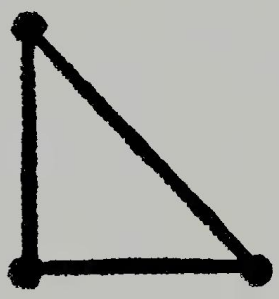
Г.А. Фрейман

Начала структурной теории сложения множеств



КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
ЕЛАБУЖСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Г. А. ФРЕЙМАН

НАЧАЛА СТРУКТУРНОЙ ТЕОРИИ СЛОЖЕНИЯ МНОЖЕСТВ

Под редакцией
А. М. Люстига и Л. П. Усольцева

Учебное пособие для студентов старших курсов и аспирантов университетов и педагогических институтов

КАЗАНЬ 1966

ПРЕДИСЛОВИЕ

Настоящая книга предназначена для студентов старших курсов и аспирантов, изучающих теорию чисел, а также для специалистов, работающих в этой области. Она написана на основе опыта работы семинара по дополнительным главам теории чисел в Елабужском педагогическом институте и дает систематическое изложение цикла работ автора по аддитивной теории чисел. Для чтения книги необходимо лишь знакомство с основами теории чисел, например, по учебникам И. М. Виноградова или А. А. Бухштаба. Многие из задач, приведенных в первой главе, могут быть использованы в качестве тем курсовых и дипломных работ, а также для самостоятельной научной работы.

В последние десятилетия в аддитивной теории чисел началось изучение общих закономерностей, возникающих при сложении множеств. Настоящая работа продолжает эту тенденцию.

В цикле работ 1959—64 гг. ([12] — [20]), появившихся под общим названием „Обратные задачи аддитивной теории чисел", изучается структура множеств с малым удвоением. Точнее, если рассматривать множество с некоторой числовой характеристикой (числом элементов для конечных множеств чисел или вычетов, плотностью для числовых последовательностей, мерой для точечных множеств), причем соответствующая числовая характеристика для удвоенного множества невелика по сравнению с исходной, можно в некотором смысле описать структуру исходного множества. Содержание упомянутых работ и излагается, главным образом, в настоящей книге.

Книга состоит из трех глав. Первая глава содержит изложение основных понятий, общих идей и элементарных результатов. Во второй главе решена трудная конкретная обратная задача. В третьей главе получены приложения.

Хотелось бы подчеркнуть значение понятия изоморфизма подмножеств множеств с алгебраической операцией, которое вводится и изучается в главе I.

Общеизвестно значение понятия изоморфизма групп, которое только и дает возможность, освобождаясь от несущественных свойств каждой данной конкретной группы, вести исследования в общей форме. При этом предполагается возможность производить неограниченное количество действий над элементами группы.

В аддитивной теории чисел, напротив, часто рассматривается ограниченное число сложений изучаемых множеств. Так, в настоящей работе мы ограничиваемся изучением вопросов, связанных с однократным сложением. Естественно ввести понятие изоморфизма, учитывающее это обстоятельство.

Можно провести аналогию между локальным изоморфизмом топологических групп и изоморфизмом подмножеств, „алгебраически локальным изоморфизмом". В первом случае изоморфизм ограничивается пределами некоторой окрестности, во втором — числом производимых действий.

Понятие изоморфизма подмножеств позволило высказать общую точку зрения на аддитивную теорию чисел, как на теорию, изучающую свойства числовых множеств, не меняющихся при изоморфных преобразованиях.

Автор стремился сделать как можно более подробным и ясным изложение материала первой главы, вводящей начинающего читателя в новый круг идей.

Задачи сосредоточены в основном в первой главе. Одни из них преследуют учебные цели, другие дают материал для самостоятельных исследований.

Материал второй и третьей глав изложен более кратко, чем в первой главе.

В главе II доказывается основная теорема о структуре конечных множеств целых чисел с малым удвоением. Для доказательства использована модификация метода тригонометрических сумм, а также язык и элементы методов геометрии чисел.

Весьма желательно получить обобщение результатов глав I и II для произвольных абелевых и, особенно, некоммутативных групп. Желанием подчеркнуть подобные возможности развития теории, наряду с перспективами ее дальнейшего теоретико-числового развития, обусловлено название работы.

Глава III посвящена приложениям теории.

В качестве резюме на английском языке приведен в обработанном виде текст доклада, прочитанного в сентябре 1965 г. в летней школе по теории чисел в г. Паланге. В этом докладе высказана общая точка зрения на исследования в области сложения конечного числа множеств, особенно существенные в аддитивной теории чисел.

ПОЯСНЕНИЯ, ОБЛЕГЧАЮЩИЕ ПОЛЬЗОВАНИЕ КНИГОЙ

1. Определения приводятся в тексте в местах, где впервые встречаются новые понятия. Их можно найти по указателю терминов, приведенному на стр. 140.

2. Если в тексте книги впервые встречается известное из литературы понятие, то оно дается курсивом (иногда курсив повторяется и в дальнейшем). В указателе терминов приводятся ссылки на соответствующую литературу.

3. Ссылки на теоремы, леммы и определения производятся по номерам глав и пунктов, в которых они находятся. Номера параграфов в нумерации не участвуют. Так, например, теорема 1.9 помещается в девятом пункте первой главы. Формулы нумеруются тремя числами; вначале идет номер главы, затем — номер пункта, наконец — номер формулы. Так, например, формула (2.3.1) — это первая формула третьего пункта второй главы. Первое число отбрасывается, если дается ссылка на формулу той же главы. Первые два числа отбрасываются, если дается ссылка на формулу того же пункта. Так, ссылка на формулу (1) на странице 68 означает ссылку на формулу (2.3.1) того же пункта.

4. Номера задач учебного характера приводятся без звездочки, остальные, проблемного характера, задачи снабжены одной, двумя или тремя звездочками.

ГЛАВА I

ИЗОМОРФИЗМ

§ 1. ИЗОМОРФИЗМ ПОДМНОЖЕСТВ МНОЖЕСТВ С АЛГЕБРАИЧЕСКОЙ ОПЕРАЦИЕЙ

1.1. Сложение множеств. Пусть E — множество, в котором определена *алгебраическая операция*, записываемая аддитивно, B и C — подмножества множества E.

Суммой $B + C$ будем называть подмножество множества E, каждый элемент x которого имеет хотя бы одно представление вида $x = b + c$, $b \in B$, $c \in C$*).

Распространение приведенного определения на случай сложения нескольких подмножеств очевидно.

Сумма $B + B$ двух одинаковых подмножеств обозначается $2B$.

Примеры.

1. Пусть N_2 — множество неотрицательных четных чисел, $\{0, 1\}$ — множество, состоящее из чисел 0 и 1, N — множество нат уральных чисел. Тогда $N_2 + \{0, 1\} = N \cup \{0\}$; $2N_2 = N_2$.

2. Пусть Q_2 — множество квадратов целых чисел. Теорема Лагранжа о возможности представления любого натурального числа в виде суммы не более чем четырех квадратов натуральных чисел записывается в виде равенства $4Q_2 = N \cup \{0\}$.

3. Пусть A — абелева группа. Имеем $2A = A$, в частности $2Z = Z$, где Z — аддитивная группа целых чисел.

*) Определенную вышеуказанным образом алгебраическую сумму $B + C$ не следует смешивать с теоретико-множественной суммой (объединением) подмножеств B и C, обозначаемой $B \cup C$.

Пусть B и C — два множества, в каждом из которых определена алгебраическая операция, причем эти множества изоморфны. Значение понятия изоморфизма при изучении алгебраической операции состоит в том, что мы можем отвлекаться от конкретных свойств множества, в котором определена алгебраическая операция, заменяя его любым другим изоморфным множеством.

В определении изоморфизма учитывается возможность выполнения любого конечного числа действий над элементами множества. Именно, если $b_i \in B$, $c_i \in C$, $b_i \leftrightarrow c_i$, $1 \leqslant i \leqslant n$, n — любое натуральное число, то $\sum_{i=1}^{n} b_i \leftrightarrow \sum_{i=1}^{n} c_i$. Если заданы соответствующие друг другу подмножества B' и C' множеств B и C, то последнее соотношение можно записать в виде

$$nB' \leftrightarrow nC', \quad n = 1, 2, \ldots . \tag{1.1.1}$$

Условие (1) оказывается, однако, слишком жестким в случаях сложения конечного числа одинаковых множеств. Именно такие случаи встречаются часто в аддитивной теории чисел. В настоящей книге мы ограничиваемся изложением вопросов, связанных с однократным сложением одинаковых множеств.

Если учесть вышесказанное, становится понятным, что для случая однократного сложения подмножества B' и C' следует считать изоморфными, если условие (1) выполняется не для всех значений n, а лишь для $n = 1$, 2. Строгое определение дается в следующем пункте.

1.2. Изоморфизм подмножеств.

Определение. *Подмножества* B' и C' множеств B и C с алгебраическими операциями, записываемыми аддитивно, называются *изоморфными*, если существует взаимно-однозначное отображение B' на C' $(B' \to C')$ такое, что естественным образом индуцируемое им отображение $2B' \to 2C'$ существует и является взаимно-однозначным. *Отображение* $B' \to C'$ называется тогда *изоморфным*.

Приведем примеры и пояснения к этому определению.

Каким образом определяется отображение $2B' \to 2C'$? Если $b_1, b_2 \in B'$, $c_1, c_2 \in C'$, $b_1 \to c_1$, $b_2 \to c_2$, то, говоря, что *отображение* $2B' \to 2C'$ *индуцируется* отображением $B' \to C'$ *естественным образом*, мы подразумеваем, что элемент $b_1 + b_2$ из $2B'$ отображается в элемент $c_1 + c_2$ из $2C'$.

Примеры изоморфных множеств.

1. Пусть B' и C' — подмножества множеств B и C с алгебраическими операциями. Если B' и C' содержат по два элемента, то они изоморфны.

2. Подмножества $\{0, 1, 3\}$ и $\{0, 1, 5\}$ аддитивной группы целых чисел изоморфны.

3. Подмножество $\{0, 1, 3\}$ аддитивной группы целых чисел и подмножество $\{(0, 0), (1, 0), (0, 1)\}$ аддитивной группы *целых векторов* плоскости изоморфны между собой.

4. Пусть S_p — аддитивная группа классов вычетов по модулю p. Множество целых чисел $\{0, 1, 2, 3\}$ изоморфно множеству $\{0, 1, 2, 3\}$ вычетов группы S_7, но не изоморфно множеству $\{0, 1, 2, 3\}$ вычетов S_5.

5. *Полугруппы* целых чисел по сложению $B' = \{0, 1, 2, \ldots\}$ и $C' = \{10, 11, 12, \ldots\}$ изоморфны.

Возможность осуществить взаимно-однозначное отображение $B' \to C'$ еще не означает изоморфизма B' и C', ибо отображение $2B' \to 2C'$ может не существовать.

Пример. Пусть $B' = \{b_1, b_2, b_3\}$, $C' = \{c_1, c_2, c_3\}$, где B', C' — множества целых чисел, расположенных в порядке возрастания. Пусть $b_1 + b_3 = 2b_2$, $c_1 + c_3 \neq 2c_2$. Пусть $B' \to C'$ — какое-то произвольное взаимно-однозначное отображение B' на C'. Пусть, например, $b_i \to c_i$, $1 \leqslant i \leqslant 3$, (остальные случаи рассматриваются аналогично). Тогда должно быть $2b_2 \to 2c_2$, $b_1 + b_3 \to c_1 + c_3$.

Таким образом, один и тот же элемент $b_1 + b_3 = 2b_2$ множества $2B'$ должен отобразиться одновременно на два различных элемента $c_1 + c_3$ и $2c_2$ множества $2C'$, что противоречит определению отображения.

Отображение $2B' \to 2C'$ может существовать, но не быть взаимно-однозначным.

Пример. Рассмотрим отображение $C' \to B'$ для множеств предыдущего примера. В этом случае отображение $2C' \to 2B'$ существует. Однако, например, для отображения $c_i \to b_i$ элементы $c_1 + c_3$ и $2c_2$ отображаются в один и тот же элемент, так что отображение $2C' \to 2B'$ не является взаимно-однозначным.

В последних двух примерах число элементов множества $2B'$ не равно числу элементов множества $2C'$ (см., однако, задачу 1).

Определение *изоморфизма подмножеств* можно сформулировать также следующим образом.

Пусть заданы подмножества B' и C' множеств B и C, причем в каждом из последних определена алгебраическая операция. B' и C' называются изоморфными, если может быть:

1) установлено взаимно-однозначное соответствие между B' и C', 2) установлено взаимно-однозначное соответствие между $2B'$ и $2C'$, причем 3) соответствуют суммы соответствующих элементов ($b_1, b_2 \in B'$; $c_1, c_2 \in C'$; $b_1 + b_2 \leftrightarrow c_1 + c_2$, если $b_1 \leftrightarrow c_1$ и $b_2 \leftrightarrow c_2$).

Пусть отображения $B' \to C'$, $2B' \to 2C'$ согласуются между собой, то есть любой общий элемент подмножеств B' и $2B'$ переходит при каждом из этих отображений в один и тот же элемент.

Если при этом $B' = B$ и $C' = C$, то приведенное определение превращается в обычное определение изоморфизма множеств с алгебраической операцией, так как в этом случае $2B' \subset B'$ и $2C' \subset C'$.

Задачи.

1. Указать неизоморфные множества B' и C', каждое из которых состоит из четырех целых чисел, причем множества $2B'$ и $2C'$ содержат одинаковое количество чисел.

2. Показать, что в группе S_5 любые два множества, состоящие из трех элементов, изоморфны.

3. Пусть A подмножество группы S_5, состоящее из k элементов.

При $k \leqslant 3$ существует изоморфное отображение множества A в аддитивную группу Z целых чисел. При $k > 3$ такое отображение невозможно.

4. Не существует автоморфизма группы Z, переводящего множества примера 2 друг в друга. При каком n нарушается соотношение (1.1)?

5. Проверить, что в примере 5 отображения $B' \to C'$ и $2B' \to 2C'$ не согласуются.

1.3. Изоморфизм подмножеств на s-ой ступени. Определение изоморфизма подмножеств, приведенное в 1.2, используется при изучении однократного сложения множеств. Оно является частным случаем (для $s = 2$) нижеследующего определения.

Определение. *Подмножества* B' и C' множеств B и C с алгебраической операцией называются *изоморфными на s-ой ступени*, если отображение $sB' \to sC'$, естественным образом индуцируемое взаимно-однозначным отображением $B' \to C'$, существует и является взаимно-однозначным. Отображение $B \to C'$ называется тогда изоморфным на s-ой ступени. Множества, изоморфные в смысле 1.2, следовало бы называть изоморфными на второй ступени. Мы не будем этого делать, так как в дальнейшем будет рассматриваться лишь случай однократного сложения множеств. Может иметь место изоморфизм на s-ой ступени при отсутствии изоморфизма на $s+1$-ой ступени (см. задачу 1).

При любом натуральном s изоморфное отображение множества B с алгебраической операцией на множество C индуцирует изоморфное отображение на s-ой ступени любого подмножества $B' \subset B$ на $C' \subset C$, как это видно из (1.1).

Задачи.

1. Показать, что множества целых чисел $K_1 = \{0, 1, s+1\}$ и $K_2 = \{0, 1, s+2\}$, $s \geqslant 1$, изоморфны на s-ой ступени, но не изоморфны на $s+1$-ой ступени.

2*. Пусть B' и C' подмножества множеств B и C, в каждом из которых определена алгебраическая операция. Следует ли из их изоморфизма на s-ой ступени изоморфизм на $(s-1)$-ой ступени?

1.4. Изоморфизм двух конечных совокупностей подмножеств. Дадим, наконец, определение изоморфизма, приспособленное к случаю сложения нескольких не обязательно одинаковых множеств.

Определение. Пусть заданы два множества B и C, в каждом из которых определена алгебраическая операция, и две конечные совокупности подмножеств $B_i \subset B$ и $C_i \subset C$, $1 \leqslant i \leqslant s$. Совокупность $\{B_i\}$ называется изоморфной совокупности $\{C_i\}$, если существуют взаимно-однозначные отображения $B_i \to C_i$,

$1 \leqslant i \leqslant s$, такие, что естественным образом индуцируемое ими отображение $B_1 + B_2 + \ldots + B_s \to C_1 + C_2 + \ldots + C_s$ существует и является взаимно-однозначным.

Определения п. п. 1.2, 1.3 являются частными случаями приведенного общего определения.

1.5. Критерий изоморфизма. Если множества B и C являются абелевыми группами, то имеет место следующий простой критерий изоморфизма подмножеств.

Теорема Пусть B' и C' являются подмножествами абелевых групп B и C. Пусть, далее, между B' и C' может быть установлено взаимно-однозначное соответствие такое, что из $b_1 - b_2 = b_3 - b_4$ следует $c_1 - c_2 = c_3 - c_4$, а из $b_1 - b_2 \neq b_3 - b_4$ следует $c_1 - c_2 \neq c_3 - c_4$, где $b_i \in B'$, $c_i \in C'$, $b_i \leftrightarrow c_i$, $1 \leqslant i \leqslant 4$. Это является необходимым и достаточным условием изоморфизма подмножеств B' и C'.

Покажем, что из условий теоремы следует изоморфизм B' и C'. Для этого нужно показать, что отображение $2B' \to 2C'$, естественным образом индуцируемое отображением $B' \to C'$, является взаимно-однозначным. Это следует из того, что если $b_1 + b_4 \overset{(\neq)}{=} b_2 + b_3$, то $b_1 - b_2 \overset{(\neq)}{=} b_3 - b_4$, откуда следует $c_1 - c_2 = c_3 - c_4$, и $c_1 + c_4 = c_2 + c_3$.

Пусть теперь B' изоморфно C'. Если $b_1 + b_4 = b_2 + b_3$, то есть какой-то элемент из $2B'$ имеет два представления $b_1 + b_4$ и $b_2 + b_3$, то и соответствующий элемент из $2C'$ имеет два представления $c_1 + c_4$ и $c_2 + c_3$, то есть $c_1 + c_4 = c_2 + c_3$. Если же $b_1 + b_4 \neq b_2 + b_3$, то и $c_1 + c_4 \neq c_2 + c_3$, так как из $c_1 + c_4 = c_2 + c_3$ следовало бы $b_1 + b_4 = b_2 + b_3$.

Задачи.

1. Установить изоморфизм множеств примеров 2, 3, 4 п. 1.2, используя критерий изоморфизма.

2. Любая арифметическая прогрессия, состоящая из m действительных чисел, если ее рассматривать, как подмножество аддитивной группы действительных чисел, изоморфна множеству $\{0, 1, 2, \ldots, m-1\}$.

3. Доказать теорему 1.6 для случая $k = 3$.

4. Линейное преобразование аддитивной группы D действительных чисел индуцирует изоморфное преобразование любого конечного подмножества группы D.

1.6. Число классов изоморфных множеств. Через K мы будем обозначать конечное подмножество абелевой группы, состоящее из k элементов. В этом пункте $K \subset D$, в п. п. 2.1, 2.3, 3.12 и 3.13 $K \subset S_p$, в остальных случаях $K \subset Z_n$, где Z_n — аддитивная группа целых векторов евклидова пространства E_n.

Таким образом, $K = \{\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{k-1}\}$, где $\bar{a}_i$ — целые векторы, если $K \subset Z_n$. При $K \subset D$ имеем $K = \{a_0, a_1, \ldots, a_{k-1}\}$, a_i — действительные числа, причем всегда можно предположить, что $a_i < a_{i+1}$, $i = 0, 1, \ldots, k-2$.

Рассмотрим аддитивную группу D действительных чисел, и конечные ее подмножества K, состоящие из k чисел. Отношение изоморфизма для двух таких подмножеств является *отношением эквивалентности* (оно рефлексивно, симметрично и транзитивно). Таким образом, множества, состоящие из действительных чисел, разбиваются на *классы изоморфных множеств*. Нижеследующая теорема описывает эти классы для $k = 3$, 4 и 5.

Теорема. Рассмотрим конечные, состоящие из k элементов, подмножества K аддитивной группы действительных чисел. Любое множество, состоящее из трех действительных чисел, изоморфно одному из двух множеств $K_{1,3} = \{0, 1, 2\}$ или $K_{2,3} = \{0, 1, 3\}$.

Любое множество, состоящее из четырех чисел, изоморфно одному из пяти множеств $K_{1,4} = \{0, 1, 2, 3\}$, $K_{2,4} = \{0, 1, 2, 4\}$, $K_{3,4} = \{0, 1, 2, 5\}$, $K_{4,4} = \{0, 1, 3, 4\}$, $K_{5,4} = \{0, 1, 3, 7\}$.

Любое множество, состоящее из пяти чисел, изоморфно одному из двадцати двух множеств $K_{1,5} = \{0, 1, 2, 3, 4\}$, $K_{2,5} = \{0, 1, 2, 4, 6\}$, $K_{3,5} = \{0, 2, 3, 4, 6\}$, $K_{4,5} = \{0, 1, 2, 3, 5\}$, $K_{5,5} = \{0, 1, 2, 3, 6\}$, $K_{6,5} = \{0, 1, 2, 3, 7\}$, $K_{7,5} = \{0, 1, 2, 4, 5\}$, $K_{8,5} = \{0, 1, 2, 4, 7\}$, $K_{9,5} = \{0, 1, 2, 4, 8\}$, $K_{10,5} = \{0, 3, 4, 5, 7\}$, $K_{11,5} = \{0, 4, 5, 6, 8\}$, $K_{12,5} = \{0, 2, 4, 5, 8\}$, $K_{13,5} = \{0, 1, 2, 4, 9\}$, $K_{14,5} = \{0, 3, 4, 5, 10\}$, $K_{15,5} = \{0, 3, 4, 5, 8\}$, $K_{16,5} = \{0, 1, 2, 5, 6\}$, $K_{17,5} = \{0, 1, 2, 5, 7\}$, $K_{18,5} = \{0, 4, 5, 6, 9\}$, $K_{19,5} = \{0, 1, 2, 5, 8\}$, $K_{20,5} = \{0, 1, 2, 5, 11\}$, $K_{21,5} = \{0, 1, 3, 4, 9\}$, $K_{22,5} = \{0, 1, 3, 7, 15\}$.

Доказательство. Если $k=3$, то K либо является арифметической прогрессией и изоморфно $K_{1,3}$, либо не является таковой и изоморфно $K_{2,3}$.

Если $k=4$ и K — арифметическая прогрессия, то $K\sim K_{1,4}$ (K изоморфно $K_{1,4}$). Пусть теперь в K содержится арифметическая прогрессия из трех чисел: $\{a, a+q, a+2q\}\subset K$. Если одно из чисел $a+4q$, $a-2q$, $a+\frac{q}{2}$, $a+\frac{3q}{2}\in K$, то $K\sim K_{2,4}$, в противном случае $K\sim K_{3,4}$. Если в K не содержится арифметическая прогрессия из трех чисел, но есть одинаковые разности, то $K\sim K_{4,4}$, если нет одинаковых разностей, то $K\sim K_{5,4}$.

Пусть теперь $k=5$. Если K — арифметическая прогрессия, то $K\sim K_{1,5}$. Пусть теперь в K содержится арифметическая прогрессия из четырех чисел, $\{a, a+q, a+2q, a+3q\}\subset K$. Если $a+\frac{q}{2}$ или $a+\frac{5q}{2}$ входит в K, то $K\sim K_{2,5}$, если $a+\frac{3q}{2}\in K$, то $K\sim K_{3,5}$, если $a+5q$ или $a-2q$ входит в K, то $K\sim K_{4,5}$, если $a+6q$ или $a-3q$ входит в K, то $K\sim K_{5,5}$, в остальных случаях $K\sim K_{6,5}$.

Рассмотрим случай, когда в K содержится подмножество, изоморфное $K_{2,4}$, но нет арифметической прогрессии из четырех чисел. Пусть $\{a, a+q, a+2q, a+4q\}\subset K$. Если $a+5q\in K$, то $K\sim K_{7,5}$, если $a+7q\in K$, то $K\sim K_{8,5}$, если $a+8q\in K$, то $K\sim K_{9,5}$, если $a-3q\in K$, то $K\sim K_{10,5}$, если $a-4q\in K$, то $K\sim K_{11,5}$, если $a+\frac{q}{2}\in K$, то $K\sim K_{9,5}$, если $a+\frac{3q}{2}\in K$, то $K\sim K_{11,5}$, если $a+\frac{5q}{2}\in K$, то $K\sim K_{12,5}$, во всех прочих случаях $K\sim K_{13,5}$.

Пусть теперь в K содержится подмножество $K_3=\{a, a+q, a+2q\}$, но нет подмножества, изоморфного $K_{1,4}$ или $K_{2,4}$. Пусть в K входят еще числа b и c. Предположим, что среди чисел множеств

$$K_3+\{-b\},\ K_3+\{-c\} \tag{1.6.1}$$

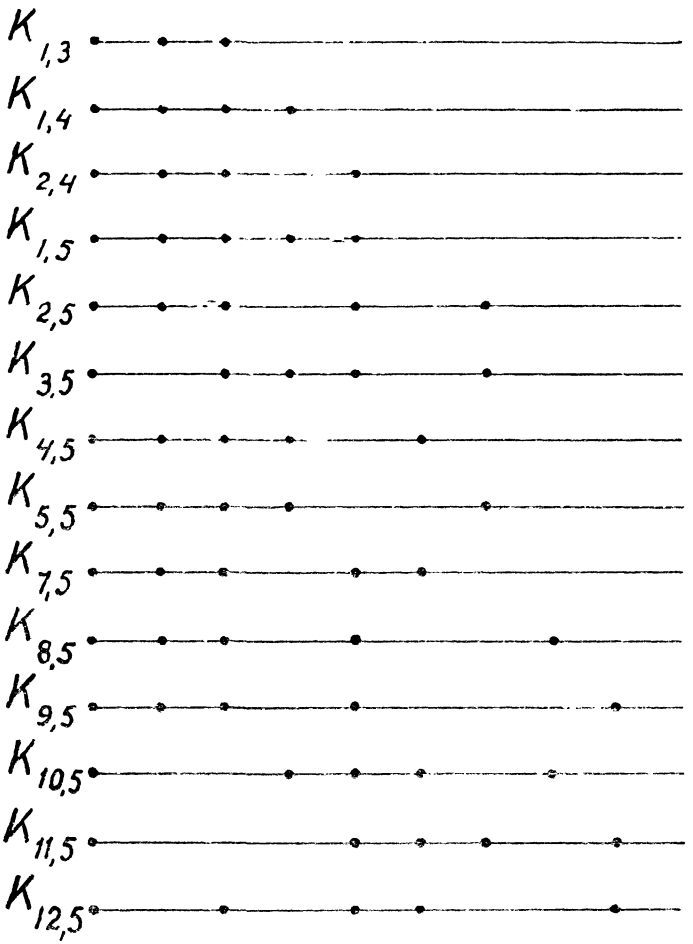


Рис. 1а.

есть совпадающие по абсолютной величине. Если $a-b=c-a$, то $K\sim K_{14,5}$, если $a+q-b=c-a-q$, то $K\sim K_{15,5}$, если $a-b=a+q-c$, то $K\sim K_{16,5}$, если $a-b=a+2q-c$, то $K\sim K_{17,5}$, если $a-b=c-a-q$, то $K\sim K_{18,5}$, остальные случаи совпадения по абсолютной величине к новым множествам не приводят. Пусть теперь среди чисел множеств (1) нет совпадающих по абсолютной величине, но число $b-c$ сов-

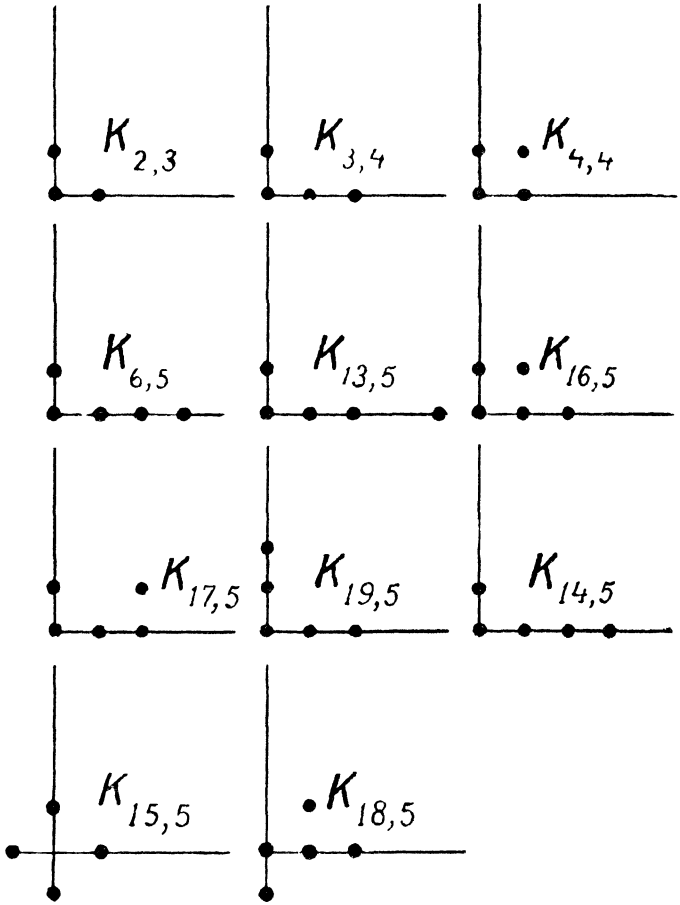


Рис. 16.

падает по абсолютной величине с одним из чисел множеств (1). Если $a - b = b - c$, то $K \sim K_{19,5}$, остальные случаи к новым множествам не приводят. Наконец, если $b - c$ не совпадает по абсолютной величине ни с одним из чисел (1), то $K \sim K_{20,5}$.

Пусть теперь в K не содержится множество, изоморфное $K_{1,3}$. Если в K есть равные разности, то $K \sim K_{21,5}$. Если же в K нет равных разностей, то $K \sim K_{22,5}$.

Таблица 1

K	k	T	r	M'	R
$K_{1,3}$	3	5	1	5	2
$K_{2,3}$	»	6	2	3	3
$K_{1,4}$	4	7	1	14	3
$K_{2,4}$	»	8	1	10	4
$K_{3,4}$	»	9	2	8	5
$K_{4,4}$	»	9	2	10	4
$K_{5,4}$	»	10	3	6	6
$K_{1,5}$	5	9	1	30	4
$K_{2,5}$	»	11	1	20	6
$K_{3,5}$	»	11	1	22	5
$K_{4,5}$	»	10	1	24	5
$K_{5,5}$	»	11	1	20	6
$K_{6,5}$	»	12	2	18	7
$K_{7,5}$	»	11	1	22	5
$K_{8,5}$	»	12	1	16	7
$K_{9,5}$	»	12	1	16	7
$K_{10,5}$	»	12	1	18	6
$K_{11,5}$	»	12	1	16	7
$K_{12,5}$	»	12	1	16	7
$K_{13,5}$	»	13	2	14	8
$K_{14,5}$	»	13	2	14	8
$K_{15,5}$	»	13	2	18	6
$K_{16,5}$	»	12	2	20	6
$K_{17,5}$	»	13	2	16	7
$K_{18,5}$	»	13	2	14	7
$K_{19,5}$	»	13	2	14	8
$K_{20,5}$	»	14	3	12	9
$K_{21,5}$	»	14	3	14	8
$K_{22,5}$	»	15	4	10	10

На рисунках 1а и 1б приведены изоморфные образы множеств теоремы 1.6. Обозначим $t(k)$ число классов изоморфных множеств, состоящих из k действительных чисел. Из теоремы 1.6 следует, что $t(1)=1$, $t(2)=1$, $t(3)=2$, $t(4)=5$, $t(5)=22$.

В таблице 1 приведены значения T для множеств теоремы 1.6, а также некоторые другие числовые характеристики (пп. 1.18 и 1.28).

Задачи.

1*. Описать все классы изоморфных множеств действительных чисел и найти $t(k)$ для $k=7$.

2*. Получить конкретные числовые оценки для $t(k)$ для малых значений κ $(7 \leqslant k \leqslant 10)$.

3. Доказать конечность функции $t(k)$.

4**. Выяснить порядок роста функции $t(k)$.

5*. Рассмотрим конечные подмножества, состоящие из k элементов, входящие в произвольные абелевы группы. Обобщить на этот случай результаты и постановки задач п. 1.6 и задач 1—4.

6*. То же для некоммутативных групп.

§ 2. СЛОЖЕНИЕ КОНЕЧНЫХ МНОЖЕСТВ. ЭЛЕМЕНТАРНЫЕ РЕЗУЛЬТАТЫ.

1.7. Прямые и обратные задачи аддитивной теории чисел. Классическая аддитивная теория чисел имеет дело с представлениями натуральных чисел в виде сумм слагаемых определенного вида. Обычно оговариваются условия, накладываемые на число слагаемых. Основные проблемы — возможность представления и оценка числа представлений.

Типичным примером таких задач является проблема Варинга, в которой слагаемыми являются степени натуральных чисел.

Задачи, в которых заданы множества слагаемых и исследуются свойства множества, являющегося их суммой, мы будем называть прямыми аддитивными задачами.

Обратная задача аддитивной теории чисел — это такая задача, при решении которой мы узнаем что-либо о заданных множествах чисел, располагая какими-то сведениями об их сумме.

Можно провести аналогию между прямой задачей и нахождением суммы двух чисел по заданным слагаемым, а также между обратной задачей и нахождением слагаемых по заданной сумме двух чисел и некоторым дополнительным условиям.

Не настаивая на арифметической природе множеств, являющихся слагаемыми, можно изучать структурную теорию сложения множеств, часть которой составляют обратные задачи.

Термин „обратная задача аддитивной теории чисел" появился в 1955 году в работах [10] и [11].

Сформулируем обратную задачу, решению которой посвящены, в основном, главы 1 и 2 настоящей книги.

1.8. Постановка обратной задачи. Число элементов конечного множества M мы будем обозначать $T(M)$.

Пусть $K = \{a_i\}$, $0 \leqslant i \leqslant k-1$, a_i — целые числа, $a_i < a_{i+1}$, $i = 0, 1, \ldots, k-2$, $T = T(2K)$.

Что можно сказать о величине T? Имеют место неравенства

$$2k - 1 \leqslant T \leqslant \frac{k(k+1)}{2}. \tag{1.8.1}$$

Справедливость оценки снизу для T видна из того, что во всяком множестве $2K$ имеется $2k-1$ различных чисел $2a_0$, $a_0 + a_1$, $a_0 + a_2, \ldots, a_0 + a_{k-1}$, $a_1 + a_{k-1}$, $a_2 + a_{k-1}, \ldots, 2a_{k-1}$.

Справедливость оценки сверху для T следует из того, что имеется не более $\frac{(k-1)k}{2}$ сумм попарно различных чисел из K, к которым следует прибавить не более k сумм одинаковых чисел.

Обратная задача: определить структуру множества K при заданном T.

Мы увидим, что при малых значениях T структура K является весьма жесткой и может быть хорошо описана.

При решении прямых задач мы заинтересованы обычно в получении возможно более сильных оценок для T снизу.

Если для некоторого множества K мы сможем убедиться, что его структура отличается от той, которую имеют множества с малым T, то тем самым мы для изучаемого нами множества K оценим величину T снизу.

Таким образом, решение обратных задач сформулированного здесь типа дает естественный подход к решению прямых задач.

Задачи.

1. Показать, что оценки (1) достижимы.

2. Множество целых чисел K при $T=\frac{k(k+1)}{2}$ изоморфно множеству вершин тетраэдра в E_{k-1}.

1.9. Структура K при $T<3k-3$. Оказывается, что при очень малых ($T<3k-3$) значениях T множество K содержится в короткой арифметической прогрессии. Так, $T=2k-1$ тогда и только тогда, когда K является арифметической прогрессией из k членов. В самом деле, если для какого-то $0\leqslant j\leqslant k-3$

$$a_{j+1}-a_j\neq a_{j+2}-a_{j+1}$$

то к различным числам $2a_0$, a_0+a_1, $2a_1$, a_1+a_2, $2a_2,\ldots,$ $2a_{k-1}$ можно добавить еще отличное от них число a_j+a_{j+2}.

Индукцией по k можно доказать, что справедлива следующая

Теорема. При $0\leqslant b<k-2$ и $T=2k-1+b$ множество K является подмножеством множества K_a вида

$$K_a=\{a,\ a+q,\ a+2q,\ldots,\ a+(k+b-1)q\},$$

где a — целое число, q — натуральное число.

Таким образом, при $T<3k-3$ множество K содержится в арифметической прогрессии, число членов которой не превышает $T-k+1$.

Прежде чем перейти к доказательству этой теоремы (п. 1.10), сделаем некоторые замечания.

Так как две арифметические прогрессии с одинаковым числом членов изоморфны (задача 2 п. 1.5), теорема 1.9 описывает структуру множества K с точ-

ностью до изоморфизма*). Это обстоятельство вообще характерно для нашей обратной задачи, так как изоморфные множества K имеют равные значения T. Поэтому, не ограничивая общности, вместо каждого класса изоморфных множеств, удовлетворяющего условиям обратной задачи, можно отыскивать некоторое подмножество этого класса, определяемое заранее заданными условиями.

Прибавление ко всем числам данного множества одного и того же числа, а также умножение всех чисел данного множества на одно и то же число приводит к множеству, изоморфному данному (см. задачу 4 п. 1.5). Поэтому, не ограничивая общности, можно считать, что $a_0 = 0$, $d(K) = 1$, где $d(K) = (a_1 - a_0,\ a_2 - a_0, \ldots,\ a_{k-1} - a_0)$ — общий наибольший делитель чисел $a_1 - a_0,\ a_2 - a_0, \ldots,\ a_{k-1} - a_0$. При этих условиях в теореме 1.9 мы получим $a_0 = 0$, $q = 1$, $a_{k-1} \leqslant k + b - 1$ и ее можно переформулировать следующим образом.

Если во множестве K $a_0 = 0$ и $d(K) = 1$, то при $0 \leqslant b < k - 2$ и $T = 2k - 1 + b$ выполняется условие $a_{k-1} \leqslant k + b - 1$.

1.10. Доказательство теоремы 1.9. Приведем еще одну эквивалентную формулировку теоремы 1.9.

Теорема. Пусть $K = \{a_0, a_1, \ldots, a_{k-1}\}$, a_i — целые числа, $a_0 = 0$, $d(K) = 1$, $a_i < a_{i+1}$, $i = 0, 1, 2, \ldots, k-2$. Если $a_{k-1} \geqslant k + b$, где $0 \leqslant b < k - 2$, b — целое число, то $T \geqslant 2k + b$.

Доказательство. Покажем вначале, что при $a_{k-1} = k + b$, где $0 \leqslant b < k - 2$, будет выполняться неравенство $T \geqslant 2k + b$.

Пусть s — любое целое число, $s \overline{\in} K$, $1 \leqslant s \leqslant k + b$. Число таких s равно $b + 1$. Пусть a_j — максимальное из чисел a_i, меньших s. Числа

$$a_{k-1} + s - a_i, \quad 1 \leqslant i \leqslant k - 2 \tag{1.10.1}$$

*) Это означает, что если некоторое множество K удовлетворяет условиям теоремы, то и любое множество, изоморфное множеству K, также удовлетворяет условию теоремы. Отметим, что существуют, вообще говоря, неизоморфные множества с равными T (см. задачу 1 п. 1.2).

так же, как и числа

$$a_{j+1},\ a_{j+2},\ \dots,\ a_{k-1},\quad a_{k-1}+a_1,$$
$$a_{k-1}+a_2,\ \dots,\ a_{k-1}+a_j \qquad (1.10.2)$$

находятся среди $a_{k-1}-1$ последовательных чисел $s+1,\ s+2,\dots,\ s+a_{k-1}-1$. Общее число чисел (1) и (2) равно $2k-3$. Так как $a_{k-1}-1\leqslant 2k-4$, то одно из чисел (1) совпадает с одним из чисел (2). Это означает, что или $s\in 2K$, или $s+a_{k-1}\in 2K$. Учитывая еще числа множеств K и $a_{k-1}+K$, мы получим

$$T\geqslant 2k-1+b+1=2k+b. \qquad (1.10.3)$$

Для завершения доказательства нам осталось доказать теперь, что при $a_{k-1}\geqslant 2k-2$ имеет место неравенство $T\geqslant 3k-3$.

Это верно при $k=3$ ($T=6$). Предположим, что это верно для всех чисел, не меньших трех и не превышающих $k-1$, где $k\geqslant 4$.

Рассмотрим вначале тот случай, когда $d(K')>1$, где $K'=K\setminus a_{k-1}$. В этом случае числа $a_{k-1}+a_s$, $s=0,\ 1,\dots,\ k-1$ не входят в $2K'$. Поэтому, полагая $T'=T(2K')$, получим $T\geqslant T'+k\geqslant 2(k-1)-1+k=3k-3$.

Таким образом, впредь мы можем предполагать, что $d(K')=1$.

1) $a_{k-1}-a_{k-2}=1$, $a_{k-1}-a_{k-3}>2$. В этом случае числа $a_{k-1}+a_s$, $s=k-3,\ k-2,\ k-1$ не входят в $2K'$. Так как по предположению индукции $T'\geqslant 3k-6$, то $T\geqslant T'+3\geqslant 3k-3$.

2) $a_{k-1}-a_{k-2}\geqslant 2$, $a_{k-2}\geqslant 2k-4$. Пусть j таково, что $a_{k-1}\equiv a_s \pmod{a_{k-1}-a_{k-2}}$ при $s=j+1,\ j+2,\dots,\ k-2$ и $a_{k-1}\not\equiv a_j \pmod{a_{k-1}-a_{k-2}}$. В этом случае числа $a_{k-1}+a_j$, $a_{k-1}+a_{k-2}$ и $2a_{k-1}$ не входят в $2K'$.

Проверим, что это так для числа $a_{k-1}+a_j$. В противном случае имело бы место равенство $a_{k-1}+a_j=a_s+a_t$, $j<s$, $t<k-1$, откуда мы получили бы $a_{k-1}-a_j=a_{k-1}-a_s+a_{k-1}-a_t$, что невозможно, ибо левая часть равенства не делится на $a_{k-1}-a_{k-2}$, а правая — делится.

3) $a_{k-2}<2k-4$.

3а) $a_i<2i$, $i=1,\ 2,\dots,\ k-2$.

Пусть $s\notin K$, $1\leqslant s\leqslant 2k-4$, a_j — максимальное из чисел a_i, меньшее s. Рассматривая числа a_i и $s-a_i$,

$1 \leqslant i \leqslant j$, покажем, как при доказательстве (3), что $s \in 2K$. Если учесть нуль и k чисел $a_{k-1} + a_s$, $s = 0, 1, \ldots, k-1$, то получим $T \geqslant 2k - 4 + 1 + k = 3k - 3$.

3б) Существует такое j, что

$$a_{j-1} \geqslant 2j - 2, \; a_s < 2s, \; s = j, \; j+1, \ldots, \; k-2.$$

Так как $a_{j-1} \geqslant 2j - 2$ и $a_j \leqslant 2j - 1$, то

$$a_{j-1} = 2j - 2, \; a_j = 2j - 1.$$

Рассмотрим два множества

$$\overline{K} = \{0, \; a_1, \ldots, \; a_{j-1}, \; a_j\} \tag{1.10.4}$$

и

$$\overline{\overline{K}} = \{a_{j-1}, \; a_j, \ldots, \; a_{k-1}\}. \tag{1.10.5}$$

Применяя к множеству $\overline{K}$ неравенство (3) для $k = j + 1$ и $b = j - 2$, получим $T(2\overline{K}) \geqslant 3j$. Из предположения индукции следует, что $T(2\overline{\overline{K}}) \geqslant 3(k - j)$.

Учитывая, что суммы $2a_{j-1}$, $a_{j-1} + a_j$ и $2a_j$ считались дважды, мы получим

$$T \geqslant T(2\overline{K}) + T(2\overline{\overline{K}}) - 3 \geqslant 3k - 3.$$

Заметим, что вместо множества K можно рассматривать изоморфное ему множество

$$K^* = \{0, \; a_{k-1} - a_{k-2}, \; a_{k-1} - a_{k-3}, \ldots, \; a_{k-1} - a_1, \; a_{k-1}\}.$$

Применяя это замечание к рассмотрению оставшегося случая $a_{k-1} - a_{k-2} = 1$, $a_{k-1} - a_{k-3} = 2$, мы получим множество, для которого $a_1 = 1$, $a_2 = 2$. Если исключить для множеств K с таким свойством уже рассмотренные случаи 1) — 3), то останется лишь рассмотреть случай

4) $a_2 = 2$, $a_{k-1} - a_{k-3} = 2$.

Здесь найдется j такое, что $a_{j-1} < 2j - 2$, $a_j \geqslant 2j$. Доказательство заканчивается, как в случае 3б).

Рассмотрение примера

$$K = \{0, \; 1, \ldots, \; k-2, \; k - 1 + b\}, \; 0 \leqslant b < k - 2, \tag{1.10.6}$$

для которого $T = 2k - 1 + b$, показывает, что теорему усилить нельзя.

Задачи.

1. Определить все классы изоморфных множеств целых чисел при $T = 2k$, $k \geqslant 4$.

2. Определить все классы изоморфных множеств целых чисел при $T = 2k + 1$, $k \geqslant 5$.

3*. Обобщить на плоскость (более общим образом, n — мерное евклидово пространство) результаты теоремы 1.9.

4*. Определить классы множеств целых чисел, изоморфных на s—ой ступени при $T(sK) = sk - s + 1 + b$, где b — малые неотрицательные целые числа, k—достаточно велико.

5*. Сформулировать и доказать обобщение теоремы 1.9 на случай сложения s одинаковых множеств целых чисел.

1.11. О дальнейшем изучении структуры K. Сохраняются ли существенные черты структуры K, найденные в теореме 1.9 для $T < 3k - 3$ и в том случае, когда $T \geqslant 3k - 3$?

Точнее. Если рассмотреть все арифметические прогрессии, содержащие множество K, и выбрать из их числа арифметическую прогрессию с минимальным числом членов, то это последнее число можно назвать *„длиной" множества* K. Можно ли, рассматривая совокупность множеств K с заданными k и T, оценить их длину в зависимости от k и T (независимо от вида K)? Что это не так уже при $T = 3k - 3$, показывает пример

$$K = \{0, 1, 2, \ldots, k_1 - 1, b, b + 1, \ldots, b + k_2 - 1\}, \quad k_1 + k_2 = k, \quad k_1, k_2 \geqslant 1, \quad b + k_2 \geqslant 2k, \tag{1.11.1}$$

так как b может быть выбрано неограниченно большим.

Таким образом, как кажется, структуры множеств K при $T < 3k - 3$ и $T \geqslant 3k - 3$ коренным образом отличаются. И все-таки, как мы увидим в дальнейшем, их можно описать в общих терминах, что можно проиллюстрировать, рассматривая случай $T = 3k - 3$.

Множество K примера (1) изоморфно следующему множеству $K_0 \subset Z_2$:

$$K_0 = \{(0, 0), (0, 1), (0, 2), \ldots, (0, k_1 - 1), (1, 0), (1, 1), \ldots, (1, k_2 - 1)\}, \quad k_1 + k_2 = k, \quad k_1, k_2 \geqslant 1,$$

и имеет длину, большую $2k-1$. Оказывается, множество K примера (1), состоящее из двух арифметических прогрессий с одинаковой разностью, достаточно полно характеризует общее положение для случая $T=3k-3$.

Именно, справедлива следующая

Теорема. Пусть $T=3k-3$. Тогда возможны следующие случаи:

1. Длина множества K не превышает $2k-1$,
2. K изоморфно K_0,
3. K для $k=6$ изоморфно

$$K_6=\{(0,\ 0),\ (0,\ 1),\ (0,\ 2),\ (1,\ 0),\ (1,\ 1),\ (2,\ 0)\}.$$

Таким образом, множество K содержится во множестве целых чисел, изоморфном множеству внутренних целых точек некоторой выпуклой замкнутой области D ограниченного объема евклидова пространства E_n, одномерной в случае 1, двумерной в случаях 2 и 3. Теперь видно, что теорема 1.11 описывает структуру K в тех же терминах, что и теорема 1.9, с той лишь разницей, что в теореме 1.9 область D — одномерная.

В рассмотренном примере подмечены все существенные черты структуры K и при бо́льших T*).

1.12. Доказательство теоремы 1.11 о структуре множества K при $T=3k-3$. Теорему будем доказывать по индукции. Правильность ее при $2\leqslant k\leqslant 5$ следует из теоремы 1.6. Предположим, что теорема верна для всех чисел, меньших некоторого k, причем $k\geqslant 6$.

Пусть

$$K=\{a_0,\ a_1,\ a_2,\ \dots,\ a_{k-1}\},\ a_i<a_{i+1},\ i=0,\ 1,\ 2,\ \dots,\ k-2.$$

Можно считать, что $a_0=0$, $d(K)=1$. Тогда $a_{k-1}\geqslant 2k-1$.

Обозначим $K'=K\setminus a_{k-1}$, $K''=K\setminus a_0$.

Предположим вначале, что $d(K')=d_1>1$.

Тогда числа $a_{k-1}+a_s$, $s=0,\ 1,\ 2,\dots,\ k-1$ не входят в $2K'$ и поэтому $T'=2k-3$, $K'=\{0,\ a,$

*) Читатель может сейчас просмотреть содержание основной теоремы, приведенной в п. 2.10 стр. 74.

$2a, \ldots, (k-2)a\}$, $a > 1$, K изоморфно K_0 с $k_1 = k-1$. В дальнейшем мы будем считать, что $d_1 = 1$.

Доказательство мы подразделим на рассмотрение таких двух случаев:

А) $a_{k-2} \geqslant 2k-3$ или $a_{k-1} - a_1 \geqslant 2k-3$

В) $a_{k-2} \leqslant 2k-4$ и $a_{k-1} - a_1 \leqslant 2k-4$.

В случае А) мы можем ограничиться рассмотрением случая

A_1) $a_{k-2} \geqslant 2k-3$, так как при выполнении неравенства $a_{k-1} - a_1 \geqslant 2k-3$ можно перейти к рассмотрению множества K^* (п. 1.10). И, наконец, мы можем в этом случае ограничиться рассмотрением множества K со свойством

A_2) $a_{k-2} \geqslant 2k-3$ и среди чисел $a_{k-1} + a_s$, $s = 0, 1, \ldots, k-1$ найдется не менее трех, не входящих в $2K'$.

Покажем, что это так.

1) $a_{k-1} - a_{k-2} = 1$, $a_{k-1} - a_{k-3} > 2$,

2) $a_{k-1} - a_{k-2} \geqslant 2$.

Эти два случая рассмотрены при доказательстве теоремы 1.10.

3) $a_{k-1} - a_{k-2} = 1$, $a_{k-1} - a_{k-3} = 2$. Перейдем к рассмотрению множества K^*. Мы получим $a_1 = 1$, $a_2 = 2$.

3а) $a_i < 2i$, $i = 1, 2, \ldots, k-2$. Если бы одно из чисел $2k-3$, $2k-2$ входило в $2K'$, то воспользовавшись рассмотрением случая 3а) в теореме 1.10, мы получили бы $T \geqslant 3k-2$, что невозможно. Итак, числа $2k-3$, $2k-2$ не входят в $2K'$. Тогда числа

$$2k-3-a_1,\ 2k-3-a_2, \ldots,\ 2k-3-a_{k-2} \qquad (1.12.1)$$

и

$$2k-2-a_1,\ 2k-2-a_2, \ldots,\ 2k-2-a_{k-2} \qquad (1.12.2)$$

не входят в K'. Число положительных чисел, не превышающих $2k-3$ и не входящих в K', равно $k-1$. Но в множестве (1) число чисел равно $k-2$, поэтому в множестве (2) имеется не более одного числа, отличного от чисел (1). Но множество (2) получается путем прибавления единицы к числам множества (1). Поэтому множество (1) состоит из $k-2$ последовательных целых чисел и $K' = \{0, 1, 2, \ldots, k-2\}$.

Отсюда видно, что 0, 1 и a_{k-1} не входят в $2K''$. Заметим еще, что в рассматриваемом случае мы показали, что K изоморфно K_0.

3б) $a_i<2i$, $i=1, 2, \ldots, k-3$, $a_{k-2}=2k-4$. В этом случае все числа от 0 до $2k-6$ входят в $2K'$, $a_{k-2}=2k-4$, $a_{k-2}+a_1=2k-3$, $a_{k-2}+a_2=2k-2$, т. е. $T\geqslant 2k-5+3+k=3k-2$, что противоречит условию теоремы. Это означает, что такой случай невозможен.

3в) Существует j, $3\leqslant j\leqslant k-2$, такое, что

$$a_i<2i,\ i=1, 2, \ldots, j-1,\ a_j>2j.$$

Рассмотрим множества $\overline{K}$ и $\overline{\overline{K}}$, определенные в (1.10.4) и (1.10.5). Из теоремы 1.10 следует, что $\overline{T}\geqslant 3j$. К множеству $\overline{K}$ можно также применить теорему 1.10, так как можно считать, что в $\overline{K}$ всегда найдутся два числа, отличающиеся на единицу. Это так, если $a_{k-1}-a_{k-2}=1$ или $a_{k-2}\leqslant 2k-4$. Если же $a_{k-1}-a_{k-2}>1$ и $a_{k-2}\geqslant 2k-3$, то мы получаем случай 2). Для $\overline{\overline{T}}$ получится неравенство $\overline{\overline{T}}\geqslant 3(k-j)$. Поэтому

$$T\geqslant \overline{T}+\overline{\overline{T}}-3\geqslant 3k-3.$$

Так как $T=3k-3$, то $\overline{T}=3j$. Как показано в 3а) отсюда следует, что

$$\overline{K}=\{0, 1, 2, \ldots, j-1, a_j\}.$$

Поэтому числа 0, 1 и a_j не входят в $2K''$.

3г) Существует j, $4\leqslant j\leqslant k-2$, такое, что

$$a_i<2i,\ i=1, 2, \ldots, j-2,\ a_{j-1}=2j-2,\ a_j>2j.$$

Доказательство проводится как в случае 3в), причем неравенство $\overline{T}\geqslant 3j+1$ получается на основании 3б), откуда следует невозможность этого случая.

3д) $a_i<2i$, $i=1, 2, \ldots, j-2$, $a_{j-1}=2j-3$, $a_j=2j$, $4\leqslant j\leqslant k-2$.

Доказательство проводится как в 3в), причем неравенство $\overline{T}\geqslant 3j+1$ получается ввиду того, что в $2K$ входят все числа от 0 до $2j-1$ ($2j-2=a_{j-1}+a_1$, $2j-1=a_{j-1}+a_2$) и $j+1$ число вида

$$a_j+a_s,\quad s=0, 1, \ldots, j.$$

3е) $a_i<2i$, $i=1, 2, \ldots, j-3$, $a_{j-2}=2j-4$, $a_{j-1}\leqslant 2j-2$, $a_j>2j$, $5\leqslant j\leqslant k-1$.

Заметим, что если $a_1 = 1$ и $a_2 = 2$, то или 0, 1, a_3 не входят в $2K''$, или же a_3 принимает одно из двух значений 3 или 4. Поэтому числа от $2j-4$ до $2j$ включительно входят в $2K$ и, как и раньше, мы получим $\overline{T} \geqslant 3j+1$.

3ж) $a_i < 2i$, $i = 1, 2, \ldots, j-2$, $a_{j-1} = 2j-2$, $a_{j+1} = 2j$, $4 \leqslant j \leqslant k-3$.

Рассмотрим те же, что и в случае 3в), множества $\overline{K}$ и $\overline{\overline{K}}$. Число $a_{j-2} + a_{j+1}$ не входит ни в $2\overline{K}$, на в $2\overline{\overline{K}}$. Поэтому $T > \overline{T} + \overline{\overline{T}} - 3 + 1 \geqslant 3k-2$.

3з) $a_i < 2i$, $i = 1, 2, \ldots, j-2$, $a_{j-2} \leqslant 2j-6$, $a_{j-1} = 2j-2$, $2j+1 \leqslant a_{j+1} \leqslant 2j+2$, $4 \leqslant j \leqslant k-3$.

Рассмотрим множества

$$\overline{K}_1 = \{0, a_1, \ldots, a_{j-1}, a_{j+1}\}$$

и $\overline{\overline{K}}$. Общими членами множеств $2\overline{K}_1$ и $2\overline{\overline{K}}$ являются $2a_{j-1}$, $a_{j-1} + a_{j+1}$, $2a_{j+1}$ ($a_{j-1} + a_j$ не может входить в $2\overline{K}_1$, так как $a_{j-1} + a_j > a_{j-2} + a_{j+1}$). Поэтому (если хоть одно из чисел $2j-3$, $2j-2$ входит в $2\overline{K}_1$)

$$T \geqslant \overline{T}_1 + \overline{\overline{T}} - 3 \geqslant 3j + 1 + 3(k-j) - 3 \geqslant 3k-2.$$

Покажем, что мы рассмотрели все возможные случаи. Если условие 3а) не имеет места, то существует такое j, что

(I) $a_i < 2i$, $i \leqslant j-1$

(II) $a_j \geqslant 2j$

(III) $j \leqslant k-2$.

В 3в) рассмотрен случай $a_j > 2j$, в 3б) случай $a_{k-2} = 2k-4$. Вместо условий (I) — (III) остаются условия:

(I) $a_i < 2i$, $i \leqslant j-1$

(II*) $a_j = 2j$

(III*) $j \leqslant k-3$.

После рассмотрения случая 3г) добавляется (если учесть разницу в обозначениях индексов) условие (IV) $a_{j+2} \leqslant 2j+2$, после исключения случая 3д) — условие (V) $a_{j-1} \leqslant 2j-4$, исключение 3е) дает (VI) $a_{j+2} \leqslant 2j+4$, после рассмотрения 3ж) получаем (VII) $a_{j+2} \geqslant 2j+3$. Случай 3д) завершит рассмотрение.

Итак, мы показали, что в случае А) можно ограничиться рассмотрением K со свойством A_2). Легко проверить выполнение условий теоремы для множе-

ства K'. Так как $d(K')=1$ и $a_{k-2}\geqslant 2k-3$, то, ввиду теоремы 1.10, $T'\geqslant 3k-6$. Но $T'\leqslant T-3=3k-6$, ввиду A_2), так что $T'=3k-6$.

Таким образом, к K' можно применить предположение индукции. Если K' не изоморфно K_6, то K' имеет вид

$$K'=\{0,\ a,\ 2a,\ \ldots,\ (k_1-1)a,\ b,\ b+a,\ \ldots,\ b+(k_2-1)a\}, \tag{1.12.3}$$

где $k_1+k_2=k-1$, a и b — натуральные числа.

Разберем тот исключительный случай, когда $k=7$ и K' изоморфно K_6. Нулю соответствует одна из точек (0,0), (0,2), (2,0).

В любом случае K' можно представить в виде

$$K'=\{0,\ b,\ 2b,\ a,\ a+b,\ 2a\},\quad b<a,\ (a,\ b)=1.$$

Тогда

$$2K'=\{\begin{array}{ccccc} 0 & b & 2b & 3b & 4b \\ a & a+b & a+2b & a+3b & \\ 2a & 2a+b & 2a+2b & & \\ 3a & 3a+b & & & \\ 4a\}. & & & & \end{array} \tag{1.12.4}$$

Так как a_5+a_6 и $2a_6$ не входят в $2K'$, то одно из чисел a_6 и a_6+a входит в $2K'$.

а) $a_6+a_4=2a_5$, т. е. $a_6=3a-b$. Сравнивая числа $3a-b$ и $4a-b$ с числами (4), получим, что всегда $a\leqslant 5$, что невозможно ввиду $a_5=2a\geqslant 11$.

Так, если, например,

$$4a-b=4b,\ 4a=5b,\ \text{то}\ a=5.$$

б) $a_6+a_4\neq 2a_5$. В этом случае $a_6+2b\in 2K'$.

Приравнивая это число к различным числам из (4), получим такие случаи:

$a_6+2b=3a$, $a_6+b=3a-b\in 2K'$, что разобрано в а)

$$a_6+2b=3a+b,\quad a_6=3a-b\in 2K'$$

$$a_6+2b=4a,\ a_6+b=4a-b\in 2K'.$$

Итак, мы показали, что K' не изоморфно K_6 и, следовательно, имеет вид (3).

Покажем, что в этом случае K изоморфно K_0, причем условие $a_{k-1} \geqslant 2k-1$ не будем считать обязательным, не исключая, таким образом, случай $a_{k-1} = 2k-2$.

Предположим вначале, что $a = 1$. В этом случае

$$K' = \{K'_1,\ K'_2\},\ \text{где}\ K'_1 = \{0,\ 1, \ldots,\ k_1 - 1\},$$
$$K'_2 = \{b,\ b+1, \ldots,\ b+k_2-1\}.$$

Если $a_{k-1} = b + k_2 + 1$, то

$$T = T(2K'_1) + T(K'_1 + \{K'_2,\ a_{k-1}\}) +$$
$$+ T(2\{K'_2,\ a_{k-1}\}) \geqslant 3k-2. \qquad (1.12.5)$$

Пусть теперь $a_{k-1} > b + k_2 + 1$.

Если $k_2 = 1$, то $2a_{k-1}$, $a_{k-1} + a_{k-2}$ и два из трех чисел $a_{k-1} + a_s$, $s = k-5$, $k-4$, $k-3$ не входят в $2K'$; отсюда

$$T \geqslant T' + 4 = 3k-2. \qquad (1.12.6)$$

Если $k_2 = 2$, то в случае, когда $k = 6$ и числа

$$a_{k-1} + a_s \qquad (1.12.7)$$

при $s = 0,\ 1,\ 2$ совпадают с числами $2K'_2$, мы получаем $a_{k-1} = 2b$ и K изоморфно K_6. В противном случае одно из чисел (7) при $k = 6$ и $s = 0,\ 1,\ 2$ или одно из чисел (7) при $k-7 \leqslant s \leqslant k-4$ не совпадает с $2K'$. Так как и числа (7) при $k-3 \leqslant s \leqslant k-1$ не совпадают с $2K'$, то имеет место (6).

Наконец, если $k_2 \geqslant 3$, то числа (7) при $k-4 \leqslant s \leqslant k-1$ не входят в $2K'$ и снова имеет место (6).

Итак, за исключением особого случая, когда $a_{k-1} = 2b$ при $k = 6$ и $k_2 = 2$, всегда $a_{k-1} = b + k_2$.

В случае $a = 2$, если $a_{k-1} = a_{k-2} + 4$, получается неравенство (5). Дальнейшее рассмотрение проходит аналогично случаю $a = 1$.

Покажем, что при $a \geqslant 3$ невозможно одновременно

$$a_{k-1} \not\equiv 0 \pmod a \quad \text{и} \quad a_{k-1} \not\equiv b \pmod a.$$

Пусть вначале $a = 3$. Тогда должно было бы быть $a_{k-1} \equiv 2b \pmod a$. Множество K' имеет вид

$$K' = \{0,\ 3, \ldots,\ 3(k_1-1),\ b,\ b+3, \ldots,\ b+3(k_2-1)\}.$$

Предположим вначале, что число $3(k_1-1)$ — наибольшее в K'. Тогда $3(k_1-1)>2k-4$, $k_1>\frac{2k-1}{3}$.

Числа

$$a_{k-1},\ a_{k-1}+3,\ \ldots,\ a_{k-1}+3(k_1-1) \qquad (1.12.8)$$

могут совпасть только с нижеследующими числами из $2K'$:

$$2b,\ 2b+3,\ \ldots,\ 2b+3(2k_2-2). \qquad (1.12.9)$$

Этих чисел $2k_2-1$. Так как $k_1+k_2=k-1$, то

$$2k_2-1=2k-2k_1-3<k_1-2.$$

Поэтому среди чисел (8) имеется не менее трех, не входящих в $2K'$, а если еще учесть $2a_{k-1}$, то $T\geqslant T'+4\geqslant 3k-2$, что невозможно.

Пусть теперь наибольшим числом в K' является $b+3(k_2-1)$.

При $k_2=1$, два из чисел $a_{k-1}+a_s$, $s=k-5$, $k-4$, $k-3$ не входят в $2K'$.

При $k_2\geqslant 2$ и $3(k_1-1)<b+3(k_2-2)$ рассмотрение проходит как и в случае $a=1$. Пусть теперь $3(k_1-1)>b+3(k_2-2)$, $k_2\geqslant 2$.

При $b\equiv 1\pmod 3$ не может быть $a_{k-1}-a_{k-2}>1$, так как тогда было бы $a_{k-1}-a_{k-2}\geqslant 4$ и числа $a_{k-1}+a_s$, $s=k-4$, $k-3$, $k-2$, $k-1$ не входили бы в $2K'$.

Рассмотрим случай $a_{k-1}-a_{k-2}=1$. Так как $b+3(k_2-1)>2k-4$, то $3(k_1-1)>2k-5$ и $k_1>\frac{2k-2}{3}$.

Поэтому $2k_2<k_1$. Таким образом, среди чисел (8) имеется не менее двух, не входящих в $2K'$, а кроме них такими числами являются $a_{k-1}+a_{k-2}$, $2a_{k-1}$.

При $b\equiv 2\pmod 3$ имеем $a_{k-1}-a_{k-2}=2$ и числа

$$a_{k-1}+b+3(k_2-1),\ a_{k-1}+b+3(k_2-2)$$

не входят в $2K'$. Так как $b+3(k_2-1)>2k-4$, то

$$3(k_1-1)>2k-6 \text{ и } k_1>\frac{2k-3}{3},$$

а отсюда $2k_2-1<k_1$. Среди чисел (8) имеется не менее одного, не входящего в $2K'$, а всего, вместе с $2a_{k-1}$, их будет не менее четырех.

Пусть теперь $a \geqslant 4$. В этом случае числа вида

$$a_{k-1} + sa, \quad s = 0, 1, \ldots, k_1 - 1,$$

могут равняться числам из $2K'$ только тогда, когда они имеют вид $a_j + a_t$, где a_j, $a_t \equiv b \pmod a$, а числа вида

$$a_{k-1} + b + sa, \quad s = 0, 1, \ldots, k_2 - 1$$

могут равняться числам из $2K'$ только в том случае, если они имеют вид $a_j + a_t$, где a_j, $a_t \equiv 0 \pmod a$. Два числа, одно из которых имеет вид $a_{k-1} + s_1 a$, а другое имеет вид $a_{k-1} + b + s_2 a$, не могут одновременно равняться числам из $2K'$, так как тогда одновременно выполнялись бы сравнения $a_{k-1} \equiv 2b \pmod a$ и $a_{k-1} + b \equiv 0 \pmod a$, откуда было бы $3b \equiv 0 \pmod a$, что при $a \geqslant 4$ невозможно, ввиду $(a, b) = 1$.

Пусть имеет место одно из упомянутых двух сравнений, например, $a_{k-1} \equiv 2b \pmod a$. В этом случае для чисел a_j, для которых $a_j \equiv b \pmod a$, числа $a_{k-1} + a_j$ не входят в $2K'$. Число их равно k_2. Среди чисел $a_{k-1} + a_j$, для которых $a_j \equiv 0 \pmod a$, а число таких чисел равно k_1, не совпадает с числами из $2K'$ самое меньшее $\max(0, k_1 - (2k_2 - 1))$.

Общее число чисел вида $a_{k-1} + a_s$, $s = 0, 1, \ldots, k-1$, не входящих в $2K'$, не меньше, чем $1 + k_2 + \max(0, k_1 - 2k_2 + 1)$.

Это число всегда $\geqslant 4$ (за тем исключением, когда оно равно 3 при $k_2 = 2$ и $k_1 = 3$, приводящим к случаю, когда K изоморфно K_6).

Аналогично рассматривается случай, когда $a_{k-1} \equiv \equiv -b \pmod a$.

Итак, мы доказали, что при $a \geqslant 3$ выполняется одно из сравнений $a_{k-1} \equiv 0 \pmod a$ или $a_{k-1} \equiv b \pmod a$.

Пусть, например, выполняется второе из этих сравнений. Тогда числа

$$a_{k-1} + b + (k_2 - 1)a, \quad a_{k-1} + (k_1 - 1)a, \quad 2a_{k-1}$$

не входят в $2K'$. Поэтому, если $k_1 = 1$, то

$$a_{k-1} + b + (k_2 - 2)a = 2b + 2(k_2 - 1)a,$$

если же $k_1 \geqslant 2$, то

$$a_{k-1} + (k_1 - 2)a = (k_1 - 1)a + b + (k_2 - 1)a,$$

т. е. $a_{k-1} = b + k_2 a$. Аналогично рассматривается и случай, когда

$$a_{k-1} \equiv 0 \pmod{a}.$$

Случай А) рассмотрен полностью. Перейдем теперь к рассмотрению случая В).

Очевидно, что $a_1 > 2$. Найдем число $j \geqslant 2$ из условия $a_i > 2i$ при $i = 1, 2, \ldots, j-1$, $a_j \leqslant 2j$. Тогда, очевидно,

$$a_{j-1} = 2j - 1,\ a_j = 2j.$$

Рассмотрим множества $\overline{K}$ и $\overline{\overline{K}}$, определенные в (1.10.4) и (1.10.5). Как и при рассмотрении случая 3в), здесь можно показать, что $\overline{T} = 3j$, $\overline{\overline{T}} = 3(k-j)$.

Покажем, что $a_{j-2} < 2j - 2$. Предположим, что $a_{j-2} = 2j - 2$ и вместо $\overline{\overline{K}}$ рассмотрим множество

$$\overline{\overline{K}}_1 = \{a_{j-2},\ a_{j-1}, \ldots,\ a_{k-1}\}.$$

Тогда $\overline{\overline{T}}_1 \geqslant 3(k-j) + 3$ и, так как множества $2\overline{K}$ и $2\overline{\overline{K}}_1$ имеют пять общих точек $2a_{j-2} + s$, $s = 0, 1, 2, 3, 4$, то

$$T \geqslant \overline{T} + \overline{\overline{T}}_1 - 5 \geqslant 3k - 2.$$

что противоречит условию теоремы.

Точно так же можно показать, что $a_{j+1} > 2j + 1$.

Ввиду того, что числа $a_j + a_s$, $s = j-2$, $j-1$, j не входят в $2K'$,

$$\overline{T}' = 3j - 3.$$

Точно так же можно показать, что $\overline{\overline{T}}'' = 3(k-j) - 3$.

Используя предположение индукции, мы можем сделать вывод, что множества $\overline{K}'$ и $\overline{\overline{K}}''$ состоят каждое из двух арифметических прогрессий. Если использовать рассмотрение случая А) и учесть, что там нигде не использовалось требование $a_{k-1} \geqslant 2k - 1$, то мы получим, что и множества $\overline{K}$ и $\overline{\overline{K}}$ имеют такую же структуру.

а) $j = 2$, $a_1 = 3$, $a_2 = 4$. В этом случае $\overline{K} = K''$. Если a в K'' равняется трем или четырем, то теорема доказана. Если $a = 5$, то $a_3 = 8$ и $a_4 = 9$ или 13. Тогда 0, a_1, a_2 и a_4 не входят в $2K''$. Если $a > 5$, то 0, a_1, a_2 и a_3 не входят в $2K''$.

б) $j = k-2$. Ясно, что, ввиду $a_{j-2} = 2j-3$, число a в $\overline{K}$ равно трем. Неравенство $a_{k-1} \geqslant a_{k-2} + 4$ невозможно, так как тогда числа $a_{k-1} + a_s$, $s = k-4, k-3, k-2, k-1$ не принадлежали бы $2K'$. Поэтому $a_{k-1} = a_{k-2} + 3$.

в) $2 < j < k-2$. Ввиду $a_{j-2} = 2j-3$, число a в $\overline{K}$ равно трем. Если и в множестве $\overline{\overline{K}}$ число a равно трем, то теорема доказана. Предположим, что $a = 4$. Тогда $a_{j+1} = a_{j-1} + 4$, $a_{j+2} = a_j + 4$ или $a_{j+2} = a_{j-1} + 8$. В любом случае число $a_{j-2} + a_{j+2}$ не входит ни в $2\overline{K}$, ни в $2\overline{\overline{K}}$. Тогда $T \geqslant \overline{T} + \overline{\overline{T}} - 3 + 1 \geqslant 3k-2$. Если же предположить, что $a \geqslant 5$, то тогда число $a_{j-2} + a_{j+1}$ не входит ни в $2\overline{K}$, ни в $2\overline{\overline{K}}$. Итак, $a = 3$.

Мы закончили рассмотрение случая В) и, таким образом, полностью завершили доказательство теоремы.

Задача 1. Привести пример, показывающий, что результат теоремы 1.11 для случая 1 усилить нельзя.

1.13. Структура K при $T = 3k-2$. С ростом T изучение структуры K все более усложняется, как это можно проследить на примере доказательства теорем 1.9 и 1.11.

В работе [13] был рассмотрен элементарными методами случай $T = 3k-2$. Доказана

Теорема. Пусть $T = 3k-2$. Тогда возможны следующие случаи:

1. Длина множества K не превышает $2k+1$.
2. K изоморфно множеству

$$K_0 = \{(0, 0), (0, 1), \ldots, (0, k-3), (0, k-1), (1, 0)\}.$$

3. K для $k = 10$ изоморфно

$$K_{10} = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (3, 0)\}.$$

Доказательство этой теоремы очень громоздко, и мы не будем здесь приводить его.

Для изучения структуры K при $T > 3k-2$ оказалось необходимым привлечение аналитических методов. Эти результаты изложены в главе II.

Задача 1. Привести пример, показывающий, что результат теоремы 1.13 для случая 1 усилить нельзя.

1.14. Оценка снизу для T, $K \subset E_n$.

Обозначения.

E_n — *евклидово пространство* размерности n.

Целый вектор — вектор с целыми координатами. Вектор иногда называется также точкой и обозначается латинской буквой с чертой наверху или $(x_1, x_2, \ldots, x_n)$, где x_i, $1 \leqslant i \leqslant n$ — координаты вектора.

Z_n — аддитивная группа целых векторов E_n.

$\{\bar{e}_i\}$, $1 \leqslant i \leqslant n$ — ортонормированный базис в E_n.

Смежные классы по линейному подпространству размерности s, $1 \leqslant s \leqslant n-1$ называются *плоскостями*. В частности, при $s=1$ мы получаем *прямые* при $s = n-1$ — *гиперплоскости*.

Размерность точечного множества — это ранг совокупности векторов, соединяющих пары точек этого множества. $L(\bar{a}, \bar{b}, \ldots, \bar{l})$ — линейное подпространство, порожденное векторами $\bar{a}, \bar{b}, \ldots, \bar{l}$.

Лемма. Пусть конечное множество $K \subset E_n$, $T(K) = k$, и K имеет размерность n.

Тогда

$$T \geqslant (n+1)\,k - \frac{n(n+1)}{2} \qquad (1.14.1)$$

Доказательство (1) проведем по индукции. Лемма верна при $n=1$ и любом k. При любом n и $k = n+1$ (1) справедливо, так как $T = \frac{(n+1)(n+2)}{2}$. Предположим теперь, что неравенство (1) справедливо при $n = 1, 2, \ldots, m-1$ и любом k и при $n=m$, $k = m+1, m+2, \ldots, p-1$ (так как K имеет размерность n, то $k \geqslant n+1$). Докажем справедливость (1) для $n=m$, $k=p$.

Рассмотрим минимальный выпуклый многогранник, содержащий K и одну из его вершин $\bar{a}$, принадлежащую, очевидно, K.

Пусть $K \setminus \bar{a}$ содержится в некоторой гиперплоскости. Множество $K \setminus \bar{a}$ имеет размерность $n-1$, так как если бы оно имело меньшую размерность, то K имело бы размерность не большую $n-1$. Поэтому $T(2(K \setminus \bar{a})) \geqslant m(p-1) - \frac{(m-1)m}{2}$ и

$$T = T(2(K \setminus \bar{a})) + T((K \setminus \bar{a}) + \bar{a}) + 1 \geqslant$$

$$\geqslant m(p-1) - \frac{(m-1)m}{2} + p - 1 + 1 =$$

$$= (m+1)p - \frac{m(m+1)}{2}.$$

Пусть теперь размерность $K \setminus \bar{a}$ равна m. Рассмотрим минимальный выпуклый многогранник, содержащий $K \setminus \bar{a}$. Пусть L его грань, относительно которой точка $\bar{a}$ лежит по иную сторону, чем некоторые из точек $K \setminus \bar{a}$. На L лежит не менее m точек из K. Поэтому

$$T \geqslant T(2(K \setminus \bar{a})) + T(K \cap L + \bar{a}) + 1 \geqslant$$

$$\geqslant (m+1)(p-1) - \frac{m(m+1)}{2} + m + 1 =$$

$$= (m+1)p - \frac{m(m+1)}{2}.$$

1. 15. Структура $K \subset Z_2$, при $T < \frac{10}{3}k - 5$. В пункте 1.13 говорилось о трудностях изучения структуры K при $T > 3k - 3$ элементарными методами. Решение этой задачи становится более простым, если вместо множества целых чисел рассматривать множество целых точек плоскости, не лежащих, разумеется, на одной прямой. В пп. 1.15—1.17 мы исследуем структуру множества $K \subset Z_2$ при

$$3k - 3 \leqslant T < \frac{10}{3}k - 5. \qquad (1.15.1)$$

Лемма. Пусть $K \subset Z_2$ и $T < \frac{10}{3}k - 5$. Тогда возможны следующие случаи:

1. Множество K лежит на двух параллельных прямых.

2. Множество K при $k = 10$ изоморфно K_{10}.

Доказательство. Рассмотрим вначале тот случай, когда множество K разбивается на подмножества $K_1, K_2, \ldots, K_s$, лежащие на s параллельных прямых.

Тогда

$$T \geqslant T(2K_1) + T(K_1 + K_2) + T(2K_2) + \\ + T(K_2 + K_3) + \ldots + T(K_{s-1} + K_s) + T(2K_s) \geqslant 2k_1 - 1 + \\ + k_1 + k_2 - 1 + 2k_2 - 1 + \ldots + 2k_s - 1 = \\ 4k - (k_1 + k_s) - (2s - 1) \qquad (1.15.2)$$

и

$$T \geqslant T(2K_1) + T(K_1 + K_2) + T(K_1 + K_3) + \\ + \ldots + T(K_1 + K_s) + T(K_2 + K_s) + \\ + \ldots + T(2K_s) \geqslant 2k_1 - 1 + k_1 + k_2 - 1 + k_1 + k_3 - 1 + \\ + \ldots + k_1 + k_s - 1 + k_2 + k_s - 1 + \ldots + 2k_s - 1 = \\ 2k + (k_1 + k_s)(s - 1) - (2s - 1). \qquad (1.15.3)$$

Из (2) и (3) следует:

$$T \geqslant \left(4 - \frac{2}{s}\right)k - (2s - 1). \qquad (1.15.4)$$

Если $3 \leqslant s \leqslant \frac{k}{3}$, то из (4) следует, что $T \geqslant \frac{10}{3}k - 5$, так что при $s \leqslant \frac{k}{3}$ лемма справедлива.

Доказательство леммы будем проводить по индукции. Из (1) при $k \leqslant 6$ следует $T \leqslant 3k - 4$. Из теоремы 1.9 следует тогда, что K лежит на одной прямой. Если $7 \leqslant k \leqslant 9$, то из (1) следует, что $T \leqslant 3k - 3$. Из теоремы 1.11 следует тогда, что K лежит на двух прямых. Если $10 \leqslant k \leqslant 12$, то из (1) следует, что $T \leqslant 3k - 2$. Из теоремы 1.13 следует, что и в этом случае K лежит на двух прямых, за исключением того возможного при $k = 10$ случая, когда K изоморфно K_{10}.

Предположим, что утверждение леммы справедливо для всех значений, не превышающих $k - 1$, где $k \geqslant 13$, и докажем, что оно справедливо для k.

Рассмотрим выпуклую оболочку D множества K, то есть минимальное выпуклое множество, содержащее K, которая, очевидно, является многоугольником, все вершины которого принадлежат K. Рассмотрим любую вершину $\bar{a}_1$, содержащие $\bar{a}_1$ два звена ломаной — границы D, и две точки $\bar{a}_2$ и $\bar{a}_3$, лежащие на каждом из этих звеньев. Рассмотрим *решетку*, порожденную точками $\bar{a}_1$, $\bar{a}_2$, $\bar{a}_3$. Любой вектор $\bar{b}$ из K представляется однозначно в виде $\bar{b} = \alpha_1(\bar{a}_2 - \bar{a}_1) + \alpha_2(\bar{a}_3 - \bar{a}_1)$.

Среди векторов $\bar{b}$, для которых числа α_1, α_2 не являются оба целыми, выберем такой, что для него уже нет вектора $\bar{b}' \neq \bar{b}$ с числами α_1', α_2' такими, что $\alpha_1' \leqslant \alpha_1$, $\alpha_2' \leqslant \alpha_2$.

Точки $2\bar{a}_1$, $\bar{a}_1 + \bar{a}_2$, $\bar{a}_1 + \bar{a}_3$, $\bar{a}_1 + \bar{b} \in 2(K \setminus \bar{a}_1)$. Поэтому $T(2(K \setminus \bar{a}_1)) \leqslant T - 4 < \frac{10}{3}(k-1) - 5$, множество $K \setminus \bar{a}_1$ находится на двух параллельных прямых, а множество K — не более, чем на трех, что доказывает лемму, так как здесь $s < \frac{k}{3}$.

Итак, можно считать, что все α_1, α_2 являются парами целых чисел. Рассмотрим линейное преобразование плоскости, для которого $\bar{a}_1 \to (0,0)$, $\bar{a}_2 \to (0,1)$, $\bar{a}_3 \to (1,0)$. Множество K преобразуется в изоморфное ему множество, лежащее в первом координатном углу с точками, имеющими целые неотрицательные координаты. Образ K мы по-прежнему будем обозначать через K.

Предположим, что на прямой $x_1 = 0$ лежит не менее пяти точек из K. Рассмотрим s прямых, параллельных $x_1 = 0$, на которых лежат точки множества K. Нам нужно рассмотреть лишь случай $s > \frac{k}{3}$. Ввиду (3) получим

$$T \geqslant 2k + (s-1)(k_1 + k_s - 2) - 1 >$$
$$> 2k + \left(\frac{k}{3} - 1\right)(6-2) - 1 = \frac{10}{3}k - 5,$$

что невозможно ввиду условия (1).

Итак, на прямой $x_1 = 0$ лежит не более четырех точек. Если их больше двух, то $(0,2) \in K$. В самом деле, если t минимальное из чисел, для которых $(0,t) \in K$, $t > 1$, то $(0,0) + (0,0)$, $(0,0) + (1,0)$, $(0,0) + (0,1)$, $(0,0) + (0,t) \in 2(K \setminus (0,0))$. Если на оси ординат лежат четыре точки, то точка $(0,3) \in K$. В противном случае ее можно подходящим линейным преобразованием перевести в $(0,0)$ и повторить только что проведенное рассуждение.

Пусть точки с максимальными ординатами на прямых $x_1 = 0$ и $x_1 = 1$ будут $(0,c)$ и $(1,d)$. Если $d \leqslant c$, то K лежит не более чем на четырех прямых, что

доказывает лемму. Остается случай $d > c$. Обозначим $K_1 = K \cap \{x_1 = 0\}$, $K_2 = K \cap \{x_1 = 1\}$. Тогда

$T(K_1 + K_2) \geqslant T(K_1 + \{1,0\}) + T(K_1 + \{1, d\}) = 2T(K_1)$.

Кроме того, $T(2K_1) \geqslant 2T(K_1) - 1$.

Таким образом,

$$T(2(K \setminus K_1)) < \frac{10}{3}k - 5 - 4T(K_1) + 1 < \frac{10}{3}(k - T(K_1)) - 5.$$

Если $T(K_1) = 3$ и $k = 13$, то $T(2(K \setminus K_1)) \leqslant 27$.

Если $T(K_1) = 4$ и $k = 14$, то $T(2(K \setminus K_1)) \leqslant 26$.

Итак, $K \setminus K_1$ лежит на двух параллельных прямых.

На прямой $x_1 = 1$ лежит не менее трех точек из K. В противном случае $(0,0) + (1, d) \bar{\in} 2(K \setminus (0,0))$. Итак, прямые, на которых лежит множество $K \setminus K_1$, параллельны прямой $x_1 = 0$ и K лежит не более чем на трех параллельных прямых. Лемма доказана.

Задачи.

1. Для множества $K \subset Z_2$, не расположенного на одной прямой, имеет место неравенство $T \geqslant 3k - 3$.

2. Обобщить лемму 1.15 на случай трех прямых.

3. Доказать, что если $K \subset Z_2$, $T < \left(4 - \frac{2}{s}\right) k - (2s - 1)$ и k достаточно велико, то существует $s - 1$ параллельных прямых, содержащих K.

4.** Пусть $K \subset Z_2$ и никакие три его точки не лежат на одной прямой. Найти оценку для T снизу.

5.** Обобщение предыдущей задачи. Пусть $K \subset Z_n$ и никакие m его точек не лежат на плоскости размерности s. Найти оценку для T снизу.

Можно рассматривать частные случаи для $s = 1$ (прямая), для $s = n - 1$ (гиперплоскость), для $n = 2$ и других малых натуральных значений n, для $m = s + 2$ и других малых натуральных значений $m > s + 2$, для $m = [k^{\varepsilon}]$, $0 < \varepsilon < 1$.

1.16. Проекция множества целых точек к плоскости.

Рассмотрим все точки из заданного множества целых векторов $K \subset E_n$, для которых первые $n - 1$ координат $x_1, x_2, \ldots, x_{n-1}$ одинаковы. Пусть для некоторого фиксированного набора $x_1, \ldots, x_{n-1}$ число этих точек равно s, так что $\bar{x}_i = (x_1, x_2, \ldots, x_{n-1}, x_{n_i})$,

$1 \leqslant i \leqslant s$. Вместо этих s точек возьмем точки $(x_1, x_2, \ldots, x_{n-1}, u)$, $u = 0,1, \ldots, s-1$.

Произведем такую замену для всех фиксированных наборов $x_1, x_2, \ldots, x_{n-1}$, для которых $s \geqslant 1$. Полученное множество K^0 назовем *проекцией* множества K *к плоскости*

$$L(\bar{e}_1, \bar{e}_2 \ldots, \bar{e}_{n-1})$$

параллельно $\bar{e}_n$. Если $s \leqslant 1$ для любого набора $x_1, x_2, \ldots, x_{n-1}$, то мы получаем обычную проекцию.

Теорема. Если K^0 — проекция множества K к $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$ параллельно $\bar{e}_n$, то

$$T(2K^0) \leqslant T(2K). \tag{1.16.1}$$

Доказательство. Рассмотрим числа $b_1, b_2, \ldots, b_{n-1}$ такие, что существуют две точки из K

$$\bar{x}' = (x_1', x_2', \ldots, x_n') \text{ и } \bar{x}'' = (x_1'', x_2'', \ldots, x_n'')$$

такие, что

$$x_j' + x_j'' = b_j, \quad 1 \leqslant j \leqslant n-1. \tag{1.16.2}$$

Пусть в K^0 число s, определенное числами $x_1', x_2', \ldots, x_{n-1}'$, равно s_1, числами $x_1'', x_2'', \ldots, x_{n-1}''$ — равно s_2.

Пусть $t = \max(s_1 + s_2 - 1)$, где максимум берется по всем парам $\bar{x}', \bar{x}''$, со свойством (2). Точки

$$(b_1, b_2, \ldots, b_{n-1}, u), \quad u = 0,1, \ldots, t-1$$

входят в $2K^0$ и для заданных b_j, $1 \leqslant j \leqslant n-1$, только они. Но в $2K$ входит не менее t точек с заданными $n-1$ первыми координатами, равными $b_1, b_2, \ldots, b_{n-1}$.

Примечание. Пусть задан базис $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ решетки Z_n. Ясно, как определить проекцию K к гиперплоскости $L(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n-1})$ параллельно $\bar{a}_n$ (введением соответствующей системы координат). Свойство (1) сохраняется.

1.17. Уточнение структуры $K \subset Z_2$ при $T < \frac{10}{3}k - 5$.

Теорема. Пусть $K \subset Z_2$, причем не существует прямой, содержащей K, $T < \frac{10}{3}k - 5$, $k \geqslant 11$*).

*) При $k < 11$ структура K получена при доказательстве леммы 1.15.

Тогда K содержится в множестве, изоморфном множеству:

$K_0 = \{(0,0),\ (0,1),\ \ldots,\ (0,\ k_1-1),\ (1,0),\ (1,1),\ \ldots,\ (1,\ k_2-1)\}$,

где $k_1,\ k_2 \geqslant 1,\ k_1 + k_2 = T - 2k + 3$.

Доказательство. Из леммы 1.15 следует, что множество K лежит на двух параллельных прямых l_1 и l_2. Можно предположить, что K лежит на прямых $x_2 = 0$ и $x_2 = 1$, так так всегда существует линейное преобразование плоскости, переводящее целые точки прямых l_1 и l_2 в целые точки прямых $x_2 = 0$ и $x_2 = 1$, а множество K в изоморфное ему множество.

Пусть множества абсцисс при $x_2 = 0$ и $x_2 = 1$ равны соответственно $\{a_0,\ a_1,\ \ldots,\ a_{m-1}\}$ и $\{b_0,\ b_1,\ \ldots,\ b_{n-1}\}$, $m + n = k$.

Можно предположить, что $a_0 = 0,\ b_0 = a_{m-1}$, $(a_1,\ a_2,\ \ldots,\ a_{m-1},\ b_1,\ b_2,\ \ldots,\ b_{n-1}) = 1$, так как в противном случае существовал бы изоморфный образ K, удовлетворяющий этим требованиям. Спроектируем множество $K\varphi$ к прямой $x_2 = 0$. Мы получим множество $K^0 = K_1^0 \cup K_2^0$, где множество K_1^0 таково, что ординаты его точек равны 0, множество абсцисс — $\{a_0,\ a_1,\ \ldots,\ a_{m-1},\ b_1,\ b_2,\ \ldots,\ b_{n-1}\}$, а множество K_2^0 состоит из одной точки $(b_0,\ 1)$.

Так как, ввиду теоремы 1.16,

$$T(2K^0) = T(2K_1^0) + T(K_1^0 + K_2^0) + T(2K_2^0) = T(2K_1^0) + \\ + k - 1 + 1 \leqslant T(2K),$$

то

$$T(2K_1^0) \leqslant T - k$$

и, ввиду теоремы 1.9, применяемой к K_1^0,

$b_{n-1} - b_0 + a_{m-1} - a_0 = k_1 + k_2 - 2 \leqslant T - 2k + 2$.

Задачи.

1. Привести пример, показывающий, что теорему 1.17 нельзя усилить за счет уменьшения величины $k_1 + k_2$.

2. Привести пример, показывающий, что теорему 1.17 нельзя усилить за счет увеличения верхней границы T.

3. Обобщить примеры задач пп. 1.11, 1.12, а именно, привести примеры множеств K длины $k + b$, для ко-

торых $T = 2k - 1 + b$ и которые нельзя изоморфно отобразить во множество K_0 п. 1.17.

4. Сформулировать гипотетический аналог теорем 1.11 и 1.13.

5. Сформулировать и доказать усиление теоремы 1.17 за счет максимально возможного увеличения верхней границы T при том дополнительном условии, что K лежит на двух прямых.

§ 3. ФУНКЦИЯ $W(r, T, k)$.

1.18. Определение функции $W(r, T, k)$. В настоящем пункте мы определим функцию, которая достаточно полно описывает структуру K при заданном T.*)

Изоморфное отображение $K \subset E_m$ в E_n назовем *невырожденным*, если образ K имеет размерность n, вырожденным, если образ K имеет размерность меньшую, чем n.

Так, отображение $K_{2,3} \to E_2 : O \to (0,0), 1 \to (1,1), 3 \to \to (3,3)$ является вырожденным. Изоморфное отображение $K_{2.3} \to E_2 : 0 \to (0,0), 1 \to (1,0), 3 \to (0,1)$ является невырожденным.

Пусть существует невырожденное изоморфное отображение множества K в E_n, но не существует невырожденного изоморфного отображения множества K в E_{n+1}. Число n с таким свойством мы будем обозначать через r. Таким образом, r определяется множеством K однозначно.

Например, $r(K_{1,3}) = 1$, так как изоморфный образ $K_{1,3}$ при любом отображении в E_n, $n \geqslant 2$, лежит на прямой. Значения r для множеств, рассмотренных в теореме 1.6, смотри в таблице 1.

На рис. 1а и 1б приведены невырожденные изоморфные образы для этих множеств при отображении в E_r.

Через V_K обозначим число целых точек в замкнутой оболочке множества K.

---

*) Читатель несомненно заметит связь дальнейшего изложения с предварительными соображениями в 1.11, о которой в дальнейшем (п. 1.26) будет сказано более подробно.

Введем обозначения

$$W_K = \min_{\varphi} V_{K\varphi}, \tag{1.18.1}$$

где минимум берется для образов K, обозначаемых $K\varphi$, при всех невырожденных изоморфных отображениях φ данного множества K в Z_r,

$$W(r, T, k) = \max_{K} W_K, \tag{1.18.2}$$

где максимум берется среди всех множеств K с заданными r, T и k.

Величина W_K является обобщением понятия „длины“ множества K, введенного нами в 1.11.

Величина W_K будет называться *объемом множества целых точек* K.

Задачи.

1. Проверить значения r для множеств теоремы 1.6, приведенных в таблице 1.
2. Вычислить значения $W(r, T, k)$ для аргументов из таблицы 1.
3. Доказать, что если $T \leqslant 3k-4$, то $r=1$.
4. Доказать, что если $k \geqslant 3$ и $T \leqslant 3k-4$, то

$$W(1, T, k) = T - k + 1.$$

5. Доказать, что

а) $W(1,3k-3,k) = 2k-1$, $k \geqslant 5$,
б) $W(2,3k-3,k) = k$, $k \geqslant 3$,
в) $W(1,3k-2,k) = 2k+1$, $k \geqslant 10$,
г) $W(2\,3k-2,k) = k+1$, $k \geqslant 10$,
д) $W(2, T, k) = T-2k+3$, $T < 4k-6$.

1.19. Об области определения функции $W(r, T, k)$. Число k может принимать любое натуральное значение. В 1.8 для T указано неравенство

$$2k-1 \leqslant T \leqslant \frac{k(k+1)}{2}.$$

В 1.14 доказывается неравенство

$$T \geqslant (r+1)k - \frac{r(r+1)}{2},$$

дающее оценку r сверху. При любом k и любых T и r, удовлетворяющих приведенным выше неравенствам, существует множество K с такими характеристиками. Примеры таких K приведены в 1.20 и 1.21.

1.20. Оценка $W(1, T, k)$ снизу. В настоящем пункте мы построим примеры множеств K, для которых $r=1$, а T принимает значения от $2k-1$ до $\frac{(k-1)k}{2}+2$. Значения W_K для этих примеров дадут оценку $W(1, T, k)$ снизу.

Для любых заданных натуральных значений s и t, удовлетворяющих неравенствам $2 \leqslant s \leqslant k-1, 1 \leqslant t \leqslant \max(1, k-s-1)$, рассмотрим множество

$$K(k, s, t) = \{0, 1, 2, \ldots, k-s, k-s+t, 2(k-s+t), 2^2(k-s+t), \ldots, 2^{s-2}(k-s+t)\}. \quad (1.20.1)$$

Вычисляя значение $T(2K)$, мы получаем

$$T = sk - \frac{s(s+1)}{2} + t + 1. \quad (1.20.2)$$

Если s пробегает значения от 2 до $k-1$, а t при заданном s пробегает значения от 1 до $k-s-1$ (при $s=k-1$ значение t равно 1), то T принимает значения от $2k-1$ до $\frac{(k-1)k}{2}+2$.

Обратно, если задать значение T такое, что

$$2k-1 \leqslant T \leqslant \frac{(k-1)k}{2}+2,$$

то s и t определяются из (2) по формулам

$$s = \left[\frac{2k^{(1)} - 1 - \sqrt{(2k^{(1)}-1)^2 - 8T^{(1)} + 16}}{2}\right], \quad (1.20.3)$$

$$t = T^{(1)} - sk^{(1)} + \frac{s(s+1)}{2} - 1, \quad (1.20.4)$$

где $T^{(1)} = T$, $k^{(1)} = k$, а s в (4) определяется из (3).

Рассмотрение $K(k, s, t)$ дает следующую оценку снизу для $W(1, T, k)$.

Теорема. Для значений T таких, что

$$2k-1 \leqslant T \leqslant \frac{(k-1)k}{2}+2,$$

имеет место неравенство

$$W(1,\ T,\ k) \geqslant 2^{s-2}(k-s+t)+1, \qquad (1.20.5)$$

где s и t определяются по формулам (3) и (4).

Обозримая оценка нижней границы в (5) при малых T дана в конце 1.21 оценкой (21.4) при $r=1$.

1.21. Оценка $W(r, T, k)$ снизу. При заданных r, T и k (см. 1.19), множество $P(r, T, k) \subset E_r$ построим следующим образом. Включим в $P(r, T, k)$ целые точки $(0, x_2, x_3, \ldots, x_r)$, для которых $x_i \geqslant 0$, $x_2 + x_3 + \ldots + x_r = 1$ (таким образом, одно из $x_i = 1$, а остальные — нулю, $i \geqslant 2$). Включим также в $P(r, T, k)$ точки $(x_1, 0, 0, \ldots, 0)$, где $\{x_1\} = K(k-r+1,\ s,\ t)$, а s и t определяются по формулам (20.3) и (20.4), где

$$T^{(1)} = T - \frac{(2k-r+2)(r-1)}{2}, \qquad (1.21.1)$$

$$k^{(1)} = k - r + 1. \qquad (1.21.2)$$

Легко проверить, что $T = T(2P(r, T, k))$. Очевидно также, что $P(1, T, k) = K(k, s, t)$. Рассмотрение множества $P(r, T, k)$ дает следующую оценку $W(r, T, k)$ снизу:

Теорема. Для значений T, таких, что

$$(r+1)k - \frac{r(r+1)}{2} \leqslant T \leqslant \frac{(k-1)k}{2} + r + 1,$$

имеет место неравенство

$$W(r, T, k) \geqslant 2^{s-2}(k^{(1)} - s + t) + r, \qquad (1.21.3)$$

где s и t определяются по формулам (20.3) и (20.4), в которых $T^{(1)}$ и $k^{(1)}$ определяются по формулам (1) и (2).

Пусть задано любое, сколь угодно малое $\varepsilon > 0$. Можно найти такое достаточно малое $c > 0$, зависящее от ε, что при $T < ck^{3/2}$ из (20.3) и (1) будут следовать неравенства

$$s = \left[\frac{T^{(1)}}{k^{(1)}} + 0\left(\frac{T^{(1)^2}}{k^3}\right)\right] = \left[\frac{T}{k} - r + 1 + \theta_1\right],$$

где θ_1 как угодно мало при надлежащем выборе c,

$$(1-\theta_1)k < k^{(1)} - s + t < 2k$$

и

$$2^{s-2}(k^{(1)}-s+t)+r=\theta\cdot 2^{\frac{1}{k}-r}k, \qquad (1.21.4)$$

где

$$\frac{1}{2}-\varepsilon<\theta<2+\varepsilon.$$

1.22. Не зависящая от T оценка $W(r, T, k)$ сверху. *Теорема.*

$$W(r, T, k)\leqslant 2^{k-1-r}+r. \qquad (1.22.1)$$

Доказательство. Можно предположить, что K имеет размерность r и $K\subset E_r$. Пусть $K=\{\bar{a}_0, \bar{a}_1, \ldots, \ldots, \bar{a}_{k-1}\}$, где $\bar{a}_i$, $0\leqslant i\leqslant k-1$ упорядочены следующим образом: $\bar{a}'=\{a'_1, a'_2, \ldots, a'_r\}$ следует за $\bar{a}''=\{a''_1, a''_2, \ldots, a''_r\}$, если $a'_j=a''_j$, $1\leqslant j\leqslant s-1$, $a'_s>a''_s$.

Построим изоморфное отображение φ множества K в E_{2k-2}, которое мы построим по индукции, определяя последовательно изоморфные отображения φ_{s-1} множеств $K_s=\{\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{s-1}\}$, $2\leqslant s\leqslant k$ в E_{2k-2}.

Отметим сразу, что построение будет проводиться таким образом, что будут совпадать первые r координат векторов $\bar{a}_i$ и $\bar{a}_i\varphi_{s-1}$, $2\leqslant s\leqslant k$ при любом фиксированном i, $0\leqslant i\leqslant s-1$. Ввиду этого, любые две неравные разности элементов из K_s перейдут при отображении φ_{s-1} в неравные. Для установления факта изоморфизма нам понадобится лишь проверить, что равные разности перейдут в равные (критерий 1.5).

Заметим еще, что среди разностей $\pm(\bar{a}_s-\bar{a}_i)$, $1\leqslant i\leqslant s-1$ нет одинаковых ввиду способа упорядочения.

Положим,

$$\bar{a}_0\varphi_1=(a_{01}, a_{02}, \ldots, a_{0r}, 0, \ldots, 0),$$
$$\bar{a}_1\varphi_1=(a_{11}, a_{12}, \ldots, a_{1r}, 1, 0, \ldots, 0).$$

Предположим, что образ $K_s\varphi_{s-1}$ множества K_s построен и размерность его равна p_s. Построим образ $K_{s+1}\varphi_s$ множества K_{s+1}. Здесь возможны следующие три случая.

а) $\bar{a}_s - \bar{a}_i \neq \bar{a}_j - \bar{a}_t$, где i, j, t — любые целые числа, удовлетворяющие условию $0 \leqslant i, j, t \leqslant s-1$. В этом случае полагаем $K_s\varphi_s = K_s\varphi_{s-1}$,

$$\bar{a}_s\varphi_s = (a_{s1}, a_{s2}, \ldots, a_{sr}, 0, 0, \ldots, 1, \ldots, 0),$$

где 1 стоит на $p_s + r + 1$-ом месте. Из предварительных замечаний сразу следует изоморфизм множеств K_{s+1} и $K_{s+1}\varphi_s$.

б) Существует единственное t, для которого есть пара i, j, $1 \leqslant i, j, t \leqslant s-1$, так что

$$\bar{a}_s + \bar{a}_t = \bar{a}_i + \bar{a}_j. \tag{1.22.2}$$

В этом случае полагаем $K_s\varphi_s = K_s\varphi_{s-1}$,

$$\bar{a}_s\varphi_s = \bar{a}_i\varphi_s + \bar{a}_j\varphi_s - \bar{a}_t\varphi_s. \tag{1.22.3}$$

Множества K_{s+1} и $K_{s+1}\varphi_s$ изоморфны. В самом деле, множества K_s и $K_s\varphi_s$ изоморфны.

Равенство $\bar{a}_s - \bar{a}_p = \bar{a}_q - \bar{a}_u$, $0 \leqslant p, q, u \leqslant s-1$, может иметь место лишь в случае, когда $u = t$ и $\bar{a}_p + \bar{a}_q = \bar{a}_i + \bar{a}_j$, откуда следует $\bar{a}_p\varphi_s + \bar{a}_q\varphi_s = \bar{a}_i\varphi_s + \bar{a}_j\varphi_s$ и, ввиду (3), $\bar{a}_s\varphi_s - \bar{a}_p\varphi_s = \bar{a}_q\varphi_s - \bar{a}_t\varphi_s$.

в) Существует более одного значения t с соответствующими ему парами значений i и j, для которых имеют место p равенств вида (2):

$$\bar{a}_s + \bar{a}_{t_w} = \bar{a}_{i_w} + \bar{a}_{j_w}, \qquad 1 \leqslant w \leqslant p.$$

Точки $\bar{a}'_{sw}$ определим равенствами вида (3)

$$\bar{a}'_{sw} = \bar{a}_{i_w}\varphi_{s-1} + \bar{a}_{j_w}\varphi_{s-1} - \bar{a}_{t_w}\varphi_{s-1}. \tag{1.22.4}$$

Пусть эти точки (не все из них различные), определяют плоскость P_1, через них проходящую, размерность которой m равна размерности совокупности этих точек.

Плоскость P_2 размерности p_s, параллельная $L(\bar{e}_{r+1}, \bar{e}_{r+2}, \ldots, \bar{e}_{r+p_s})$ и проходящая через точку $(a_{s1}, a_{s2}, \ldots, a_{sr}, 0, 0, \ldots, 0)$ содержит P_1. Пусть *базис* $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m$ *решетки*, состоящей из всех целых точек плоскости P_1, дополняется до базиса решетки $P_2 \cap Z_{2k-2}$ векторами $\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_{p_s-m}$.

Пусть $\bar{x}\varphi_{\text{пр}}$ — проекция точки $\bar{x} \in L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{p_s+r})$ на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_r, \bar{w}_1, \bar{w}_2, \ldots, \bar{w}_{p_s-m})$ параллельно $L(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m)$.

Пусть далее $\bar{\varphi}$: $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_r, \bar{w}_1, \bar{w}_2, \ldots, \bar{w}_{p_s-m}) \to E_{2k-2}$ гомоморфизм, определяемый соотношениями

$$\bar{e}_i\bar{\varphi} = \bar{e}_i, \quad 1 \leqslant i \leqslant r, \quad \bar{w}_j\bar{\varphi} = \bar{e}_{r+j}, \quad 1 \leqslant j \leqslant p_s - m.$$

Тогда

$$K_s\varphi_s = K_s\varphi_{s-1}\varphi_{\text{пр}}\bar{\varphi}, \quad \bar{a}_s\varphi_s = \bar{a}'_{s1}\varphi_{\text{пр}}\bar{\varphi}\ (\bar{a}_{sw}\varphi_{\text{пр}} = \bar{a}'_{s1}\varphi_{\text{пр}}$$

при любом w).

Множества K_{s+1} и $K_{s+1}\varphi_s$ изоморфны. Покажем это. Если две разности в K_s равны, то соответствующие разности в $K_s\varphi_{s-1}$ равны, а равные разности при проектировании переходят в равные. Итак, K_s изоморфно $K_s\varphi_{s-1}\varphi_{\text{пр}} = K_s\varphi_s$.

Пусть теперь имеет место равенство

$$\bar{a}_s - \bar{a}_{i_w} = \bar{a}_{j_w} - \bar{a}_{t_w}, \quad 1 \leqslant i_w, \ j_w, \ t_w \leqslant s-1.$$

Рассмотрим в этом случае равенство (4) с тем же значением w. После проектирования получим

$$\bar{a}_s\varphi_s - \bar{a}_{i_w}\varphi_s = \bar{a}_{j_w}\varphi_s - \bar{a}_{t_w}\varphi_s. \qquad (1.22.5)$$

Для любых p и q, для которых

$$\bar{a}_s - \bar{a}_p = \bar{a}_q - \bar{a}_{t_w},$$

получим равенство $\bar{a}_s\varphi_s - \bar{a}_p\varphi_s = \bar{a}_q\varphi_s - \bar{a}_t\varphi_s$, как в конце б).

Отображение $\varphi = \varphi_{k-1}$ является искомым.

Множество $K\varphi$ имеет размерность r (она не может быть ни меньше r, так как первые r координат точек множеств K и $K\varphi$ совпадают, ни больше r, так как r — максимальная размерность образов K при изоморфном отображении).

Каждое из множеств $K_s\varphi_{s-1}$ тривиальным образом содержится в решетке, порожденной этим множеством. Покажем по индукции, что отношение объема выпуклой оболочки множества $K_s\varphi_{s-1}$ к объему *фундаментального параллелепипеда* этой решетки (*приве-*

денный объем) оценивается сверху числом $\frac{1}{p_s!}2^{s-1-p_s}$. При $s=2$ это отношение равно 1 и $p_s=1$.

В случае а) получается $p_{s+1}=p_s+1$ — мерная пирамида с высотой, равной единице и площадью основания, не превышающей $\frac{1}{p_s!}2^{s-1-p_s}$, объем которой не превышает

$$\frac{1}{(p_s+1)!}2^{s-p_s-1}=\frac{1}{p_{s+1}!}2^{(s+1)-1-p_{s+1}}.$$

В случае б) $p_{s+1}=p_s$.

Пусть существует выпуклый многогранник $D\subset E_n$ и четыре точки $\bar{x}_i$ такие, что $\bar{x}_1, \bar{x}_2, \bar{x}_3\in D$, а $\bar{x}_4\overline{\in} D$ и $\bar{x}_1-\bar{x}_2=\bar{x}_3-\bar{x}_4=\bar{e}$, D_1 — выпуклая оболочка множества $D\bigcup\bar{x}_4$. Тогда $V(D_1)\leqslant 2V(D)$. В самом деле, для проверки этого необходимо лишь заметить, что расстояние от $\bar{x}_4$ до любой грани D, содержащей внутренние точки D_1, меньше, чем максимум расстояний от $\bar{x}_1$ и $\bar{x}_2$ до этой грани (первое расстояние не больше, а второе не меньше $|(\bar{e}_0, \bar{e})|$, где $\bar{e}_0$ — перпендикуляр к упомянутой грани единичной длины).

Ввиду изложенного, $V(K_{s+1}\varphi_s)\leqslant 2V(K_s\varphi_s)$.

Наконец, в случае в) выберем $m+1$ точку вида (4), которые порождают плоскость P_1. Выпуклая оболочка D_2 множества, состоящего из оболочки $K_s\varphi_{s-1}$ и указанных $m+1$ точек, имеет приведенный объем, не превышающий

$$\frac{1}{p_s!}2^{s-1-p_s}\cdot 2^{m+1}=\frac{1}{p_s!}2^{s+m-p_s}.$$

Если дано *выпуклое множество* $D\subset E_n$ объема $V(D)$ и h — расстояние между опорными гиперплоскостями, перпендикулярными $\bar{e}_n$, то множество проекций точек D на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$ имеет объем V_1, для которого

$$V_1=\frac{nV(D)}{h}$$

(максимальный объем основания при данном объеме тела D и данной высоте h имеет пирамида).

Проекция параллельно $L(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m)$ соответствует последовательному проектированию параллельно $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_m$, причем систему этих векторов можно выбрать так, что каждый из них можно поместить внутрь D_2.

В итоге получается приведенный объем, не превышающий

$$\frac{p_s(p_s-1)\ldots(p_s-m+1)}{p_s!}\,2^{s+m-p_s}=\frac{1}{p_{s+1}!}\,2^{(s+1)-1-p_{s+1}},$$

так как $p_{s+1}=p_s-m$.

Приведенный объем для множества $K\varphi$ не превышает, таким образом,

$$\frac{1}{r!}\,2^{k-1-r}.$$

Базис решетки, порождаемой $K\varphi$, можно отобразить на ортонормированный базис E_r, получив, таким образом, изоморфный образ множества K, объем выпуклой оболочки которого не превышает

$$\frac{1}{r!}\,2^{k-1-r}.$$

Покажем теперь, что в этом объеме может содержаться не более $2^{k-1-r}+r$ целых точек из Z_r, при условии, разумеется, что совокупность этих точек имеет размерность r.

Если объем равен $\frac{1}{r!}$ и в нем содержится $r+1$ точка, так что размерность можества этих точек равна r, то параллелепипед, построенный на этих точках, будет фундаментальным, тетраэдр, построенный на этих точках, будет иметь объем $\frac{1}{r!}$, и больше целых точек в нем содержаться не будет.

Всякий многогранник с вершинами в целых точках можно разбить на тетраэдры с вершинами в целых точках объема $\frac{1}{r!}$, прилегающие друг к другу по граням. Этот факт легко доказывается двойной индукцией по размерности r и числу целых точек k в многограннике.

Пусть многогранник имеет объем $\frac{t}{r!}$ и, следовательно, разбивается на t тетраэдров. Можно расположить эти тетраэдры в последовательность так, что каждый тетраэдр прилегает к одному из предыдущих. В первом тетраэдре содержится $r+1$ целая точка, с каждым из последующих добавляется не более одной точки; общее число точек не превышает $r+t$.

В нашем случае $t \leqslant 2^{k-1-r}$. Теорема доказана.

Задачи.

1. Доказать, что $W\left(r, \frac{(k-1)k}{2} + r + 1, k\right) = 2^{k-r-1} + r$.

2. С помощью теоремы 1.22 вычислить значения $W(r, T, k)$ для больших T.

1.23. Оценка $W(r, T, k)$ при $T < Ck$. Оценка (22.1) является весьма слабой. Достаточно сравнить ее с очевидной достижимой оценкой снизу $W(r, T, k) \geqslant k$. Равенство $W(r, T, k) = k$ имеет место, например, при $r = 1$, $T = 2k - 1$.

В главе II получена для достаточно больших k неусиливаемая по порядку оценка для $W(r, T, k)$ сверху для случая $T < Ck$, где C — любая заданная положительная постоянная, не зависящая от k. Именно, справедлива

Теорема. При $T < Ck$, $C \geqslant 2$, существуют положительные постоянные k_0 и c, зависящие лишь от C, так что при $k > k_0$

$$W(r, T, k) < ck.$$

Этот результат является в настоящей работе основным. Доказательству его посвящена вся вторая глава.

1.24. Гипотетическая теорема о величине $W(r, T, k)$. Можно предположить, что неравенство (21.3) не может быть усилено.

Теорема. Величина $W(r, T, k)$ определяется соотношением (21.3), где знак неравенства следует заменить знаком равенства, т. е.

$$W(r, T, k) = 2^{s-2}(k^{(1)} - s + t) + r, \qquad (1.24.1)$$

где

$$s = \left[\frac{2k^{(1)} - 1 - \sqrt{(2k^{(1)} - 1)^2 - 8T^{(1)} + 16}}{2}\right],$$

$$t = T^{(1)} - sk^{(1)} + \frac{s(s+1)}{2} - 1,$$

$$T^{(1)} = T - \frac{(2k-r+2)(r-1)}{2},$$

$$k^{(1)} = k - r + 1.$$

При $T < ck^{\frac{3}{2}}$, $c = c(\varepsilon) > 0$, из (1) и (21.4) следует

$$W(r, T, k) = \theta \cdot 2^{\frac{T}{k} - r} k,$$

где

$$\frac{1}{2} - \varepsilon < \theta < 2 + \varepsilon, \quad \varepsilon > 0.$$

Случаи, когда удается определить точное значение функции $W(r, T, k)$, рассмотренные в задачах 2, 4, 5 п. 1.18 и задаче 1 п. 1.22 и ответах к ним, согласуются с предположением о справедливости высказанной гипотетической теоремы.

Задачи.

1*. Определить $W(1, 3k-2, k)$ без помощи теоремы 1.13.

2**. Определить $W(1, 3k-1, k)$.

3***. Доказать гипотетическую теорему 1.24.

§ 4. АДДИТИВНАЯ ТЕОРИЯ ЧИСЕЛ — НАУКА ОБ ИНВАРИАНТАХ ИЗОМОРФНЫХ ПРЕОБРАЗОВАНИЙ

1.25. Изоморфное преобразование — это аффинное преобразование. Прежде всего следует пояснить смысл утверждения, вынесенного в заголовок данного пункта, и подчеркнуть его ограниченность. Выясним, можно ли найти аффинное преобразование, индуцирующее заданное изоморфное преобразование. Ясно, что при такой постановке вопроса следует рассматривать два изоморфных подмножества евклидова пространства E_n с аффинной группой преобразований.

На первый взгляд, казалось бы, следует дать отрицательный ответ на поставленный вопрос. В самом деле, изоморфное отображение лежащих на прямой множеств $\{0, 1, 3\}$, $\{0, 1, 4\}$ нельзя индуцировать никаким аффинным преобразованием.

Можно привести еще пример множеств $\{(0, 0), (1, 0), (3,0)\}$ и $\{(0, 0), (1, 0), (0, 1)\}$, лежащих на плоскости.

Введем теперь следующее ограничение. Предположим, что размерности обоих рассматриваемых изоморфных множеств, как и размерность евклидова пространства, равны величине r этих множеств. Это условие уже обеспечивает положительное решение вопроса. Заметим, что в первом примере все размерности равны 1, а $r=2$; во втором примере размерность первого из множеств равна единице, а $r=2$.

Теперь мы можем сформулировать и доказать соответствующую теорему.

Теорема. Пусть даны два изоморфные множества K и K', имеющие размерность r.

$$K,\ K' \subset E_r,\ K \sim K',\ K = \{\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{k-1}\},$$
$$K' = \{\bar{a}'_0, \bar{a}'_1, \ldots, \bar{a}'_{k-1}\},\ \bar{a}_i \sim \bar{a}'_i,\ \bar{a}_0 = \bar{a}'_0 = 0.$$

Можно найти такие два базиса решетки Z_r, что если рассматривать точки K по отношению к первому базису, а точки K' — ко второму базису, то соответствующие точки имеют равные координаты.

Следствие. В условиях теоремы 1.25 существует аффинное преобразование E_r на себя, индуцирующее изоморфное отображение K на K'.

Доказательство теоремы. Теорема 1.25 следует из доказательства теоремы 1.22 почти непосредственно.

В самом деле, выберем при данном s из системы векторов

$$\bar{a}_0\varphi_{s-1},\ \bar{a}_1\varphi_{s-1},\ \ldots,\ \bar{a}_{s-1}\varphi_{s-1}$$

линейно-независимую подсистему следующим образом. Включим в нее $\bar{a}_1\varphi_{s-1}$. Если уже выбраны векторы $\bar{a}_{i_1}\varphi_{s-1}, \ldots, \bar{a}_{i_t}\varphi_{s-1}$, то среди векторов $\bar{a}_p\varphi_{s-1}$ выбираем вектор с наименьшим $p > i_t$, который не зависит линейно от выбранных t векторов. Число векторов в получаемой линейно-независимой системе равно p_s. Полученное на последнем шаге множество $K\varphi$ с линейно-независимой системой r векторов можно спроектировать на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_r)$. Процесс построения множеств $K_s\varphi_{s-1}$ и выбора линейно-независимой подсистемы вполне однозначен и одинаков для любых двух изоморфных

множеств K и K'. Описанный процесс приводит к двум базисам Z_r, относительно которых координаты соответствующих точек из K и K' одинаковы.

Теорема 1.25 означает, что для двух изоморфных множеств K и K', удовлетворяющих условиям этой теоремы, существует линейное невырожденное преобразование E_r в себя, переводящее K в K'.

1.26. О возможности индуцирования изоморфизма гомоморфизмом. Если провести рассуждения пункта 1.22 в предположении, что $K \subset E_m$ имеет размерность меньшую или равную r, и что $\bar{a}_0 = 0$, то аналогично получим изоморфное отображение φ множества K в E_{k-1}, причем $K\varphi$ будет иметь размерность r. Выбирая в $K\varphi$ базис (в E_r, порождаемом $K\varphi$), как это сделано в 1.25, мы получим гомоморфное отображение $\varphi^{-1}: E_r \to E_m$, индуцирующее изоморфное отображение $\varphi^{-1}: K\varphi \to K$.

Итак, доказана

Теорема. Пусть $K = \{\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{k-1}\}$, $\bar{a}_0 = 0$, $K \subset Z_m$. Существует такой гомоморфизм $\varphi: Z_r \to Z_m$ и такое множество $K_1 \subset Z_r$ размерности r, что $K_1\varphi = K$ и K_1 изоморфно K.

Таким образом, изоморфизм конечных подмножеств векторов, одно из которых имеет размерность r, можно индуцировать гомоморфным отображением содержащих их векторных пространств.

Мы можем теперь подробнее остановиться на вопросе, затронутом в примечании к п. 1.18. Там отмечена связь между результатами вида упомянутого в п. 1.11 и результатами, которые получаются, если известны значения функций $W(r, T, k)$.

В обоих случаях получается выпуклая замкнутая область D ограниченного объема евклидова пространства E_n. Пусть K' множество всех целых точек области D. В первом случае K входило в изоморфный образ множества K', во втором — оно изоморфно некоторому подмножеству K'' множества K'. Ясно, что в первом случае, вообще говоря, дается бóльшая информация о структуре множества K, чем во втором. Так, например, множество $\{0, 2, 8\}$ содержится во множестве, изоморфном множеству $\{0, 1, 2, 3, 4\}$, то есть в арифметической прогрессии длины 5, мно-

жество же $\{0, 1, 100\}$, которое можно изоморфно отобразить во множество $\{0, 1, 2, 3, 4\}$, имеет длину большую пяти. В пределах этого пункта мы будем говорить, что в первом случае дается полное описание структуры K, во втором — частичное описание структуры K. Оказывается, если размерность n области D равна r, то из частичного описания структуры K можно получить полное. В качестве первого шага для этого нужно применить теорему 1.26. Пусть множество K изоморфно множеству K_1, размерности r, причем объем множества целых точек K', входящих в замкнутую оболочку множества K_1, не превышает $W(r, T, k)$. По теореме 1.26, существует гомоморфизм $\varphi: Z_r \to Z_1$ такой, что $K'\varphi \supset K$, то есть K содержится в образе K' при некотором гомоморфном отображении. В п. 2 будет показано, как с помощью гомоморфного отображения множества K' всех целых точек области D перейти к изоморфному отображению в смысле п. 1.2 множества целых точек некоторой новой области D', образ которого по-прежнему содержит множество K и получить тем самым описание структуры K.

1.27. Общая точка зрения на аддитивные задачи. В своей Эрлангенской программе Феликс Клейн предложил рассматривать геометрию как теорию, изучающую свойства фигур, сохраняющихся при всех преобразованиях из данной группы преобразований.

Изоморфные множества обладают одинаковыми аддитивными свойствами. Мы можем поэтому сформулировать нижеследующую точку зрения на аддитивные задачи.

Аддитивная теория чисел — это теория, изучающая свойства числовых множеств, сохраняющиеся при изоморфных преобразованиях.

Называя *инвариантом* число, характеризующее свойства множества и не меняющееся при изоморфных преобразованиях этого множества, мы можем сказать, что аддитивная теория чисел изучает инварианты изоморфных преобразований.

При конкретизации изучаемых вопросов следует уточнять и вид изоморфного соответствия (см. пп. 1.3 и 1.4). Напомним, что в нашем изложении изоморфизм — это изоморфизм на второй ступени.

1.28. Определение основных инвариантов. Пусть $K \subset Z_n$. Так как всегда возможно изоморфное отображение K в Z_1, то без ограничения общности можно считать, что $K \subset Z_1$. Укажем некоторые основные инварианты множества K.

1) $T = T(2K)$ — основной для аддитивной теории чисел инвариант.

2) R — число различных положительных разностей элементов из K, то есть число элементов во множестве

$$P = \{x,\ x = a_i - a_j,\ a_i > a_j\}.$$

3) Пусть $2K = \{b_1,\ b_2,\ \ldots,\ b_T\}$; r_s — число представлений числа b_s в виде $b_s = a_i + a_j$, $s = 1, 2, \ldots, T$; два представления, отличающиеся порядком слагаемых, считаются различными.

$$M = \sum_{s=1}^{T} r_s^2.$$

4) Пусть $P = \{c_1,\ c_2,\ \ldots,\ c_R\}$; u_s — число представлений числа c_s в виде $c_s = a_i - a_j$, $a_i > a_j$, $s = 1, 2, \ldots, R$.

$$M' = \sum_{s=1}^{R} u_s^2.$$

5) Величина r, определенная в п. 1.18, является инвариантом.

6) Расположим числа $b_i \in 2K$ таким образом, чтобы $r_i \geqslant r_{i+1}$, $i = 1, 2, \ldots, T-1$. Числа $r_1, r_2, \ldots, r_T$ образуют систему инвариантов.

7) Расположим числа $c_i \in P$ таким образом, чтобы $u_i \geqslant u_{i+1}$, $i = 1, 2, \ldots, R-1$. Числа $u_1, u_2, \ldots, u_R$ образуют систему инвариантов.

8) Величина W_K, определенная в п. 1.18, инвариант.

Задача.**

Найти полную систему инвариантов множества K.

§ 5. ПРОБЛЕМАТИКА

1.29. Прямые и обратные задачи. В п. 1.7 мы разделили аддитивные задачи на прямые и обратные. Используя определение инварианта (п. 1.27), мы можем сказать, что прямая задача — это задача вычисления инвариантов числовых множеств, обратная задача — задача нахождения множеств по заданным инвариантам.

В классических аддитивных задачах, как правило, изучаются инварианты конкретных числовых множеств. Если не определять заранее природу складываемых множеств, то можно изучать области возможных значений инвариантов. Тривиальные примеры такого рода смотри в задаче 1, п. 1.29, смотри также более сложные задачи 5, 6 п. 1.30.

В настоящей книге детально изучается лишь одна обратная задача: изучение структуры множества по заданному значению T. Оказывается, что структура K достаточно хорошо определяется при малых T. Предлагаемые методы не могут, однако, дать хороших результатов при больших значениях T. В самом деле, объем точечного множества, в которое изоморфно отображается множество K, при $T = 0(k^{3/2})$ имеет порядок роста, не меньший, чем $2^{\frac{T}{k}-r}$ (см. п. 1.21). С ростом T этот объем быстро увеличивается, а информация о структуре K быстро уменьшается.

Как преодолеть это затруднение? Во-первых, можно привлечь к описанию структуры K новые понятия. Некоторые указания на этот счет см. в п. 1.33. Во-вторых, можно привлечь дополнительную информацию о множестве K, то есть считать известными, кроме T, еще и значения некоторых других инвариантов и решать соответствующие обратные задачи.

Решение обратных задач возможно, разумеется, и для систем инвариантов, не содержащих T.

Некоторые возможные направления исследований иллюстрируются простейшими примерами, рассмотренными в задачах 1—4 п. 1.31.

Задачи:

1. Найти область значений следующих инвариантов а) R, б) M, в) M', г) r.

2. Определить структуру K, если

а) $M' = \frac{(k-1)\,k\,(2k-1)}{6}$; $M' = \frac{(k-1)\,k}{2}$;

б) $R = k-1$; $R = \frac{k\,(k-1)}{2}$;

в) $T = 2k+2$, $M' = \frac{(k-2)\,(k-1)\,(2k-3)}{6} + 3$;

г) $u_1 = k-1$; $u_1 = k-2$.

1.30. Зависимость между инвариантами. В некоторых случаях геометрические инварианты связаны функциональной зависимостью (радиус окружности и ее длина, длины сторон и площадь треугольника).

Можно поставить аналогичную задачу отыскания функциональных зависимостей между теоретико-числовыми инвариантами.

Не всегда зависимость между инвариантами является функциональной. Они могут быть связаны неравенствами (соотношения между сторонами в треугольнике, между периметром и площадью выпуклой фигуры на плоскости).

Нахождение подобных соотношений между теоретико-числовыми инвариантами существенно для корректной постановки обратных задач.

Задачи:

1. Найти M, если $T = 2k - 1$, $2k$, $\frac{k(k+1)}{2}$.

2. Найти M, если $T = 3k - 3$, $r = 2$.

3. Доказать, что $M' = \frac{M - k^2}{2}$.

4. Найти область значений M, если $T = 2k + 1$, $2k + 2$, $2k + b$, где $b < k - 3$.

5*. Найти область значений M при заданном T.

6*. Найти область значений R при заданном T.

1.31. Обратная задача, аналогичная изопериметрической задаче. Известно, что периметр p и площадь S плоской фигуры связаны соотношением $S \leqslant \frac{p^2}{4\pi}$. Ясно, что значения p и S не определяют однозначно вид фигуры. Однако, если S принимает максимальное значение при заданном p, то есть $S = \frac{p^2}{2\pi}$, то рассматриваемая фигура определяется единственным образом и является кругом с радиусом равным $\frac{p}{4\pi}$. Если S мало отличается от $\frac{p^2}{4\pi}$, то фигура мало отличается от круга. Постановка задач, аналогичных описанной выше изопериметрической задаче, совершенно ясна.

Задачи.

1**. Решить „изопериметрическую" задачу для инвариантов T и M.

2**. То же для T и R.

3**. То же для T и r.

4**. То же для T, r и M.

1.32. Определение мономорфного отображения подмножеств. Теорема 1.24, как мы знаем, даже если ее доказать в полном объеме, даст большую информацию о структуре K лишь при малых $W(r, T, k)$, т. е. при малых T. В 1.32 и 1.33 намечается возможное направление дальнейших исследований.

Определение. Рассматриваются подмножества B' и C' множеств B и C с алгебраическими операциями. Отображение B' на C' называется *мономорфным*, если оно взаимно-однозначно и существует естественным образом индуцируемое отображение $2B' \to 2C'$.

Таким образом, если какой-то элемент из $2B'$ представляется двояким образом суммами элементов из B': $b_1 + b_2 = b_3 + b_4$, то из условия существования отображения $2B' \to 2C'$ получим $c_1 + c_2 = c_3 + c_4$.

Как и в п 1.5, получим критерий мономорфности отображения для множеств векторов евклидова пространства: пусть B', $C' \subset E_n$. Взаимно-однозначное отображение $\varphi: B' \to C'$ будет мономорфным, если из $\bar{b}_1 - \bar{b}_2 = \bar{b}_3 - \bar{b}_4$ следует $\bar{c}_1 - \bar{c}_2 = \bar{c}_3 - \bar{c}_4$, где $\bar{b}_i \in B'$, $\bar{c}_i \in C'$, $\bar{b}_i\varphi = \bar{c}_i$, $1 \leqslant i \leqslant 4$.

Для множеств, полученных в теореме 1.6 при $k = 3$ и $k = 4$, возможны мономорфные отображения, указанные на рис. 2.

1.33. О возможности уточнения структуры K. Уточнить структуру K возможно путем нахождения множества K_1, мономорфно отображающегося на K, для которого невелика величина W_{K_1}, определенная в (18.1), и одновременно невелика величина $r(K_1)$.

Чем больше объем выпуклого множества, в котором содержится „накрывающее" множество K_1, тем труднее установить закономерности взаимного расположения точек K_1, а затем и K.

Нежелательность увеличения величины $r(K_1)$ ясно характеризуется тем фактом, что множество K, для которого $T = \frac{k(k+1)}{2}$, $r = k - 1$ и $W_K = k$, мономорф-

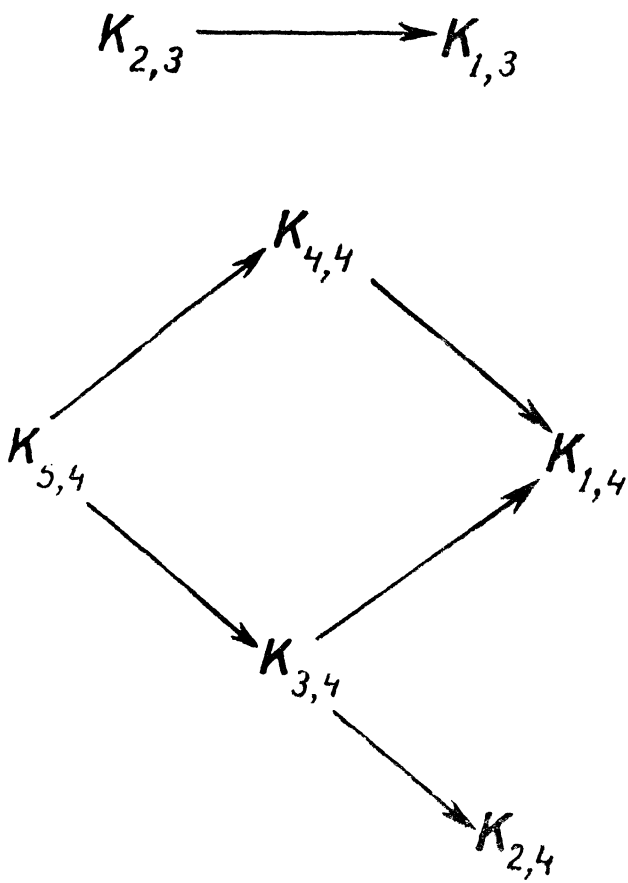


Рис. 2.

но отображается на любое множество, состоящее из k чисел, не давая тем самым никакой информации о структуре последнего.

Определим функцию

$$r(w,\ T,\ k) = \max_{K}\ \min_{W_{K_1} \leqslant w} r(K_1).$$

Минимум здесь берется по всем таким множествам K_1, которые можно мономорфно отобразить на K и которые удовлетворяют условию $W_{K_1} \leqslant w$, где w —

любое заданное натуральное число, такое, что $w \geqslant k$. Максимум берется по всем K с заданным T.

Оценки сверху функции $r(w, T, k)$ и дадут дополнительные сведения о структуре K с заданным T.

Можно надеяться, что значения этой функции не будут большими даже при малых значениях w, при условии, что T не будет слишком большим.

В качестве примера „хорошего" накрытия можно рассмотреть мономорфное отображение множества

$$K_1 = \{0, \bar{e}_1, 2\bar{e}_1, \ldots, (k-s)\bar{e}_1, (k-s+t)\bar{e}_1, \bar{e}_2, \bar{e}_3, \ldots, \bar{e}_{s-1}\}$$

на множество (п. 1.20)

$$K(k, s, t) = \{0, 1, 2, \ldots, k-s, k-s+t, 2(k-s+t), 2^2(k-s+t), \ldots, 2^{s-2}(k-s+t)\},$$

где $2 \leqslant s \leqslant k-1$, $1 \leqslant t \leqslant \max(1, k-s-1)$.

Для K_1 имеют место равенства

$$W_{K_1} = k + t - 1, \quad r(K_1) = s - 1.$$

1.34. Сложение нескольких множеств. Результаты и постановки задач §§ 2—5 настоящей главы могут быть последовательно обобщены на случай сложения s одинаковых множеств.

Назовем *инвариантом s-го порядка* число, характеризующее свойства множества и не меняющееся при изоморфных преобразованиях s-ой ступени этого множества.

Мы не будем приводить конкретные постановки задач, аналогичные разобранным для двукратного сложения; отметим возникновение новых вопросов — задачи пп. 1.30—1.31 могут рассматриваться для совокупности инвариантов, содержащих инварианты разных порядков.

Задачи.

1*. Пусть $T_3 = T(3K)$. Найти область значений T_3 при заданном T.

2*. Пусть $T_s = T(sK)$. Найти область значений T_s при заданном T.

3*. Пусть $M_s = \int_0^1 \left| \sum_{j=0}^{k-1} e^{2\pi i \alpha a_j} \right|^{2s} d\alpha$. Найти область значений M_s при заданном M. Показать, что $M_2 = M$.

1.35. Сложение нескольких различных множеств. Следующим шагом в обобщении рассматриваемой теории является рассмотрение случая сложения нескольких, вообще говоря, различных множеств. В работе [15] рассмотрено обобщение теоремы 1.9 на случай сложения двух различных множеств.

1.36. Обобщение вида алгебраических структур. Мы рассматривали в основном случай, когда $K \subset Z_n$. Можно считать, что K является подмножеством некоторой алгебраической структуры, например, некоммутативной группы.

Глава II

ОСНОВНАЯ ТЕОРЕМА О СЛОЖЕНИИ КОНЕЧНЫХ МНОЖЕСТВ

§ 1. СЛОЖЕНИЕ МНОЖЕСТВ ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ

2.1. Вводные замечания. В настоящей главе излагается метод, с помощью которого описывается структура множеств целых чисел K с малым удвоением ($T < Ck$, $C \geqslant 2$). В настоящем параграфе дается иллюстрация основных идей метода на примере сложения множеств вычетов по простому модулю, представляющем самостоятельный интерес.

Вопрос о сложении множеств вычетов рассмотрели Коши [25] и, независимо, Г. Давенпорт [6]. Они доказали, что если $A \subset S_p$ и $B \subset S_p$, то $T(A+B) \geqslant \geqslant \min(T(A) + T(B) - 1, p)$.

Это неравенство аналогично неравенству 1.8.1.

В 1956 г. А. Воспер [35] рассмотрел простейшую обратную аддитивную задачу для множеств вычетов по простому модулю. Он исследовал структуру A и B при условии, что $T(A+B) = T(A) + T(B) - 1$ и доказал, что если $T(A) + T(B) < p$, $\min(T(A), T(B)) \geqslant 2$, то множества A и B являются арифметическими прогрессиями одинаковой разности по модулю p.

Мы получим ниже усиление упомянутых результатов, ограничиваясь, впрочем, как обычно, лишь случаем сложения одинаковых множеств.

Теорема. Пусть $K = \{a_0, a_1, \ldots, a_{k-1}\}$ — множество, состоящее из k элементов группы S_p классов вычетов

по $\bmod p$, p — простое число. Если $T < 2{,}4k - 3$ и $k < \frac{p}{35}$, то вычеты из K содержатся в арифметической прогрессии по модулю p длины $k + b$, где b определяется из равенства $T = 2k - 1 + b$.

Для доказательства этой теоремы мы используем видоизменение часто применяемого в теории чисел метода тригонометрических сумм, а также элементарные результаты § 2 главы 1, а именно, теорему 1.9.

Прежде чем перейти к доказательству теоремы, сформулируем и докажем вспомогательную лемму, которая будет существенным образом использована и при доказательстве основной теоремы.

2.2. Лемма о неравномерности расположения точек на окружности.

Лемма.* Пусть $\alpha_1, \alpha_2, \ldots, \alpha_k$ числа из полуотрезка $[0,1)$. Пусть β — любое вещественное число. Обозначим через $k_1(\beta)$ количество чисел среди $\alpha_1, \ldots, \alpha_k$, удовлетворяющих неравенству

$$\beta \leqslant \alpha_j < \beta + \frac{1}{2} \pmod 1$$

(то есть найдется такое целое m, что $\beta + m \leqslant \alpha_j < \beta + \frac{1}{2} + m$).

Если предположить, что при любом β

$$k_1(\beta) \leqslant f(k),$$

то

$$|S| \leqslant 2f(k) - k, \quad \text{где } S = \sum_{j=0}^{k-1} e^{2\pi i \alpha_j}.$$

Доказательство. Поскольку при любом вещественном γ

$$\left| \sum_{j=1}^{k} e^{2\pi i (\alpha_j + \gamma)} \right| = \left| \sum_{j=1}^{k} e^{2\pi i \alpha_j} \right|$$

и последовательность $\{\alpha_j + \gamma\}$ тоже обладает свойст-

*) Настоящая лемма сформулирована и доказана в [16]. Здесь приводится ее более простое доказательство, данное Л. П. Постниковой (ДАН СССР, т. 161, № 6, 1965, 1282—1284).

вом, что для нее $k_1(\beta) \leqslant f(k)$, то мы можем сразу считать, что

$$\left|\sum_{j=1}^{k} e^{2\pi i \alpha_j}\right| = \sum_{j=1}^{k} e^{2\pi i \alpha_j} = \sum_{j=1}^{k} \cos 2\pi\alpha_j.$$

Имеем

$$\sum_{j=1}^{k} \cos 2\pi\alpha_j = \sum_{0 \leqslant \alpha_j < \frac{1}{4}} \cos 2\pi\alpha_j - \sum_{\frac{1}{4} \leqslant \alpha_j < \frac{1}{2}} \cos 2\pi\left(\frac{1}{2} - \alpha_j\right) -$$

$$- \sum_{\frac{1}{2} \leqslant \alpha_j < \frac{3}{4}} \cos 2\pi\left(\alpha_j - \frac{1}{2}\right) + \sum_{\frac{3}{4} \leqslant \alpha_j < 1} \cos 2\pi(1 - \alpha_j) =$$

$$= 2\pi\Bigg(\sum_{0 \leqslant \alpha_j < \frac{1}{4}} \int_{\alpha_j}^{\frac{1}{4}} \sin 2\pi t\, dt - \sum_{\frac{1}{4} \leqslant \alpha_j < \frac{1}{2}} \int_{\frac{1}{2} - \alpha_j}^{\frac{1}{4}} \sin 2\pi t dt -$$

$$- \sum_{\frac{1}{2} \leqslant \alpha_j < \frac{3}{4}} \int_{\alpha_j - \frac{1}{2}}^{\frac{1}{4}} \sin 2\pi t dt + \sum_{\frac{3}{4} \leqslant \alpha_j < 1} \int_{1 - \alpha_j}^{\frac{1}{4}} \sin 2\pi t dt \Bigg) =$$

$$= 2\pi \int_0^{\frac{1}{4}} \Bigg(\sum_{0 \leqslant \alpha_j < t} 1 - \sum_{\frac{1}{2} - t \leqslant \alpha_j < \frac{1}{2}} 1 - \sum_{\frac{1}{2} \leqslant \alpha_j < \frac{1}{2} + t} 1 +$$

$$+ \sum_{1 - t \leqslant \alpha_j < 1} 1 \Bigg) \sin 2\pi t dt.$$

Так как

$$k = 2\pi \int_0^{\frac{1}{4}} \Bigg(\sum_{0 \leqslant \alpha_j < 1} 1 \Bigg) \sin 2\pi t dt,$$

то

$$\sum_{j=1}^{k} \cos 2\pi\alpha_j + k = 2\pi \int_0^{\frac{1}{4}} \Big(\sum_{\substack{\alpha_j < \frac{1}{2} - t \\ \alpha_j \geqslant 1 - t}} 1 \Big) \sin 2\pi t dt +$$

$$+ 2\pi \int_0^{\frac{1}{4}} \Big(\sum_{\substack{\alpha_j < t, \\ \alpha_j \geqslant \frac{1}{2} + t}} 1 \Big) \sin 2\pi t dt \leqslant 2f(k),$$

что и требовалось доказать.

Следствие. Если $|S| > 2f(k) - k$, то найдется такое β, что $k_1(\beta) > f(k)$.

2.3. Доказательство теоремы 2.1. Рассмотрим сумму

$$I = \sum_{x_1,\, x_2 \in K} \sum_{x_3 \in 2K} \sum_{a=0}^{p-1} e^{2\pi i a \frac{x_1 + x_2 - x_3}{p}} = \sum_{a=0}^{p-1} S_1^2 S, \qquad (2.3.1)$$

где

$$S_1 = \sum_{j=0}^{k-1} e^{2\pi i \frac{a}{p} a_j}, \quad S = \sum_{x \in 2K} e^{-2\pi i \frac{a}{p} x}.$$

Так как при x, принимающем все значения из полной системы вычетов по модулю p,

$$\sum_{x \in S_p} e^{2\pi i \frac{a}{p} x} = \begin{cases} p, & \text{если } p \text{ делит } a \\ 0, & \text{если } p \text{ не делит } a \end{cases}$$

(см., например, [8]), то

$$I = k^2 p. \qquad (2.3.2)$$

В самом деле, любым двум значениям x_1 и x_2, а число таких пар значений равно k^2, соответствует одно значение x_3, для которого $x_1 + x_2 - x_3 = 0$.

Если предположить, что при любом $a \not\equiv 0 \pmod p$

$$|S_1| \leqslant 0{,}6k,$$

то

$$|I| \leqslant k^2T + \sum_{a=1}^{p-1} |S_1^2||S| \leqslant k^2T + 0{,}6k\Big[\sum_{a=0}^{p-1} |S_1|^2 \sum_{a=0}^{p-1} |S|^2\Big]^{\frac{1}{2}} =$$

$$= k^2T + 0{,}6k\sqrt{kp \cdot Tp}.$$

Так как $T < 2{,}4k$, а $k < \frac{p}{35}$, то

$$|I| < k^2p,$$

что противоречит (2).

Итак, мы доказали, что существует $a' \not\equiv 0 \pmod p$ такое, что

$$|S_1(a')| = \Big|\sum_{j=0}^{k-1} e^{2\pi i \frac{a'}{p} a_j}\Big| > 0{,}6\,k. \qquad (2.3.3)$$

Анализируя приведенные рассуждения, отметим уже теперь некоторые особенности применения метода тригонометрических сумм к решению обратных аддитивных задач.

Решение прямых аддитивных задач методом тригонометрических сумм проводится обычно по следующей схеме (см., например, [8]).

Искомая величина (например, число представлений некоторого числа в виде суммы слагаемых определенного вида) представляется в виде интеграла (или суммы), в подинтегральное выражение которого входят тригонометрические суммы. Интервал интегрирования (соответственно область суммирования) разбивается на две части, называемые главными и дополнительными интервалами. Дальнейшие вычисления проходят в следующей последовательности:

а) Показывается, что модуль тригонометрической суммы на дополнительных интервалах хорошо оценивается сверху. Это позволяет оценить сверху значения интеграла на дополнительных интервалах, которое оказывается небольшим.

б) Часть интеграла, соответствующая главным интервалам, преобразуется и дает главный член асимптотической формулы.

в) Сравнение результатов, получаемых в а) и б), показывает, что величина интеграла на дополнительных

интервалах уходит в остаточный член асимптотической формулы для интеграла на главных интервалах, что и решает вопрос приближенного вычисления искомой величины.

Решение обратной аддитивной задачи также начинается с рассмотрения некоторого интеграла (или суммы), содержащего тригонометрические суммы. В нашем примере это — сумма I (1). Далее, как и для прямой задачи, производится разбиение на главные и дополнительные интервалы. В разбираемом примере главным интервалам соответствует часть суммы (1) для $a=0$.

Дальнейшие вычисления проходят в следующей, обратной обычной, последовательности.

а) Величина рассматриваемого интеграла (суммы) легко вычисляется и, таким образом, является известной с самого начала. В нашем примере $I=k^2p$.

б) Оценивается сверху значение интеграла на главных интервалах. Эта величина оказывается существенно меньшей значения интеграла на всем интервале, полученного в а). В нашем примере получается оценка k^2T, что ввиду $T<2{,}4k$ и $k<\frac{p}{35}$, не превышает $0{,}07k^2p$.

в) Сравнение результатов а) и б) показывает, что значение интеграла на дополнительных интервалах велико. Отсюда получается оценка снизу модуля тригонометрических сумм для некоторого подмножества значений интервала интегрирования — оценка (3) в рассматриваемом нами примере.

Рассмотрение полученной таким образом системы неравенств (в нашем примере одного неравенства), позволяет получить некоторые первоначальные сведения о структуре изучаемого множества (заметим, что факт существования больших значений модуля тригонометрической суммы на главных интервалах не содержит информации о структуре изучаемого множества; так, в нашем примере $S=k$ при $a=0$ и любом K.

Дальнейшие рассуждения содержат три основных этапа, которые можно условно наименовать следующим образом:

1) „Выделение существенной части множества K высшей размерности".

2) „Выделение сжатой части множества K".

3) „Стягивание множества K к его сжатой части".

Этап 1. Из следствия к лемме 2.2 и из (3) следует существование целых чисел u и v (последнее можно определить с помощью сравнения $a'v \equiv 1 \pmod p$) таких, что множество K_1 вычетов из K, сравнимых с числами

$$u + vs, \quad 0 \leqslant s \leqslant \frac{p-1}{2}, \tag{2.3.4}$$

удовлетворяет условию

$$k_1 = T(K_1) \geqslant 0{,}8k. \tag{2.3.5}$$

Пусть вычеты из K_1 получаются при значениях s, входящих в множество

$$P = \{s_0, s_1, \ldots, s_{k_1-1}\}, \quad s_i < s_{i+1}, \quad i = 0,1,\ldots, k_1 - 2.$$

Изменяя, если нужно, значения u и v должным образом, можно удовлетворить требованиям $s_0 = 0$, $d(P) = 1$. Множество чисел P изоморфно множеству K_1.

В самом деле, если для четырех вычетов вида (4), для которых s принимает значения $s^{(1)}$, $s^{(2)}$, $s^{(3)}$ и $s^{(4)}$, имеет место сравнение

$$u + vs^{(1)} + u + vs^{(2)} \equiv u + vs^{(3)} + u + vs^{(4)} \pmod p,$$

то из

$$s^{(1)} + s^{(2)} \equiv s^{(3)} + s^{(4)} \pmod p$$

следует, ввиду (4),

$$s^{(1)} + s^{(2)} = s^{(3)} + s^{(4)}.$$

Таким образом, разным числам из $2P$ не может соответствовать один вычет из $2K_1$.

Мы получили „существенное", ввиду (5), подмножество K_1 множества вычетов K, и показали, что оно изоморфно „множеству высшей размерности" — некоторому множеству целых чисел.

Этап II. Если бы выполнялось неравенство $s_{k_1-1} \geqslant 2k_1 - 2$, то из теоремы 1.9 следовало бы, что

$$T \geqslant T(2K_1) \geqslant 3k_1 - 3 \geqslant 2{,}4k - 3.$$

Итак, $s_{k_1-1} \leqslant 2k_1 - 3$.

Мы показали, что K_1 лежит в короткой прогрессии по $\bmod p$.

Этап III. Если бы в K существовал вычет a, сравнимый с $u + vs$ при

$$4k_1 - 6 < s < p - (2k_1 - 3),$$

то мы имели бы

$$T \geqslant T(2P) + T(P + a) \geqslant 2k_1 - 1 + k_1 = 3k_1 - 1.$$

Итак, все вычеты из K сравнимы с числами $u + vs$ при

$$-(2k_1 - 3) \leqslant s \leqslant 4k_1 - 6.$$

Отсюда следует справедливость доказываемой теоремы, если провести для K все те рассуждения, которые мы провели для K_1.

Задачи.

1*. Получить усиление теоремы 2.1 для случая $T < 3k - 3$.

2*. Ограничение $k < \frac{p}{35}$ не является необходимым. Найти необходимое и достаточное условие этого типа, при котором справедлива теорема 2.1.

3*. Получить обобщение теоремы 2.1 на случай составного модуля.

§ 2. НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ ТЕОРИИ ЧИСЕЛ

В настоящем параграфе содержится сводка теоретико-числовых результатов, используемых в дальнейшем изложении.

2.4. Ряд Фарея и разбиение Фарея. О свойствах ряда Фарея можно прочитать в работе [8]. Здесь мы приводим без доказательства лишь необходимые сведения.

Расположив в порядке возрастания все несократимые рациональные дроби, имеющие положительные знаменатели, не превышающие действительное число N и лежащие между нулем и единицей, мы получим *ряд Фарея* порядка N. Так, для $N = 4.3$ ряд Фарея будет

$$\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}.$$

Если $\frac{p}{q}$ и $\frac{p_1}{q_1}$ две соседние дроби ряда Фарея, то

$$|p_1 q - p q_1| = 1.$$

Если $\frac{p}{q}$ и $\frac{p_1}{q_1}$ две соседние дроби ряда Фарея, то

между этими дробями содержится единственная дробь $\frac{p+p_1}{q+q_1}$ ряда Фарея порядка $q+q_1$.

Если $\frac{p}{q}$, $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$ — три последовательные дроби ряда Фарея порядка N, то интервал

$$\left[\alpha'\left(\frac{p_1}{q_1}\right), \alpha''\left(\frac{p_1}{q_1}\right)\right] = \left[\frac{p+p_1}{q+q_1}, \frac{p_1+p_2}{q_1+q_2}\right),$$

в котором содержится дробь $\frac{p_1}{q_1}$, называется *интервалом дроби* $\frac{p_1}{q_1}$, а совокупность таких интервалов для всех дробей ряда Фарея порядка N называется разбиением интервала $[0, 1)$, соответствующим ряду Фарея порядка N, или, короче, *разбиением Фарея порядка* N. Интервал дроби $\frac{p}{q}$ имеет длину, не превышающую $\frac{2}{qN}$.

2.5. Сведения из геометрии чисел.

Теорема. (Минковский). Пусть $R \subset E_n$ — выпуклая область, симметричная относительно начала, объем которой $V > 2^t$ (возможно, $V = \infty$). Тогда R содержит точку с целыми координатами, не совпадающую с началом.

Доказательство этой теоремы, а также доказательство теоремы 2.6 изложено в работе [7], стр. 182 и 187.

2.6. Сведения из геометрии чисел (продолжение). Пусть R — выпуклая, симметричная относительно начала замкнутая область, имеющая объем V, $0 < V < \infty$. Для каждого l, $1 \leqslant l \leqslant n$, существует наибольшее λ, например λ_l, такое, что λR содержит l линейно независимых точек ([7], стр. 186 — 187). Будем называть λ_l l-м последовательным минимумом области R.

Теорема. (Минковский). Последовательные минимумы удовлетворяют неравенству

$$V\lambda_1\lambda_2 \ldots \lambda_n \leqslant 2^n.$$

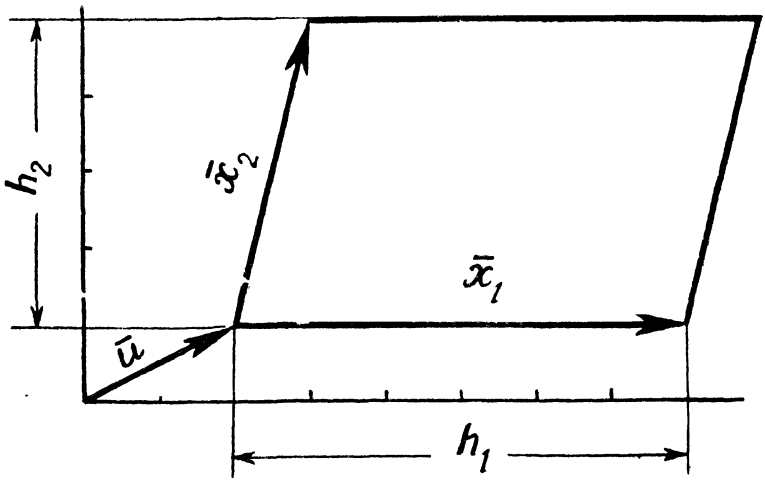


Рис. 3.

§ 3. ФОРМУЛИРОВКА ОСНОВНОЙ ТЕОРЕМЫ

2.7. Канонический параллелепипед.

Определение*. Параллелепипед $H = \{\bar{u} + \sigma_1\bar{x}_1 + \sigma_2\bar{x}_2 + \ldots + \sigma_n\bar{x}_n\}$, где $\bar{u}$, $\bar{x}_i \in E_n$, $0 \leqslant \sigma_i < 1$, $1 \leqslant i \leqslant n$, называется *каноническим*, если

$$(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) = (\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n) \begin{pmatrix} x_{11} x_{12} \ldots x_{1n} \\ x_{22} \ldots x_{2n} \\ 0 \cdot \quad \ldots \ldots \\ \ldots \ldots \ldots \\ x_{nn} \end{pmatrix}, \quad (2.7.1)$$

причем $\bar{u}$ — целый вектор, $h_j = x_{jj}$ — натуральные числа и

$$|x_{ij}| > x_{jj}, \quad i < j, \quad 1 \leqslant j \leqslant n. \quad (2.7.2)$$

Отметим, что число целых точек в каноническом параллелепипеде равно его объему.

Для случая $n = 2$ канонический параллелепипед изображен на рис. 3.

2.8. Формулировка основной теоремы. Нижеследующая теорема о структуре конечных множеств

*) Определение несколько изменено по сравнению с первоначальным определением, приведенным в [18], стр. 156. Там $\bar{u} = 0$ и $h_j \geqslant 2$. Эти требования, однако, не существенны.

целых чисел с малым удвоением ($T < Ck$) является основной в настоящей книге. Она является, по сути, первым серьезным результатом, показывающим плодотворность общих идей главы I, которые там иллюстрировались элементарными примерами.

Теорема. Пусть $K \subset Z_m$, $0 \in K$, $T < Ck$, $C \geqslant 2$, C — постоянная, не зависящая от k. Существует натуральное число n, гомоморфизм φ: $Z_n \to Z_m$, канонический параллелепипед $H \subset E_n$ и положительные постоянные k_0 и c, зависящие лишь от C, такие, что при $k > k_0$

1) $K \subset (H \cap Z_n)\varphi$,
2) $H \cap Z_n$ и $(H \cap Z_n)\varphi$ изоморфны,
3) $T(H \cap Z_n) < ck$,
4) $n \leqslant [C - 1]$.

2.9. Частные случаи, иллюстрирующие теорему 2.8. Пусть $K \subset Z_1$. Рассмотрим вначале случай $2 \leqslant C < 3$; тогда, ввиду 4) из 2.8, $n = 1$, H — интервал, число целых точек которого ввиду 3) не превышает ck. Ввиду 1) K содержится в арифметической прогрессии, число элементов которой не превышает ck. В 1.9 приведена формулировка более сильной теоремы, полученной элементарно.

Пусть $3 \leqslant C < 4$; тогда $n \leqslant 2$. Если $n = 1$, то K содержится в арифметической прогрессии, число элементов которой не превышает ck. Если $n = 2$, то H — параллелограмм. Используя (1.15.4), легко показать, что в качестве H может быть взят прямоугольник.

Итак, в этом случае K содержится в множестве арифметических прогрессий с одинаковой разностью, начала которых содержатся в прогрессии с иной разностью.

Действительно, образы целых точек прямоугольника, лежащих на каждой из прямых, параллельных оси абсцисс, являются арифметическими прогрессиями с одинаковыми разностями. Образ точек прямоугольника, лежащих на некоторой прямой, параллельной оси ординат, будет совокупностью начал этих прогрессий.

2.10. Еще одна формулировка основной теоремы. Формулировка теоремы 2.8 дана в виде, удобном для доказательства. В ней выбран специальный вид области, содержащий множество изоморфное K (канонический параллелепипед) и указан способ получения изоморфного образа K (изоморфное отображение индуцируется

некоторым гомоморфизмом аддитивной группы целых векторов $Z_n \subset E_n$ в аддитивную группу Z_m). Эти уточнения не имеют принципиального характера. Поэтому основную теорему можно сформулировать следующим образом.

Теорема. Если $T < Ck$, $C \geqslant 2$, $K \subset Z_m$, то существуют такие положительные постоянные c, k_0, зависящие только от C и такое натуральное число $n \leqslant [C-1]$, что при $k > k_0$ множество K является подмножеством некоторого множества целых точек K_0, которое изоморфно множеству внутренних целых точек некоторого выпуклого множества $D \subset E_n$ и $T(K_0) < ck$.

Из теоремы 2.10 нетрудно получить уточненную формулировку основной теоремы 2.8 (см. 2.29).

§ 4. ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ

2.11. Вероятностная оценка.

Лемма. Заданы действительное число γ, $\frac{1}{2} < \gamma < 1$, и r случайных величин ξ_i, $1 \leqslant i \leqslant r$, вообще говоря зависимых, каждая из которых принимает два значения 0 и 1.

Если

$$P(\xi_i = 0) = \sum_{\substack{u_j = 0,1 \\ j \neq i \\ u_i = 0}} P_{u_1 u_2 \ldots u_r} \geqslant \gamma, \quad 1 \leqslant i \leqslant r, \qquad (2.11.1)$$

где

$$P_{u_1 u_2 \ldots u_r} = P(\xi_1 = u_1, \ \xi_2 = u_2, \ldots, \ \xi_r = u_r),$$

то для $r > r_0(\gamma)$ существует совокупность значений u_1, $u_2, \ldots u_r$, такая, что

$$P_{u_1 u_2 \ldots u_r} > c(\gamma)(\sqrt{r})^{-1} c_1^r,$$

где

$$c_1(\gamma) = (1-\gamma)^{1-\gamma}\gamma^{\gamma}.$$

Замечание. Так как функция $(\log c_1(u))' = \log \frac{u}{1-u}$ на интервале (0,1) монотонно возрастает и равна нулю при $u = \frac{1}{2}$, то

$$\min_{0<u<1} c_1(u) = c_1\left(\frac{1}{2}\right) = \frac{1}{2}$$

и

$$c_1(\gamma) > \frac{1}{2}.$$

Доказательство. Введем обозначения

$$m = \max_{u_j,\, 1 \leqslant j \leqslant r} P_{u_1 u_2 \ldots r_r}, \quad s_0 = [(1-\gamma)r + 2].$$

Из (1) получим

$$\gamma r \leqslant \sum_{i=1}^{r} P(\xi_i = 0) = \sum_{s=1}^{r} (r+1-s) \sum_{\substack{u_1, u_2, \ldots, u_r \\ \sum_{i=1}^{r} u_i = s-1}} P_{u_1 u_2 \ldots u_r} \leqslant$$

$$\leqslant \sum_{s=1}^{s_0} (r+1-s) \sum_{\sum u_j = s-1} P_{u_1 u_2 \ldots u_r} +$$

$$+ (r - s_0) \sum_{s=s_0+1}^{r} \sum_{\sum u_i = s-1} P_{u_1 u_2 \ldots u_r} \leqslant mr \sum_{s=0}^{s_0-1} C_r^s + r - s_0. \quad (2.11.2)$$

Так как при $r > r_1(\gamma)$

$$\gamma r - (r - s_0) \geqslant 1,$$

$$\sum_{s=0}^{s_0-1} C_r^s < C_r^{s_0-1} \sum_{j=0}^{\infty} \left(\frac{s_0 - 1}{r - s_0 + 2} \right)^j =$$

$$= C_r^{s_0-1} \frac{r - s_0 + 2}{r - s_0 + 3} < \left(\frac{\gamma}{2\gamma - 1} + 1 \right) C_r^{s_0-1},$$

то из (2) следует

$$m > \frac{2\gamma - 1}{3\gamma - 1} \frac{1}{r C_r^{s_0-1}}. \quad (2.11.3)$$

По локальной теореме Муавра — Лапласа (см. [1], стр. 75)

$$\lim_{r \to \infty} \left(\frac{r!}{(s_0 - 1)!\,(r - s_0 + 1)!} (1-\gamma)^{s_0-1} \gamma^{r-s_0+1} : \right.$$

$$\left. : \frac{e^{-\frac{1}{2}(\gamma x_1^2 + (1-\gamma) x_2^2)}}{\sqrt{2\pi\gamma(1-\gamma) r}} \right) = 1,$$

где

$$x_1 = -x_2 = \frac{s_0 - 1 - r(1-\gamma)}{\sqrt{\gamma(1-\gamma) r}}.$$

Так как $\lim_{r\to\infty} x_1 = 0$, найдется такая положительная постоянная $r_2(\gamma)$, что при $r > r_2(\gamma)$

$$C_r^{s_0-1} < \frac{1}{(1-\gamma)^{\frac{3}{2}} r^{\frac{1}{2}}} c_1^{-r}. \qquad (2.11.4)$$

Из (3) и (4) получим при $r > \max(r_1, r_2)$

$$m > \frac{(2\gamma-1)(1-\gamma)^{\frac{3}{2}}}{2} r^{-\frac{1}{2}} c_1^r,$$

так что утверждение леммы справедливо при

$$c(\gamma) = \frac{(2\gamma-1)(1-\gamma)^{\frac{3}{2}}}{2}, \quad r_0(\gamma) = \max(r_1(\gamma), r_2(\gamma)).$$

2.12. О структуре $K \subset E_n$ при $T < Ck$, $C < 2^n$.

Лемма. Дано $K \subset E_n$, $K = \{\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{k-1}\}$,

$$T < Ck, \quad 2 \leqslant C < 2^r, \quad 1 < r \leqslant n.$$

При $k > k_0 = \varepsilon_1^{-i_0}$, $\varepsilon_1 = \dfrac{2^r - C}{3^r (4C)^{2^r}}$, $i_0 = \left[\dfrac{C-1}{\varepsilon_1}\right] + 1$

существует такая гиперплоскость L, при $r < n$ параллельная линейному подпространству $L_1(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-r})$, что

$$T(L \cap K) > \varepsilon_1 k.$$

Доказательство. Предположим, что K обладает нижеследующим свойством: если

$$K' \subset K, \; T(2K') < Dk', \; D \leqslant C, \; k' = T(K') > \varepsilon_1^{-1},$$

то существует $K'' \subset K'$, для которого

$$k'' = T(K'') > ck', \quad T(2K'') < (D - \varepsilon_1) k''.$$

В этом случае можно было бы построить последовательность множеств $R_0 = K, R_1, \ldots, R_p$ таких, что для R_i мы имели бы

$$T(2R_i) < (C - i\varepsilon_1) r_i, \quad r_i = T(R_i), \quad r_i > \varepsilon_1^{i-i_0}$$

и при $p = i_0$ пришли бы к противоречию, получив $T(2R_p) < r_p$, что невозможно.

Итак, для доказательства леммы от противного достаточно теперь показать, что указанное свойство следует из предположения, что для любой (при $r < n$ параллельной L_1) гиперплоскости L выполняется неравенство

$$T(L \cap K) \leqslant \varepsilon_1 k.$$

Множество $2K'$ содержит $\frac{k'(k'+1)}{2}$ сумм $\bar{a}_i + \bar{a}_j$, $0 \leqslant i \leqslant j \leqslant k'-1$. Найдется не менее $\frac{k'+1}{2D}$ таких сумм, равных некоторому вектору $\bar{b}_1$. Через точку $\frac{\bar{b}_1}{2}$ проведем произвольную гиперплоскость B_1 (при $r < n$ параллельную L_1). Из множества точек, попарно симметричных относительно $\frac{\bar{b}_1}{2}$, выберем точки, не лежащие на B_1 и расположенные по какую-нибудь одну сторону от B_1, полученное множество обозначим K_1. Имеем

$$\begin{gathered} k_1 = T(K_1) > \left(\frac{1}{2D} - \varepsilon_1\right) k' \geqslant \frac{1}{4D}\, k', \\ T(2K_1) < T < Dk' < D_1 k_1; \; D_1 = 4D^2. \end{gathered} \tag{2.12.1}$$

Предположим, что уже построены множества $K_1, K_2, \ldots, K_i$, причем формулы (1) содержались в числе формул (2). Примем, что $K' = K_0$, $k' = k_0$, $D = D_0$,

$$\begin{gathered} k_s = T(K_s) > \frac{k_{s-1}}{2D_{s-1}} - \varepsilon_1 k' \geqslant \frac{k_{s-1}}{4D_{s-1}}, \\ T(2K_s) \leqslant D_s k_s, \; D_s = 4^{2^s-1} D^{2^s}, \\ s = 1, 2, \ldots, i, \; i < r. \end{gathered} \tag{2.12.2}$$

Множество $2K_i$ содержит $\frac{k_i(k_i+1)}{2}$ сумм, $\bar{a}_{j_r} + \bar{a}_{j_s}$, $0 \leqslant r, \; s \leqslant k_i - 1$, $j_r \leqslant j_s$. Найдется не менее $\frac{k_i+1}{2C_i}$ таких сумм, равных некоторому вектору $\bar{b}_{i+1}$. Через точки $\frac{\bar{b}_1}{2}, \frac{\bar{b}_2}{2}, \ldots, \frac{\bar{b}_{i+1}}{2}$ проведем произвольную гиперплоскость B_{i+1} (при $r < n$ параллельную L_1). Из

множества точек, попарно симметричных относительно $\frac{\bar{b}_{i+1}}{2}$, выберем точки, не лежащие на B_{i+1} и расположенные по одну определенную сторону от B_{i+1}, полученное множество обозначим через K_{i+1}. Соотношения (2) имеют место и при $s=i+1$. Указанное построение проводим до $s=r$. Так как, ввиду (2),

$$k_r > \frac{k'}{(4D)^{2^{r-1}}(4D)^{2^{r-2}} \dots (4D)^2 4D} > \frac{(4C)^{2^r}}{(4D)^{2^r}} \geqslant 1, \qquad (2.12.3)$$

то K_r не пусто, что обеспечивает возможность построения.

Размерность множества точек $\frac{\bar{b}_1}{2}, \frac{\bar{b}_2}{2}, \dots, \frac{\bar{b}_r}{2}$ равна $r-1$ Во множестве K_r зафиксируем точку $\bar{e}$, максимально удаленную от гиперплоскости B_r. Параллелепипед с вершинами

$$\frac{\bar{b}_1}{2} + \mu_1\left(\frac{\bar{b}_2}{2} - \frac{\bar{b}_1}{2}\right) + \dots + \mu_{r-1}\left(\frac{\bar{b}_r}{2} - \frac{\bar{b}_{r-1}}{2}\right) + \\ + \mu_r\left(\bar{e} - \frac{\bar{b}_r}{2}\right), \ \mu_s = \pm 1, \ s = 1, 2, \dots, r \qquad (2.12.4)$$

обозначим H.

Обозначим через D_{i1}, D_{i2}, $1 \leqslant i \leqslant r$ гиперплоскости параллельные L_1, проходящие через те вершины (4), для которых $\mu_i = 1$ и $\mu_i = -1$ (гиперплоскость D_i, $i \leqslant r-1$ содержит точку $\frac{\bar{b}_{i+1}}{2}$). Если точка $\bar{c}_1 \in K_r$, то пусть $\bar{c}_2 = \bar{c}_1$, если $\bar{c}_1$ находится по отношению к $D_{r-1,1}$ с той же стороны, что и H, в противном случае $\bar{c}_2$ — точка, симметричная $\bar{c}_1$ относительно $\frac{\bar{b}_r}{2}$. С помощью гиперплоскости $D_{r-2,1}$ и точки $\frac{\bar{b}_{r-1}}{2}$ получаем точку $\bar{c}_3$ и т. д. до точки $\bar{c}_r$, полученной с помощью D_{11} и $\frac{\bar{b}_2}{2}$. Точка $\bar{c}_r \in H$ причем, если $\bar{c}_1 \neq \bar{d}_1$, то, очевидно, и $\bar{c}_{11} \neq \bar{d}_{11}$. Поэтому

$$T(H \cap K) \geqslant k_r - \varepsilon_1 k > \frac{1}{2} k_r > \frac{k'}{2(4D)^{2^r-1}}.$$

Гиперплоскости D_{i1}, D_{i2}, $i=1, 2, \ldots, r$, разбивают множество K' на 3^r частей $K^{(j)}$, $j=1, 2, \ldots, 3^r$, $K^{(1)} \subset H$, если исключить точки, лежащие на гиперплоскостях. Покажем, что для одного из множеств $K^{(j)}$, $j \geqslant 2$ имеют место неравенства

$$T(K^{(j)}) = k^{(j)} \geqslant \varepsilon_2 k', \quad T(2K^{(j)}) < (D - \varepsilon_3) k^{(j)},$$

где $\varepsilon_2 = \varepsilon_3 = \varepsilon_1$.

В самом деле, в противном случае, учитывая, что на гиперплоскостях D_{i1}, D_{i2} лежит не более $2\varepsilon_1 r k'$ точек из K_1, мы получили бы

$$T(2K') \geqslant \sum_{\substack{2 \leqslant j \leqslant 3^r \\ k^{(j)} \geqslant \varepsilon_2 k'}} (D - \varepsilon_3) k^{(j)} + 2^r k^{(1)} \geqslant$$

$$\geqslant Dk' + \frac{2^r - D}{2(4D)^{2^r - 1}} k' - 2\varepsilon_1 r D k' - 3^r D \varepsilon_2 k' - \varepsilon_3 k' \geqslant Dk'.$$

Лемма доказана.

2.13. Вложение выпуклого множества в параллелепипед.

Лемма. Пусть выпуклое ограниченное замкнутое множество $D \subset E_n$ имеет объем $V(D)$. Можно найти параллелепипед H, ребра которого $\bar{x}_i$ бу ут удовлетворять условию (7.1), $D \subset H$, $V(H) \leqslant n!\, V(D)$.

Доказательство. Пусть L_1 и L_2 опорные гиперплоскости*), параллельные $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$, прямая l проходит через точки $\bar{a}_1$ и $\bar{a}_2$, такие, что $\bar{a}_1 \in D \cap L_1$, $\bar{a}_2 \in D \cap L_2$, P — множество проекций точек из D на L_1 параллельно l, $V(P)$ — объем P, U — цилиндр с образующей, параллельной l, длины $|\bar{a}_2 - \bar{a}_1|$ и нижним основанием P, $V(U)$ — объем U. Для $n=1$ лемма верна. Пусть она справедлива для всех значений, меньших некоторого n. Тогда существует $n-1$-мерный парал-

*) Гиперплоскость L делит E_n на две части. Если одна из этих частей не содержит D, а L содержит точки D, то гиперплоскость — *опорная*.

лелепипед H_1, удовлетворяющий условию (7.1), такой, что $P \subset H_1$ и $V(H_1) \leqslant (n-1)!\, V(P)$. Пусть W — пирамида с основанием P и вершиной $\bar{a}_2$. Тогда $V(W) \leqslant V(D)$ и $nV(W) = V(U)$, откуда $V(U) \leqslant nV(D)$. Пусть H — параллелепипед с основанием H_1 и такой же образующей, как у цилиндра U. Так как $V(U)/V(P) = V(H)/V(H_1)$, то $V(H) \leqslant (n-1)!\, V(U) \leqslant n!\, V(D)$.

Для случая $n = 2$ см. рис. 4.

Примечание. Если D — параллелепипед, то можно уточнить способ выбора ребер параллелепипеда H с помощью следующего предложения.

Пусть задан параллелепипед D с линейно независимыми ребрами $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$, N_i — цилиндр

$$\sigma_1\bar{x}_1 + \sigma_2\bar{x}_2 + \ldots + \sigma_n\bar{x}_n, \quad -\infty < \sigma_i < +\infty, \quad 0 < \sigma_j < 1, \quad j \neq i,$$

F — полоса между двумя параллельными опорными к D гиперплоскостями.

Тогда i можно определить так, что объем $V(D_1)$ параллелепипеда $D_1 = N_i \cap F$ будет удовлетворять соотношению $V(D_1) < nV(D)$.

В самом деле,

$$\frac{V(D_1)}{V(D)} = \frac{\sum_{j=1}^{n} |(\bar{x}_j, \bar{e})|}{|(\bar{x}_i, \bar{e})|},$$

где $\bar{e}$ — вектор единичной длины, перпендикулярный к опорным гиперплоскостям.

Последнее отношение не превышает n для такого i, для которого $|(\bar{x}_i, \bar{e})|$ принимает максимальное значение.

2.14. Накрытие выпуклого множества каноническим параллелепипедом.

Лемма. Пусть $T(D \cap Z_m) = V_D$, где D выпуклое множество в E_m. Существует натуральное число $n \leqslant m$, мономорфизм $\varphi : Z_n \to Z_m$ и канонический параллелепипед $H \subset E_n$ такие, что $D \cap Z_m \subset (H \cap Z_n)\varphi$, $V(H) < c(m)\, V_D$.

Доказательство. В множестве U плоскостей, содержащих $D \cap Z_m$, выберем плоскость L минимальной

размерности n (если U пусто, то полагаем $L = E_m$). Множество $D_1 = L \cap D$ является выпуклым. Найдется целый репер размерности n, лежащий в D_1, то есть существуют целые векторы $\bar{u}$, $\bar{v}_1$, $\bar{v}_2, \ldots, \bar{v}_n$ такие, что $\bar{u}$, $\bar{u} + \bar{v}_1$, $\bar{u} + \bar{v}_2, \ldots, \bar{u} + \bar{v}_n \subset D_1$, причем $\bar{v}_1$, $\bar{v}_2, \ldots, \bar{v}_n$ — линейно независимы.

Вектор $\bar{v}_1$ может быть выбран таким образом, чтобы длина его среди всех целых векторов, лежащих на прямой $\lambda \bar{v}_1$, $-\infty < \lambda < \infty$ была наименьшей. Пусть $\bar{y}_1 = \bar{v}_1$, $\bar{x}_i$ — целая точка на $\bar{u} + L(\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_i)$, расстояние которой от $\bar{u} + L(\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{i-1})$ минимально, $\bar{y}_i = \bar{x}_i - \bar{u}$, $2 \leqslant i \leqslant n$. Полученный таким образом репер $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n$ будет базисом решетки $L \cap Z_m$.

Линейное преобразование $\varphi_1 : L(\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n) \to E_n$ определим соотношениями $\bar{e}_i = \bar{y}_i \varphi_1$, $1 \leqslant i \leqslant n$. Пусть $D_2 = (D_1 - \bar{u})\varphi_1$. Применяя лемму 2.13 к $D_2 \subset E_n$, мы получим параллелепипед $H_1 \supset D_2$, для которого $V(H_1) \leqslant n!\, V(D_2)$ и выполняется условие (7.1). Метод построения H_1 обеспечивает выполнение условия $x_{jj} \geqslant 1$. Так как выпуклое тело, содержащее лишь одну целую точку, имеет объем, не больший 2^m (это сразу следует из теоремы 2.5), то

$$V(H_1) < n!\ V(D_2) = n!\, V(D_1) < 2^m n! V_{D_1}.$$

Если $L(a, b)$ — интервал длины $l = b - a \geqslant 1$, то содержащий его интервал $L_1 = (a_1, b_1)$ минимальной длины l_1 при целых a_1 и b_1 удовлетворяет, очевидно, условию $l_1 < 3l$. Из этого соображения видно, что можно построить параллелепипед $H_2 \supset H_1$ с целой вершиной $\bar{v}$ и ребрами $\bar{x}_j$, для которых координаты x_{jj} — целые числа, $V(H_2) < 3^n V(H_1)$.

Если для получившегося параллелепипеда H_2 условие $|x_{ij}| < x_{jj}$, для некоторого j не выполняется, то можно применить сдвиг φ_j, определенный нижеследующим преобразованием координат

$$y_{sj} = x_{sj} - q_{sj} x_{jj}, \quad 1 \leqslant s \leqslant j-1$$
$$y_{sj} = x_{sj}, \qquad\qquad j \leqslant s \leqslant n,$$

где целые числа q_{sj} можно подобрать так, чтобы для параллелепипеда $H_2\varphi$ соответствующее условие уже выполнялось. Параллелепипед $H = H_2\varphi_1\varphi_2 \dots \varphi_n$ и будет искомым.

2.15. Основная лемма.

Лемма. Пусть $K \subset Z_m$, $T(K) = k$, $T < Ck$, $C \geqslant 2$, $K \subset D \subset E_m$, где D — выпуклое множество, для которого $T(D \cap Z_m) = V$. Существует натуральное число n, гомоморфизм $\varphi : Z_n \to Z_m$ и выпуклое множество $D_1 \subset E_n$, такие, что

$$1)\ K \subset (D_1 \cap Z_n)\varphi$$

и

$$2)\ T(D_1 \cap Z_n) < c_1 V (V/k)^{-c_2},\ c_1 = c_1(m, C),$$

$$c_2 = c_2(m, C). \qquad (2.15.1)$$

Доказательство леммы проводится в 2.16—2.25.

2.16. Оценка меры множества с большим $|S(\bar{\alpha})|$.

Рассмотрим интеграл

$$W = \sum_{\bar{x}' \in K} \sum_{\bar{x}'' \in K} \sum_{\bar{x}''' \in 2K} \int_0^1 e^{2\pi i \alpha_1 (x_1' + x_1'' - x_1''')} d\alpha_1 \dots$$

$$\dots \int_0^1 e^{2\pi i \alpha_m (x_m' + x_m'' - x_m''')} d\alpha_m = \int_0^1 \dots \int_0^1 S^2 S_1 d\alpha_1 \dots d\alpha_m,$$

где

$$S = \sum_{\bar{x} \in K} e^{2\pi i (\bar{\alpha}, \bar{x})},$$

$$S_1 = \sum_{\bar{x} \in 2K} e^{-2\pi i (\bar{\alpha}, \bar{x})},\quad \bar{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_m),\ \bar{x} = (x_1, x_2, \dots, x_m).$$

Пусть I_1 — та часть области интегрирования, для которой

$$|S(\bar{\alpha})| > \frac{1}{\sqrt{C + \varepsilon}} k,\ \varepsilon > 0, \qquad (2.16.1)$$

Оценим $\operatorname{mes} I_1$:

$$k^2 = |W| \leqslant k^2 T(2K) \operatorname{mes} I_1 + \frac{1}{\sqrt{C+\varepsilon}} k \int_0^1 \dots$$

$$\dots \int_0^1 |SS_1| \, d\alpha_1 \dots d\alpha_m \leqslant Ck^3 \operatorname{mes} I_1 + \frac{\sqrt{C}}{\sqrt{C+\varepsilon}} k^2;$$

$$\operatorname{mes} I_1 \geqslant \frac{\varepsilon}{2(C+\varepsilon)k}.$$

2.17. Разбиение многомерной области интегрирования. Ввиду леммы 2.14 мы без ограничения общности можем считать, что D является каноническим параллелепипедом, который мы будем обозначать H, с ребрами $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_m$.

Область интегрирования интеграла W — куб

$$\alpha_1 \bar{e}_1 + \alpha_2 \bar{e}_2 + \dots + \alpha_m \bar{e}_m, \quad 0 \leqslant \alpha_i < 1, \ 1 \leqslant i \leqslant m,$$

разобьем на части следующим способом. Произведем разбиение отрезка $\alpha_i \bar{e}_i$, $0 \leqslant \alpha_i < 1$, $1 \leqslant i \leqslant n$, соответствующее ряду Фарея порядка $Q_i = \max\left(1, \frac{h_i}{M}\right)$, где $h_i = x_{li}$, $M = (V/k)^{\frac{1}{4m}}$. Для любого i каждое число $\alpha_i = \frac{p_i}{q_i}$, $(p_i, q_i) = 1$, $q_i \leqslant Q_i$, содержится в интервале разбиения $\left[\alpha_i'\left(\frac{p_i}{q_i}\right), \alpha_i''\left(\frac{p_i}{q_i}\right)\right)$. Как обычно, число O будем считать содержащимся в интервале $[\alpha_i''(1) - 1, \alpha_i'(0))$.

Пусть $\bar{a} = \left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_m}{q_m}\right)$, $(p_i, q_i) = 1$, $1 \leqslant q_i \leqslant Q_i$. Через точки $\bar{a} + \alpha_i' \bar{e}_i$ и $\bar{a} + \alpha_i'' \bar{e}_i$, для которых в $\bar{a}$ все $\frac{p_i}{q_i} < 1$, проводим перпендикулярно $\bar{x}_i$ пару гиперплоскостей. Все m пар этих гиперплоскостей ограничивают параллелепипед $H_{\bar{a}}$. Если вместо куба взять в качестве области интегрирования для W совокупность всех параллелепипедов $H_{\bar{a}}$, то ввиду периодичности подинтегральной функции, интеграл W от такой замены области интегрирования не изменится.

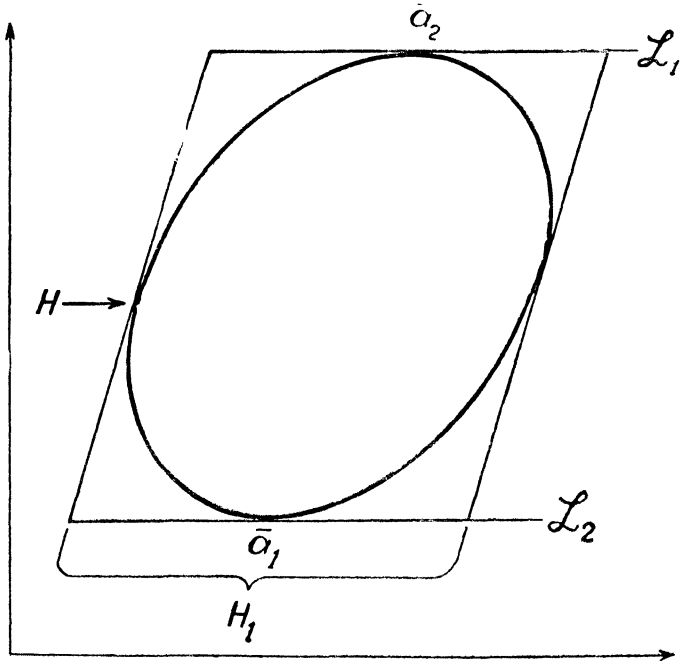


Рис. 4.

Имеет место оценка

$$\left|\frac{p_i}{q_i} - \alpha_i'\right| < \frac{1}{q_i Q_i}, \quad \left|\frac{p_i}{q_i} - \alpha_i''\right| < \frac{1}{q_i Q_i},$$

и такой же величиной оценивается сверху расстояние от $\bar{a}$ до построенных нами плоскостей, перпендикулярных $\bar{x}_i$.

На рис. 5 изображено многомерное разбиение Фарея, как мы будем называть построенное нами разбиение куба на параллелепипеды, для случая $m = 2$, $Q_1 = Q_2 = 3$.

2.18. Оценка меры „главных интервалов". Множество I_1' определим так: $I_1' = \bigcup_{p_i,\, q_i} H_{\bar{a}}$, где $(p_i, q_i) = 1$,

$$1 \leqslant i \leqslant m, \quad 1 \leqslant q_i \leqslant q_0, \quad q_0 = M^2.$$

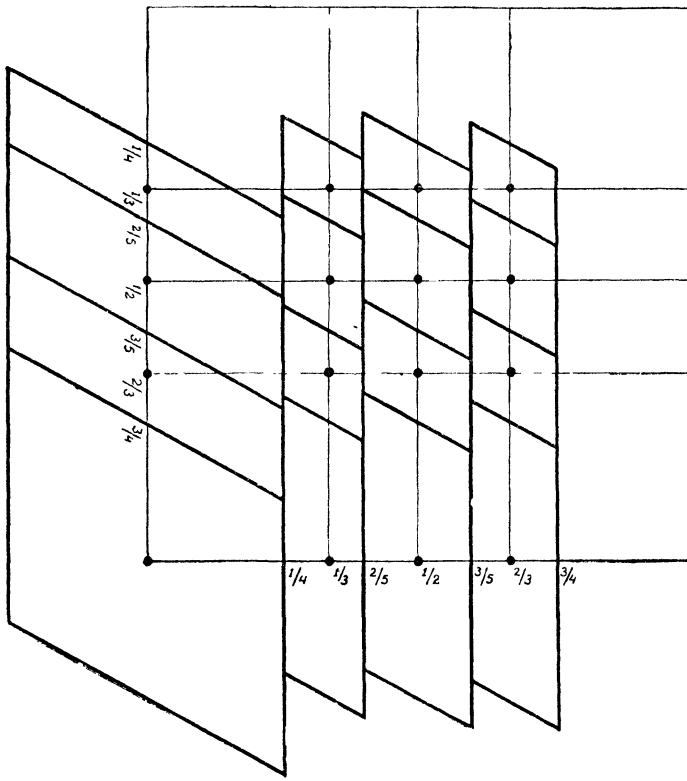


Рис. 5.

Тогда

$$\operatorname{mes} I_1' \leqslant \sum_{p_i,\ q_i} \frac{2^m}{q_1 q_2 \dots q_m Q_1 Q_2 \dots Q_m} \leqslant \frac{2^m}{V} M^{3m}.$$

2.19. Сведение к рациональным тригонометрическим суммам. Пусть для некоторого $\overline{\alpha} \in I_1'$, $\overline{\alpha} \in H_{\overline{a}}$ имеет место неравенство

$$|S(\overline{\alpha})| > \frac{1}{\sqrt{C+\varepsilon}} k, \ \varepsilon > 0.$$

Так как

$$|(\bar{z}, \bar{x})| \leqslant \sum_{i=1}^{m} |(\bar{z}, \bar{x}_i)| < c_3 \sum_{i=1}^{m} \frac{h_i}{q_i Q_i} < \frac{c_3 m}{M},$$

то

$$|(S(\bar{\alpha}) - S(\bar{a})| \leqslant \sum_{\bar{x} \in K} \left| e^{2\pi i (\bar{z}, \bar{x})} - 1 \right| < c_4 \frac{k}{M},$$

откуда при k достаточно большом и V достаточно большом по сравнению с k следует неравенство

$$|S(\bar{a})| \geqslant \frac{1}{\sqrt{C + 2\varepsilon}} k. \qquad (2.19.1)$$

2.20. Построение параллелепипедов $H_{u_1 u_2 \dots u_r} \subset E_{m+}$ с помощью леммы 2.2. Из неравенства (19.1) с помощью леммы 2.2 следует, что для k_1 векторов $\bar{x}$ из K, $k_1 > \frac{1 + \frac{1}{\sqrt{C + 2\varepsilon}}}{2} k$ выполняются условия $\{(\bar{a}, \bar{x})\} = A_{\bar{x}} + \beta + \theta_{\bar{x}}$, $0 \leqslant \theta_{\bar{x}} < \frac{1}{2}$, где $A_{\bar{x}}$ — целое, $\beta = P/Q$, $Q = [q_1, q_2, \dots, q_m]$, $0 \leqslant \beta < 1$.

Мы будем предполагать, что для некоторого натурального числа r существуют r различных векторов $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r$, для каждого из которых выполняется неравенство (19.1). Способ выбора $\bar{a}_i$, $1 \leqslant i \leqslant r$, при наличии некоторых дополнительных связывающих их между собой условий, будет указан позднее, в 2.22.

Ввиду (19.1) для любого i, $1 \leqslant i \leqslant r$, можно указать такое P_i, $0 \leqslant P_i < Q_i$, что для каждого из k_{1i} векторов $\bar{x}$ из K, $k_{1i} > \frac{1 + \frac{1}{\sqrt{C + 2\varepsilon}}}{2} k$, можно указать такое s, $0 \leqslant s < \frac{Q_i}{2}$, что имеет место равенство

$$\frac{p_{i1}}{q_{i1}} Q_i x_1 + \frac{p_{i2}}{q_{i2}} Q_i x_2 + \dots + \frac{p_{im}}{q_{im}} Q_i x_m + Q_i x_{m+i} = P_i + s, \qquad (2.20.1$$

где

$$\bar{a}_i = \left(\frac{p_{i1}}{q_{i1}}, \frac{p_{i2}}{q_{i2}}, \ldots, \frac{p_{im}}{q_{im}}\right), \quad Q_i = [q_{i1}, q_{i2}, \ldots, q_{im}].$$

Для каждого из оставшихся $k_{2i} = k - k_{1i}$ векторов $\bar{x}$ из K можно указать $\frac{Q_i}{2} \leqslant s < Q_i$ такое, что (1) будет иметь место.

Рассмотрим гиперплоскости L_{i0}, L_{i1} и $L_{i2} \subset E_{m+r}$, определяемые соотношением (1), соответственно с $s = 0, \frac{Q_i}{2}, Q_i$. Пусть $P_{i0}(P_{i1})$ — полоса между L_{i0} и L_{i1} (L_{i1} и L_{i2}), включающая $L_{i0}(L_{i1})$; N — цилиндр, ограничиваемый гиперплоскостями, проходящими через каждую из граней $H \subset E_m = L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_m)$ параллельно $L(\bar{e}_{m+1}, \bar{e}_{m+2}, \ldots, \bar{e}_{m+r})$, 2^r параллелепипедов $H_{u_1 u_2 \ldots u_r}$ где $u_i = 0, 1$, $i = 1, 2, \ldots, r$, определим так:

$$H_{u_1 u_2 \ldots u_r} = \left(\bigcap_{i=1}^{r} P_{iu_i}\right) \cap N.$$

Введем обозначение

$$H_1 = \bigcup_{\substack{u_i = 0, 1 \\ 1 \leqslant i \leqslant r}} H_{u_1 u_2 \ldots u_r}.$$

2.21. Применение лемм 2.11 и 2.12. Определим $\varphi_1 : Z_{m+r} \to Z_m$ соотношением

$$(x_1, x_2, \ldots, x_{m+r})\varphi_1 = (x_1, x_2, \ldots, x_m).$$

Задание точки $(x, x_2, \ldots, x_m) \in H$ ввиду (20.1), однозначно определяет точку $(x_1, x_2, \ldots, x_{m+r}) \in H_1$. Поэтому соответствие φ_1 между целыми точками этих двух параллелепипедов является взаимно-однозначным.

Применяя лемму 2.11 для случая, когда

$$P_{u_1 u_2 \ldots u_r} = \frac{T(K\varphi_1^{-1} \cap H_{u_1 u_2 \ldots u_r})}{k} \quad \text{и} \quad \gamma = \frac{1 + \frac{1}{\sqrt{C + 2\varepsilon}}}{2},$$

мы получим, что существует $H_{u_1 u_2 \ldots u_r} = H_2$, такой, что

$$T(K\varphi_1^{-1} \cap H_2) > c_5 (\sqrt{r})^{-1} c_6^r k. \qquad (2.21.1)$$

Пусть даны $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4 \in K$, такие, что

$$\bar{x}_1 + \bar{x}_2 = \bar{x}_3 + \bar{x}_4, \tag{2.21.2}$$

и существуют $\bar{y}_j = \bar{x}_j \varphi_1^{-1} \in H_{u_1 u_2 \dots u_r}$, $1 \leqslant j \leqslant 4$. Пусть $x_s^{(j)}$, $1 \leqslant j \leqslant m+r$, s-я координата $\bar{y}_j$ запишется в виде

$$\frac{p_{i1}}{q_{i1}} Q_i x_1^{(j)} + \frac{p_{i2}}{q_{i2}} Q_i x_2^{(j)} + \dots + \frac{p_{im}}{q_{im}} Q_i x_m^{(j)} + Q_i x_{m+i}^{(j)} = P_i + s_j; \quad 1 \leqslant j \leqslant 4. \tag{2.21.3}$$

Из (2) и (3) получаем

$$Q_i (x_{m+i}^{(1)} + x_{m+i}^{(2)} - x_{m+i}^{(3)} - x_{m+i}^{(4)}) = s_1 + s_2 - s_3 - s_4.$$

Так как $|s_1 + s_2 - s_3 - s_4| < Q_i$, то $s_1 + s_2 - s_3 - s_4 = 0$ и $x_{m+i}^{(1)} + x_{m+i}^{(2)} = x_{m+i}^{(3)} + x_{m+i}^{(4)}$, $1 \leqslant i \leqslant r$, т. е. $\bar{y}_1 + \bar{y}_2 = \bar{y}_3 + \bar{y}_4$.

Мы показали, что $K\varphi_1^{-1} \cap H_{u_1 u_2 \dots u_r}$ и $(K\varphi_1^{-1} \cap H_{u_1 u_2 \dots u_r})\varphi$ изоморфны.

Отсюда и из (1) при достаточно большом r

$$T(2(K\varphi_1^{-1} \cap H_2)) < T < Ck < 2^r k_2, \quad k_2 = T(K\varphi_1^{-1} \cap H_2).$$

Поэтому, ввиду леммы 2.12, существует гиперплоскость $L \subset E_{m+r}$ такая, что $T(L \cap (K\varphi_1^{-1} \cap H_2)) > \varepsilon k$; $\varepsilon = \varepsilon(m, C) > 0$, L параллельна $L(\bar{e}, \bar{e}_2, \dots, \bar{e}_m)$.

2.22. Способ выбора совокупности больших тригонометрических сумм. Покажем, что при любом заданном натуральном r можно выбрать $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_r \in I_1$, для которых имеет место (19.1), таким образом, чтобы при любом выборе $m+r$ целых чисел A_j, $1 \leqslant j \leqslant m+r$, для которых

$$|A_j| \leqslant R, \; R = (V/k)^{\frac{1}{3(m+r)}}, \quad \sum_{j=m+1}^{m+r} A_j^2 > 0, \tag{2.22.1}$$

хотя бы при одном i, $1 \leqslant i \leqslant m$, не выполнялось неравенство

$$|A_1 x_{1i} + A_2 x_{2i} + \dots + A_m x_{mi} - (\bar{a}_1, \bar{x}_i) A_{m+1} - (\bar{a}_2, \bar{x}_i) A_{m+2} - \dots - (\bar{a}_r, \bar{x}_i) A_{m+r}| \leqslant g = (V/k)^{\frac{1}{3m}}. \tag{2.22.2}$$

Предположим, наоборот, что для одного из указанных наборов чисел A_j неравенства (2) имеют место для любого значения i, $1 \leqslant i \leqslant m$. Ввиду (1) найдется $j \geqslant m+1$ такое, что $A_j \neq 0$, $A_s = 0$, $s > j$.

Из (2) получим

$$\frac{1}{|A_j|} G_{ji} - g \leqslant (\bar{a}_{j-m}, \bar{x}_i) \leqslant \frac{1}{|A_j|} G_{ji} + g, \quad 1 \leqslant i \leqslant m,$$

где (2.22.3)

$$G_{ji} = \pm (A_1 x_{1i} + A_2 x_{2i} + \ldots + A_m x_{mi} - (\bar{a}_1, \bar{x}_i) A_{m+1} - (\bar{a}_2, \bar{x}_i) A_{m+2} - \ldots - (\bar{a}_{j-m-1}, \bar{x}_i) A_{j-1}).$$

Условие (3) для одного из i определяет полосу, перпендикулярную $\bar{x}_i$, ширины $\frac{2g}{|\bar{x}_i|}$, совокупность условий для (2) для всех i — параллелепипед H_3 объема, не превышающего $c_7 \frac{g^m}{V}$. При заданных $\bar{a}_1, \bar{a}_2, \ldots,$ $\bar{a}_{j-m-1}$ точка $\bar{a}_{j-m}$ должна находиться в этом параллелепипеде. Пусть $H(\varkappa)$ — параллелепипед, гомотетичный по отношению к H с центром гомотетии в центре H и коэффициентом гомотетии, равным $\varkappa$. Любой параллелепипед $H_{\bar{a}}$ — такой, что $\bar{a} \in H_3$, — содержится в $H_3(2)$. В самом деле, ширина минимальной содержащей $H_{\bar{a}}$ полосы между двумя гиперплоскостями, перпендикулярными $\bar{x}_i$, равна $\frac{2}{q_i Q_i} \leqslant \frac{2M}{h_i} < \frac{2g}{|x_i|}$, т. е. она меньше ширины соответствующей (перпендикулярной $\bar{x}_i$) полосы для H_3. Объединение P_j параллелепипедов $H_3(2)$ для всех возможных наборов $A_1, A_2, \ldots, A_j$ имеет объем, не превышающей $c_8 \frac{g^m}{V} R^j$.

Проведем теперь последовательное построение $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_r$. Пусть точки $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{s-1}$ уже построены. Найдем $\bar{\alpha}$, удовлетворяющее условию (16.1), которое не содержится ни в одном из параллелепипедов $H_{\bar{a}_1}, H_{\bar{a}_2}, \ldots, H_{\bar{a}_{s-1}}$ и не входит в P_s. Такое $\bar{\alpha}$ существует, так как

$$V\left(\bigcup_{i=1}^{s-1} H_{\bar{a}_i} \cup P_s\right) \leqslant r \frac{M^m}{V} + c_9 \frac{g^m}{V} R^{m+r} < \frac{1}{2} \operatorname{mes} I_1.$$

Если $\bar{\alpha} \in H_{\bar{a}}$, то полагаем $\bar{a}_s = \bar{a}$. Так как $\bar{\alpha} \in H_3(2) \subset P_s$, то $\bar{a}_s \in H_3 \subset H_3(2)$ для любого $H_3(2) \subset P_s$.

2.23. Оценка $T(L \cap H_1 \cap Z_{m+r})$*. Пусть L_1 — плоскость минимальной размерности, содержащая $L \cap H_1 \cap \cap Z_{m+r}$. Если размерность L_1 меньше $m+r-1$, то можно указать точки, входящие в $H_1(2)$ такие, что плоскость L_2 минимальной размерности, проходящая через них и $L \cap H_1 \cap Z_{m+r}$, является гиперплоскостью. В самом деле, если бы существовала плоскость, содержащая все точки параллелепипеда $H_1(2)$, то она была бы параллельна каждому из векторов $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{m+r}$. Это следовало бы из того, что L параллельна $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_m)$ и $\bar{e}_{m+1}, \bar{e}_{m+2}, \ldots, \bar{e}_{m+r}$ — ребра H_1. Найдем целый репер, являющийся базисом решетки $L_2 \cap Z_{m+r}$, построенный на нем параллелепипед H_4 размерности $m+r-1$, лежащий в $L_2 \cap H_1(2(n+r))$, т. е. целые векторы $\bar{u}, \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{m+r-1}$ такие, что $\bar{u}, \bar{u}+\bar{v}_1, \bar{u}+\bar{v}_2, \ldots, \bar{u}+\bar{v}_{m+r-1} \in L_2 \cap H_1(2)$.

Рассмотрим множество $Q = \{L_3\}$ плоскостей, параллельных L_2, каждая из которых содержит целые точки. Пусть h минимальное расстояние между двумя акими плоскостями. Площадь параллелепипеда, построенного на $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{m+r-1}$ равна $\frac{1}{h}$.

Предположим вначале, что $h < (V/k)^{-c_{10}}$, $c_{10} = \frac{1}{3(m+r)^2}$.

Рассмотрим вектор $\bar{w}$, перпендикулярный $L_3 \subset Q$ и и имеющий длину h. Для $\bar{w} = w_1\bar{e}_1 + w_2\bar{e}_2 + \ldots + w_{m+r}\bar{e}_{m+r}$ существует $|w_i| \geqslant \frac{h}{\sqrt{m+r}}$. Тогда отрезок вектора, параллельного $\bar{e}_i$, между двумя плоскостями, параллельными L_2, с расстоянием между ними, равным h, имеет длину, не большую $\sqrt{n+r}\,h$. Таким образом, число плоскостей из Q, имеющих с H_1 не-

---

* В работе [20] на стр. 1040 допущена неточность, именно, там рассмотрен лишь случай $A_j = 1$ в (22.3). В настоящем параграфе приведено исправленное рассуждение.

пустое пересечение, не меньше $\frac{c_{11}}{h}$. Фундаментальный параллелепипед H_4 лежит в $H_5 = H_1(2(r+m))$. Поэтому, если $L_4 \subset Q$ имеет непустое пересечение с H_1, то в $L_4 \cap H_5(4)$ лежит параллелепипед, полученный параллельным сдвигом H_4, а значит, есть целая точка. Отсюда следует, что в $L_4 \cap H_5(16)$ лежит фигура, полученная из $L_3 \cap H_1$ параллельным сдвигом на расстояние, равное целому вектору.

Таким образом,

$$T(L_4 \cap H_5(16) \cap Z_{m+r}) \geqslant T(L_3 \cap H_1 \cap Z_{m+r}).$$

Так как $T(Z_{m+r} \cap H_5(16)) < c_{12} T(Z_{m+r} \cap H_1)$,

а

$$T(Z_{m+r} \cap H_5(16)) \geqslant \frac{c_{11}}{h} T(L_3 \cap H_1 \cap Z_{m+r}),$$

то

$$T(L_2 \cap H_1 \cap Z_{m+r}) < c_{13} Vh < c_{14} V (V/k)^{-c_{10}}.$$

Остается рассмотреть случай $h \geqslant \left(\frac{V}{k}\right)^{-c_{10}}$. Векторы $\bar{e}_{m+1}, \bar{e}_{m+2}, \ldots, \bar{e}_{m+r}$ являются ребрами H_1. Укажем остальные m ребер. Так как множество проекций точек H_1 на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_m)$ совпадает с H, то ребра H_1 имеют вид

$$\bar{y}_j = \bar{x}_j + \alpha_{m+1,j}\bar{e}_{m+1} + \alpha_{m+2,j}\bar{e}_{m+2} + \ldots + \alpha_{m+r,j}\bar{e}_{m+r}, \quad 1 \leqslant j \leqslant m.$$

Векторы $\bar{y}_j$ параллельны каждой из L_{i0}, то есть, ввиду (20.1), перпендикулярны векторам

$$\bar{u}_i = \frac{p_{i1}}{q_{i1}}\bar{e}_1 + \frac{p_{i2}}{q_{i2}}\bar{e}_2 + \ldots + \frac{p_{im}}{q_{im}}\bar{e}_m + \bar{e}_{m+i}, \quad 1 \leqslant i \leqslant r.$$

Так как

$$(\bar{y}_j, \bar{u}_i) = (\bar{x}_j, \bar{a}_i) + \alpha_{m+ij} = 0,$$

то

$$\bar{y}_j = \bar{x}_j - (\bar{x}_j, \bar{a}_1)\bar{e}_{m+1} - (\bar{x}_j, \bar{a}_2)\bar{e}_{m+2} - \ldots - (\bar{x}_j, \bar{a}_r)\bar{e}_{m+r}, \quad 1 \leqslant j \leqslant m.$$

Рассмотрим решетку, подобную решетке $L_2 \cap Z_{m+r}$ с коэффициентом подобия $h^{\frac{1}{m+r-1}}$. Площадь фундаментального параллелепипеда такой решетки F равна единице, минимальное расстояние l между точками

решетки не менее $h^{\frac{1}{m+r-1}}$. Пусть R — шар с центром в точке решетки F и радиусом, равным l. Из теоремы 2.6, где $V \geqslant cl^{m+r-1} \geqslant ch$, $\lambda_1 = 1$, следует $\lambda_i \leqslant \frac{2^{m+r-1}}{V}$. Итак, в F существует базис, длины векторов которого не превышают $c_{17}h^{\frac{1}{m+r-1}-1}$, это означает, что в $L_2 \cap Z_{m+r}$ существует базис $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_{m+r-1}$, длины векторов которого не превышают ch^{-1}.

Если $f = \max V_i$, где V_i — объем параллелепипеда, построенного на $\bar{y}_i$, и $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_{m+r-1}$, то существует не менее $[f]$ плоскостей $L \subset Q$, пересечение которых с H_1 не пусто. В самом деле, если h_i — длина проекции $\bar{y}_i$ на перпендикуляр к L_2, то $V_i = h_i \frac{1}{h}$.

Мы имеем

$$V_i = \pm \begin{vmatrix} u_{11} & u_{12} & \ldots & u_{1\,m+r} \\ u_{21} & u_{22} & \ldots & u_{2\,m+r} \\ \ldots & \ldots & \ldots & \ldots \\ u_{m+r-1,1} & u_{m+r-1,2} & \ldots & u_{m+r-1,\,m+r} \\ y_{1i} & y_{2i} & \ldots & y_{m+ri} \end{vmatrix} =$$

$$= |A_1 x_{1i} + A_2 x_{2i} + \ldots + A_m x_{mi} - (\bar{a}_1, \bar{x}_i) A_{m+1} - (\bar{a}_2, \bar{x}_i) A_{m+2} - \ldots - (\bar{a}_r, \bar{x}_i) A_{m+r}|,$$

где $|A_i| < c_{18}h^{-(m+r-1)}$ и $\sum_{j=m+1}^{m+r} A_j^2 \neq 0$, так как L_2 параллельна векторам $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_m$, т. е. $\sum_{j=1}^{m} A_j^2 = 0$.

Ввиду указанного в 2.22 способа выбора $\bar{a}_j$, $1 \leqslant j \leqslant r$, найдется такое i, для которого $V_i \geqslant g$, так) что и в случае неравенства $h \geqslant (V/k)^{-c_{10}}$ мы получим

$$T(L_2 \cap H_1 \cap Z_{m+r}) < c_{19} V g^{-1} < c_{20} V (V/k)^{-c_{21}}.$$

2.24. Оценка числа гиперплоскостей, содержащих прообразы векторов из K. Оценим сверху количество

$L_3 \subset Q$, для которых $T(L_3 \cap H_1 \cap K\varphi_1^{-1}) > 0$. Найдутся такие $H^0_{u_1u_2\dots u_r}$ и L_5, для которых $T(L_5 \cap H^0 \cap K\varphi_1^{-1}) \geqslant \frac{\varepsilon_1}{2^m} k$. Пара множеств $H^{(1)}_{u_1u_2\dots u_r}$ и $H^{(2)}_{u_1u_2\dots u_r}$ изоморфна в смысле 1.4 паре $(H^{(1)} \cap Z_{m+r})\varphi_1$ и $(H^{(r)} \cap Z_{m+r})\varphi_1$. Пусть r_1 — число плоскостей $L_5 \subset Q$, в пересечении которых с $H_{u_1u_2\dots u_r}$ содержатся точки, соответствующие точкам из K. Тогда $T \geqslant r_1 \cdot \frac{\varepsilon_1}{2^m} k$. Отсюда $\frac{r_1\varepsilon_1}{2^m} \leqslant C$, $r_1 \leqslant \frac{2^m C}{\varepsilon_1}$. Всего в H_1 имеется не более $r_2 \leqslant \frac{4^m C}{\varepsilon_1}$ плоскостей $L^{(1)}, L^{(2)}, \dots, L^{(r_2)} \subset Q$, в пересечении которых с H_1 содержатся точки, соответствующие точкам из K.

2.25. Завершение доказательства леммы. Ввиду рассуждений, проведенных в 2.23 и 2.24, мы получим, что $\left(\left(\bigcup_{s=1}^{r_2} L^{(s)}\right) \cap H_1 \cap Z_{m+r}\right)\varphi_1 \supset K$,

$$T(L_s^{(s)} \cap H_1 \cap Z_{m+r}) < c_{22} V (V/k)^{-c_{23}}, \quad 1 \leqslant s \leqslant r_2.$$

Каждый из r_2 подобных параллелепипедов $H'' \cap L_s$, $1 \leqslant s \leqslant r_2$, заключим в $m + r - 1$-мерный канонический параллелепипед $H^{(s)}$ с помощью леммы 2.14 (φ_1 — тождественное отображение) с высотами $h_1^{(s)}, h_2^{(s)}, \dots, h_{m+r-1}^{(s)}$. Пусть H_6 — канонический параллелепипед с ребрами, параллельными ребрам $H^{(s)}$ и $h_{i6} = \max h_i^{(s)}$, $1 \leqslant i \leqslant m + r - 1$.

Пусть $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_s$ — вершины параллелепипедов $H^{(s)}$.

Гомоморфное отображение φ_2: $E_{m+r-1+r_1} \to E_{m+r}$ определим соотношениями $\bar{e}_i\varphi_2 = \bar{e}_i$, $1 \leqslant i \leqslant m + r - 1$, $\bar{e}_{m+r-1+s}\varphi_2 = \bar{a}_s$, $1 \leqslant s \leqslant r_1$.

Пусть H_7 — канонический параллелепипед с ребрами $\bar{x}_1^{(s)}, \bar{x}_2^{(s)}, \dots, \bar{x}_{m+r-1}^{(s)}$, $2\bar{e}_{m+r}, 2\bar{e}_{m+r+1}, \dots, 2\bar{e}_{m+r-1+r_1}$, где $\bar{x}_j^{(s)}$ — ребра H_6. Мы имеем

$$(H_7 \cap Z_{m+r-1+r_1})\varphi_2\varphi_1 \supset K,$$

$$V(H_7) < c_{24} V (V/k)^{-c_{23}}.$$

Остается положить $H = H_7$, $n = m + r - 1 + r_1$, $\varphi = \varphi_2\varphi_1$. Лемма 2.15 доказана.

2.26. Переход к изоморфному множеству.

Лемма. Если заданы гомоморфизм φ: $Z_n \to Z_m$, такой, что Z_n/N является *группой без кручения*, $N = Ker\varphi$, и канонический параллелепипед $H \subset E_n$, то можно указать такие гомоморфизм φ_1: $Z_s \to Z_m$, $s \leqslant n$ и канонический параллелепипед $H_1 \subset E_s$, что

1) $(H_1 \cap Z_s)\varphi_1 \supset (H \cap Z_n)\varphi$,
2) $(H_1 \cap Z_s)\varphi_1$ и $H_1 \cap Z_s$ изоморфны,
3) $V(H_1) < c(n)\, V(H)$.

Доказательство. Если множества $H \cap Z_n$ и $(H \cap Z_n)\varphi$ не изоморфны (в противном случае доказывать нечего), то существуют две целые точки $\bar{a}$, $\bar{b} \in 2H$ такие, что $\bar{a}\varphi = \bar{b}\varphi$. Пусть $\bar{d}_1$ — целый вектор наименьшей длины среди целых векторов, коллинеарных $\bar{b} - \bar{a}$. Так как Z_n/N — группа без кручения, то $\bar{d}_1\varphi = 0$. Базис решетки Z_n, содержащий $\bar{d}_1$, построим следующим образом. Пусть i таково, что $(\bar{d}_1, \bar{e}_i) \neq 0$. В параллелепипеде с ребрами $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_n, \bar{d}_1$ (или на его границе) выберем точку $\bar{d}_2$, наиболее близкую к $L_1(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_{n-1}, \bar{d}_1)$, но не принадлежащую L_1, в параллелепипеде с ребрами $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_{n-1}, \bar{d}_1$, возьмем точку $\bar{d}_3$, наиболее близкую к $L_2(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_{n-2}, \bar{d}_1)$ и т. д.

К параллелепипеду H применим лемму 2.14, полагая для определения φ, $\bar{y}_{n+1-i} = d_i$, $1 \leqslant i \leqslant n$. Мы получим канонический параллелепипед H', для которого $(H' \cap Z_n)\varphi \supset H \cap Z_n$. Пусть h_n это n-ая высота H', P — площадь его основания. Тогда $h_n V(P) < c_1 V(H)$.

Рассмотрим плоскости $x_n = t$, $t = a$, $a+1, \ldots, a + h_n - 1$, каждая из которых имеет с H' непустое пересечение P_t объема $V(P_t) = \bar{P}$. Пусть $\bar{P}_t$, $1 \leqslant t \leqslant h_n$ — проекции P_t на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$, Q — выпуклая оболочка множества $\bigcup_{t=1}^{h_n} \bar{P}_t$.

Из способа выбора d_1 следует, что существует i такое, что $2\bar{P}_i \cap 2\bar{P}_{i+1}$ не пусто. Отсюда следует, что $V(Q) < c_2 h_n V(P) < c_3 V(H)$.

С помощью леммы 2.13 заключим Q в параллелепипед H'', для которого выполняется условие (2. 7. 1). Так как для этого параллелепипеда $\bar{x}_{jj} \geqslant 1$ (так как $Q \supset \bar{P}_a$, P_a это $n-1$-мерный канонический параллелепипед), то H'' содержится в каноническом параллелепипеде H''', $V(H''') < c_4 V(H'')$ (см. окончание доказательства леммы 2.14).

Пусть $\bar{v} \in Z_n$, $\bar{\bar{v}}$ — проекция $\bar{v}\varphi$ на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$. Гомоморфизм φ: $Z_n \to Z_m$ индуцирует гомоморфизм φ_1: $Z_{n-1} \to Z_m$ так, что если $\bar{v}\varphi = \bar{\bar{v}}_1 \in Z_m$, то $\bar{\bar{v}}\varphi_1 = \bar{\bar{v}}_1$. Если $(H''' \cap Z_{n-1})\varphi$ еще не изоморфно $H''' \cap Z_{n-1}$, то повторяем все приведенное рассуждение вторично и т. д.

2.27. Усиление леммы 2.26.

Лемма. Если заданы гомоморфизм φ: $Z_n \to Z_m$ такой, что Z_n/N является группой без кручения, $N = Ker\,\varphi$, канонический параллелепипед $H \subset E_n$, p — натуральное число, $p \geqslant 2$, то можно указать такие гомоморфизм φ_1: $Z_s \to Z_m$, $s \leqslant n$ и канонический параллелепипед $H_1 \subset E_s$, что

1) $(H_1 \cap Z_s)\varphi_1 \supset (H_1 \cap Z_n)\varphi$,

2) не существует такой пары целых точек, что

$$\bar{a},\ \bar{b} \in pH,\ \bar{a}\varphi_1 = \bar{b}\varphi_1,$$

3) $V(H_1) < c(n, p)\, V(H)$.

В 2.26 настоящая лемма доказана для случая $p=2$. Для любого $p \geqslant 2$ доказательство проходит без всяких изменений.

2.28. Доказательство теоремы 2.8. Построим последовательность гомоморфизмов φ_i: $Z_{n_i} \to Z_m$ и канонических параллелепипедов $H_i \subset E_{n_i}$ таких, чтобы при любом i для φ_i, H_i, n_i выполнялись условия 1), 2) и 4) теоремы и условие $V_i < V_{i-1}/2$, $i \geqslant 2$.

При $i = 1$ в качестве φ_i берем тождественное отображение φ_1: $Z_m \to Z_m$, а в качестве $H_1 \subset E_m$ берем, например, один из канонических параллелепипедов наименьшего объема, среди содержащих множество K. Пусть наша последовательность построена для $1 \leqslant i \leqslant s$. Применив леммы 2.15 и 2.26, мы получим

гомоморфизм φ_{s+1}: $Z_{n_{s+1}} \to Z_{n_s}$ и канонический параллелепипед $H_{s+1} \subset E_{n_{s+1}}$, такие, что удовлетворяются требования 1) и 2) теоремы.

Мы можем считать, что множество прообразов точек множества K, содержащихся в H_{s+1}, имеет размерность n_{s+1}, так как в противном случае, применив к $H_{s+1} \cap L$ (L — гиперплоскость, содержащая прообразы точек множества K) лемму 2.14, мы могли бы снизить размерность.

Отсюда, ввиду леммы 1.14, следует выполнение условия 4).

Ввиду условия 2) леммы 2.15, $V_{s+1} < c_1 V_s (V_s/k)^{-c_2}$, где c_1, c_2 — положительные постоянные, зависящие лишь от C. Можно указать достаточно большую положительную постоянную c_3 такую, что при $V_s > c_3 k$ будет выполняться неравенство $V_{s+1} < V_s/2$. Построение последовательности мы доведем до такого i_0, при котором $V_{i_0} < c_3 k$. Тогда $\varphi = \varphi_{i_0}$, $H = H_{i_0}$ будут искомыми, так как и последнее условие 3) будет выполняться.

Замечание. Для множеств K, удовлетворяющих условиям $a_0 = 0$, $a_{k-1} < ck$, где c — постоянная в условии 3) теоремы 2.8, эта теорема, очевидно, не дает никакой дополнительной информации о структуре таких множеств. Для малых T ($\leqslant 3k - 3$) элементарный метод дает здесь более сильные результаты.

Таким образом, метод тригонометрических сумм применим к исследованию достаточно „редких" множеств, подобно тому, как при решении прямых аддитивных задач метод тригонометрических сумм дает результаты лишь для достаточно больших чисел.

2.29. Связь между различными формулировками основной теоремы. Если предположить, что размерность K равна m, а размерность $K\varphi^{-1} \cap H$ равна n (что имеет место ввиду рассуждений п. 2.28), то ввиду того, что гомоморфное отображение сохраняет линейную зависимость, будет выполняться неравенство

$$m \leqslant n. \qquad (2.29.1)$$

Применяя основную теорему к изоморфному отображению K в E_r и учитывая (1), мы получаем теорему 1.23.

Наоборот, из теоремы 1.23, применяя лемму 2.14 и теорему 1.26, можно получить теорему 2.8. Таким же образом теорема 2.8 получается из теоремы 2.10.

§ 5. АДДИТИВНЫЕ СВОЙСТВА МНОЖЕСТВ РОТА

2.30. Аддитивные свойства множеств Рота. Рот [36] доказал, что если в множестве K нет арифметических прогрессий длины 3, то есть, если для любых a_i, a_j, $a_t \in K$,

$$a_i + a_t \neq 2a_j, \tag{2.30.1}$$

то

$$\lim_{k\to\infty} \frac{a_{k-1} - a_0}{k} = +\infty. \tag{2.30.2}$$

Для множеств с таким свойством справедлива следующая

Теорема. Рассмотрим множество $K \supset 0$, для любых трех элементов a_i, a_j, a_t которого имеет место (1). Тогда

$$\lim_{k\to\infty} \frac{T}{k} = +\infty.$$

Доказательство. Предположим, что существует постоянная $C > 0$, такая, что $T < Ck$. Рассмотрим канонический параллелепипед $H \subset E_n$, получающийся применением теоремы 2.8. Заключим H в параллелепипед H_1 с ребрами, параллельными ребрам H, с центром симметрии в 0 и объемом $V(H_1) \leqslant 2^n V(H)$. Так как $H_2 = \frac{c_1}{k^{\frac{1}{n}}} H_1$ при достаточно большом c_1 имеет объем, больший 2^n, то в H_2 содержится целая точка, отличная от центра, а в H_1 содержится отрезок некоторой прямой l, содержащий не менее $\frac{2}{c_1} k^{\frac{1}{n}}$ целых точек.

Построим базис $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ решетки Z_n, такой, что $\bar{a}_n$ и l параллельны Пусть H_3 — параллелепипед, канонический по отношению к этому базису, содержащий H_1, и такой, что $V(H_3) \leqslant n!\ V(H_1)$ (см. примечание к лемме 2.13). Основание H_3 — параллелепипед H_4, канонический относительно базиса $\bar{a}_1, \ldots, \bar{a}_{n-1}$ и объема, не

превышающего $c_2 k^{1-\frac{1}{n}}$. Мы получили, что все целые точки параллелепипеда H содержатся в отрезках, число которых равно $V(H_4)$, а число целых точек в каждом равно $V(H_3)/V(H_4)$. Так как $k \leqslant V(H_3) < c_4 k$, а $V(H_4) \leqslant c_2 k^{1-\frac{1}{n}}$, то

$$V(H_3)/V(H_4) \geqslant c_3 k^{\frac{1}{n}}. \tag{2.30.3}$$

В H содержится k прообразов множества K. Поэтому найдется такой отрезок, в котором содержится не менее $k/V(H_4) > V(H_3)/c_4 V(H_4)$ прообразов. Ввиду (3) и (2) найдутся три точки $\bar{b}_1$, $\bar{b}_2$, $\bar{b}_3$, являющиеся прообразами точек K, для которых $\bar{b}_1 + \bar{b}_3 = 2\bar{b}_2$, что противоречит условию (1) теоремы.

Глава III

СЛОЖЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, МНОЖЕСТВ ВЫЧЕТОВ И ТОЧЕЧНЫХ МНОЖЕСТВ

Настоящая глава посвящена приложениям.

Получено усиление теоремы Кнезера для случая сложения последовательностей положительной асимптотической плотности и доказательство гипотезы Эрдеша для последовательностей нулевой плотности.

Изучена структура множеств вычетов по простому модулю и точечных множеств положительной меры n-мерного евклидова пространства.

§ 1. КРАТКИЙ ОБЗОР ИЗВЕСТНЫХ РЕЗУЛЬТАТОВ

3.1. Обозначения.

A — возрастающая последовательность целых неотрицательных чисел:

$$A = \{a_0, a_1, \dots, a_i, \dots\}, \quad a_{i+1} > a_i, \quad i \geqslant 0,$$

$$d(A) = \lim_{k \to \infty} (a_1 - a_0, a_2 - a_0, \dots, a_k - a_0);$$

здесь $(a_1 - a_0, a_2 - a_0, \dots, a_k - a_0)$ — общий наибольший делитель чисел $a_1 - a_0, a_2 - a_0, \dots, a_k - a_0$.

$A(x)$, $A_2(x)$ — число натуральных чисел последовательности A (соотв. $2A$), не превосходящих x.

$\alpha' = \alpha'(A)$ — *шнирельмановская плотность* последовательности, определяемая равенством

$$\alpha' = \inf_{x \in N} \frac{A(x)}{x},$$

где N — множество натуральных чисел.

$\alpha = \alpha(A)$ — *асимптотическая плотность* последовательности, определяемая равенством

$$\alpha = \lim_{x \to \infty} \frac{A(x)}{x},$$

$$\gamma = \alpha(2A).$$

3.2. Метрическая аддитивная теория чисел. Л. Г. Шнирельман [22] начал изучать аддитивные свойства весьма широкого класса целочисленных последовательностей с положительной шнирельмановской плотностью.

Для случая сложения двух одинаковых последовательностей А. Я. Хинчин [21] получил следующий результат:

Если $\alpha'(A) = \alpha$, $\alpha'(2A) = \gamma$, то при $a_0 = 0$

$$\gamma \geqslant \min(2\alpha, 1). \tag{3.2.1}$$

Манн [32] получил доказательство аналогичной теоремы для случая сложения различных последовательностей. *)

М. Кнезер [30] получил аналог теоремы Манна для случая сложения последовательностей, имеющих положительные асимптотические плотности.

Приведем несколько видоизмененную формулировку теоремы М. Кнезера [30] для случая сложения двух одинаковых последовательностей.

Теорема. Мы имеем $\gamma \geqslant \min(2\alpha, 1)$ или существует такое натуральное число g и h вычетов $r_1, r_2, \ldots, r_h$, по модулю g, что для них

$$T(2\{r_1, r_2, \ldots, r_h\}) = 2h - 1,$$

$$\alpha > \frac{h - \frac{1}{2}}{g}, \tag{3.2.2}$$

и A содержится в h классах вычетов, определяемых вычетами $r_1, r_2, \ldots, r_h$.

В работе [23] П. Эрдеш сформулировал на стр. 118 гипотезу 15, являющуюся аналогом теоремы А. Я. Хинчина для последовательностей нулевой плотности. П. Эрдеш высказал предположение, что выполняется неравенство

$$\delta = \overline{\lim_{x \to \infty}} \frac{A_2(x)}{A(x)} \geqslant 3,$$

---

*) Формулировку и подробное доказательство теоремы Манна можно найти в книге А. Я. Хинчина „Три жемчужины теории чисел".

если

$$\lim_{x\to\infty}\frac{A(x)}{x}=0.$$

Были доказаны также сходные теоремы для случаев сложения множеств вычетов по простому модулю (Коши [25], Давенпорт [6], п. 2.1), сложения точечных множеств с положительной мерой (Хенсток и Макбет [28]).

В настоящей главе получены усиления большинства из упомянутых результатов.

3.3. Работы по обратным аддитивным задачам. Понятие обратной аддитивной задачи (п. 1.7) позволяет с единой точки зрения рассматривать многие ранее опубликованные работы, посвященные решению разнообразных конкретных вопросов аддитивной теории чисел.

В работе П. Эрдеша [27] и работах [10] и [11] рассматривались обратные аддитивные задачи нижеследующего типа для разбиений чисел на неограниченное число слагаемых.

Пусть $q(u)$ — число решений неравенства

$$a_1n_1+a_2n_2+\ldots+a_rn_r+\ldots\leqslant u$$

в целых неотрицательных числах n_i, где $a_i\in A$.

Пусть $q(u)$ задано. Каково $A(u)$?

В [27] П. Эрдеш рассмотрел и такую обратную задачу.

Если $\lim\limits_{u\to\infty}q(u)/cu^{2\alpha}=1$, где $q(u)$ — число решений неравенства

$$a_i+a_j\leqslant u,$$

то

$$\lim_{u\to\infty}A(u)/c_1u^{\alpha}=1,\ c_1=c_1(c).$$

В. Ташбаев в [9] в 1960 году рассмотрел вопрос об остаточном члене для этой обратной задачи.

Укажем на связь обратных задач с вопросами распределения простых чисел. Если положить $q(u)=[e^u]$, то $a_i=\ln p_i$, где p_i есть i-е простое число. Поэтому задачу распределения простых чисел можно рассматривать как обратную задачу аддитивной теории чисел указанного вида (Берлинг [24], Бредихин [2] — [5]).

Легко переформулировать теорему Кнезера [30] таким образом, чтобы она давала решение обратной

задачи: если $\alpha(A)=\alpha>0$ и $\alpha(2A)<2\alpha$, $\alpha\leqslant\frac{1}{2}$, то A имеет структуру, определяемую предыдущей теоремой.

Если в первоначальной формулировке теорема Кнезера носила законченный характер, то в новой формулировке естественно возникает вопрос об ее усилении: если $\alpha(A)=\alpha$ и $\alpha(2A)<C\alpha$, $C\geqslant 2$, то какова структура A? (п. 3.6).

Решение обратных задач аддитивной теории чисел дают исследования, выясняющие, в каких случаях достигаются нижние границы оценок в прямых метрических теоремах.

А. Г. Воспер [38] в 1956 г. исследовал случай сложения подмножеств аддитивной группы вычетов по простому модулю. Теорема 2.1 является усилением его результатов.

Х. Б. Кемперман в [29] решил обратную задачу для абелевых групп. Он выяснил структуру подмножеств B и C абелевой группы с числами элементов b и c при условии, что число элементов в $B+C$ не превышает $b+c-1$. Работа Кемпермана является естественным продолжением цитированных работ Кнезера, у которого фигурирует аддитивная группа вычетов по любому модулю, и Воспера, у которого соответствующая задача решена для аддитивной группы вычетов по простому модулю.

В работе Хенстока и Макбета [28] выясняется вид точечных множеств положительной меры при условии, что мера их суммы принимает минимальное возможное значение (неравенство Бруна-Минковского).

В работах [12] — [20] содержатся результаты, основная часть которых излагается в настоящей книге.

§ 2. СЛОЖЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПОЛОЖИТЕЛЬНОЙ АСИМПТОТИЧЕСКОЙ ПЛОТНОСТИ

3.4. Элементарный метод. В [26] П. Эрдеш показал, что из теоремы Хинчина следует такой результат: если $0,1\in A$, то $\gamma\geqslant\min\left(1,\frac{3}{2}\alpha\right)$. Мы покажем сейчас,

что необходимое и достаточное условие $\alpha \leqslant \frac{2}{3d(A)}$ того, что $\gamma \geqslant \frac{3}{2}\alpha$, можно получить из элементарной теоремы 1.9.

Теорема.

$$\gamma \geqslant \min\left(\frac{1}{d(A)}, \frac{3}{2}\alpha\right).$$

Доказательство. Предположим, что $a_0 = 0$ и $d(A) = 1$, что не ограничивает общности.

Если $\alpha > \frac{1}{2}$, то все числа натурального ряда, начиная с некоторого, входят в $2A$ и $\gamma = 1$. Итак, мы считаем, что $\alpha \leqslant \frac{1}{2}$ и $d(A) = 1$.

Предположим, проводя доказательство от противного, что $\gamma < \frac{3}{2}\alpha$.

Определим последовательность натуральных чисел $y_1 < y_2 < \cdots < y_j < \cdots$ так, чтобы

$$\lim_{j\to\infty} \frac{A_2(y_j)}{y_j} = \gamma.$$

Тогда, как бы ни было мало положительное число ε, при $j > j_0(\varepsilon)$ будут иметь место неравенства

$$A_2(y_j) < (\gamma + \varepsilon) y_j, \tag{3.4.1}$$

$$A\left(\frac{y_j}{2}\right) > (\alpha - \varepsilon)\frac{y_j}{2}. \tag{3.4.2}$$

Пусть M — минимальное число i такое, что $a_i > \frac{y_j}{2}$. Тогда $a_{M-1} \leqslant \frac{y_j}{2}$. Обозначим

$$\Delta = a_M - \frac{y_j}{2}, \quad \Delta_1 = \frac{y_j}{2} - a_{M-1}.$$

Если предположить, что

$$a_M \leqslant 2M - 1,$$

то из теоремы 1.3 следовало бы

$$A_2(y_j) \geqslant a_M + M - \Delta - 1 = (a_M - \Delta) + (M - 1),$$

а отсюда, ввиду (1) и (2),

$$(\gamma + \varepsilon) y_j > \frac{y_j}{2} + (\alpha - \varepsilon)\frac{y_j}{2}$$

и, наконец,

$$\gamma \geqslant \frac{1+\alpha}{2} \geqslant \frac{3\alpha}{2}.$$

Итак, можно предположить, что

$$a_M > 2M - 1. \tag{3.4.3}$$

Из (1) и (2) при достаточно малом ε следует

$$\frac{A_2(y_j)}{A\left(\frac{y_j}{2}\right)} < 2\frac{\gamma+\varepsilon}{\alpha-\varepsilon} < 3,$$

откуда, ввиду теоремы 1.9,

$$a_{M-1} < 2M - 3$$

и снова, ввиду теоремы 1.9,

$$(\gamma+\varepsilon)\, y_j > A_2(y_j) \geqslant a_{M-1} + M \geqslant a_{M-1} + (\alpha-\varepsilon)\, a_M =$$

$$= \frac{y_j}{2} - \Delta_1 + (\alpha-\varepsilon)\left(\frac{y_j}{2} + \Delta\right). \tag{3.4.4}$$

Отсюда, ввиду $\alpha \leqslant \frac{1}{2}$ и $\alpha < \frac{3}{2}\gamma$ при достаточно малом ε следует

$$\Delta < 2\Delta_1. \tag{3.4.5}$$

Ввиду (3) и теоремы 1.9,

$$(\gamma+\varepsilon)\, y_j \geqslant A_2(y_j) \geqslant 3M - (\Delta - \Delta_1) - 3 \geqslant 3(\alpha-\varepsilon)\, a_M -$$

$$-(\Delta - \Delta_1) = 3(\alpha-\varepsilon)\frac{y_j}{2} - (\Delta - 3(\alpha-\varepsilon)\,\Delta - \Delta_1). \tag{3.4.6}$$

Если $(1-3\alpha)\Delta < \Delta_1$ $\left(\text{при } \alpha > \frac{1}{6} \text{ это так ввиду (5)}\right)$, то из (6) следует $\gamma \geqslant \frac{3}{2}\alpha$.

Если же $(1-3\alpha)\Delta \geqslant \Delta_1$ и, следовательно, $\alpha \leqslant \frac{1}{6}$, то, ввиду (4),

$$\frac{\Delta}{y_j} > \frac{1}{2},$$

а тогда, ввиду $(\gamma+\varepsilon)\, y_j > A_2(y_j) \geqslant 2A\left(\frac{y_j}{2}\right) - 1 = 2A(y_j) - 1 \geqslant 2(\alpha-\varepsilon)\, y_j - 1$, было бы $\gamma \geqslant 2\alpha$.

3.5. Вспомогательная лемма геометрии чисел.

Лемма. Пусть заданы решетка $\Gamma \subset E_n$, объем фундаментального параллелепипеда которой равен единице, и центрально-симметричное выпуклое замкнутое множество R с центром в точке O, не содержащее никаких двух точек, сравнимых по $\bmod \Gamma$. Можно указать такой базис $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ решетки Γ, что $R \subset H$, где H — параллелепипед с ребрами $c\bar{a}_1, c\bar{a}_2, \ldots, c\bar{a}_n$, $c = 2n!$, и центром в точке O.

Доказательство. Пусть $\bar{a}_1$ — любая, отличная от нуля целая точка, такая, что $\bar{a}_1 \in \lambda_1 R$ (определение чисел λ_i см. в 2.6). Если $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{i-1}$ определены, то в качестве $\bar{a}_i$ выбираем любую целую точку $\bar{a}_i \in \lambda_i R$, не являющуюся линейной комбинацией точек $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{i-1}$. Векторы $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ — базис решетки Γ. Линейное преобразование $\varphi : E_n \to E_n$ определим соотношениями $\bar{a}_i \varphi = \bar{e}_i$, $1 \leqslant i \leqslant n$. Множество $R_1 = R\varphi$ подвергаем растяжению вдоль оси $\bar{e}_1$, так, чтобы $\bar{e}_1$ стала его граничной точкой, вдоль оси $\bar{e}_2$ так, чтобы $\bar{e}_2$ стала его граничной точкой и т. д. В результате мы получим множество R_2, объем которого, по теореме 2.5, не превосходит 2^n.

Мы также имеем

$$V(R_2 \cap L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_n)) \geqslant \frac{2^{n-1}}{(n-1)!},$$

$$1 \leqslant i \leqslant n,$$

так как оболочка точек $O, \bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1}$ имеет объем $\frac{1}{(n-1)!}$. Поэтому, если в R_1 входит точка на расстоянии h от $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_n)$, то

$$V(R) \geqslant 2h \cdot \frac{1}{n} \cdot \frac{2^{n-1}}{(n-1)!} = \frac{2^n}{n!} h.$$

Но, так как R не содержит никаких двух точек, сравнимых по $\bmod \Gamma$, то $V(R) = V(R_1) \leqslant V(R_2) \leqslant 2^n$. Поэтому $h \leqslant n!$

3.6. Сложение последовательностей положительной плотности.

Теорема.[*] Пусть для последовательности A, для которой $a_0 = 0$, $d(A) = 1$, имеют место условия $\alpha > 0$, $\gamma < C\alpha$, $C \geqslant \frac{3}{2}$ и существует постоянная C_1, такая, что условие

$$a_{l+1} > C_1 a_l \tag{3.6.1}$$

выполняется лишь в конечном числе случаев.

Существует цилиндр $N \subset E_n$, $n \geqslant 2$, основанием которого является выпуклое множество $P \subset L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$ и положительные постоянные c и α_0, зависящие лишь от C и C_1, такие, что при $\alpha < \alpha_0$

1) $A \subset (N \cap Z_n)\varphi$,
2) $N \cap Z_n$ и $(N \cap Z_n)\varphi$ изоморфны,
3) $V(P) < c\alpha$, $T(N^{(x)} \cap Z_n) < c\alpha x$,
4) $n \leqslant [2C - 1]$.

Здесь $N^{(x)}$ — подмножество множества N, для то, чек которого $x_n \leqslant x$, $\varphi : Z_n \to Z_1$, гомоморфизм, такой-что $\bar{e}_i\varphi = 0$, $1 \leqslant i \leqslant n-1$, $\bar{e}_n\varphi = 1$.

Доказательство. Заметим прежде всего, что, так как $d(A) = 1$ и α_0 достаточно мало, то, ввиду теоремы 3.4, выполняется неравенство

$$\gamma \geqslant \frac{3}{2}\alpha,$$

что делает понятным ограничение, наложенное в условии теоремы на C.

Ввиду неравенства

$$\gamma = \varliminf_{x \to \infty} \frac{A_2(x)}{x} < C\alpha,$$

при любом заданном $\varepsilon > 0$ существует последовательность натуральных чисел

$$y_1 < y_2 < \cdots < y_j < \cdots, \tag{3.6.2}$$

для которых, как в (4.1),

$$\frac{A_2(y_j)}{y_j} < \gamma + \varepsilon. \tag{3.6.3}$$

---

[*] Здесь устранены погрешности, допущенные в формулировке этой теоремы в [19]. Доказательство сохранилось без изменений.

Обозначим

$$K_j = \left\{a_i \leqslant \frac{y_j}{2}\right\}.$$

Ввиду определения числа α можно считать, что, как в (4.2),

$$A\left(\frac{y_j}{2}\right) = T(K_j) > (\alpha - \varepsilon)\frac{y_j}{2}. \qquad (3.6.4)$$

Ясно, что

$$T(2K_j) \leqslant A_2(y_j). \qquad (3.6.5)$$

Ввиду (3), (4) и (5), можно выбрать столь малое ε, что

$$\frac{T(2K_j)}{T(K_j)} \leqslant 2\frac{A_2(y_j)}{y_j} : \frac{T(K_j)}{y_j/2} < \frac{2(\gamma + \varepsilon)}{\alpha - \varepsilon} < 2C. \qquad (3.6.6)$$

К любому из множеств K_j, ввиду (6), можно применить теорему 2.8 в случае, если $T(K_j) > k_0$, где k_0 определяется величиной $2C$, как об этом сказано в условии теоремы 2.8. Чтобы это условие выполнялось для любого j, нужно лишь выбрать y_1 достаточно большим, что, очевидно, всегда возможно.

В результате применения теоремы 2.8 для каждого j найдется натуральное число n_j, гомоморфизм $\varphi_j : Z_{n_j} \to Z_1$ и канонический параллелепипед H_j, такие, что для них будут выполняться условия 1) — 4) теоремы 2.8.

Можно считать, что все n_j равны: $n_j = n$. В самом деле, последовательность чисел n_j ограничена в силу условия 4) теоремы 2.8. Поэтому последовательность (2) можно, изменив нумерацию, заменить такой ее подпоследовательностью, для которой соответствующие n_j одинаковы.

В зависимости от C можно выбрать α_0 достаточно малым так, чтобы, ввиду условия 3) теоремы 2.8, выполнялось неравенство $n \geqslant 2$.

Обозначив через L_j такую гиперплоскость, что $L_j \cap Z_n$ является ядром φ_j, L_{m_j} — гиперплоскость, для которой $(L_{m_j} \cap Z_n)\varphi_j = m$. Пусть $a_{k_{j-1}}$ — максимальное из всех чисел $a_i \leqslant \frac{x_j}{2}$. Построим цилиндр N_j, продлив одно из ребер параллелепипеда H_j (о способе выбора этого ребра см. ниже).

Пусть F — полоса между гиперплоскостями L_j и $L_{a_{k_j-1}j}$, $H_j' = N_j \cap F$. Как это следует из примечания к лемме 2.13, в качестве образующей можно выбрать такое ребро параллелепипеда H_j, что

$$V(H_j') \leqslant nV(H_j).$$

Какова бы ни была положительная постоянная c_1, можно считать, что в cP_j', где $P_j' = N_j \cap L_j$, не содержится никаких двух точек, сравнимых по mod Γ_j ($\Gamma_j = L_j \cap Z_n$). Это следует из того, что при завершении доказательства теоремы 2.8 в 2.8 можно применить лемму 2.27 вместо леммы 2.26. Постоянная c в условии 3) теоремы 2.8 будет в этом случае зависеть от c_1.

Применяя лемму 3.5, найдем базис $\bar{a}_{1j}, \bar{a}_{2j}, \ldots, \bar{a}_{n-1j}$ решетки Γ_j такой, что параллелепипед с ребрами $c_2\bar{a}_{1j}, c_2\bar{a}_{2j}, \ldots, c_2\bar{a}_{n-1j}$, где c_2 — некоторое положительное число, которое можно выбрать сколь угодно малым, и центром в O содержит P_j'.

Линейное преобразование $\varphi_j' : E_n \to E_n$ определим нижеследующим образом. Пусть $\bar{a}_{ij}\varphi_j' = \bar{e}_i$, $1 \leqslant i \leqslant n-1$. Вектор $\bar{a}_{nj} \in L_{1j}$, для которого положим $\bar{a}_{nj}\varphi_j' = \bar{e}_n$, определим так, чтобы параллелепипед $H_j'' = H_j\varphi_j'$ удовлетворял условию (2.7.2) определения канонического параллелепипеда. H_j'' имеет высоту $h_{nj} = a_{k_j-1}$ и основание P_j'', лежащее в квадрате P' с ребрами $c_2\bar{e}_1$, $c_2\bar{e}_2, \ldots, c_2\bar{e}_{n-1}$ и центром в точке O. Последовательность ребер параллелепипедов H_j'', не лежащих в $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$, можно считать сходящейся по направлению к некоторому лучу l, не параллельному $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$. В самом деле, из указанной последовательности ребер можно выбрать сходящуюся по направлению последовательность, а затем последовательность (2) заменить соответствующей подпоследовательностью, изменив нумерацию. Условие (2.7.2) обеспечивает, что предельная прямая l не параллельна $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$.

Рассмотрим цилиндр N' с основанием P' и образующей l. Множества $N' \cap Z_n$ и $(N' \cap Z_n)\varphi$ изоморфны.

В N' содержится по одному прообразу каждого из чисел a_l (т. е. $N' \bigcap a_i\varphi^{-1} \neq \varnothing$). Действительно, $N_j'' \bigcap a_i\varphi^{-1} \neq \varnothing$ при достаточно большом j и образующие N_j'' сходятся по направлению к l.

Рассмотрим множество проекций прообразов $a_i\varphi^{-1}$ чисел a_i, лежащих в N', на $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$ параллельно l. Пусть P — минимальное выпуклое множество, его содержащее.

Покажем, что $V(P) < c\alpha$, где c — некоторая положительная постоянная, зависящая от C и C_1. Для k достаточно большого минимальный выпуклый многогранник P'', содержащий проекции $a_0, a_1, \ldots, a_{k-1}$, имеет объем, сколь угодно мало отличающийся от $V(P)$. Но при достаточно большом j $V(P) < (1+\varepsilon)\, V(P_j'')$, где ε — сколь угодно малое положительное число, $P_j'' = N_j'' \bigcap L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$. Так как $V(H_j'') < c_3 k_j$, то $V(P_j'') < \dfrac{c_3 k_j}{a_{k_j-1}} < c_4\alpha$.

Наконец, условие $T(N^{(x)} \bigcap Z_n) < c\alpha x$ следует из условия $V(H_j'') < c_3 k_j$, а также ввиду того, что $a_i\varphi^{-1} \bigcap N'$ совпадает с $a_i\varphi^{-1} \bigcap N_j''$ для достаточно большого j во всех случаях, когда последнее пересечение не пусто. Но последнее условие следует из (1), если предположить, что c_2 достаточно мало в зависимости от C_1.

Следствие 1. При выполнении условий теоремы 3.6 имеет место неравенство

$$\overline{\lim_{x\to\infty}} \frac{A(x)}{x} < c\alpha.$$

Следствие 2. При выполнении условий теоремы 3.6 порядок r базиса A удовлетворяет неравенству

$$r > c/\alpha^{\frac{1}{n}}.$$

3.7. Разбор случая $C < 2$. Частный случай задачи, рассмотренной в 3.6, а именно, когда $C < 2$, был рассмотрен М. Кнезером [30]. Мы сейчас увидим, что следует для этого случая из наших общих результатов, и в 3.8 проведем сравнение с результатами М. Кнезера.

Теорема. Пусть для последовательности A, для которой $a_0 = 0$, $d(A) = 1$, имеют место условия $\alpha > 0$, $\gamma < C\alpha$, $\frac{3}{2} \leqslant C < 2$.

Существует положительное число $\alpha_0 = \alpha_0(C)$ и натуральные числа g, h, l, $h_0 = h_0(C)$ и u_0, $(g, l) = 1$, так что $h < h_0$ и при $\alpha < \alpha_0$ последовательность A содержится в совокупности h классов вычетов по модулю g, сравнимых с вычетами, лежащими в арифметической прогрессии

$$a_0,\ a_0 + l,\ a_0 + 2l, \ldots,\ a_0 + (h-1)l, \tag{3.7.1}$$

и

$$\sigma > \varkappa \frac{h}{g}, \tag{3.7.2}$$

где

$$\varkappa > \frac{h-1}{4h},$$

а в случае $h = 2$

$$\varkappa > \frac{1}{2}. \tag{3.7.3}$$

Доказательство. Рассмотрим последовательность множеств K_j, полученную при доказательстве теоремы 3.6.

Вместо этой теоремы нам удобнее далее в случае $C < 2$ использовать теорему 2.8, которую можно, ввиду (6.6), применить к каждому K_j, начиная с j достаточно большого.

Мы получим последовательность прямоугольников H_j, содержащих точку O, стороны которых параллельны осям координат, причем множество длин ребер, параллельных оси ординат, ограничено в совокупности числом c, зависящим лишь от C.

Пусть $(1,0)\varphi_j = g_j$. Числа g_j, которые можно считать положительными, ограничены в совокупности, ибо на отрезке $[0, g_j]$ содержится лишь по одному образу из множества целых точек, лежащих на пересечении H_j с какой-либо прямой, параллельной оси абсцисс, а таких прямых с непустым пересечением не больше c. Можно поэтому, путем выбора соответствующей подпоследовательности, свести рассмотрение к случаю, когда $g_j = g$, затем к случаю, когда все точки $(0,1)\varphi_j$ принадлежат одному классу по модулю g. Можно,

наконец, считать, что все точки $f_j = (\cap,1)\varphi_j$ совпадают и лежат, например, между 0 и g ($f_j = f$, $0 < f < g$). Такого совпадения можно добиться, изменяя φ_j сдвигами параллельно оси абсцисс.

Таким образом, все φ_j можно считать одинаковыми.

В результате получается полоса F, содержащая прямые $x_2 = b$, $-t_1 \leqslant b \leqslant t_2$, t_1 и t_2 — заданные неотрицательные числа, и гомоморфизм $\varphi: Z_2 \to Z_1$, такой, что $A \subset (F \cap Z_2)\varphi$ и $F \cap Z_2$ изоморфно $(F \cap Z_2)\varphi$.

Для доказательства теоремы осталось доказать неравенство (2).

Для этой цели проведем уточнение структуры A.

Пусть $\{b_i\}$ — упорядоченное по возрастанию множество целых чисел b_i, для которых

$$A \cap \{(x_2 = b_i) \cap Z_2\}\varphi \neq \varnothing.$$

Пусть $M^{(x)}$ — та часть множества M, для точек которой $x_1 < x$.

Пусть $D_i = A\varphi^{-1} \cap F^{(x)} \cap \{x_2 = b_i\}$, $T(D_i) = \delta_i$.

Предположим, что для любого x, начиная с некоторого, имеет место неравенство

$$T((2 \bigcup_{i>i_1}^{i_2} D_i)^{(x)}) \geqslant 4(\delta_{i_1} + \ldots + \delta_{i_2}) - c, \qquad (3.7.4)$$

где c, как и c_1, c_2, c_3, c_4, c_5 ниже в этом пункте — некоторые достаточно большие положительные постоянные.

Отсюда сразу следует, что

$$T((2 \bigcup_{i>i_1}^{i_2+1} D_i)^{(x)}) \geqslant 4(\delta_{i_1} + \ldots + \delta_{i_2} + \delta_{i_2+1}) - c_1.$$

В самом деле,

$$T((2 \bigcup_{i\geqslant i_1}^{i_2+1} D_i)^{(x)}) \geqslant T((2D_{i_2+1})^{(x)}) + T((D_{i_2} + D_{i_2+1})^{(x)}) +$$

$$+ T((2 \bigcup_{i\geqslant i_1}^{i_2} D_i)^{(x)}) \geqslant 2\delta_{i_2+1} - c_3 + 2(\delta_{i_1} + \cdots + \delta_{i_2}) - c.$$

В самом деле, если $\bar{z}_1$ и $\bar{z}_2$ — точки с минимальными абсциссами, принадлежащие, соответственно D_{i_2+1} и D_{i_2}, то

$$\bar{z}_1 + D_{i_2+1} \subset 2D_{i_2+1} \quad \text{и} \quad \bar{z}_2 + D_{i_2+1} \subset D_{i_2} + D_{i_2+1}.$$

Таким образом, неравенство (4) противоречит предположению $C < 2$.

Можно считать, что о. н. д. чисел b_i равен единице, чего можно добиться сжатием по оси ординат. Покажем, что всякое b, для которого $-t_1 \leqslant b \leqslant t_2$, входит в $\{b_i\}$. Можно считать, разумеется, что $-t_1$, $t_2 \in \{b_i\}$, так как иначе некоторое число прямых $x_2 = b$, $b \in \{b_i\}$, можно выбросить, сузив полосу F.

Если предположить, что существует $b \in \{b_i\}$, $-t_1 < b < t_2$, то существует такое i_1, что $b_{i_1} + b_{i_1+2} \neq 2b_{i_1+1}$.

Множества

$$D_j + D_t, \tag{3.7.5}$$

где $j = t = i$, или $j = t = i_1 + 1$, или $j = t = i_1 + 2$, или $j = i_1$, $t = i_1 + 1$, или $j = i_1$, $t = i_1 + 2$, или $j = i_1 + 1$, $t = i_1 + 2$, не пересекаются между собой, откуда для $\bigcup\limits_{i \geqslant i_1}^{i_1+2} D_i$ следует неравенство (4).

Обозначим через q_i общий наибольший делитель попарных разностей чисел последовательности $A_i = A \cap (\{x_2 = b_i\} \cap Z_2)\varphi$.

Величины g и l теоремы определяются равенствами $(1, 0)\varphi = g$, $(0, 1)\varphi = l$. Ясно, что $(l, g) = 1$ ввиду $d(A) = 1$, $h < h_0$ при достаточно малом α_0.

Поясним, что

$$q = (q_1, q_2, \ldots) = g. \tag{3.7.6}$$

В самом деле, пусть $q > g$.

Если предположить, что есть i_1 такое, что $a_{i_1} + a_{i_1+2} \not\equiv 2a_{i_1+1} \pmod q$, где $a_j \in A_j$, $j = i_1, i_1 + 1, i_1 + 2$, то, как для (5), можно показать, что шесть множеств $D_j + D_t$ не пересекаются попарно и для $\bigcup\limits_{i \geqslant i_1}^{i_1+2} D_i$ справедливо неравенство (4).

Можно считать, что $(0, 1)\varphi$ сравнимо с числами $A \cap (\{x_2 = 1\} \cap Z_2)\varphi$ по модулю q, а тогда и $(b, 1)\varphi$ сравнимо с числами $A \cap (\{x_2 = b\} \cap Z_2)\varphi$ по модулю q. Ясно, что сжатием по оси абсцисс в $\frac{q}{g}$ раз можно удовлетворить требованию (6).

Пусть множество K расположено в плоскости; ординаты его точек лежат между числами $-t_2$ и $-t_2+h-1$, точки $(0, j)\in K$, $-t_2\leqslant j\leqslant -t_2+h-1$, абсциссы точек K неотрицательны и максимальная из них равна p. Можно считать, что $(p, 0)\in K$. Спроектируем множество K к прямой $x_2=0$ параллельно вектору $(-p, 1)$. Точки на оси ординат спроектируются к точкам pr, $-t_2\leqslant r\leqslant -t_2+h-1$, отрезок, на котором лежат проекции, содержит не менее $(h-1)p+1$ точек.

Если $T<4k-c_4$, то, как в 1.17 (задача 5 п. 1.17), показываем, что

$$(h-1)p<T-2k+c_5. \tag{3.7.7}$$

Обозначим через p максимальное из чисел a_i, не превышающих $\frac{y_j}{2}$. Если бы было $p<\frac{y_j}{4g}$, то мы получили бы

$$A_2(y_j)\geqslant T\left(2\left\{a_i\leqslant\frac{y_j}{2}\right\}\right)+A(y_j)-A\left(\frac{y_j}{2}\right)\geqslant$$

$$\geqslant 3A\left(\frac{y_j}{2}\right)+A(y_j)-A\left(\frac{y_j}{2}\right)\geqslant(\alpha-\varepsilon)y_j+$$

$$+2(\alpha-\varepsilon)\frac{y_j}{2}=2(\alpha-\varepsilon)y_j.$$

Итак, $p\geqslant\frac{y_j}{4g}$ и, ввиду (7),

$$(h-1)\frac{y_j}{4g}<(\gamma+\varepsilon)y_j-2(\alpha-\varepsilon)\frac{y_j}{2}<\alpha y_j,$$

откуда следует (2).

В качестве примера возможностей получения более сильных результатов разберем случай $h=2$.

Предположим вначале, что $\alpha<\frac{1}{2g}$. Пусть z_1 и z_2 — максимальные числа из A в двух прогрессиях с разностью g, содержащих A, такие, что z_1, $z_2\leqslant\frac{y_j}{2}$. Мы имеем (задача 5 п. 1.17)

$$\frac{z_1+z_2}{g}<(\gamma-\alpha+\varepsilon)y_j<\alpha y_j\leqslant\frac{1}{2g}y_j.$$

Если $z_1 \leqslant z_2$, то $2z_1 \leqslant \frac{y_j}{2}$,

$$2\left\{a_i < \frac{y_j}{2}\right\} \bigcap \left\{\frac{y_j}{2} < a_i < y_j\right\} = \varnothing$$

и

$$\left(\left\{a_i < \frac{y_j}{2}\right\} + \left\{a_i < \frac{y_j}{2},\ a_i \in A_2\right\}\right) \bigcap_{a_i \in A_1}$$

$$\bigcap_{a_i \in A_2,\ a_j \in A_1} \left(\left\{\frac{y_j}{2} < a_i < y_j\right\} + a_j\right) = \varnothing,$$

так что

$$A_2(y_j) \geqslant 3A\left(\frac{y_j}{2}\right) + A(y_j) - A\left(\frac{y_j}{2}\right) \geqslant 2(\alpha - \varepsilon) y_j. \quad (3.7.8)$$

Итак,

$$\alpha > \frac{1}{2g}.$$

Пусть z_3 — минимальное из чисел a_i, такое, что $a_i \geqslant \frac{y_j}{2}$. Пусть, например, $z_3 \in A_1$. Пусть $K = \{a_i \leqslant z_3\}$, $k = T(K)$. Тогда

$$A\left(\frac{y_j}{2}\right) = A(z_3) - 1 > (\alpha - \varepsilon) z_3.$$

Предположим, что $T(2K) \geqslant 4k - 6$. Тогда

$$A_2(y_j) \geqslant 4k - \frac{2\left(z_3 - \frac{y_j}{2}\right)}{g} - 8,$$

то есть

$$(\gamma + \varepsilon) y_j \geqslant 4(\alpha - \varepsilon) z_3 - \frac{2z_3 - y_j}{g}$$

или

$$(\gamma + \varepsilon - 2\alpha + 2\varepsilon) y_j \geqslant (2z_3 - y_j)\left(2\alpha - 2\varepsilon - \frac{1}{g}\right),$$

что невозможно ввиду (8).

Пусть $T < 4k - 6$. Тогда

$$\frac{z_2 + z_3}{g} < (\gamma + \varepsilon) y_j - 2(\alpha - \varepsilon) z_3.$$

Если $z_2 + z_3 \geqslant y_j$, то отсюда $\alpha > \frac{1}{g}$.

Пусть теперь $z_2 + z_3 < y_j$.
Рассмотрим $K = \{a_i < y_j - z_2\}$.
Пусть вначале $T \geqslant 4k - 6$.
Тогда

$$A_2(y_j) \geqslant 4(\alpha - \varepsilon)(y_j - z_2) - \frac{2\left(\frac{y_j}{2} - z_2\right)}{g}$$

$$(\gamma + 3\varepsilon - 2\alpha) y_j \geqslant (y_j - 2z_2)\left(2\alpha - 2\varepsilon - \frac{1}{g}\right).$$

Если же $T < 4k - 6$, то

$$(\gamma + \varepsilon) y_j - 2(\alpha - \varepsilon)(y_j - z_2) \geqslant \frac{\frac{y_j}{2} + z_2}{g},$$

откуда

$$\left(\gamma + 2\varepsilon - \alpha - \frac{1}{g}\right) y_j \geqslant \left(\frac{y_j}{2} - z_2\right)\left(2\alpha - 2\varepsilon - \frac{1}{g}\right).$$

Ввиду (8), отсюда следует $\alpha > \frac{1}{g}$.

3.8. Сравнение с теоремой М. Кнезера. Теорема 3.7 определяет такую же структуру последовательности A, как и теорема 3.2: она показывает, что A содержится в ограниченном числе классов вычетов. В теореме 3.7 уточняется взаимное расположение этих классов, что не сделано в теореме 3.2 (в этом направлении уточнения произвел Кемперман [29]). Однако нижняя граница для α в теореме 3.7 получена гораздо более слабая, чем указанная в (2.2).

Трудности получения наилучших оценок снизу для α связаны с тем, уже упоминавшимся обстоятельством, что метод тригонометрических сумм может успешно применяться лишь при исследовании структуры достаточно „редких“ множеств.

Следует, впрочем, подчеркнуть, что главное значение развитых в настоящей книге методов заключается в возможности изучать структуру последова-

тельностей при любых значениях C, в то время как ранее существовавшие методы не позволяли исследовать значения $C \geqslant 2$.

Для случая $h = 2$ получена оценка $\alpha > \frac{1}{g}$. Весьма вероятно, что в теореме 3.7 может быть доказано неравенство

$$\alpha > \frac{h-1}{g}, \tag{3.8.1}$$

для которого оценка (7.3) является частным случаем (при $h = 2$).

Для этой цели необходимо рассмотреть случай $T < Ck$, $C < 4$ так, как это было сделано для $T < \frac{10}{3}k - 5$ в 1.17.

Сделаем еще некоторые замечания о сравнении теоремы 3.2 с теоремой 3.7, если предположить, что для последней неравенство (1) доказано в полном объеме.

Из (1) следует, что для любого класса по модулю g, вычеты которого сравнимы с одним из чисел

$$2u_0 + l,\ 2u_0 + 2l, \ldots, 2u_0 + (2h-3)\,l,$$

все числа, начиная с некоторого, входят в $2A$.

Неравенство (1) для указанной в 3.7 структуры классов не может быть усилено. В самом деле, рассмотрим пример последовательности, в которую входят все положительные числа, сравнимые по модулю g с первыми $h-1$ числами (7.1) и по модулю tg с числом $a_0 + (h-1)\,l$.

В теореме 3.2 не оговаривается наличие структуры классов вычетов, определяемой числами (7.1). Поэтому в указанном примере можно рассмотреть все классы вычетов по модулю tg, содержащие числа последовательности. Таких классов будет $t(h-1)+1$, а в $2A$ их будет $2t(h-1)+1$, и неравенство (2.2) по отношению к этим классам будет выполняться.

Уточнение структуры A с получением неравенства (2.2.1) связано с рассмотрением структуры A с большими α и не вытекает из приведенных в книге результатов.

§ 3. СЛОЖЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НУЛЕВОЙ АСИМПТОТИЧЕСКОЙ ПЛОТНОСТИ

3.9. Обратная аддитивная теорема для последовательностей нулевой асимптотической плотности.

Теорема. Предположим, что $\delta = \overline{\lim\limits_{x\to\infty}} \frac{A_2(x)}{A(x)} \leqslant C$, $C > 0$, $\alpha = \overline{\lim\limits_{x\to\infty}} \frac{A(x)}{x} = 0$. Тогда существует бесконечное множество $a_i \in A$, таких, что $2a_i < a_{i+1}$.

Доказательство. Если бы существовало лишь конечное число k, таких, для которых $2A(a_{k-1}) = 2k \geqslant A(2a_{k-1})$, то отсюда следовало бы, что существует достаточно большое u, для которого $A(2^s a_{u-1}) \geqslant 2^s u$ для любого натурального s, откуда видно, что $\alpha > 0$. Но так как, по условию теоремы, $\alpha = 0$, существует бесконечное число k, для которых $2A(a_{k-1}) \geqslant A(2a_{k-1})$. Для достаточно больших таких k имеем

$$T(2K) \leqslant A_2(2a_{k-1}) =$$

$$= \frac{A_2(2a_{k-1})}{A(2a_{k-1})} A(2a_{k-1}) \leqslant (C+\varepsilon)\,2k = 2(C+\varepsilon)\,k.$$

К каждому из этих K можно применить теорему 2.8.

Выберем теперь числа k и k_0 так, чтобы $\varepsilon = \frac{k_0}{a_{k_0-1}}$ было достаточно малым, а $\varepsilon_2 = \frac{V}{M}$, где $V = V(H)$ — объем параллелепипеда H, определяемого применением теоремы 2.8 к K, $M = a_{k-1}$, причем ε_2 достаточно мало по сравнению с ε_1 (способ выбора постоянных будет виден из дальнейшего).

Теорема 2.8 определяет гомоморфное отображение φ: $Z_n \to Z_1$. Пусть $\overline{e_i}\varphi = g_i$, $1 \leqslant i \leqslant n$. Можно считать, что $g_i > 0$. Тогда $\overline{f_i}\varphi = u$, где $\overline{f_i} = \frac{u}{g_i}\overline{e_i}$ и $u = [g_1, g_2, \ldots, g_n]$.

Для любого действительного μ обозначим через D_μ гиперплоскость $\nu_1\bar{f}_1+\nu_2\bar{f}_2+\cdots+\nu_n\bar{f}_n, \sum_{i=1}^{n}\nu_i=\mu$.

Множество $D_0\cap Z_n$ — *ядро гомоморфизма* φ.

Пусть цилиндр N_i — совокупность точек

$$\bar{u}+\sigma_1\bar{x}_1+\sigma_2\bar{x}_2+\ldots+\sigma_n\bar{x}_n,\ -\infty<\sigma_i<\infty \qquad (3.9.1)$$
$$0\leqslant\gamma_j<1,\ 1\leqslant j\leqslant n,\ j\neq i,$$

где $\bar{u}$ — вершина параллелепипеда H.

Замкнутую полосу, лежащую между гиперплоскостями D_0 и D_μ, обозначим F_μ. Пусть $D_{\underline{\mu}}$ — опорная к H гиперплоскость, параллельная D_0, выбранная с той стороны D_0, для которой образы целых точек — положительны. Пусть также $W_\mu=N_i\cap F_\mu$.

Как это следует из примечания к лемме 2.13, число i можно определить так, что $W_{\underline{\mu}}$ будет иметь объем, не больший, чем nV. Поэтому для отрезка $\lambda_{\underline{\mu}}\bar{x}_i$ прямой $\lambda\bar{x}_i$, $-\infty<\lambda<+\infty$, заключенного между гиперплоскостями D_0 и $D_{\underline{\mu}}$, имеет место условие $\lambda_{\underline{\mu}}\leqslant n$.

Покажем, что можно найти (при достаточно малых ε_1 и ε_2) такие $\lambda_{\mu'}$ и $\lambda_{\mu''}$, для которых $\lambda_{\mu'}/\lambda_{\mu_0}\geqslant 1$, $\lambda_{\mu_0}=\dfrac{a_{k_0-1}}{u}$, $\lambda_{\mu''}/\lambda_{\mu'}>2$, причем $Z_n\cap(W_{\mu''}\setminus W_{\mu'})=\varnothing$. Так как это означает, что $A\cap\left[u\dfrac{\lambda_{\mu'}}{\lambda_u},\ u\dfrac{\lambda_{\mu''}}{\lambda_u}\right]=\varnothing$, то отсюда сразу будет следовать справедливость теоремы.

Размерность множества $Z_n\cap W_\mu$ обозначим p_μ.

Дадим по индукции способ построения чисел

$$\mu_1,\ \bar{\mu}_1,\ \mu_2,\ \bar{\mu}_2,\ \ldots,\ \mu_{i_0},\ \bar{\mu}_{i_0}. \qquad (3.9.2)$$

Полагаем $\mu_1=\mu_0$. Пусть числа (μ_i) уже построены до некоторого i. Рассмотрим множество действительных чисел μ, для которых $\lambda_\mu/\lambda_{\underline{\mu}}>0$, $p_\mu=p_{\mu_i}$ и

$$T(W_\mu\cap D_\mu)>0.$$

Обозначим через $\bar{\mu}_i$ верхнюю (нижнюю) грань чисел μ, если эти числа положительны (отрицательны). Рас-

смотрим теперь множество действительных чисел μ, для которых $\lambda_\mu/\lambda_{\underset{\mu}{-}} > 0$ и $W_\mu \setminus (W_{\underset{\mu_j}{-}} \cup D_\mu) = \varnothing$; μ_{i+1} — верхняя (нижняя) грань чисел μ, если эти числа положительны (отрицательны). Указанное построение продолжим до такого i_0, при котором $p_{\mu_{i_0}} = n$. Определим $\bar{\mu}_{i_0}$ из соотношения $\lambda_{\underset{\mu_{i_0}}{-}} = \lambda_{\underset{\mu}{-}}$. Выберем множество из $p_{\mu_i} + 1$ точек размерности p_{μ_i}, содержащееся в W_{μ_i}. Построим параллелепипед H_i с вершинами в этих точках. Обозначим через U_1 цилиндр, определенный в (1), где $-2n \leqslant \sigma_j < 2n + 1$, $j \neq i$, $W_{1\mu} = U_1 \cap F_\mu$.

Проекция точек параллелепипеда H_i на $\lambda\bar{x}_i$ параллельно D_0 даст отрезок длины не свыше $n|\lambda_{\mu_i}||\bar{x}_i|$. В любом отрезке длины $n|\lambda_{\mu_i}||\bar{x}_i|$, содержащемся в отрезке $\lambda_{\underset{\mu_i}{-}}\bar{x}_i$, имеются проекции (параллельно D_0) целых векторов, входящих в $W_{\underset{\mu_i}{-}}$. В самом деле, во-первых, все целые точки, содержащиеся в $W_{\underset{\mu_i}{-}}$ (в том числе и лежащие на $D_{\underset{\mu_i}{-}}$), входят в линейное подпространство, порожденное вершинами H_i; во-вторых, любой параллелепипед этого линейного подпространства, получающийся параллельным переносом H_i, всегда содержит целую точку. Поэтому, если обозначить

$$k_i = T(W_{\mu_i} \cap Z_n),\ \bar{k}_i = T(W_{1\bar{\mu}_i} \cap Z_n),\ i = 1, 2, \ldots, i_0,$$

то справедливы неравенства

$$\bar{k}_i \geqslant \frac{\lambda_{\underset{\mu_i}{-}}}{4n\lambda_{\mu_i}} k_i,\ i = 1, 2, \ldots, i_0. \tag{3.9.3}$$

Предположим, что

$$\frac{\lambda_{\mu_{i+1}}}{\lambda_{\underset{\mu_i}{-}}} \leqslant 2,\ i = 1, 2, \ldots, i_0 - 1. \tag{3.9.4}$$

Тогда существует $c = c(n) > 0$ такое, что

$$\bar{k}_i < ck_{i+1},\ i = 1, 2, \ldots, i_0 - 1. \tag{3.9.5}$$

Из (3), (4) и (5) следует неравенство

$$\overline{k}_{l_0} \geqslant \frac{\lambda_{\overline{\mu}_{i_0}}}{\lambda_{\mu_1}} \frac{1}{(4n)^{i_0}(2c)^{i_0-1}} k_1.$$

Но $k_1 = k_0$,

$$\overline{k}_{i_0} < c_1(n)\, V,$$

а

$$\frac{\lambda_{\overline{\mu}_{i_0}}}{\lambda_{\mu_1}} \geqslant \frac{M}{a_{k_0-1}},$$

поэтому

$$\varepsilon_2 \geqslant C_2 \varepsilon_1, \tag{3.9.6}$$

где

$$C_2 = \frac{1}{(4n)^{i_0-1}(2c)^{i_0-1} c_1(n)}.$$

При любом сколь угодно малом ε_1 можно выбрать ε_2 так, чтобы неравенство (6) не выполнялось. Это означает, что предположение (4) неверно, и найдется такое i, что $\lambda_{\mu_{i+1}}/\lambda_{\overline{\mu}_i} > 2$. Теорема доказана.

Следствие. Если $\alpha = 0$ и неравенство $a_{i+1} > 2a_i$ выполняется лишь в конечном числе случаев, то

$$\overline{\lim_{x\to\infty}} \frac{A_2(x)}{A(x)} = +\infty.$$

3.10. Доказательство гипотезы П. Эрдеша. В работе [23] (проблема 15) П. Эрдеш высказал предположение, что $\delta = \overline{\lim_{x\to\infty}} \frac{A_2(x)}{A(x)} \geqslant 3$, если $\lim_{x\to\infty} \frac{A(x)}{x} = 0$.

Имеет место несколько более сильный результат.

Теорема. $\delta \geqslant 3$, если $\alpha = 0$ и $\overline{\lim_{x\to\infty}} \frac{A(x)}{x} < \frac{1}{2d(A)}$.

Доказательство. Предположим, что $\delta < 3$. Рассмотрим последовательность таких k_i, $i = 1, 2, \ldots$, при которых $a_{k_i} > 2a_{k_i-1}$. Если бы для бесконечного числа k_i было $T(2K_i) \geqslant 3k_i - 3$, то, ввиду

$$\frac{A_2(2a_{k_i-1})}{A(2a_{k_i-1})} \geqslant \frac{3k_i - 3}{k_i},$$

было бы $\delta \geqslant 3$. Итак, отбрасывая, если нужно, конечное число членов последовательности k_i, можно считать, что всегда $T(2K_i) < 3k_i - 3$. Из теоремы 1.9 для достаточно больших k_i следует $a_{k_i} \leqslant (2k_i - 4)\, d(A)$, что дает

$$\overline{\lim_{x\to\infty}} \frac{A(x)}{x} \geqslant \frac{1}{2d(A)}.$$

Теорема доказана.

3.11. Структура A при $\delta < \frac{10}{3}$. Результат предыдущего пункта можно усилить следующим образом.

Теорема. Если $\delta < \frac{10}{3}$, $d(A) = 1$ и $\lim\limits_{x\to\infty} \frac{A(x)}{x} = 0$, то найдется последовательность натуральных чисел $i_1 < i_2 < \ldots < i_s < \ldots$, такая, что

$$\overline{\lim_{s\to\infty}} \frac{a_{i_s} + a_{i_{s+1}} - a_{i_s+1}}{A(a_{i_{s+1}})} \leqslant \delta - 2.$$

Доказательство. Рассмотрим последовательность всех i_s, $s = 1, 2, \ldots$, при которых $a_{i_s+1} > 2a_{i_s}$, $i_s > i_0$ (i_0 — достаточно большое положительное число). Если бы для бесконечного числа s было

$$T(2K_s) \geqslant \frac{10}{3}(i_s + 1) - 5,$$

где $K_s = \{a_0, a_1, \ldots, a_{i_s}\}$, то отсюда следовало бы, что $\delta \geqslant \frac{10}{3}$. Поэтому всегда можно считать

$$T(2K_s) < \frac{10}{3}(i_s + 1) - 5.$$

Без ограничения общности полагаем $d(K_s) = 1$. Ввиду теоремы 1.17, множества K_s лежат каждое в двух арифметических прогрессиях с одинаковой разностью d_s общей длины не свыше $i_s + 1 + b_s$, где b_s определяется из равенства $T(2K_s) = 3i_s + b_s$. Поэтому на отрезке $[0, d_s - 1]$ могут лежать не более двух точек из A, откуда следует, что d_s не могут принимать неограниченно большие значения. Допустим, существует бесчисленное множество $d_s > 1$; тогда можно

получить подпоследовательность $\{K_{s_t}\}$, для которой $d_{s_t} = d > 1$. Так как $d(A) = 1$, то на ограниченном расстоянии от нуля существуют числа любой из двух прогрессий разности d. Отсюда $T(K_{s_t}) > c\frac{a_{is_t}}{d}$, что противоречит условию $\lim\limits_{x\to\infty}\frac{A(x)}{x} = 0$. Итак, можно считать все $d_s = 1$. Теорема доказана.

§ 4. СЛОЖЕНИЕ МНОЖЕСТВ ВЫЧЕТОВ ПО ПРОСТОМУ МОДУЛЮ.

3.12. Структура множеств вычетов с малым удвоением. Некоторые результаты в этом направлении получены в § 1 главы II. С помощью теоремы 3.6 можно исследовать случай $T < Ck$, где C — любое положительное постоянное число.

Теорема. Пусть K — множество, состоящее из k вычетов по простому модулю p. Если $T < Ck$, $C \geqslant 2$, то существуют положительные постоянные c и c_1, зависящие лишь от C, гомоморфизм φ: $Z_n \to S_p$, где S_p — аддитивная группа вычетов по простому модулю p, канонический параллелепипед $H \subset E_n$, такие, что при $k < cp$

1) $K \subset (H \cap Z_n)\varphi$,
2) $H \cap Z_n$ и $(H \cap Z_n)\varphi$ изоморфны,
3) $T(H \cap Z_n) < c_1 k$,
4) $n \leqslant [C - 1]$.

Доказательство. Рассмотрим последовательность неотрицательных чисел, получаемую объединением неотрицательных чисел классов вычетов по модулю p, содержащих вычеты множества K. Для этой последовательности, очевидно, $\alpha = \frac{k}{p}$, $\gamma = \frac{T}{k} < \frac{Ck}{p}$. Таким образом, можно применить теорему 3.6. Очевидно, что образующая l цилиндра N теоремы 3.6 проходит через множество целых точек, отображающихся на класс вычетов по модулю p. Рассмотрим базис $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n$ решетки Z_n такой, что вектор $\bar{a}_n$ параллелен l так, что $\bar{a}_n\varphi = p$.

Множество $P_1 = N \cap L(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n-1})$ — выпуклое.

Его можно заключить в канонический параллелепипед H' по отношению к базису $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n-1}$.

Гомоморфизм, индуцируемый φ на $L(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n-1})$, и параллелепипед H' являются искомыми.

Следствие. Если $k < cp$, где $c > 0$ некоторая достаточно малая абсолютная постоянная, $T < 3k - 3$, то K входит в прогрессию по mod p длины $k + b$, $b = T - 2k + 1$.

3.13. Дальнейшие соображения о сложении множеств вычетов по простому модулю. Главный результат теоремы 3.12 можно сформулировать так: если $T < Ck$ и $k < cp$, $c = c(C) > 0$, то K можно изоморфно отобразить во множество целых чисел.

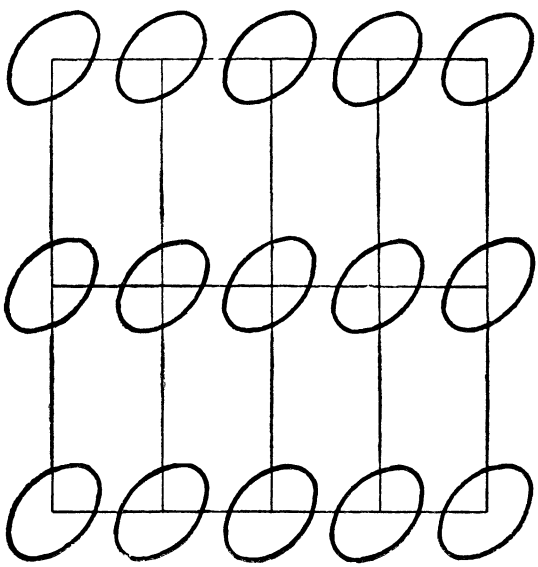


Рис. 6

Известно, что множества целых чисел и вычетов не тождественны с аддитивной точки зрения: в целых числах сложение идет „по прямой", в множестве вычетов — „по окружности". Однако при однократном сложении не очень большого множества вычетов эта окружность „разрывается", что выражается в факте изоморфизма множества вычетов множеству целых чисел.

Если $k > \frac{p}{2} + 1$, то $T < 2k - 1$ и изоморфизма явно нет.

Если же $k < \frac{p}{2}$, то из результата Воспера следует, что при $T = 2k - 1$ множество вычетов изоморфно арифметической прогрессии, состоящей из k целых чисел.

Можно предположить, что если k и T такие, что

$$W(1, T, k) < \frac{p}{2},$$

где $W(1, T, k)$ определяется соотношением (1.24.1), то множество вычетов можно изоморфно отобразить на некоторое множество целых чисел и свести, таким образом, задачу сложения множества вычетов по простому модулю к задаче сложения целых чисел.

§ 5. СЛОЖЕНИЕ ТОЧЕЧНЫХ МНОЖЕСТВ

3.14. Сложение точечных множеств положительной меры.

Теорема. Пусть $\mu^*(2D) < C\mu^*(D)$, $C \geqslant 2^m$, D — множество в E_m, для которого *внешняя мера Лебега* $\mu^*(D)$ положительна. Существуют φ: $Z_n \to E_m$, прямоугольный канонический параллелепипед $H \subset E_n$, выпуклое множество $D_1 \subset E_m$, такие, что:

1) $D \subset (H \cap Z_n)\varphi + D_1$,
2) $(H \cap Z_n) \times D_1 \subset E_n \times E_m$ изоморфно $(H \cap Z_n)\varphi + D_1$,
3) $T(H \cap Z_n)\mu(D_1) < c\mu^*(D)$, $c = c(C, m)$,
4) $n \leqslant [C - 2^m]$.

Доказательство. Разобьем E_m на m-мерные кубы ранга p*).

Именно, рассмотрим m систем гиперплоскостей

$$x_j = 0, \ \pm 1, \ \pm 2, \ \pm 3, \ldots, 1 \leqslant j \leqslant m.$$

Эти гиперплоскости разбивают E_m на счетное множество кубов (к каждому из которых мы причисляем

*) И. П. Натансон. Теория функций вещественного переменного. Гостехиздат, М., 1957, 350–351.

его границу), с ребром, равным 1. Эти кубы попарно не имеют общих внутренних точек. Назовем их кубами первого ранга.

Далее, проведем гиперплоскости вида

$$x_j = 0,\ \pm\frac{1}{2},\ \pm 1,\ \pm\frac{3}{2},\ \ldots,\ 1 \leqslant j \leqslant m.$$

Те замкнутые кубы, на которые разбивается E_m этими гиперплоскостями, назовем кубами 2-го ранга. Ясно, что каждый куб первого ранга состоит из 2^m кубов второго ранга.

Проведя, далее, системы гиперплоскостей вида

$$x_j = \frac{s_j}{4},\ s_j = 0,\ \pm 1,\ \pm 2,\ \ldots,\ 1 \leqslant j \leqslant m,$$

$$x_j = \frac{s_j}{8},\ s_j = 0,\ \pm 1,\ \pm 2,\ \ldots,\ 1 \leqslant j \leqslant m,$$

и продолжая этот процесс неограниченно, мы получим кубы рангов 3, 4, ...

Все эти кубы замкнуты, грани их параллельны координатным гиперплоскостям. Два куба одного и того же ранга не имеют общих внутренних точек, всякий куб ранга p состоит из 2^m кубов ранга $p+1$, ребро куба ранга p имеет длину 2^{1-p}; наконец, множество всех таких кубов счетно.

Пусть некоторое $M \subset E_m$. Рассмотрим множество всех тех кубов ранга p, каждый из которых имеет общие точки с M. Обозначим через $U_p(M)$ объединение множеств точек этих кубов.

Через $W_p(M)$ обозначим множество вершин (кубов ранга p), входящих в некоторое заданное множество M.

Рассмотрим множество всех таких кубов, получающихся параллельным переносом кубов ранга p, для которых одна из вершин входит в некоторое множество M. Обозначим через $Q_p(M)$ объединение множеств точек этих кубов.

Пусть задано $M \subset E_m$.

Найдем открытое множество $G \supset M$ такое, что

$$\mu(G) < \mu^*(M) + \varepsilon,$$

где ε — заданное положительное число.

При любом сколь угодно малом $\varepsilon_1 > 0$ можно выбрать p настолько большим, что

$$\mu(U_p(G)) < \mu(G) + \varepsilon_1. \qquad (3.14.1)$$

Пусть R — некоторый куб ранга p. Покажем, что для любого $\varepsilon_2 > 0$ найдется такое $p_1 > p$, что

$$\mu(Q_{p_1}(W_{p_1}(R))) < \mu(R)(1 + \varepsilon_2). \qquad (3.14.2)$$

В самом деле, в R содержится $(2p_1 - 2p + 1)^m$ вершин квадратов ранга $p_1 > p$. Поэтому

$$\mu(Q_{p_1}(W_{p_1}(R))) = (2p_1 - 2p + 2)^m 2^{m(1-p_1)}.$$

Так как

$$\mu(R) = (2p_1 - 2p)^m 2^{m(1-p_1)},$$

то при достаточно большом значении $p_1 - p$ выполняется.

Ввиду (1) и (2) при любом $\varepsilon_3 > 0$ имеет место неравенство

$$\mu(Q_{p_1}(W_{p_1}(U_p(G))) < \mu(G)(1 + \varepsilon_3),$$

а значит и

$$\mu(Q_{p_1}(W_{p_1}(U_{p_1}(G))) < \mu(G)(1 + \varepsilon_3). \qquad (3.14.3)$$

Рассмотрим открытое множество $G_1 = 2D$, такое, что

$$\mu(G_1) < \mu^*(2D) + \varepsilon_4;$$

рассмотрим далее множество $U_p(G_1)$, такое, что

$$\mu(U_p(G_1)) < \mu(G_1) + \varepsilon_5.$$

Рассмотрим множество $Q_p(W_p(U_p(G_1)))$, для которого, ввиду (3),

$$\mu(Q_p(W_p(U_p(G_1)))) < \mu^*(2D)(1 + \varepsilon_6).$$

Ясно, что $2U_p(D) \subset Q_p(W_p(U_p(G_1)))$, так как любой куб с ребром $2 \cdot 2^{1-p}$ содержит точки $2D$, входит в Q_p, а сумма любых двух кубов из U_p, каждый из которых содержит по точке из D, дает куб, содержащий точку $2D$.

Аналогично,

$$2Q_p(W_p(U_p(D))) \subset Q_{p-1}(W_{p-1}(U_{p-1}(2D))).$$

Обозначим

$$K = W_p(U_p(D)).$$

Ясно, что

$$T \leqslant \frac{1}{2^{1-p}} \mu(Q_{p-1}(W_{p-1}(U_{p-1}(2D)))).$$

Ввиду

$$T < (C + \varepsilon) k,$$

к множеству K можно применить теорему 2.8. Мы получим $\varphi_0 : Z_{n_1} \to 2^{1-p} Z_m$ и канонический параллелепипед H_1, для которых выполняются условия теоремы.

Можно считать, что $0 \in D$. Поэтому для некоторого p_0 в G_1 входит такой квадрат ранга p_0, что его вершина и координаты его вершин — неотрицательные числа.

Найдем векторы $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_m \in E_{n_1}$, такие, что $\bar{a}_i \varphi_0 = 2^{1-p} \bar{e}_i$. Дополним их векторами $\bar{a}_{m+1}, \bar{a}_{m+2}, \ldots, \bar{a}_{n_1}$ до базиса Z_{n_1}. Рассмотрим линейное преобразование $\varphi_1 : Z_{n_1} \to Z_{n_1}$, определяемое соотношениями $(2^{1-p} \bar{e}_i) \varphi_1 = \bar{a}_i$, $1 \leqslant i \leqslant m$, $\bar{e}_i \varphi_1 = \bar{a}_i$, $i > m$. Преобразование $\varphi_1 \varphi_0$ определяет гомоморфное отображение решетки $\Gamma_1 \subset E_{n_1}$ с базисом $2^{1-p} \bar{e}_1, \ldots, 2^{1-p} e_m, \bar{e}_{m+1}, \ldots, \bar{e}_{n_1}$ в решетку $2^{1-p} Z_m$, причем точка, входящая в $L(\bar{e}_1, \ldots, \bar{e}_m)$, переходит в точку z_m с теми же первыми m координатами. Каждое из преобразований решеток дает соответствующее линейное преобразование евклидовых пространств. $H_1 \varphi_1^{-1}$ является некоторым выпуклым множеством D'. Пользуясь леммой 2.13, можно D' заключить в параллелепипед H_2, удовлетворяющий условию (2.7.2). Так как $h_j < c$, c — достаточно большая положительная постоянная, H_2 можно заключить в H_3, для которого вектор $\bar{x}_j$ параллелен $\bar{e}_j$, $m + 1 \leqslant j \leqslant n_1$. Все эти включения, разумеется, производятся с увеличением объема в ограниченное постоянной число раз. Отображение $\varphi_1 \varphi_0$ индуцирует отображение $\varphi_2 : (L(\bar{e}_{m+1}, \ldots, \bar{e}_{n_1}) \cap Z_{n_1}) \to Z_m$. Обозна-

чим H_4 параллелепипед с ребрами $\bar{x}_{m+1}, \ldots, \bar{x}_{n_1}$ и общей с H_1 вершиной.

$$Z_n = L(\bar{e}_{m+1}, \ldots, \bar{e}_{n_1}) \cap Z_{n_1}, \quad H = H_4$$

будут искомыми.

Чтобы доказать, что $n \leqslant [C - 2^m]$, рассмотрим множество точек решетки Γ_3, лежащих в H_3. Как в 1.17, спроектируем это множество, вначале к $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n_1-1})$, затем к $L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n_1-2}, \bar{e}_{n_1})$ и т. д. до $L(\bar{e}_1, \ldots, \bar{e}_m, \bar{e}_{m+2}, \ldots, \bar{e}_{n_1})$, выбирая каждый раз вектор, параллельно которому происходит проектирование, так, чтобы вне $L(\bar{e}_1, \ldots, \bar{e}_{n_1-1})$ было лишь конечное число точек (не больше $\bar{h}_{n_1}$), как и вне $L(\bar{e}_1, \ldots, \bar{e}_{n_1-2}, \bar{e}_{n_1})$ и т. д. Таким образом, в $L(\bar{e}_1, \ldots, \bar{e}_m)$ будет содержаться более $k - c$ точек, где c — достаточно большое положительное число. Теперь ясно, что

$$T \geqslant (n_1 - m)\, k + 2^m k + o(k),$$

откуда

$$n = n_1 - m \leqslant [C - 2^m].$$

Из факта, что равные канонические параллелепипеды с достаточно большими высотами и близкими вершинами имеют общие целые точки, что легко доказывается по индукции, следует, при $\bar{z}_1$ и $\bar{z}_2 \in H$, что $\bar{z}_1 \varphi_2 + H_3 \varphi_1 \varphi_0$ и $\bar{z}_2 \varphi_2 + H_3 \varphi_1 \varphi_0$ не пересекаются и объединение их содержит D.

ЛИТЕРАТУРА

1. С. Н. Бернштейн. Теория вероятностей. ОГИЗ. Гостехиздат, М.—Л., 1946.
2. Б. М. Бредихин. Свободные числовые полугруппы со степенными плотностями. ДАН СССР, 118, № 5, 1958, 855—857.
3. Б. М. Бредихин. Свободные числовые полугруппы со степенными плотностями. Матем. сб., т. 46 (88), № 2, 1958, 143—158.
4. Б. М. Бредихин. Элементарное решение обратных задач о базисах свободных полугрупп. Матем. сб., т. 50 (92), № 2, 1960, 221—232.
5. Б. М. Бредихин. Остаточный член в асимптотической формуле для функции $\nu_G(x)$. Изв. вузов, Матем., № 6 (19), 1960, 40—49.
6. Г. Давенпорт. О сложении классов вычетов. УМН, 7, 1940, 90—92.
7. Дж. В. С. Касселс. Введение в теорию диофантовых приближений. ИЛ, М., 1961.
8. Б. И. Сегал. Тригонометрические суммы и некоторые их применения в теории чисел. УМН, 1, вып. 3—4 (13—14), 1946, 148—193.
9. В. Х. Ташбаев. Обратная аддитивная задача. Матем. сб., т. 52 (94), № 4, 1960, 947—952.
10. Г. А. Фрейман. Обратные задачи аддитивной теории чисел. Учен. зап. КГУ, т. 115, кн. 14, 1955, 109—115.
11. Г. А. Фрейман. Обратные задачи аддитивной теории чисел. ИАН СССР, Матем., т. 19, 1955, 275—284.
12. Г. А. Фрейман. О сложении конечных множеств, I. Изв. вузов, Матем., № 6 (13), 1959, 202—213.
13. Г. А. Фрейман. Обратные задачи аддитивной теории чисел, IV. О сложении конечных множеств, II. Учен. зап. Елабужского госпединститута, т. VIII, 1960, 72—116.
14. Г. А. Фрейман. Обратные задачи аддитивной теории чисел. О сложении множеств вычетов по простому модулю. ДАН СССР, т. 141, № 3, 1961, 571—573.
15. Г. А. Фрейман. Обратные задачи аддитивной теории чисел, VI. О сложении конечных множеств, III. Сложение различных множеств. Изв. вузов, Матем., № 3 (28), 1962, 151—157.
16. Г. А. Фрейман, Обратные задачи аддитивной теории чисел. VII. О сложении конечных множеств, IV. Метод тригонометрических сумм. Изв. вузов, Матем., № 6 (31), 1962, 131—144.

17. Г. А. Фрейман. Обратные задачи аддитивной теории чисел. Труды 4-го Всесоюзного математического съезда, „Наука", Л., том II, 1964. 142—146.
18. Г. А. Фрейман. Обратные задачи аддитивной теории чисел, VIII. Об одной гипотезе П. Эрдеша. Изв. вузов, Матем., № 3 (40), 1964, 156—169.
19. Г. А. Фрейман. Обратные задачи аддитивной теории чисел, IX. О сложении конечных множеств, V. Изв. вузов, Матем., № 6 (43), 1964, 168—178.
20. Г. А. Фрейман. О сложении конечных множеств. ДАН СССР, т. 158, № 5, 1964, 1038—1041.
21. А. Я. Хинчин. О сложении последовательностей натуральных чисел. Матем. сб., № 6 (48) (1939), 161—166 (УМН, 7 (1940), 57—61).
22. Л. Г. Шнирельман. Об аддитивных свойствах чисел. Ростов н/Д. Изв. Донск. политехн. ин-та, 14:2—3 (1930), 3—28.
23. П. Эрдёш. Некоторые нерешенные проблемы. Математика, сб. переводов, т. 7, № 4, 1963, 109—143.
24. A. Beurling. Analyse de la loi asymptotique de la distribution des nombres premiers generalises. I, v. 68, 1937, 255—291.
25 A. Cauchy. Journal Ecole Polytechnique, 9 (1813), 99—116.
26. P. Erdos. On the asymptotic density of the sum of two sequences one of which forms a basis for the integers. 11. Труды Тбилисского матем. инст., 3, 1933, 217—223.
27. P. Erdos. On an elementary proof of some asymptotic formulas in the theory of partitions. Ann. of Mathem., v. 43, № 3, 1942, 437—450.
28. R. Henstock and A. M. Macbeath. On the measure of sum—sets (1). The theorems of Brunn, Minkowski and Lusternik. Proc. London Math. Soc. 3,3, 1953, 182—194.
29. I. H. B. Kemperman. On small sumsets in an Abelian group. Acta math., 103, № 1—2, 1960, 63—88.
30. M. Kneser. Abschätzung der asymptotischen Dichte von Summenmengen. Math. Zeit. Bd. 58. 1953, 459—414.
31. M. Kneser. Ein Satz über Abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen. Math. Zeit. 61, 1955, 429—434.
32. H. B. Mann. A proof of the fundamental theorem on the density of sums of sets of positive integers, Annals of Math. 43, 2, 1942, 523—527.
33. H. B. Mann. Addition theorems. Neu York, 1965, 114 p.
34. H. Ostmann. Additive Zahlentheorie. T. I. Allgemeine Untersuchungen. Berlin, 1956, 233 S.
35. H. Ostmann. Additive Zahlentheorie. T. II. Spezielle Zahlenmengen. Berlin, 1956, 136 S.
36. K. F. Roth. On certain sets of integers. The Journal of the London Math. Soc., 28, P. 1, №. 109, 1953, 104—109.
37. E. Schmidt. Die Brunn-Minkowskische Ungleichung sowie die isoperimetrische Eigenschaft der Kugel in der Euklidischen und nicht-euklidischen Geometrie. I. Math. Nachrichten I (1948), 81—157.
38. A. G. Vosper. The critical pairs of subsets of a group of prime order. The Journal ot the London Math. Soc. 31, P. 2, № 122, 1956, 200—205.

ENGLISH SUMMARY. CONCERNING GENERAL REGULARITIES OF THE ADDITIVE THEORY OF NUMBERS

Report delivered at the Number Theory Summer School, in Palang, September 5, 1965.

The title of the report has been chosen in the association with Ostmann's ([34], [35]) survey of the additive theory of numbers the two volumes of which were published in 1955—1956. The first volume of this survey is devoted to general investigations, i. e. to the questions of addition of sequences of positive density. As to the second volume, it contains a review of special problems: Golbach, Waring, theory of partitions etc.

1. Mann's theorem (1942) was the main result of the theory of density.

Shnirelmann's density of an increasing sequence of nonnegative integral numbers $A = \{a_0, a_1, \ldots, a_i, \ldots\}$ is

$$\alpha'(A) = \inf_{x \in N} \frac{A(x)}{x},$$

where $A(x)$ is the number of natural numbers of the sequence A each of which is not larger than x, and N is the set of natural numbers.

Mann's theorem. Let B and C be the two sequences of nonnegative integral numbers, where $0 \in B$, $0 \in C$.

Then

$$\alpha'(B + C) \geqslant \min(1, \alpha'(B) + \alpha'(C)).$$

In recent years, the evolution of the density theory was slow, due to the fact that both in methods and in results it essentially amounted to developments of Mann's theorem and no new applications in classical problems

had been obtained (though at the outset such applications were given by Shnirelmann).

This report suggests a new way of approach to the study of the general additive regularities.

2. The special problem that we shall now discuss will give us an opportunity to introduce gradually the necessary new notions.

Let K be a final set of k integral numbers:

$$K=\{a_0,\ a_1,\ \ldots,\ a_{k-1}\},\ a_i<a_{i+1},\ i=0,1,\ \ldots,\ k-2.$$

Let $T(M)$ be a number of elements of a final set M, $T=T(2K)$.

Obviously, $T\geqslant 2k-1$. Actually, in the set a_0+K, where there are k numbers, the maximum is a_0+a_{k-1} and in the set $a_{k-1}+K$, the minimum is $a_{k-1}+a_0$.

Let $T<Ck$, where C is a positive number.

The problem. What is the structure of K?

Here are some examples, to clarify the question.

If $T=2k-1$, then K is an arithmetical progression containing k numbers. In fact, if for some $0\leqslant j\leqslant k-3$

$$a_{j+1}-a_j\neq a_{j+2}-a_{j+1},$$

then besides the different numbers $2a_0$, a_0+a_1, $2a_1$, a_1+a_2, $2a_2$, ..., $2a_{k-1}$ there exists another number a_j+a_{j+2} distinct from them.

By induction through k it is possible to prove the following

Theorem 1. 9. If $0\leqslant b<k-2$ and $T=2k-1+b$ then the set K is a subset of the set

$$K_a=\{a,\ a+q,\ a+2q,\ \ldots,\ a+(k-1+b)\,q\}$$

where a is an integral number, q a natural number.

Thus, if $T<3k-3$, the set K is a subset of arithmetical progression whose number of members is not larger than $T-k+1$.

Now will it make any difference if $T\geqslant 3k-3$? To specify: If we take all arithmetical progressions containing the set K and choose from them an arithmetical progression with the minimum of members, then we can call this minimum the „length" of K. The question arises whether it is possible, when examining the assembley of sets K with given k and T, to evaluate their length according to k and T for any K.

The example

$$K = \{0,\ 1,\ 2,\ \ldots,\ k-2,\ u\},\ u > 2k-4$$

proves that this is wrong even for $T = 3k-3$.

Nevertheless, results rather close to those obtained in theorem 1.9 take place even in case when $T \geqslant 3k-3$.

To formulate these results some new notions will be necessary, the most important of which is the generalisation of the notion of isomorphism of sets with algebraical operations.

3. Definition. Subsets B' and C' of sets B and C with algebraical operation written additively are called isomorphic if there is one-to-one mapping $B' \to C'$ such that the mapping $2B' \to 2C'$ induced naturally by the preceding mapping exists and is a one-to-one mapping. The mapping $B' \to C'$ of the above-mentioned definition is called isomorphic.

An isomorphic mapping of K does not change the value of T.

That is why the description of the structure of K must be invariant in respect of isomorphic mapping.

If $B' = B$, $C' = C$ and the mappings $B' \to C'$ and $2B' \to 2C'$ correspond, then our definition becomes a usual definition of isomorphism of sets with algebraical operations. In this case, the addition of any number of elements corresponding to summands gives an element corresponding to the sum.

Let us take two additive semi-groups $B' = \{0, 1, 2, \ldots\}$ and $C' = \{10,\ 11,\ 12,\ \ldots\}$. Then $B' \to C'$ $(u \to u + 10,$ $u = 0,\ 1,\ 2,\ \ldots)$, $2B' \to 2C'$ $(u \to u + 20,\ u = 0,\ 1,\ 2,\ \ldots)$ and therefore B' and C' are isomorphic. This example shows that correspondences $B' \leftrightarrow C'$, $2B' \leftrightarrow 2C'$ are sometimes contrary.

In case isomorphism of the two subsets correspondence exists, in general, when addition takes place only once. Thus the concept of isomorphism of subsets seems specially fitting for the study of the questions of addition of final number of sets.

And this is the very thing necessary for the purposes of the additive theory of numbers when we have a problem with a limited number of summands.

An analogy can be seen between local isomorphism of topological groups and isomorphism of subsets („al-

gebraically local isomorphism"). In the first case isomorphism is limited by a certain vicinity, in the second,— by the number of operations.

Let $B', C' \subset E_n$ (Euclid's space) and assume that there exists one-to-one correspondence of B' and C' such that $\bar{b}_1 - \bar{b}_2 = \bar{b}_3 - \bar{b}_4$ leads to $\bar{c}_1 - \bar{c}_2 = \bar{c}_3 - \bar{c}_4$, and $\bar{b}_1 - \bar{b}_2 \neq \bar{b}_3 - \bar{b}_4$ leads to $\bar{c}_1 - \bar{c}_2 \neq \bar{c}_3 - \bar{c}_4$, where $\bar{b}_i \in B'$, $\bar{c}_i \in C', \bar{b}_i \leftrightarrow \bar{c}_i$, $1 \leqslant i \leqslant 4$.

The above formulated conditions are the necessary and sufficient for B' and C' to be isomorphic.

4. ***The main theorem.*** If $T < Ck$, $C \geqslant 2$ then there exist such c, k_0 dependant only on C and such $n \leqslant [C-1]$, that in case when $k > k_0$ the set K is a part of a certain set K_0 of integral numbers which is isomorphic to a set of inner points of some convex set $D \subset E_n$, and $T(K_0) < ck$.

Here are some examples illustrating the main theorem.

If $2 \leqslant C < 3$, then $n = 1$, and D is an interval whose number of integral points is not larger than ck. Theorem 1.9 gives an elementary proof of a more powerful similar result. If $3 \leqslant C < 4$, then $n \leqslant 2$. If $n = 1$, then K is contained in the arithmetical progression whose number of elements is not larger than ck.

If $n = 2$ then it is possible to show that a rectangle can be taken as D.

Thus, in this case K is a part of some arithmetical progressions with equal differences, the first members of which form an arithmetical progression with another difference.

In fact, integral points of the rectangle situated on every line parallel to the axis of abscissas are transformed in arithmetical progressions with equal differences. The images of integral points of the rectangle situated on a certain line parallel to the axis of ordinates will be the assembly of the first members of these progressions.

The main theorem was proved with the help of a modification of the method of trigonometrical sums.

5. At present it is possible to express a certain general point of view concerning the study of additive regularities.

For this purpose we shall recall Klein's view of geometry as a science studying properties of geometrical objects that remain invariant when the latter are subjected to a certain group of transformations.

We can state now (see sect. 3) that *the goal of the additive theory of numbers while studying sets addition consists in the investigation of properties of sets, invariant under isomorphic transformations.*

From this point of view the study of relations between invariants of isomorphic transformations (henceforward called additive characteristics) appears to be very important.

The most important additive characteristics are T, R — the number of not equal positive differences $a_i - a_j$ and $M = \int_0^1 |S|^4 \, d\alpha$, where $S = \sum_{j=0}^{k-1} e^{2\pi i \alpha a_j}$ (if $b_1, b_2, \ldots, b_T$ are numbers of $2K$, and r_s is the number of representations $a_i + a_j = b_s$, then $M = \sum_{s=1}^{T} r_s^2$).

Inverse problems of the additive theory of numbers (sect. 1.7) can be stated as the problems of description of sets with given invariants.

The main theorem is the first step to realise the expressed ideas. In formulating and proving it, one of the important means used are isomorphic mappings of certain sets of integral numbers into lattices of Euclid's spaces of higher demension. It was possible to use them due to a fact that had naturally remained previously unnoticed, namely, that dimension is not an invariant of isomorphic transformation.

It is worth mentioning that density is not invariant and during isomorphic transformation can be altered:

$$A = \{0, 1, 4, 8, 12, \ldots\}, \quad \alpha'(A) = {}^1/_4,$$

$$B = \{0, 1, 3, 6, 9, \ldots\}, \quad \alpha'(B) = {}^1/_3.$$

This explains why the application of the concept of dencity has certain limitations.

6. The analogy between Klein's view of geometry and the view of the additive theory of numbers as a theory of isomorphic transformations is more deep-going than it may seem at first sight. It turns out that the

isomorphic transformation is an affinity in a specially chosen Euclid's space.

An isomorphic transformation of $K \subset E_m$ into E_n is called nonsingular if none of hyperplanes from E_n contains the image of K.

Let the non-singular transformation of the set K into E_n exist while the non-singular isomorphic transformation of K into E_{n+1} does not exist. Let r denote such number n. The number r is the additive characteristic of the set K.

Theorem. Let anyone of the hyperplanes from E_r contain neither final set $K_1 \subset E_r$ nor $K_2 \subset E_r$. Then and only then the sets K_1 and K_2 will be isomorphic if an affinity of E_r in itself can be found which transforms K_1 into K_2.

7. ***Applications***. Khinchin's theorem is a special case for Mann's theorem when two equal sequences are added:

$$\text{If } \alpha'(A) = \alpha,\ \alpha'(2A) = \gamma, \text{ then in case } a_0 = 0$$
$$\gamma \geqslant \min(2\alpha, 1).$$

An analogue to Mann's theorem for the case of addition sequences with positive asymptotic density was obtained by M. Kneser (1953).

Roughly, as a development to the theory of density it became possible to show that when two equal sequences are added the density becomes at least doubled, is multiplied by 2.

It was found that, in general, the figure 2 can be substituted by any positive constant C. Such is the essense of the results obtained from the main theorem.

Let A be an increasing sequence of integral nonnegative numbers:

$$A = \{a_0, a_1, \ldots, a_i, \ldots\},\ a_{i+1} > a_i,\ i \geqslant 0,$$
$$d(A) = \lim_{k \to \infty} (a_1 - a_0,\ a_2 - a_0,\ \ldots,\ a_k - a_0).$$

Here $(a_1 - a_0, a_2 - a_0, \ldots, a_k - a_0)$ is the greatest common divisor of numbers $a_1 - a_0, a_2 - a_0, \ldots, a_k - a_0$.

$A(x)$ (resp. $A_2(x)$) is the number of natural numbers of the sequence A (resp. sequence $2A$) that is not larger than x.

$\alpha = \alpha(A)$ is an asymptotical density of the sequence determined by equality

$$\alpha = \varliminf_{x\to\infty} \frac{A(x)}{x},$$

$$\gamma = \alpha(2A),$$

Z_n is a set of integral points of Euclid's space E_n, $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n$ is orthonormal basis in E_n.

Let φ: $Z_n \to Z_1$ be such a homomorphism that $\bar{e}_i\varphi = 0$, $1 \leqslant i \leqslant n-1$, $\bar{e}_n\varphi = 1$, $N^{(x)}$ is a subset of the set $N \subset E_n$ for points of which $x_n \leqslant x$.

As a consequence of the main theorem, the following theorem is proved in chapter III.

Theorem. Let sequence A satisfy the following conditions: $a_0 = 0$, $d(A) = 1$, $\alpha > 0$, $\gamma < C\alpha$, $C \geqslant 3/2$ and assume that there exists such constant C_1 that the inequality $a_{i+1} > C_1 a_i$ is fulfilled only for the final number of i.

There exist a cylinder $N \subset E_n$, $n \geqslant 2$, the base of which is the convex set $P \subset L(\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_{n-1})$, and positive constants c and α_0, depending only on C and C_1, such that for $\alpha < \alpha_0$

(1) $A \subset (N \cap Z_n)\varphi$,

(2) $N \cap Z_n$ and $(N \cap Z_n)\varphi$ are isomorphic,

(3) $V(P) < c\alpha$, $T(N^{(x)} \cap Z_n) < c\alpha x$,

(4) $n \leqslant [2C - 1]$.

A hypothesis for sequences of the zero density being the analogue of Khinchin's theorem was formulated by P. Erdos [23]. He supposed that

$$\delta = \varlimsup_{x\to\infty} \frac{A_2(x)}{A(x)} \geqslant 3,$$

if

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0.$$

With the help of the main theorem the following broader proposition was proved.

Theorem $\sigma \geqslant 3$, if $\lim\limits_{x\to\infty} \frac{A(x)}{x} = 0$, and

$$\overline{\lim_{x\to\infty}} \frac{A(x)}{x} < \frac{1}{2d(A)}.$$

The main theorem gives also applications for cases of sets addition for prime modulo residues (strengthening the results received by Cauchy, Davenport and Vosper) and for point sets of positive measure (strengthening Brun-Minkowsky's inequality).

8. In the main theorem the structure of the set K with small doubling ($T < Ck$) is investigated. The further possible ways of the investigation are the following: study of the structure of K when $T/k \to \infty$, generalisation of the problem for the case when several summands are taken or when the summands are different. It is possible to investigate the structure of K when different additive characteristics of the set K or their combinations are given. After dividing the sets consisting of a final number of integral numbers into classes of isomorphic sets it is possible to study the order of increase of the function $t(k)$,— i. e. the number of such classes for the given k. All these problems can be studied for sets of a more general nature than sets of integral numbers, specially in groups both Abelian and non-Abelian which is especially interesting.

УКАЗАТЕЛЬ ТЕРМИНОВ

В указателе терминов приводятся ссылки на нижеследующие книги.

Натансон И. П. Теория функций вещественной переменной, ГИТТЛ, М., 1957.

Курош А. Г. Лекции по общей алгебре, ФМ., М., 1962.

Касселс Дж. Введение в геометрию чисел, «Мир», М., 1965.

Оглавление

стр.

Сдано в набор 14/VI-1966 г. Подписано к печати 4/VIII-1936 г. ПФ 03140.
Формат бумаги 84 × 108¹/₃₂. Печ. л. 8,75. Заказ Б-298.
Тираж 1000 экз. Цена 80 коп.

Типография „Татполиграф" Управления по печати при Совете Министров ТАССР
Казань, ул. Мирславского, 9.