Определение набора чисел по набору его кратных сумм

Д. В. Фомин

В статье дан обзор всей доступной информации по тематике, связанной с замечательной задачей из комбинаторной теории чисел, поставленной Лео Мозером в 1957 году. Обобщённая задача Мозера такова: если нам дан набор всех сумм по s различных элементов неизвестного набора (мультимножества) из n чисел, то возможно ли однозначно восстановить исходный набор? В данном обзоре обсуждаются результаты и методы, использовавшиеся за последние 60 лет. Также представлены некоторые новые факты, предложены важные нерешённые задачи и гипотезы. Английский вариант статьи см. в [10].

Посвящается памяти
Олега Ижболдина (1963–2000)

§ 1. Введение

Ровно шестьдесят лет назад, в 1957 году, журнал «American Mathematical Monthly» опубликовал следующую сравнительно несложную задачу по теории чисел, предложенную Лео Мозером (см. [16]).

Задача 1.1. (а) Десять чисел $s_1 \leqslant s_2 \leqslant \ldots \leqslant s_{10}$ являются попарными суммами набора из пяти неизвестных чисел $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_5$. Найдите числа x_i.

(б) Некоторые шесть различных чисел $s_1 < s_2 < \ldots < s_6$ получены как набор попарных сумм набора из четырёх чисел. Докажите, что существует другой набор из четырёх чисел, попарные суммы которых образуют тот же самый набор из шести чисел.

После того как эта задача была быстро решена, она была переформулирована и обобщена. В результате возникла весьма интересная и нетривиальная проблема, сочетающая аддитивную теорию чисел и комбинаторику.

Задача 1.2. Пусть A является набором (мультимножеством) из n чисел a_i, $i = 1, 2, \ldots, n$. Рассмотрим набор $A^{(2)}$, состоящий из $\binom{n}{2}$ чисел, являющихся 2-суммами набора A, т. е. набор всех сумм вида $a_{i_1} + a_{i_2}$, где $1 \leqslant i_1 < i_2 \leqslant n$. Для каких значений n всегда можно однозначно восстановить набор A по набору $A^{(2)}$?

Числа, упомянутые здесь, могут быть вещественными, комплексными или даже принадлежать произвольному полю характеристики нуль. Как мы вскоре узнаем, это не имеет никакого значения.

Таким образом, в этом обобщении проблемы Мозера спрашивается, можно ли однозначно восстановить набор чисел по набору его попарных сумм.

Немного позже эта же задача была представлена (см., например, [6]) с использованием несколько отличной терминологии.

Задача 1.3. Зловредный подручный мельника, которому было поручено взвесить n мешков с мукой, решил вместо этого взвешивать их по два. После этого он записал в некоем произвольном порядке все полученные $n(n-1)/2$ чисел. Можно ли по этому списку определить веса самих мешков (с точностью до перестановки)?

Хочется отметить, что подручный был не только зловреден, но и туповат: вместо того, чтобы выполнить лишь n взвешиваний, он зачем-то произвёл гораздо большее количество этих операций.

Как видим, задача опять была поставлена как вопрос о возможности «восстановления набора чисел»: может ли неизвестный набор быть однозначно восстановлен по набору своих попарных сумм?

Безусловно, любая интересная задача, теорема или гипотеза заслуживает, чтобы ей было дано симпатичное имя, которое удобно для использования в лекциях и научных дискуссиях. «Последняя теорема Ферма», «Гипотеза Римана», «P = NP», «$(3k + 1)$-гипотеза Коллатца» — все эти названия коротки и вполне информативны. Мне кажется, что в нашем случае вполне уместно название «Задача Мозера» (а если хочется сделать название длиннее и подробнее, то «Задача Мозера о восстановлении набора чисел»).

Итак, исходная задача 1.1 была и в самом деле совсем проста. Однако этого нельзя сказать о её обобщении 1.2. Тем не менее и оно было довольно быстро решено, и, как следствие, возникла ещё более обобщённая задача.

Обозначение. Для любой пары таких натуральных чисел n и s, что $n \geqslant s$, будем обозначать через $A^{(s)}$ набор всех s-сумм набора A, т. е. набор всех сумм вида $a_{i_1} + a_{i_2} + \ldots + a_{i_s}$, где $1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant n$.

Задача 1.4 (обобщённая задача Мозера). Натуральные числа n и s таковы, что $n > s$. Существуют ли такие два разных n-набора A и B, что $A^{(s)} = B^{(s)}$?

Подобная пара наборов представляла бы пример невозможности однозначного восстановления.

Определение. Если два набора A и B таковы, что наборы их s-сумм совпадают — то есть $A^{(s)} = B^{(s)}$, — то мы будем называть такие наборы *s-эквивалентными* и обозначать это отношение как $A \overset{s}{\sim} B$.

Определение. Назовём пару натуральных чисел (n, s) *сингулярной*, если она допускает нетривиальную «невозможность восстановления набора», т. е. $n > s$ и при этом существуют два различных s-эквивалентных набора A и B из n чисел ($A \neq B$ и $A \overset{s}{\sim} B$).

Таким образом, все упомянутые выше задачи можно переформулировать как вопросы о сингулярных парах. Главная цель состоит в том, чтобы описать все такие пары неким «легко вычислимым» способом.

Обозначение. Для произвольного натурального числа s обозначим через $\mathcal{M}_s$ множество всех таких натуральных чисел $n > s$, что пара (n, s) сингулярна.

Например, множество $\mathcal{M}_1$ пусто. А вот задача 1.1 может быть переформулирована так: содержит ли множество $\mathcal{M}_2$ числа 10 и 4? (хотя это и не совсем точно в отношении второй половины этой задачи).

В этой статье мы перечислим все известные на данный момент результаты по обобщённой проблеме Мозера, равно как и основные методы исследования. Мы также представим некоторые новые факты и перечислим несколько важных нерешённых вопросов и гипотез.

§ 2. Историческая справка

(1957)

Начнём с предположения о том, чем именно был вызван интерес Мозера к данной тематике. За несколько лет до того, в 1954 году, Лео Мозер и Джим Ламбек опубликовали статью [14] о разбиениях множества натуральных чисел. В ней они доказали известную теорему Ламбека — Мозера о связи разбиений натурального ряда $\mathbb{N}$ на два подмножества и последовательностей вида $\{f(n) + n\}$, где $f\colon \mathbb{N} \to \mathbb{Z}_{\geqslant 0}$ — произвольная монотонно неубывающая и неограниченная сверху функция.

Это исследование было посвящено некоторым, весьма схожим с проблемой Мозера, задачам о том, как множества (конечные или бесконечные) натуральных чисел накладываются или дополняют друг друга при сдвигах.

Скорее всего, именно так Мозер натолкнулся на вопрос о восстановлении набора чисел для случая $s = 2$ — но, разумеется, это лишь предположение. Однако стоит отметить, что в своей более поздней короткой заметке [15] Ламбек и Мозер упоминают, причём буквально на одной и той же странице, как проблему восстановления, так и вопросы, связанные с дополняющими друг друга последовательностями целых чисел.

(1958)

В 1958 году, почти сразу же после публикации исходной задачи, Джон Селфридж и Эрнст Штраус в своей статье [18] решили задачу 1.2 и ответили на некоторые вопросы, возникшие по ходу дела. Начали они с того, что доказали следующую теорему.

Теорема 2.1. *Набор A из n чисел однозначно определяется набором своих 2-сумм тогда и только тогда, когда n не является степенью двойки.*

Другими словами, пара $(n, 2)$ сингулярна в точности тогда, когда n есть степень двойки. Или, с использованием введённых нами обозначений,

$$\mathcal{M}_2 = \{4, 8, 16, 32, \ldots\} = \{2^k \colon k > 1\}.$$

Во-вторых, они исследовали случай $s = 3$ обобщённой проблемы Мозера 1.4 и показали, что для $n = 6$ существуют многочисленные и легко конструируемые примеры различных наборов A и B из n чисел, для которых $A \overset{3}{\sim} B$. Вот один из них:

$$\begin{aligned} A = \{1^5, -5\},\ B = \{(-1)^5, 5\} \quad &\Rightarrow \quad A \neq B, \\ A^{(3)} = \{3^{10}, (-3)^{10}\},\ B^{(3)} = \{(-3)^{10}, 3^{10}\} \quad &\Rightarrow \quad A^{(3)} = B^{(3)}, \end{aligned}$$

где 1^5 это не 1, как вы могли бы подумать. В стандартных обозначениях мультимножеств (наборов) a^b обозначает элемент a с кратностью b (т. е. b-кратное вхождение числа a в соответствующий набор). Стало быть, имелось в виду вот что:

$$A = \{1, 1, 1, 1, 1, -5\}, \quad B = \{-1, -1, -1, -1, -1, 5\}.$$

Что касается других значений n, то авторы работы [18] доказали, что примеры 3-эквивалентных n-наборов могут существовать, только если $n^2 - (2^k + 1)n + 2 \cdot 3^{k-1}$ обращается в нуль для некоторого натурального

$k \leqslant n$. Не очень сложно доказать, что остальные нетривиальные (превосходящие s) значения n, для которых это возможно, это $n = 27$ (при $k = 5, 9$) и $n = 486$ ($k = 9$) (см. статьи [2, 18]).

Таким образом, эти авторы доказали, что

$$\{6\} \subset \mathcal{M}_3 \subset \{6, 27, 486\}.$$

В-третьих, с помощью подобной же техники для $s = 4$ было доказано, что единственные нетривиальные значения n, при которых восстановление набора может быть невозможно, это $n = 8, 12$.

Найти пример для случая $n = 8$ совсем несложно. Вообще говоря, нетрудно построить пример «невозможности восстановления» для обобщённой проблемы Мозера 1.4, если $n = 2s$ (мы продемонстрируем это несколько позже в § 3). Опять-таки, этот результат можно записать как

$$\{8\} \subset \mathcal{M}_4 \subset \{8, 12\}.$$

Всё это привело авторов работы [18] к нескольким дополнительным вопросам и предположениям.

Вопрос 2.2. *В самом ли деле пары* $(27, 3)$ *и* $(486, 3)$ *сингулярны? Другими словами, можно ли найти два таких различных набора* A *и* B *из* n *чисел, что* $A^{(3)} = B^{(3)}$ *для* $n = 27$ *и* $n = 486$*?*

Вопрос 2.3. *Тот же вопрос для пары* $(12, 4)$*. То есть существуют ли два таких различных* 12*-набора* A *и* B*, что* $A^{(4)} = B^{(4)}$*?*

На момент написания статьи [18] ответа на эти вопросы у авторов не было. Приведём ещё один важный вопрос из той же статьи.

Вопрос 2.4. *В случаях когда восстановление набора невозможно, могут ли существовать более чем два* n*-набора с идентичными наборами* s*-сумм?*

Селфридж и Штраус предположили, что ответ на этот вопрос отрицателен.

(1959)

Вскоре после публикации Селфриджа и Штрауса появилась небольшая заметка Мозера и Ламбека [15]. Начиналась она с упоминания результатов статьи [18], но затем авторы двинулись в другом направлении.

А именно, они задались вопросом о том, можно ли разбить всё множество неотрицательных целых чисел $\mathbb{Z}_{\geqslant 0}$ на два таких подмножества $A = \{a_1, a_2, \ldots\}$ и $B = \{b_1, b_2, \ldots\}$, что $A^{(2)}$ и $B^{(2)}$ совпадают как мультимножества. Было доказано, что это сделать можно, причём такое разбиение единственно. Доказательство использовало производящую функцию мультимножества.

Определение. Для любого конечного набора A неотрицательных целых чисел вида $\{a_1^{k_1}, a_2^{k_2}, \ldots, a_m^{k_m}\}$ определим его производящую функцию (многочлен) $f_A(x)$ при помощи формулы

$$f_A(x) = \sum_{i=1}^{m} k_i x^{a_i}.$$

Аналогичной формулой эта производящая функция может быть определена и для бесконечного набора $A = \{a_1^{k_1}, a_2^{k_2}, \ldots\}$ в том случае, если последовательность $\{k_i^{1/a_i}\}$ ограничена сверху.

Авторы доказали, что в интересовавшем их случае производящие функции удовлетворяют системе уравнений

$$\begin{cases} f_A(x) + f_B(x) = \dfrac{1}{1-x}, \\ f_A^2(x) - f_A(x^2) = f_B^2(x) - f_B(x^2). \end{cases}$$

Они также доказали, что аналогичное разбиение множества $Z_n = \{0, 1, 2, \ldots, n-1\}$ возможно тогда и только тогда, когда n является степенью двойки. Это разбиение также единственно.

Интересно, что и в конечном, и в бесконечном случае разбиение определяется так называемой *последовательностью Морса — Туэ* $\{\alpha_n\}$, определённой как $\alpha_n = s_2(n) \pmod 2$, где $s_2(n)$ есть *двоичный* вес числа n, т. е. сумма цифр в двоичном представлении n. Например, если $n = 2^p$ и мы определим множества $A = \{a_1, \ldots, a_m\}$ и $B = \{b_1, \ldots, b_m\}$ следующим образом:

$$A = \{k \in Z_n \colon \alpha_k = 0\}, \quad B = \{k \in Z_n \colon \alpha_k = 1\},$$

то $A^{(2)} = B^{(2)}$. И в самом деле, если положить

$$f_A(x) = \sum_{i=1}^{m} x^{a_i} \quad \text{и} \quad f_B(x) = \sum_{i=1}^{m} x^{b_i},$$

то мы получим

$$f_A(x) + f_B(x) = u(x) = \frac{1 - x^{2^p}}{1-x},$$

$$f_A(x) - f_B(x) = v(x) = \prod_{i=0}^{p-1} (1 - x^{2^i}).$$

Тогда $f_A = (u+v)/2$ и $f_B = (u-v)/2$, откуда можно вывести равенство

$$f_A^2(x) - f_A(x^2) = f_B^2(x) - f_B(x^2).$$

Осталось только заметить, что выражения слева и справа от знака равенства есть не что иное, как производящие функции для наборов $A^{(2)}$ и $B^{(2)}$ соответственно.

Впоследствии похожий подход с использованием производящих функций (в сочетании с некоторыми другими идеями) был использован в статьях [11], [6] и [2].

(1962)

Следующая статья по этой теме появилась в 1962 году, когда Френкель, Гордон и Штраус опубликовали статью [11], доказав, что ответ на вопрос 2.4 положителен. Это был лишь первый, но отнюдь не последний раз, когда одна из гипотез, касающихся проблемы Мозера, была опровергнута.

Авторы нашли многочисленные примеры кратной сингулярности для простейшего случая $s=2$. Более точно: они показали, как сконструировать три таких различных набора A, B и C из 8 чисел, что $A^{(2)} = B^{(2)} = C^{(2)}$. Вот один из этих контрпримеров:

$$\begin{aligned} A &= \{0, 5, 6, 7, 9, 10, 11, 16\}; \\ B &= \{1, 4, 5, 6, 10, 11, 12, 15\}; \\ C &= \{2, 3, 4, 7, 9, 12, 13, 14\}. \end{aligned}$$

После этого исходный вопрос был «подправлен» — новый вариант спрашивал, сколь много различных n-наборов могут порождать один и тот же набор s-сумм. Максимальное возможное количество таких наборов было обозначено $\mathcal{F}_s(n)$. Конечно, тогда пара (n, s) должна быть как минимум сингулярной — что эквивалентно неравенству $\mathcal{F}_s(n) > 1$.

В статье [11] было доказано несколько неравенств для чисел $\mathcal{F}_s(n)$. Например, $\mathcal{F}_2(16) \leqslant 3$, $2 \leqslant \mathcal{F}_3(6) \leqslant 6$, $\mathcal{F}_4(12) \leqslant 2$.

Однако никаких других примеров сингулярностей тройной или более высокой кратности найдено не было. Это привело к постановке очередного вопроса.

Вопрос 2.5. а) *Существует ли число $n = 2^p > 8$ и такие три различных n-набора, что любые два из этих наборов 2-эквивалентны (то есть $\mathcal{F}_2(n) > 2$)?*

б) *Более общо, существует ли сингулярная пара (n, s), отличная от $(8, 2)$, и такие три различных n-набора, что любые два из этих наборов s-эквивалентны (то есть $\mathcal{F}_s(n) > 2$)?*

В той же статье были доказаны ещё два интересных факта. Во-первых, оказалось, что в вопросах, относящихся к восстановлению наборов чисел по наборам их кратных сумм, достаточно работать с кольцом целых чисел $\mathbb{Z}$; нет никакой нужды рассматривать экзотические случаи произвольных полей с нулевой характеристикой или абелевых групп без кручения. Во-вторых, был разрешён важный вопрос о количестве элементов в $\mathcal{M}_s$: авторы доказали, что множество $\mathcal{M}_s$ конечно для любого $s > 2$.

В том же самом году первая часть исходной задачи Мозера 1.1 была предложена на заключительном туре Московской математической олимпиады. Вполне возможно, что один из советских математиков ознакомился с публикацией [11] и, решив, что задача Мозера заслуживает более широкого распространения, предложил её жюри олимпиады. Задача попала в варианты 8 и 9 классов и оказалась одной из самых трудных задач в этих параллелях. Со всеми задачами московских олимпиад тех лет можно ознакомиться в книгах [1, 4].

(1968)

Среди двух вопросов о «подозрительных» парах (вопросы 2.2, 2.3) последний ($n = 12$, $s = 4$) выглядел более простым. Так что никого не удивило, что «всего» через десять лет после работы [18] Джон Юэлл опубликовал статью [9], в которой доказывалось, что пара $(12, 4)$ не является сингулярной — набор из 12 чисел всегда можно восстановить по набору его 4-сумм. Он также нашёл чисто комбинаторное и более прямое доказательство важной формулы (3) (см. ниже, в § 4).

Много лет спустя дополнительное исследование выявило ошибку в проведённых им вычислениях для пары $(12, 4)$. Однако другой факт в той же статье был абсолютно верен. А именно, Юэлл показал, что ответ на вопрос 2.5 б положителен. Он сделал это, доказав, что $\mathcal{F}_3(6) = 4$, после чего дал полное описание всех возможных четвёрок попарно различных, но 3-эквивалентных наборов из 6 чисел.

Вот один примеров Юэлла:

$$A = \{0, 5, 9, 10, 11, 13\}; \quad B = \{1, 5, 8, 9, 10, 15\};$$
$$C = \{1, 6, 7, 8, 11, 15\}; \quad D = \{3, 5, 6, 7, 11, 16\}.$$

Проверку их эквивалентности мы оставим читателю в качестве несложного упражнения.

(1981)

Ричард Гай включил вопрос о восстановлении набора чисел по набору его кратных сумм в свой сборник нерешённых проблем теории чисел [12, задача C5]. Вопрос сопровождался разъяснением, что задача решена для $s=2$, но её уточнение, касающееся значений функции $\mathcal{F}_2$, всё ещё не исследовано до конца. Случаи $s=3$ для $n=27$ и $n=486$ представлены в качестве открытых вопросов.

(1991)

Насколько нам известно, после статьи Юэлла проблема Мозера была отложена в сторону примерно до 1991 года, когда Боман, Болкер и О'Нил попробовали подойти к ней с несколько другой стороны в статье [6].

Если даны точка $x = (x_1, x_2, \ldots, x_n)$ в n-мерном евклидовом пространстве $\mathbb{R}^n$ и произвольное подмножество $A = \{a_1, \ldots, a_s\}$ из s элементов в $I_n = \{1, 2, \ldots, n\}$, то определим x_A как сумму $x_{a_1} + \ldots + x_{a_s}$. Далее, обозначая $\binom{n}{s} = m$, определяем линейный оператор

$$R_{n,s}\colon \mathbb{R}^n \to \mathbb{R}^m, \quad R_{n,s}(x_1, x_2, \ldots, x_n) = (x_{A_1}, x_{A_2}, \ldots, x_{A_m}),$$

где $A_1, \ldots, A_m$ — последовательность всех s-подмножеств I_n. Это не что иное, как комбинаторная (дискретная) версия интегрального преобразования Радона.

Очевидно, что отображение $R_{n,s}$ может быть перенесено из евклидовых пространств на их факторпространства по модулю стандартного действия симметрических групп S_n и S_m на $\mathbb{R}^n$ и $\mathbb{R}^m$: любой перестановке $s \in S_n$ соответствует перестановка координат $T_s\colon (x_1, \ldots, x_n) \to (x_{s(1)}, \ldots, x_{s(n)})$ и т. д. Следовательно, мы получаем отображение $R_{n,s}\colon \mathbb{L}_n \to \mathbb{L}_m$, где $\mathbb{L}_k = \mathbb{R}^k/S_k$. Тогда проблема Мозера может быть представлена как вопрос о том, является ли $R_{n,s}$ инъекцией. Или более общо: как вопрос о размере прообраза $R^{-1}_{n,s}(x)$ для $x \in \mathbb{L}_m$.

С использованием этой терминологии и соответствующей техники авторы доказали, что при восстановлении n-набора по набору его 2-сумм нельзя получить более $n-2$ различных наборов. В дополнение к этому они доказали, что для любого $n \neq 8$ эта оценка сверху может быть понижена до 2 и почти всегда до 1. Таким образом, был получен ответ на вопрос 2.5 а.

Стоит также отметить, что, судя по списку сформулированных в статье вопросов, на момент публикации авторы не знали о статье Юэлла [9].

(1992)

Совершенно случайно в 1991 году задача 1.2 была предложена на математическом конкурсе для студентов-математиков Санкт-Петербургского государственного университета. Увидев её, автор этого обзора был увлечён — как и многие математики до него — интересной и на первый взгляд несложной задачей. Этот интерес и последовавшее исследование привели к появлению статьи Фомина и Ижболдина [2], поданной для публикации в «Записках Санкт-Петербургского отделения МИАН России» в 1992 г. (английский перевод был опубликован в 1995 г.).

Бо́льшая часть этой статьи была посвящена доказательству результатов, давно полученных в [18] и [11] — к сожалению, в то время доступ к зарубежным публикациям был ограничен, а ни о каких сетевых архивах и речи не могло идти. Несмотря на это, статья содержала один новый и важный результат: примеры сингулярных пар, которые дали положительный ответ на вопрос 2.2 для обоих «подозрительных» случаев. Пары $(27, 3)$ и $(486, 3)$ и в самом деле оказались сингулярными.

Так было закрыто исследование обобщённой проблемы Мозера 1.4 для случая $s = 3$.

(1996)

По прошествии нескольких лет Боман и Линуссон независимо построили те же примеры сингулярности для пар $(27, 3)$ и $(486, 3)$ в статье [7]. Также они исследовали вопрос о построении всех возможных пар эквивалентных наборов для $s=3$. Увы, они посчитали, что вопрос о сингулярности пары $(12, 4)$ был уже разрешён Юэллом в [9] — в конце статьи они упоминают, что были проинформированы об этом факте буквально в последний момент перед публикацией.

(1997)

Росс Хонсбергер посвятил главу «A Gem from Combinatorics» своей книги [13] случаю $s = 2$ обобщённой проблемы Мозера. Любопытно, что имя Мозера там не упоминается — Хонсбергер пишет, что излагаемые результаты были переданы ему от Пала Эрдёша и Джона Селфриджа. Это единственное упоминание имени Эрдёша в контексте проблемы Мозера. Честно говоря, не очень ясно, в самом ли деле великий венгерский математик имел какое-то отношение к этим результатам, или это просто нечаянная ошибка атрибуции.

(2003)

В главе 46 своей увлекательной книги [17] Савчев и Андрееску излагают решение задачи 1.2, равно как и результаты из статьи [15], с привлечением последовательности Морса — Туэ.

(2008)

Несколько расширенная версия задачи 1.3 с добавлением некоторых фактов из [11] и [6] была опубликована как задача [8] в «American Mathematical Monthly» под авторством Элизабет Чен и Джеффри Лагариаса.

Некоторые из решений были впоследствии размещены и обсуждены на веб-сайте «Cut-The-Knot», см. [5].

(2016)

На протяжении двадцати лет с проблемой Мозера не происходило ничего содержательного, и вдруг в 2016 году Исомуродов и Кохась ([3]) обнаружили, что Джон Юэлл сделал ошибку в своих вычислениях для пары $(12,4)$. Теперь мы уже никогда не узнаем, как именно это случилось, но в любом случае в наши дни математикам не нужно проводить столь сложные полиномиальные выкладки на бумаге — авторы статьи [3] использовали для этого алгебраический пакет Maple™. После этого авторы построили пару 4-эквивалентных 12-наборов — тем самым был полностью разрешён вопрос 2.3 и завершено исследование случая $s=4$ задачи 1.4 (подробности далее в § 4).

§ 3. Несколько простых примеров

Этот короткий параграф продемонстрирует построение нескольких простых примеров сингулярных пар и s-эквивалентных наборов.

Случай $s = 2$, $n = 2^k$. Самый тривиальный случай — это пара $(2,2)$; если нам известна лишь сумма двух чисел, то, конечно же, мы не можем однозначно восстановить сами числа. Хотя эта пара и не является настоящей сингулярной парой (так как $n=s$), но мы можем использовать её как базис для построения других, уже нетривиальных примеров.

А именно, если нам даны два 2-эквивалентных набора из n чисел A и B, то для любого числа d имеем

$$A' = A \cup (B+d) \overset{2}{\sim} B' = B \cup (A+d), \tag{1}$$

где $X+d$ обозначает набор, полученный из X прибавлением d ко всем его элементам. Поэтому если мы начнём с наборов

$$A = \{1,1\}, \quad B = \{0,2\}, \quad A \overset{2}{\sim} B,$$

и выберем $d=1$, то получим

$$A' = \{1,1,1,3\}, \quad B' = \{0,2,2,2\}, \quad A' \overset{2}{\sim} B'.$$

Продолжая в том же духе, можно легко построить примеры 2-эквивалентных n-наборов для каждого n, являющегося степенью двойки. Оставим доказательство эквивалентности (1) читателю в качестве несложного упражнения.

Случай $n = 2s$. Помните пример сингулярности для $n = 6$, $s = 3$ из § 2? Он может быть легко обобщён для любой пары (n, s) при $n = 2s$.

А именно, возьмём произвольный $2s$-набор A и вычислим его среднее арифметическое a. Затем отразим A относительно a и получим *зеркальную копию*, набор $\tilde{A} = 2a - A$. Если исходный набор A не был симметричен, то $\tilde{A}$ отличен от A и при этом $A \overset{s}{\sim} \tilde{A}$. Чтобы доказать последнее утверждение, достаточно заметить, что для каждого s-набора $M \subset A$ зеркальная копия его дополнения $A \backslash M$ (которая является s-набором в $\tilde{A}$) имеет ту же самую сумму элементов.

В качестве простейшего примера можно взять набор $A = \{1^{2s-1}, 1 - 2s\}$ и его зеркальную копию $\tilde{A} = \{(-1)^{2s-1}, 2s - 1\}$.

Все s-суммы чисел из A — их всего имеется $\binom{2s}{s}$ — распадаются на две группы. Одна состоит из сумм наборов, которые включают в себя $(1 - 2s)$, и количество таковых равно $\binom{2s-1}{s-1}$. Каждая из этих сумм равна

$$(s - 1) \cdot 1 + (1 - 2s) = -s.$$

Другая группа включает в себя $\binom{2s-1}{s}$ сумм наборов, состоящих только из единиц, — каждая такая сумма равна s. Следовательно, мы получаем $A^{(s)} = \{(-s)^m, s^m\}$, где $m = \binom{2s-1}{s-1} = \binom{2s-1}{s}$. Очевидно, что набор $A^{(s)}$ зеркально симметричен относительно нуля, а значит, $\tilde{A}^{(s)} = A^{(s)}$.

Двойственность $(n, s) \longleftrightarrow (n, n - s)$

Если нам даны два s-эквивалентных n-набора A и B, то эти наборы и $(n - s)$-эквивалентны. Чтобы доказать это, достаточно убедиться в том, что сумма всех элементов A совпадает с суммой всех элементов B. Короткое вычисление показывает, что

$$\sum_{1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant n} (a_{i_1} + a_{i_2} + \ldots + a_{i_s}) = \binom{n-1}{s-1} \sum_{1 \leqslant i \leqslant n} a_i.$$

Таким образом, сумма чисел в A равна сумме чисел в B, и, обозначив это число через σ, получаем

$$A^{(n-s)} = \sigma - A^{(s)}, \quad B^{(n-s)} = \sigma - B^{(s)},$$

что доказывает двойственность. Отсюда в частности следует, что можно считать $n \geqslant 2s$; если $s < n < 2s$, то можно перейти к паре (n, s'), где $s' = n - s$ и $n > 2s'$.

Эта двойственность позволяет нам построить «новые» примеры сингулярных пар. Скажем, поскольку пара $(8, 2)$ сингулярна, то сингулярной является и пара $(8, 6)$. Как мы вскоре увидим, пары $(27, 3)$, $(486, 3)$ и $(12, 4)$ сингулярны, а значит, то же можно сказать и про пары $(27, 24)$, $(486, 483)$ и $(12, 8)$.

Далее в § 5 мы несколько подробнее исследуем эту двойственность и некоторые её вариации.

Линейные преобразования

Под занавес упомянем один очевидный, но весьма полезный факт. Если наборы A и B s-эквивалентны и $f(x) = px + q$ — произвольная линейная функция, то наборы $f(A)$ и $f(B)$ также s-эквивалентны. Это означает, что мы можем сдвигать, а также подвергать сжатию-растягиванию пары эквивалентных наборов, снова получая эквивалентные наборы.

Так, если взять наборы $A = \{0, 5, 9, 10, 11, 13\}$ и $B = \{1, 5, 8, 9, 10, 15\}$, то $A \overset{3}{\sim} B$. Применяя функцию $f(x) = 2x - 13$, мы получим новую пару 3-эквивалентных наборов $A_1 = \{-13, -3, 5, 7, 9, 13\}$ и $B_1 = \{-11, -3, 3, 5, 7, 17\}$.

Конечно же, все подобные примеры, которые получаются друг из друга линейными преобразованиями, можно считать идентичными в рамках изучаемой нами тематики.

§ 4. Симметрические многочлены. Полное решение для случаев $s = 2, 3, 4$

Давайте теперь углубимся в изучение некоторых конкретных методов, применяемых для решения задачи Мозера. Главный из них основан на применении симметрических многочленов.

По данному n-набору $A = \{a_1, \ldots, a_n\}$ построим последовательность сумм k-х степеней его элементов для $k = 1, \ldots, n$:

$$\sigma_k(A) = \sum_{i=1}^{n} a_i^k.$$

Хорошо известно, что набор A может быть однозначно восстановлен по этой последовательности — ведь значения $\sigma_k(A)$ определяют коэффициенты многочлена $(x - a_1)(x - a_2) \ldots (x - a_n)$ и, значит, однозначно определяют набор его корней.

Итак, если значения $\sigma_k(A)$ для $k = 1, \ldots, n$ могут быть получены из значений $\sigma_k(A^{(s)})$, то набор A однозначно определён набором $A^{(s)}$.

Начнём с небольших значений k. Для $k = 1$ мы уже вычислили, что

$$\sigma_1(A^{(s)}) = \binom{n-1}{s-1}\sigma_1(A),$$

и следовательно, если $A^{(s)} = B^{(s)}$, то $\sigma_1(A) = \sigma_1(B)$. Это означает, что сумма $\sigma_1(A)$ всегда может быть вычислена по набору $A^{(s)}$.

Далее, если $k = 2$, то

$$\begin{aligned}\sigma_2(A^{(s)}) &= \sum_{1\leqslant i_1<\ldots<i_s\leqslant n} (a_{i_1} + \ldots + a_{i_s})^2 =\\ &= \binom{n-1}{s-1}\sum_{1\leqslant i\leqslant n} a_i^2 + \binom{n-2}{s-2}\sum_{1\leqslant i<j\leqslant n} 2a_ia_j =\\ &= \binom{n-1}{s-1}\sum_{1\leqslant i\leqslant n} a_i^2 + \binom{n-2}{s-2}\sum_{1\leqslant i\neq j\leqslant n} a_ia_j =\\ &= \left(\binom{n-1}{s-1} - \binom{n-2}{s-2}\right)\sum_{1\leqslant i\leqslant n} a_i^2 + \binom{n-2}{s-2}\sum_{1\leqslant i,\, j\leqslant n} a_ia_j =\\ &= \binom{n-2}{s-1}\sigma_2(A) + \binom{n-2}{s-2}\sigma_1(A)^2.\end{aligned}$$

Мы уже вычислили $\sigma_1(A)$, и потому можем теперь вычислить и $\sigma_2(A)$, разве что коэффициент $\binom{n-2}{s-1}$ обращается в нуль. Это невозможно при $n > s > 0$ — значит, сумма $\sigma_2(A)$ всегда может быть восстановлена по набору $A^{(s)}$.

Теперь обратимся к общему случаю. Поскольку $\sigma_k(A^{(s)})$ является симметрическим многочленом от $a_1, \ldots a_n$, он может быть выражен в форме

$$\sigma_k(A^{(s)}) = \alpha(s,k,n)\sigma_k(A) + \mathcal{P}\big(\sigma_1(A), \sigma_2(A), \ldots, \sigma_{k-1}(A)\big). \qquad (2)$$

Здесь $\alpha(s,k,n)$ — некая константа (относительно переменных a_i), однозначно определяемая тремя числами n, s, k, а $\mathcal{P}$ — некий многочлен от $k-1$ переменных, чьи коэффициенты также полностью определены той же самой тройкой чисел. Например, как следует из вычислений в предыдущем абзаце, при $k = 2$ мы имеем $\alpha(s,2,n) = \binom{n-2}{s-1}$ и $\mathcal{P}(x) = \binom{n-2}{s-2}x^2$.

Из этого общего рассуждения ясно, что если ни один из коэффициентов $\alpha(s,k,n)$ при $1 \leqslant k \leqslant n$ не равен нулю, то пара (n, s) не сингулярна, т. е. набор A всегда однозначно восстанавливается по набору $A^{(s)}$.

Теорема 4.1.

$$\alpha(s,k,n) = \sum_{p=1}^{s}(-1)^{p-1}p^{k-1}\binom{n}{s-p}. \qquad (3)$$

Таким образом, коэффициент $\alpha(s,k,n)$ оказался многочленом от n.

Определение. Будем называть правую часть уравнения (3) *многочленом Мозера* и обозначать его $F_{s,k}(n)$.

Теорема 4.1 была доказана в статье [11] путём преобразований другой формулы, взятой из [18]. Позже более прямое комбинаторное доказательство было дано в статье [9]. Через много лет эта теорема была опять заново «открыта» и доказана (при помощи экспоненциальных производящих функций) в работе [2].

В качестве не очень сложного упражнения читателю предлагается доказать, что для $k = 2$ формула (3) даёт равенство $F_{s,2}(n) = \binom{n-2}{s-1}$.

Кстати, даже и без этой формулы случай $s = 2$ (задача 1.2) может быть теперь разрешён буквально за несколько секунд. Вычисляя $\sigma_k(A^{(2)})$ напрямую, мы получим (с использованием обозначений из (2))

$$\alpha(s, 2, n) = n - 2^{k-1}.$$

Это означает, что n-набор всегда восстанавливается по набору своих 2-сумм, если n не является степенью двойки. Как мы уже знаем (§ 3), для всех степеней двойки 2^p, $p > 1$, существуют примеры, доказывающие сингулярность пар $(2^p, 2)$.

Случай $s = 3$. Уравнение (3) даёт

$$F_{3,k}(n) = \binom{n}{2} - 2^{k-1}\binom{n}{1} + 3^{k-1},$$
$$2F_{3,k}(n) = n^2 - n(2^k + 1) + 2 \cdot 3^{k-1}.$$

Исследование этого случая также довольно прямолинейно. Сначала мы доказываем, что $F_{3,k}(n)$ не обращается в нуль для натурального n, если $k > 12$. Затем проверяем все случаи $k \leqslant 12$ и убеждаемся, что многочлены $F_{3,k}$ обладают целочисленными корнями тогда и только тогда, когда $k \in \{1, 2, 3, 5, 9\}$. Для этих пяти специальных случаев имеем

$$F_{3,1}(n) = \frac{1}{2}(n-1)(n-2), \quad F_{3,2}(n) = \frac{1}{2}(n-2)(n-3),$$
$$F_{3,3}(n) = \frac{1}{2}(n-3)(n-6), \quad F_{3,5}(n) = \frac{1}{2}(n-6)(n-27),$$
$$F_{3,9}(n) = \frac{1}{2}(n-27)(n-486).$$

Из § 3 мы уже знаем, что пара $(6, 3)$ сингулярна. Чтобы доказать то же самое для пар $(27, 3)$ и $(486, 3)$, приведём здесь следующие примеры:

$$\begin{aligned}
n &= 27 & A'_{27} &= \{0, 1^{16}, 2^{10}\},\\
& & A''_{27} &= \{0^5, 1^{10}, 2^{10}, 3^2\},\\
& & A'''_{27} &= \{0, 1^5, 2^{10}, 3^6, 4^5\},\\
n &= 486 & A_{486} &= \{0^{22}, 1^{176}, 2^{231}, 3^{56}, 4\}.
\end{aligned}$$

Проверку того, что каждый из этих наборов 3-эквивалентен своему зеркальному отражению, мы оставим читателю. В наше время это можно сделать за несколько минут при помощи одного из стандартных вычислительных пакетов. Впрочем, при наличии соответствующего опыта можно обойтись и без специального программного обеспечения.

Итог: $\mathcal{M}_3 = \{6, 27, 486\}$.

Случай $s = 4$. Из уравнения (3) получаем

$$F_{4,k}(n) = \binom{n}{3} - 2^{k-1}\binom{n}{2} + 3^{k-1}\binom{n}{1} - 4^{k-1},$$

$$6F_{4,k}(n) = n^3 - n^2(3 + 3 \cdot 2^{k-1} + 1) + n(2 + 3 \cdot 2^{k-1} + 2 \cdot 3^k) - 6 \cdot 4^{k-1}.$$

Затем, используя стандартные приёмы элементарной теории чисел, можно доказать, что при $k > 7$ многочлены $F_{4,k}$ не имеют натуральных корней. И наконец,

$$\begin{aligned}
F_{4,1}(n) &= \frac{1}{6}(n-1)(n-2)(n-3),\\
F_{4,2}(n) &= \frac{1}{6}(n-2)(n-3)(n-4),\\
F_{4,3}(n) &= \frac{1}{6}(n-3)(n-4)(n-8),\\
F_{4,4}(n) &= \frac{1}{6}(n-4)(n^2-23n+96),\\
F_{4,5}(n) &= \frac{1}{6}(n-8)(n^2-43n+192),\\
F_{4,6}(n) &= \frac{1}{6}(n-12)(n^2-87n+512),\\
F_{4,7}(n) &= \frac{1}{6}(n-8)(n^2-187n+3072).
\end{aligned}$$

Случай $n = 8$ (то есть ситуация $n = 2s$) нам уже хорошо знаком. Единственный другой нетривиальный корень многочленов $F_{4,k}$ равен 12. Как уже упоминалось ранее, этот вариант оказался крепким орешком — пара 4-эквивалентных 12-наборов была найдена только в 2016 году Исомуродовым и Кохасем. Если мы рассмотрим наборы

$$\begin{aligned}
A &= \{1^2, 4, 6, 7, 8^2, 9, 10, 12, 15^2\},\\
B &= \{0, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 16\},
\end{aligned}$$

то не так уж и трудно проверить, что $A \overset{4}{\sim} B$.

В статье [3] авторы доказали, что данная пара является единственным (с точностью до линейных преобразований) примером двух различных наборов с указанными свойствами.

Итог: $\mathcal{M}_4 = \{8, 12\}$.

§ 5. Поиск корней многочленов Мозера

Мы теперь знаем, что пара (n, s) может быть сингулярной, только если n является корнем многочлена $F_{s,k}$. Поэтому обратим более пристальное внимание на эти корни. (Этот параграф представляет собой развёрнутый пересказ и комментарий доказательства теоремы 7 из работы [18].)

Вычислим многочлены Мозера для нескольких первых значений k.

Случай $k = 1$. Нам уже известно, что

$$F_{s,1}(n) = \binom{n-1}{s-1} = \frac{1}{(s-1)!}(n-1)(n-2)\dots(n-s+1) = \frac{1}{(s-1)!}\prod_{p=1}^{s-1}(n-p).$$

Значит, корнями являются числа от 1 до $s-1$, и они нам не интересны: n должно быть больше s, чтобы пара (n, s) имела шансы на сингулярность.

Случай $k = 2$. И этот многочлен был уже вычислен:

$$F_{s,2}(n) = \binom{n-2}{s-1} = \frac{1}{(s-1)!}\prod_{p=2}^{s}(n-p).$$

Опять-таки, нужных нам корней здесь нет. Продолжим...

Случай $k = 3$. По-прежнему не очень сложно вычислить, что

$$F_{s,3}(n) = \frac{1}{(s-1)!}(n-2s)\prod_{p=3}^{s}(n-p),$$

и здесь (наконец-то!) мы находим нетривиальный корень $n = 2s$. Впрочем, о нём мы уже знаем — пара $(2s, s)$ всегда сингулярна.

Случай $k = 4$. Это вычисление может занять у вас немного больше времени, но оно опять не особенно сложно. При $s > 2$ мы имеем

$$F_{s,4}(n) = \frac{1}{(s-1)!}(n^2-(6s-1)n+6s^2)\prod_{p=4}^{s}(n-p). \tag{4}$$

Получаем квадратное диофантово уравнение, решения которого дадут нам нетривиальные корни многочленов $F_{s,k}$:

$$n^2-(6s-1)n+6s^2 = 0. \tag{5}$$

Оно может быть записано и как уравнение для s:

$$s^2 - sn + \frac{n(n+1)}{6} = 0. \tag{6}$$

Сумма корней уравнения (6) равна n — следовательно, если пара (n, s), где $n > s$, даёт корень уравнения (4), то это же верно и для пары $(n, n-s)$.

Это прямой аналог двойственности, описанной нами в § 3. Мы будем называть такие пары $\langle n, 4\rangle$-*сопряжёнными* или просто n-сопряжёнными.

Точно такое же рассуждение для уравнения (5) показывает, что если пара (n, s) — решение уравнения (4), то пара $(6s-1-n, s)$ также является его решением. Эти две пары мы будет называть $\langle s, 4\rangle$-*сопряжёнными.*

Ясно, что каждое сопряжение симметрично. Также очевидно, что для любого положительного решения (n, s) мы имеем $6s-1>n$ и $n>s$ — иначе левые стороны уравнений (6) и (5) были бы положительны. Поэтому сопряжённая пара также состоит из положительных целых чисел.

Рассмотрим теперь минимальное возможное решение уравнения (5), а именно, $r=(2,1)$ (поскольку речь идёт о натуральных числах, мы имеем право говорить о минимальных решениях). Сама по себе эта пара нам не годится, так как s должно быть не меньше 3, чтобы формула (4) имела смысл. Однако эта пара всё же удовлетворяет уравнению (5), и её можно использовать, чтобы построить из неё другие корни.

Отметим, что пара r является n-самосопряжённой $(2-1=1)$, и потому от неё мы можем перейти к другому корню только через s-сопряжение. Так и сделаем — получаем пару $(3,1)$, затем через n-сопряжение переходим к паре $(3,2)$, потом к $(8,2)$, к $(8,6)$ и т. д.

Продолжая этот процесс, получаем бесконечную цепочку решений уравнения (5):

$$\begin{gathered}\underline{(2,1)} \overset{s}{\longleftrightarrow} \underline{(3,1)} \overset{n}{\longleftrightarrow} \underline{(3,2)} \overset{s}{\longleftrightarrow} \underline{(8,2)} \overset{n}{\longleftrightarrow} (8,6) \overset{s}{\longleftrightarrow} (27,6) \overset{n}{\longleftrightarrow} \\ \overset{n}{\longleftrightarrow} (27,21) \overset{s}{\longleftrightarrow} (98,21) \overset{n}{\longleftrightarrow} (98,77) \overset{s}{\longleftrightarrow} (363,77) \overset{n}{\longleftrightarrow} (363,286) \overset{s}{\longleftrightarrow} \ldots \end{gathered} \tag{7}$$

Мы отметили стрелки буквами «n» и «s», чтобы указать, какое именно сопряжение используется в каждом переходе; также мы подчеркнули «непригодные» пары — они являются решениями (5), но не дают корни многочлена $F_{s,k}$ для $s>2$ (пара $(8,2)$ сингулярна, но мы её не рассматриваем из-за требования $s>2$). Итак, начиная с $(8,6)$, пары в этой цепочке дают полностью пригодные корни многочленов $F_{s,4}$. Потому они все представляют собой возможные сингулярности для проблемы Мозера.

Случай $k=5$. И тут вычисление не так уж сложно. При $s>3$ получаем

$$F_{s,5}(n)=\frac{1}{(s-1)!}(n^2-(12s-5)n+12s^2)(n-2s)\prod_{p=5}^{s}(n-p).$$

Опять мы имеем дело с квадратным диофантовым уравнением, которое можно записать так:

$$n^2-(12s-5)n+12s^2=0, \tag{8}$$

или
$$s^2 - sn + \frac{n(n+5)}{12} = 0. \tag{9}$$

Как и ранее, уравнение (9) даёт нам n-сопряжение (двойственность) $(n, s) \longleftrightarrow (n, n-s)$. А уравнение (8) даёт $\langle s, 5\rangle$-сопряжение — а именно, $(n, s) \longleftrightarrow (12s - 5 - n, s)$.

Совершенно так же, как и в предыдущем случае, мы приходим к цепочке решений:

$$\underline{(3,1)} \overset{s}{\longleftrightarrow} \underline{(4,1)} \overset{n}{\longleftrightarrow} \underline{(4,3)} \overset{s}{\longleftrightarrow} \underline{(27,3)} \overset{n}{\longleftrightarrow}$$
$$\overset{n}{\longleftrightarrow} (27,24) \overset{s}{\longleftrightarrow} (256,24) \overset{n}{\longleftrightarrow} (256,232) \overset{s}{\longleftrightarrow} (2523,232) \overset{n}{\longleftrightarrow} \ldots$$

Однако в этом случае имеется небольшое отличие. «Минимальное решение», которым является пара $(3, 1)$, таково, что его n-сопряжённая пара $(3, 2)$ с ним не совпадает. Поэтому цепочка решений может быть продолжена и в другую сторону:

$$\underline{(3,2)} \overset{s}{\longleftrightarrow} \underline{(16,2)} \overset{n}{\longleftrightarrow} (16,14) \overset{s}{\longleftrightarrow} (147,14) \overset{n}{\longleftrightarrow}$$
$$\overset{n}{\longleftrightarrow} (147,133) \overset{s}{\longleftrightarrow} (1444,133) \overset{n}{\longleftrightarrow} (1444,1311) \overset{s}{\longleftrightarrow} \ldots$$

и обе цепочки могут быть объединены в одну, бесконечную в обоих направлениях:

$$\ldots \overset{n}{\longleftrightarrow} (1444,1311) \overset{s}{\longleftrightarrow} (1444,133) \overset{n}{\longleftrightarrow} (147,133) \overset{s}{\longleftrightarrow} (147,14) \overset{n}{\longleftrightarrow} (16,14) \overset{s}{\longleftrightarrow}$$
$$\overset{s}{\longleftrightarrow} \underline{(16,2)} \overset{n}{\longleftrightarrow} \underline{(3,2)} \overset{s}{\longleftrightarrow} \underline{(3,1)} \overset{s}{\longleftrightarrow} \underline{(4,1)} \overset{n}{\longleftrightarrow} \underline{(4,3)} \overset{s}{\longleftrightarrow} \underline{(27,3)} \overset{n}{\longleftrightarrow}$$
$$\overset{n}{\longleftrightarrow} (27,24) \overset{s}{\longleftrightarrow} (256,24) \overset{n}{\longleftrightarrow} (256,232) \overset{s}{\longleftrightarrow} (2523,232) \overset{n}{\longleftrightarrow} \ldots \tag{10}$$

В обоих случаях $s = 4$ и $s = 5$ нетрудно проверить, что все натуральные решения уравнений (5) и (8) принадлежат к цепочкам (7) и (10) соответственно. Мы оставим это читателю в качестве несложного упражнения.

Случай $k = 6$. Было бы просто замечательно, если бы мы могли применять тот же метод и далее. Увы, вычисляя многочлен $F_{s,6}$, мы получаем (при $s > 4$)
$$F_{s,6}(n) = \frac{1}{(s-1)!} g_{s,6}(n) \prod_{p=6}^{s} (n-p),$$

где

$$g_{s,6}(n) = n^4 - (30s-16)n^3 + (150s^2 - 90s + 11)n^2 - (240s^3 - 90s^2 + 4)n + 120s^4.$$

Некоторые из многочленов $g_{s,6}$ имеют целочисленные корни. Например,

$$\begin{aligned}
g_{8,6}(n) &= (n-12)(n^3-212n^2+6347n-40\,960),\\
g_{10,6}(n) &= (n-32)(n^3-252n^2+6047n-37\,500),\\
g_{22,6}(n) &= (n-32)(n^3-612n^2+51\,047n-878\,460),\\
g_{30,6}(n) &= (n-32)(n^3-852n^2+105\,047n-3\,037\,500).
\end{aligned}$$

И на этом наше исследование случая $k=6$ заканчивается. Нет ни квадратных уравнений, ни цепочек сопряжённых решений. Весьма вероятно, что многочлены $g_{s,6}$ не имеют корней, кроме перечисленных выше.

Ну а что касается бóльших значений k — увы, никаких надежд на простые решения у нас пока что нет.

В завершение этого параграфа приведём несколько сравнительно несложных фактов о многочленах Мозера, для краткости изложения опуская их доказательства.

Упражнение 5.1. Докажите, что при $k>1$ многочлен $F_{s,k}(n)$ делится на $\prod_{p=k}^{s}(n-p)$. «Пустое» произведение, как обычно, равно 1.

Упражнение 5.2. Докажите (не пользуясь уравнением (3)), что выполнены равенства

$$\begin{aligned}
F_{s,k}(n+1)-F_{s,k}(n) &= F_{s-1,k}(n),\\
F_{s,k}(n) &= sF_{s,k-1}(n)-nF_{s-1,k-1}(n-1).
\end{aligned}$$

Упражнение 5.3. Докажите, что при $n>s+1$ и $n\geqslant k>1$ выполнена рекуррентная формула $F_{s,k}(n)=(-1)^kF_{n-s,k}(n)$.

Упражнение 5.4. Докажите равенство $F_{s,k}(k)=(-1)^{s-1}\left\langle {k-1 \atop s-1} \right\rangle$. Выражение $\left\langle {k-1 \atop s-1} \right\rangle$ обозначает здесь так называемое число Эйлера 1-го рода, которое равно количеству перестановок порядка $k-1$ с $s-1$ подъёмами (подъём в перестановке $\pi=\{\pi_1,\pi_2,\ldots,\pi_m\}$ — это такой индекс $0<j<m$, что $\pi_j<\pi_{j+1}$).

§ 6. Компьютерный эксперимент

Корни $F_{s,k}$

В попытках отыскать корни многочленов Мозера (отличные от уже найденных), которые могли бы навести нас на догадки о природе сингулярных пар, я написал не очень длинную программу на языке Sage, которая была затем запущена на веб-сервере сайта `CoCalc.com` для $s=3,4,5,6,7$ и т. д., до тех пор пока сервер не начал запинаться (это произошло где-то в окрестности значения $s = 40$). После этого я переключился на тот же пакет, установленный на моём персональном компьютере, и продолжил вычисления вплоть до значения $s = 200$, когда каждое следующее значение s стало требовать около дня работы компьютера (и примерно тогда же мой компьютер стал жаловаться на исчерпание операционной памяти).

Вот что делала эта программа. Для каждого фиксированного значения s она запускала цикл по k от 1 до 1000; на каждом шагу цикла она вычисляла многочлен $F_{s,k}$, раскладывала его на множители над кольцом целых чисел $\mathbb{Z}$ и в случае нетривиального разложения распечатывала корни многочлена. В конце цикла программа также выдавала величину $k_{\max}(s)$ — максимальное значение переменной k, для которой многочлен $F_{s,k}$ обладал хотя бы одним целочисленным корнем.

В таблице приведены итоги этого эксперимента — список всех нетривиальных корней (исключая пары $(2s, s)$), найденных этой программой.

Нетривиальные корни многочленов Мозера для $3 \leqslant s \leqslant 200$

s	3	4	6	8	10	14	21
n	$27^{[5]}$, $486^{[9]}$	$12^{[6]}$	$8^{[4]}$, $\mathbf{27}^{[4]}$	$12^{[6]}$	$\mathbf{32}^{[6]}$	$16^{[5]}$, $\mathbf{147}^{[5]}$	$\mathbf{27}^{[4]}$, $\mathbf{98}^{[4]}$

s	22	24	30	62	77	126	133
n	$\mathbf{32}^{[6]}$	$27^{[5]}$, $\mathbf{256}^{[5]}$	$32^{[6]}$	$64^{[7]}$	$\mathbf{98}^{[4]}$, $\mathbf{363}^{[4]}$	$128^{[8]}$	$\mathbf{147}^{[5]}$, $\mathbf{1444}^{[5]}$

Я пометил каждый корень n минимальным значением переменной k, для которого $F_{s,k}(n) = 0$: например, метка $^{[4]}$ соответствует цепочке (7), а метка $^{[5]}$ — цепочке (10).

Для всех других значений s от 3 до 200 корни, найденные программой, были либо $n = 2s$ (они были бы помечены в таблице меткой $^{[3]}$), либо тривиальны $(1, 2, \ldots, s)$ и потому нам не нужны.

Те корни $F_{s,k}$, про которые на данный момент не известно, представляют ли они настоящие сингулярности проблемы Мозера, выделены **жирным шрифтом**. Это — наши главные «подозреваемые».

Ещё один важный результат эксперимента состоял в том, что для всех $3 < s \leqslant 200$ вычисленное значение $k_{\max}(s)$ совпало с $2s - 1$. На основании этого факта была выдвинута $k_{\max}$-гипотеза — см. гипотезу 7.6 ниже, в § 7.

Следующее предложение можно рассматривать как весьма простую «половину» этой гипотезы.

Предложение 6.1. *Для любых $s > 2$, $n = 2s$ и любого нечётного k такого, что $1 < k < n$, верно равенство $F_{s,k}(n) = 0$.*

Доказательство. Это равенство можно переписать с использованием (3), и после добавления слагаемого с $p = 0$ и обращения порядка суммирования мы получим для произвольного чётного числа $0 < r < n$

$$\sum_{p=0}^{s} (-1)^p (s-p)^r \binom{n}{p} = 0.$$

Поскольку при этом

$$\binom{n}{p} = \binom{n}{n-p}, \quad (s-p)^r = (s-(n-p))^r,$$

уравнение выше эквивалентно такому:

$$\sum_{p=0}^{n} (-1)^p (s-p)^r \binom{n}{p} = 0.$$

Любой многочлен от p степени меньше n (например, $(s-p)^r$) может быть выражен как линейная комбинация многочленов $p^{[j]}$, $j = 0, \ldots, n-1$, где $p^{[j]} = p \cdot (p-1) \cdot \ldots \cdot (p-j+1)$ (это выражение часто обозначается также через $(p)_j$). Тогда наше предложение следует из хорошо известного равенства

$$\sum_{p=0}^{n} (-1)^p p^{[j]} \binom{n}{p} = 0,$$

которое легко доказать, использовав производящую функцию

$$\lambda(x) = (1+x)^n = \sum_{p=0}^{n} \binom{n}{p} x^p.$$

Многочлен $\lambda(x)$ имеет корень $x_0 = -1$ кратности n, и потому x_0 является корнем его j-й производной

$$\lambda^{(j)}(x) = \sum_{p=0}^{n} \binom{n}{p} p^{[j]} x^{p-j}$$

для любого $0 \leqslant j < n$. □

Взяв $k = 2s-1$, из равенства $F_{s,2s-1}(2s) = 0$ выводим

Следствие 6.2. *Для любого $s > 2$ верно неравенство $k_{\max}(s) \geqslant 2s-1$.*

Поиск сингулярности

Раз уж мы связались с компьютерами, то давайте попробуем использовать их и дальше. Следующая идея состоит в том, чтобы вместо поиска корней $F_{s,k}$ заняться поиском собственно s-эквивалентных наборов.

Можно надеяться, что нам удастся найти такие примеры для минимальных решений из нашего списка «подозреваемых» пар: $(27, 6)$ и $(32, 10)$. Числа в других парах, которые не n-сопряжены с этими двумя, слишком велики, чтобы подобный компьютерный поиск имел какие-либо шансы на успех.

Для начала ограничим область поиска наборов. А именно, рассмотрим все $\binom{n+m-1}{m-1}$ *разбиений* числа n на m упорядоченных неотрицательных целочисленных слагаемых, т. е. нас интересуют представления числа n как суммы m неотрицательных целых чисел k_i $(i = 1, 2, \ldots, m)$:

$$\mathcal{P}\colon n = k_1 + k_2 + \ldots + k_m, \quad k_i \in \mathbb{Z}_{\geqslant 0}.$$

Каждое такое разбиение будет восприниматься нами как строка кратностей мультимножества — то есть разбиению $\mathcal{P}$ соответствует n-набор

$$A_{\mathcal{P}} = \{1^{k_1}, 2^{k_2}, \ldots, m^{k_m}\}. \tag{11}$$

К сожалению, в обоих случаях $(27, 6)$ и $(32, 10)$ нет никакой надежды на то, что мы сможем найти n-набор X, который, подобно примерам для $(27, 3)$ и $(486, 3)$, s-эквивалентен своему зеркальному образу $\widetilde{X}$. В самом деле, если $X \overset{s}{\sim} \widetilde{X}$, то без потери общности можно считать, что $\sigma_1(X) = 0$. Из нашего эксперимента мы уже знаем (это можно доказать простым перебором), что $F_{6,k}(27)=0$ тогда и только тогда, когда $k=4$, а $F_{10,k}(32)=0$ тогда и только тогда, когда $k=6$. Следовательно, для любого такого X, что $X^{(s)} = \widetilde{X}^{(s)}$, имеем $\sigma_k(X) = \sigma_k(\widetilde{X})$ для всех $1 \leqslant k \leqslant n$. Ведь единственные возможные исключения — это числа 4 и 6 (для $n = 27$ и $n = 32$ соответственно), а для них равенство $\sigma_k(X) = \sigma_k(\widetilde{X})$ выполняется просто потому, что они чётны и $\widetilde{X} = -X$.

Что же нам теперь делать и каковы трудности, стоящие на пути этого эксперимента?

Во-первых, мы не можем накопить массив всех возможных разбиений (или наборов типа (11)) и затем заняться анализом этих данных — нам просто не хватит компьютерной памяти. Например, при $n=27$ и $m=10$ количество всех разбиений близко к ста миллионам (точное значение 94 143 280).

Следовательно, алгоритм должен быть итеративным. Не очень сложно написать итератор, который будет генерировать следующее разбиение, отталкиваясь от предыдущего. *Подсказка:* найдите последнее ненулевое слагаемое, увеличьте предыдущее слагаемое на единицу, а все последующие слагаемые сделайте нулями, кроме самого последнего. При необходимости то же самое можно сделать для итеративного перечисления всех s-подмножеств в n-наборе.

Во-вторых, проверочная функция, которая выясняет, эквивалентны ли два данных набора A и B, должна быть написана очень аккуратно и эффективно, поскольку она будет вызываться очень много раз. Необходимо использовать в ней так называемые методы «быстрого отказа» (quick rejection). Например, сумма первых s чисел в A (можно считать, что набор упорядочен) совпадает с минимальным элементом в $A^{(s)}$; поэтому такие суммы для A и B обязаны совпадать. Чем больше подобных «быстрых отказов» использовано в коде такой функции, тем лучше. Ведь полностью вычислять и сравнивать между собой наборы $A^{(s)}$ и $B^{(s)}$ весьма накладно, и делать это надо только тогда, когда деваться уже некуда.

В-третьих, вызывать такую проверочную функцию для каждой пары построенных наборов — это, конечно же, совершенно нереально. Поэтому вместо прямого грубого перебора нужно вычислять одну или несколько простых «сигнатур» каждого набора $A_{\mathcal{P}}$. *Сигнатурой* мы называем здесь такую функцию $\mathcal{S}$ на множестве всех наборов, что $A \overset{s}{\sim} B \ \Rightarrow\ \mathcal{S}(A) = \mathcal{S}(B)$. Найденные таким образом значения мы затем сравним между собой, и это должно заменить гораздо более громоздкую проверку на полное совпадение наборов типа $A_{\mathcal{P}}^{(s)}$. Этот способ позволяет выполнить требуемую проверку в два этапа. А именно — сначала для всех наборов $A_{\mathcal{P}}$ вычисляем несколько простейших сигнатур (сумма всех чисел, сумма первых s чисел и т. п.), находим дубликаты, а на втором этапе для наборов, соответствующих этим дубликатам, производим вычисление более сложных сигнатур или даже полную проверку.

Но даже и с использованием такого «трюка» трудно продвинуться дальше, чем $m = 10$, и причина всё та же — приходится хранить в памяти (и потом обрабатывать) огромные массивы данных. Один из способов продвинуться ещё дальше по этому пути — попробовать разбить наборы $A_{\mathcal{P}}$ на группы меньшего размера (например, по сумме всех чисел набора и т. п.).

Мой эксперимент не дал положительного результата — ни одного примера 6-эквивалентных 27-наборов не было найдено среди наборов типа (11) при $m < 10$. В качестве проверки я прогнал свою первую программу (прямой перебор) для пары $(12, 4)$ с $m = 17$, и менее чем через час работы она выдала мне тот же самый уникальный пример двух 4-эквивалентных 12-наборов, который был найден Исомуродовым и Кохасем. Аналогичная функция, построенная по схеме двухэтапного поиска, нашла этот же пример за четыре минуты.

Понятно, что отсутствие результатов в таком вычислительном эксперименте не влечёт никакого содержательного вывода относительно сингулярности пары $(27, 6)$. Вполне возможно, что для нахождения примера надо взять существенно большее значение m. И конечно же, всегда есть вероятность того, что такого примера попросту не существует. Этот вопрос по-прежнему остаётся открытым.

Если кого-то из читателей заинтересует этот подход к отысканию примеров сингулярности в проблеме Мозера, то я с удовольствием поделюсь кодом своих программ — наверняка, эти функции могут быть написаны в более эффективном виде, и по скорости исполнения, и по необходимому количеству памяти. И тогда кто знает — может быть, следующее значение m даст нам заветный пример эквивалентных наборов.

§ 7. Открытые вопросы и гипотезы

Вопрос 7.1. *Верно ли, что* $\mathcal{M}_5 = \{10\}$?

Вопрос 7.2. *Какие из новых «подозрительных» пар* (n, k), *найденных в* § 6, *являются сингулярными*?

Речь здесь, конечно же, идёт о парах, выделенных жирным шрифтом в таблице (см. с. 199). Не исключено, что какая-то «хитрая» компьютерная программа поможет ответить на этот вопрос хотя бы для пар $(27, 6)$ и $(32, 10)$.

Вопрос 7.3. *Верно ли, что наличие корня многочлена* $F_{s,k}$ *гарантирует наличие сингулярной пары*? *То есть верно ли, что для любых таких натуральных чисел* s, k, n, *что* $n > s$, $n \geqslant k$ *и* $F_{s,k}(n) = 0$, *обязательно существует пара различных* s-*эквивалентных* n-*наборов* A *и* B?

Результаты, накопленные по проблеме Мозера за последние шестьдесят лет, пока что подтверждают эту гипотезу; однако, судя по всему, эта задача крайне трудна. Следующий вопрос мог бы, возможно, послужить небольшим шагом к её решению.

Вопрос 7.4. *Сингулярная пара* $P = (n, s)$ *такова, что* $F_{s,k}(n) = 0$ *для* $k = 4$ *или* 5. *Верно ли, что пара* $P' = (m, s)$, *полученная из* P *путём* $\langle s, k\rangle$-*сопряжения, также сингулярна*?

Мы знаем, что n-сопряжение корней многочленов $F_{s,k}$ имеет прямой аналог в двойственности между сингулярными парами $(n, s) \leftrightarrow (n, n - s)$. Однако вопрос об s-сопряжении совсем не так прост.

Вопрос 7.5. *Существует ли какое-то «неслучайное» объяснение хотя бы одной сингулярной пары с* $n \neq 2s$, $s > 2$?

На данный момент все немногочисленные примеры подобных сингулярных пар были найдены полуслучайным образом, путём довольно запутанных вычислений и удавшихся попыток решения систем уравнений $\sigma_k(A^{(s)}) = \sigma_k(B^{(s)})$ для тех случаев, когда получавшиеся в итоге полиномиальные уравнения имели более или менее разумный размер. Возможно, что хотя бы для одной сингулярной пары найдётся некое «менее случайное», комбинаторное или алгебраическое, объяснение этой сингулярности.

По моему мнению, следующая гипотеза является наиболее важным из открытых вопросов по проблеме Мозера — по крайней мере из тех, которые не кажутся чрезмерно сложными.

Гипотеза 7.6 ($k_{\max}$-гипотеза). *Верно ли, что $k_{\max}(s) = 2s-1$ для всех $s > 3$? Другими словами, докажите или опровергните предположение о том, что многочлен $F_{s,k}$ может иметь целочисленные корни только если $k \leqslant 2s-1$.*

Положительный ответ на этот вопрос был бы крайне полезен для любого — ручного или на компьютере — поиска корней многочленов Мозера.

Как минимум, мы могли бы сразу же доказать, что $\mathcal{M}_s = \{2s\}$ для многих малых значений s. Вот как выглядело бы доказательство этого факта для $s = 5$ (то есть решение вопроса 7.1).

«Доказательство». Если $n > 5$ и $n \neq 10$, то $F_{5,k}(n) \neq 0$ для любого $k > 0$. В самом деле, $k_{\max}$-гипотеза позволяет не проверять значения $k \geqslant 10$. Из параграфа 5 мы знаем, что то же самое верно и для $k \leqslant 5$. Осталось лишь проверить $F_{5,6}$, $F_{5,7}$, $F_{5,8}$ и $F_{5,9}$:

$$
\begin{aligned}
F_{5,6}(n) &= \frac{1}{24}(n^4 - 134n^3 + 3311n^2 - 27\,754n + 75\,000),\\
F_{5,7}(n) &= \frac{1}{24}(n^4 - 262n^3 + 9527n^2 - 107\,570n + 375\,000),\\
F_{5,8}(n) &= \frac{1}{24}(n^4 - 518n^3 + 27\,791n^2 - 420\,490n + 1\,875\,000),\\
F_{5,9}(n) &= \frac{1}{24}(n^4 - 1030n^3 + 81\,815n^2 - 1\,653\,650n + 9\,375\,000).
\end{aligned}
$$

Как же это сделать? Здесь нам опять будет полезен компьютер, причём с его помощью можно предложить проверяемое формальное доказательство. В качестве примера докажем, что $F_{5,6}$ не имеет целочисленных корней в промежутке $[5;\infty)$. Пара строчек кода в пакете Matlab™ или в Sage даст приблизительные значения корней этого многочлена

$$
\begin{aligned}
x_1 &= 6{,}014875\ldots, & x_2 &= 7{,}745287\ldots,\\
x_3 &= 15{,}348149\ldots, & x_4 &= 104{,}891687\ldots
\end{aligned}
$$

Мы не можем использовать это в качестве доказательства. Однако, глядя на эти свалившиеся с потолка числа, можно вручную вычислить значения $F_{5,6}(x)$ для $x = 6$, 7, 8, 15, 16, 104 и 105. Получаем числа 1, -25, 15, 85, -199, $-31\,065$ и 3895 и сразу видим, что внутри каждого из четырёх отрезков $[6; 7]$, $[7; 8]$, $[15; 16]$, $[104; 105]$ должен находиться корень нашего многочлена, который, конечно же, не может быть целым числом. Следовательно, эти четыре нецелых числа составляют набор всех корней многочлена четвёртой степени $F_{5,6}$.

Точно такие же рассуждения (только вычисления будут подлиннее) годятся и для многочленов $F_{5,7}$, $F_{5,8}$ и $F_{5,9}$ (впрочем, $F_{5,7}$ и $F_{5,9}$ имеют один целочисленный корень, но он равен 10).

Поскольку $F_{5,k}(n) \neq 0$, из теоремы 4.1 следует, что n-набор A можно однозначно восстановить по набору $A^{(5)}$. $\square$

Наша последняя гипотеза «обновляет» вопрос 2.5. Назовём *магической тройкой* три различных n-набора чисел, которые попарно s-эквивалентны.

Гипотеза 7.7 (магических троек не существует). *Если $s > 2$ и $n > 2s$, то среди любых трёх различных n-наборов найдутся два, которые не s-эквивалентны друг другу.*

Данная гипотеза утверждает, что за исключением специальных случаев ($s = 2$ или $n = 2s$) *магические тройки в природе не встречаются* — другими словами, при попытке восстановить n-набор чисел по набору его s-сумм вариантов восстановления не может быть больше двух.

Список литературы

[1] *Гальперин Г. А., Толпыго А. К.* Московские математические олимпиады. М.: Просвещение, 1986.

[2] *Ижболдин О. Т., Фомин Д. В.* Наборы кратных сумм // Труды Санкт-Петербургского математического общества. 1995. Т. 3. С. 244—259.

[3] *Исомуродов Ж. Э., Кохась К. П.* Набор из 12 чисел не восстанавливается однозначно по своим 4-суммам // Зап. научн. сем. ПОМИ. 2016. Т. 448. С. 135–142.

[4] *Прасолов В. В., Голенищева-Кутузова Т. И., Канель-Белов А. Я., и др.* Московские математические олимпиады 1958–1967 г. М.: МЦНМО, 2013.

[5] *Bogomolny A.* A Property of the powers of 2. 2011. `https://www.cut-the-knot.org/Curriculum/Combinatorics/CombiGem.shtml`

[6] *Boman J., Bolker E., O'Neil P.* The combinatorial Radon transform modulo the symmetric group // Adv. Appl. Math. 1991. Vol. 12. P. 400–411.

[7] *Boman J., Linusson S.* Examples of non-uniqueness for the combinatorial Radon transform modulo the symmetric group // Math. Scand. 1996. Vol. 78. P. 207–212.

[8] *Chen E. R., Lagarias J. C.* Problem E11389 // Amer. Math. Monthly. 2008. Vol. 115(8). P. 758.

[9] *Ewell J. A.* On the determination of sets by sets of sums of fixed order // Canad. J. Math. 1968. Vol. 20. P. 596–611.

[10] *Fomin D. V.* Is the multiset of n integers uniquely determined by the multiset of its s-sums? 2017. https://arxiv.org/abs/1709.06046

[11] *Gordon B., Fraenkel A. S., Straus E. G.*. On the determination of sets by the sets of sums of a certain order // Pacific J. Math. 1962. Vol. 12. P. 187–196.

[12] *Guy R. K.* Unsolved problems in number theory. New York: Springer, 1981.

[13] *Honsberger R.* In Pólya's footsteps. Miscellaneous problems and essays. Washington, DC: Mathematical Association of America, 1997. (Dolciani Mathematical Expositions; Vol.19).

[14] *Lambek J., Moser L.* Inverse and complementary sequences of natural numbers // Amer. Math. Monthly. 1954. Vol. 61. P. 454–458.

[15] *Lambek J., Moser L.* On some two way classifications of integers // Canad. Math. Bull. 1959. Vol. 2. P. 85–89.

[16] *Moser L.* Problem E1248 // Amer. Math. Monthly. 1957. Vol. 64. P. 507.

[17] *Savchev S., Andreescu T.*. Washington, DC: Mathematical Association of America, 2003. (Anneli Lax New Mathematical Library; Vol. 43).

[18] *Selfridge J. L., Straus E. G.* On the determination of numbers by their sums of a fixed order // Pacific J. Math. 1958. Vol. 8. P. 847–856.

Дмитрий Владимирович Фомин, Бостон (США)

fomin@hotmail.com