_1 \cdot 2^{s_1} \\ \alpha_1 \cdot 2^{s_1} - m_2 & \beta_1 \cdot 2^{s_1} - n_2 \end{pmatrix}, \quad (69)$$

в тех же обозначениях, что и выше.

Доказательство теоремы 11 дается в работе [1].

ТЕОРЕМА 12. *Простые элементы SV образуют бесконечное счетное подмножество $SV_p \subset SV$.*

ДОКАЗАТЕЛЬСТВО. Среди матриц (58) при условии (61) выделяется семейство матриц вида

$$g = \begin{pmatrix} 2^{s-2} & 2^{s-2} \\ 2^{s-3} - 1 & 2^{s-3} + 3 \end{pmatrix}, \quad s \in \mathbb{N}, \quad s \geq 4. \quad (70)$$

и легко устанавливается [1] простота таких матриц.

В принципе, этого достаточно для утверждения теоремы 12, хотя, как показывают вычисления (57) при $s = 6$, возможны простые элементы, отличные от (70). Однако данное обстоятельство, очевидно, не меняет мощности множества $SV_p \subset SV$. Этим завершается доказательство теоремы 12.

СЛЕДСТВИЕ 8. *Полугруппа SP имеет бесконечную счетную систему образующих в виде множества $\{g_1, g_{-1}, h_1, h_2, g_{-2}\} \cup SV_p$. В общем случае разложение элементов SP по данной системе образующих свойством единственности не обладает.*

На этом, в принципе, можно было бы считать завершенным изучение полугруппы SP , однако остается специфичный вопрос о свободных конечно порожденных подполугруппах SP , который в полной мере рассматривается в следующем пункте.

7. Свободные 3-порожденные подполугруппы SP и генеалогия пифагоровых троек. Рассмотрим граф $\Gamma(P, P^{(2)})$, где P – множество примитивных пар (2), представляющее множество вершин, а $P^{(2)}$ – множество ребер данного графа, определяемое следующим образом:

$$P^{(2)} = \{(b, a), g(b, a)\} : (b, a) \in P, g \in SP\}.$$

Граф $\Gamma(P, P^{(2)})$ является полным, счетным и бесконечным. Существует изоморфизм $\Gamma(P, P^{(2)}) \cong \Gamma(\pi, f(P^{(2)}))$, где f – нелинейное преобразование $f(P) = \pi$, по которому $f(b, a) = (x, y, z) \in \pi$ в соответствии с (1),

$$f(P^{(2)}) = \{(f(b, a), f(g(b, a)))\}.$$

Пусть W – свободная подполугруппа в SP , порожденная некоторой конечной системой образующих w , такая, что отображение $W \times P \rightarrow P \setminus \{(2, 1)\}$ сюръективно. Тогда подграф $\Gamma(P, P_w^{(2)}) \subset \Gamma(P, P^{(2)})$, где

$$P_w^{(2)} = \{(b, a), g(b, a)\} : (b, a) \in P, g \in w\},$$

очевидно, определяет дерево решений задачи Пифагора. Существование такой подполугруппы W следует хотя бы из теоремы 7, по которой можно положить $W = SP_1$ с системой образующих $w = \{g_1, g_{-1}, h_1\}$.

Естественно, возникает вопрос, связанный с перечислением всевозможных генеалогических деревьев задачи Пифагора, одно из которых, в принципе, указывается теоремой 7 и следствием 5. Для этого следует установить некоторые характерные свойства системы образующих w подполугруппы $W \subset SP$, которые доказываются в следующих утверждениях.

ПРЕДЛОЖЕНИЕ 12. *Всякая система образующих w подполугруппы W обязательно содержит два преобразования, каждое из которых отвечает требованию*

$$g(2, 1) = (b_2, a_2), \quad b_2 + a_2 = 5. \quad (71)$$

Действительно, соотношения (71) реализуются только теми преобразованиями $g \in \text{SP}$, у которых образы $(b_2, a_2) \in \{(3, 2), (4, 1)\}$, и в силу (5) эти образы не могут быть связаны каким-либо преобразованием из SP .

ПРЕДЛОЖЕНИЕ 13. *В полугруппе SP существует только 4 преобразования g_1, h_1, h_2, g_{-2} , которые отвечают требованию (71).*

С помощью (4) условие (71) представляется в виде

$$b_2 + a_2 = 2(m_1 + m_2) + (n_1 + n_2) = 5, \quad (72)$$

где $(m_1 + m_2) \in \{1, 3\}$ в силу (10), (13). Тогда при $m_1 + m_2 = 1$ получаются преобразования h_1, h_2 , а при $m_1 + m_2 = 3$ получаются преобразования g_1 и g_{-2} . Что и требовалось доказать.

ПРЕДЛОЖЕНИЕ 14. *Из преобразований g_1, h_1, h_2, g_{-2} можно составить только три пары $\{g_1, h_1\}, \{g_{-2}, h_2\}, \{g_1, g_{-2}\}$, каждая из которых входит в некоторую систему образующих w подполугруппы $W \subset \text{SP}$.*

Рассмотрим, например, пару $\{h_1, h_2\}$. Как видно из табл. 3, у этих преобразований имеется непустая область пересечения по m_2 , следствием чего является неоднозначность представления с помощью преобразований h_1 и h_2 . Поэтому пара $\{h_1, h_2\}$ не входит в какую-либо систему образующих w . По аналогичной причине, также отбрасываются пары $\{h_1, g_{-2}\}$ и $\{g_1, h_2\}$. Оставшиеся три пары преобразований $\{g_1, h_1\}, \{g_{-2}, h_2\}, \{g_1, g_{-2}\}$, судя по свойствам в табл. 3, являются подмножеством некоторой системы образующих w подполугруппы $W \subset \text{SP}$, что и требовалось доказать.

ПРЕДЛОЖЕНИЕ 15. *В полугруппе SP условию*

$$g(2, 1) = (b_3, a_3), \quad b_3 + a_3 = 7 \quad (73)$$

отвечают 7 следующих преобразований: $h_1^2, h_2 \circ h_1, g_{-1}, g_2, h_1 \circ g_{-2}, h_2 \circ g_{-2}, g_1^2$.

Доказательство проводится по той же схеме, что и в предложении 13.

Следующая теорема, опираясь на результаты предложений 12–15, устанавливает все свободно порожденные подполугруппы $W \subset \text{SP}$.

ТЕОРЕМА 13. *В полугруппе SP имеются только три 3-порожденные свободные подполугруппы вида $\langle g_1, g_{-1}, h_1 \rangle, \langle g_2, g_{-2}, h_2 \rangle, \langle g_1, g_{-2}, h_2 \circ h_1 \rangle$, отвечающие условиям предложений 14, 15.*

ДОКАЗАТЕЛЬСТВО. Идея доказательства состоит в достройке каждой пары преобразований из предложения 14 до соответствующей системы образующих w подполугруппы $W \subset \text{SP}$ с помощью преобразований из предложения 15.

Для этого составляется табл. 4 для пар $\{g_1, h_1\}, \{g_{-2}, h_2\}, \{g_1, g_{-2}\}$ из предложения 14, в которой указаны их области ограничений по m_2 , установленные при доказательстве теорем 7, 8, в табл. 2 и 3. Аналогичным образом составляется табл. 5,

содержащая ограничения по m_2 для 7 преобразований из предложения 15. Из анализа табл. 4, 5 вытекает следующее.

1) Для пары $\{g_1, h_1\}$ “брешь” по m_2 полностью закрывается преобразованием g_{-1} , причем единственным образом, и в результате приходим к полугруппе $W = \langle g_1, h_1, g_{-1} \rangle$ из теоремы 7.

2) Для пары $\{g_{-2}, h_2\}$ имеется “брешь” по m_2 в том случае, когда речь заходит о преобразованиях из класса $[q_1]$ в табл. 1. Эта “брешь” единственным образом полностью закрывается преобразованием g_2 и в результате приходим к полугруппе $W = \langle g_2, g_{-2}, h_2 \rangle$.

3) Для пары $\{g_1, g_{-2}\}$ имеется “брешь” по m_2 в том случае, когда речь заходит о преобразованиях из класса $[q_2]$ в табл. 1. Эта “брешь” в данном случае единственным образом полностью закрывается с помощью преобразования $h_2 \circ h_1$, с учетом того, что в классе $[q_2]$ равенство $m_2 = k$ невозможно, а также в силу следствия 6. В результате приходим к полугруппе $W = \langle g_1, g_{-2}, h_2 \circ h_1 \rangle$.

Очевидно, что

$$\langle g_1, h_1, g_{-1} \rangle \cong \langle g_2, g_{-2}, h_2 \rangle \cong \langle g_1, g_{-2}, h_2 \circ h_1 \rangle.$$

Отсюда следует утверждение теоремы 13.

СЛЕДСТВИЕ 9. *Существует только три трихотомических дерева решений задачи Пифагора, которые определяются графами*

$$\Gamma(P, P_1^{(2)}) \cong \Gamma(P, P_2^{(2)}) \cong \Gamma(P, P_3^{(2)}),$$

где

$$P_1^{(2)} = \{\{(b, a), g(b, a)\} : (b, a) \in P, g \in \{g_1, g_{-1}, h_1\}\},$$

$$P_2^{(2)} = \{\{(b, a), g(b, a)\} : (b, a) \in P, g \in \{g_2, g_{-2}, h_2\}\},$$

$$P_3^{(2)} = \{\{(b, a), g(b, a)\} : (b, a) \in P, g \in \{g_1, g_{-2}, h_2 \circ h_1\}\}.$$

На рис. 1 представлено решение задачи Пифагора в виде генеалогического дерева $\Gamma(P, P_1^{(2)})$, где в вершинах указаны примитивные пары, под которыми приведены соответствующие пифагоровы тройки.

8. Заключение. Мысль об эффективном использовании полугруппового подхода при решении некоторых типов диофантовых уравнений возникла после знакомства с работами [2], [3], в которых с помощью элементарных представлений линейной алгебры вычислены тройки линейных преобразований, определяющих три варианта трихотомических деревьев, интерпретирующих (с точностью до изоморфизма) решения задачи Пифагора. Однако с помощью элементарных соображений авторам [2], [3] не удалось корректно обосновать то, что перечисленные варианты деревьев фактически исчерпывают существующие возможности. По этой же причине также остались открытыми некоторые другие вопросы, которые сформулированы в постскрипте работы [3]. Вместе с этим данные результаты, в принципе, содержат идею построения и исследования соответствующей полугрупповой структуры, связанной с решением задачи Пифагора, что, собственно, и проделано в данной работе.

Для построенной полугруппы SP с помощью преобразования

$$f(b, a) = (b + a, b - a)$$

Рис. 1

устанавливается изоморфизм с полугруппой простых пар одинаковой четности. Это позволяет несколько иначе рассматривать процедуру алгоритма Евклида и проблему доказательства бесконечности простых чисел-близнецов.

Автор благодарит Д. А. Бредихина и В. Н. Кузнецова за ряд ценных замечаний и поддержку данной работы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] В. Е. Фирстов, *Нетрадиционные геометрические интерпретации, полугрупповая теория и генеалогия пифагоровых троек*, Изд-во “Научная книга”, Саратов, 2004.
- [2] А. Hall, “Genealogy of pythagorean triads”, *Math. Gaz.*, **54** (1970), 377–379.
- [3] E. S. Selmer, “Organisering av Pytagoreiske tallsett”, *Nordisk Mat. Tidskr.*, **25–26:3–4** (1978), 139–149.

В. Е. Фирстов

Саратовский государственный университет
им. Н. Г. Чернышевского
E-mail: firstov1980@mail.ru

Поступило

16.05.2007

Исправленный вариант

19.10.2007