А. Я. ХИНЧИН

ТРИ ЖЕМЧУЖИНЫ ТЕОРИИ ЧИСЕЛ

ОГИЗ - ГОСТЕХИЗДАТ - 1948

А. Я. ХИНЧИН

ТРИ ЖЕМЧУЖИНЫ ТЕОРИИ ЧИСЕЛ

ИЗДАНИЕ ВТОРОЕ,
ПЕРЕРАБОТАННОЕ

ОГИЗ
ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1948 ЛЕНИНГРАД

11-3-1

АННОТАЦИЯ.

Аннотируемая книжка посвящена трём теоремам арифметики, бывшим, несмотря на свою кажущуюся простоту, предметом усилий многих крупных учёных-математиков. Излагаемые доказательства пользуются совершенно элементарными средствами (хотя и не очень просты). Книжка доступна учащимся старших классов средней школы и рассчитана на широкие круги любителей математики.

Редактор *Л. Я. Цлаф.* Техн. ред. *М. Д. Суховцева.*

Подписано к печати 22/X 1948 г. 4 печ. л. 3,6 уч.-изд. л. 36 000 тип. зн. в печ. л. А-07592. Тираж 25 000 экз. Цена книги 1 руб. 10 коп. Заказ № 8284.

Первая Образцовая типография имени А. А. Жданова треста «Полиграфкнига» Огиза при Совете Министров СССР. Москва, Валовая, 28.

ПИСЬМО НА ФРОНТ.
(Вместо предисловия)

Милый Серёжа!

Ваше письмо, присланное из госпиталя, трижды меня обрадовало. Прежде всего, Ваша просьба прислать Вам «каких-нибудь математических жемчужинок» показала мне, что Вы действительно поправляетесь, а не просто хотите, как мужественный боец, успокоить своих друзей. Это было для меня первой радостью.

Далее, Вы заставили меня задуматься над тем, почему в эту войну вот такие совсем юные бойцы, как Вы, при каждой небольшой передышке со всей страстью рвутся к своему любимому делу — к тому делу, которому они отдали себя ещё до войны и от которого были оторваны войной. В прошлую мировую войну этого не было. Тогда юноша, попавший на фронт, почти всегда чувствовал, что жизнь его переломилась, что всё, чем он жил прежде, стало для него невозможной сказкой. А сейчас ведь есть такие, которые в перерывах между боями пишут диссертации и защищают их, приехав в короткий отпуск! Не потому ли это, что Вы ощущаете всем существом Ваш ратный труд и Ваше любимое занятие — науку, искусство, практическую деятельность — как два звена одного и того же великого дела? И если так, то не есть ли это ощущение одна из главных движущих пружин Ваших побед, которыми мы здесь, в тылу, так восхищаемся?

Эта мысль очень меня обрадовала, и это была моя вторая радость.

И вот я стал думать о том, что бы такое Вам послать. Я Вас не очень близко знаю — всего один год Вы слушали мои лекции; и всё же у меня осталась твёрдая уверенность в Вашем глубоком и серьёзном отношении к науке, и мне не хотелось поэтому посылать Вам каких-нибудь «побрякушек», внешне эффектных, но научно мало содержательных. С другой стороны, я знал, что Ваша подготовка очень невелика — всего один год Вы провели на университетской скамье, а за три года непрерывного пребывания на фронте вряд ли имели время учиться. Поразмыслив несколько дней, я сделал выбор. Удачен он или нет — об этом судите уж Вы. Что касается меня, то я считаю те три теоремы арифметики, которые я Вам посылаю, настоящими жемчужинами нашей науки.

В арифметике, этой самой древней, но вечно юной ветви математики, от времени до времени встают замечательные, своеобразные задачи: по своему содержанию они так элементарны, что их может понять каждый школьник; речь идёт обычно о доказательстве какого-нибудь очень простого закона, господствующего в мире чисел; закона, который во всех проверенных частных случаях оказывался верным, и требуется установить, что он действительно верен всегда. И вот, несмотря на всю кажущуюся простоту задачи, решение её годами, а подчас и столетиями, не поддаётся усилиям самых крупных учёных эпохи. Согласитесь, что это очень увлекательно.

Я выбрал для Вас три таких задачи; все они разрешены в недавнее время, и в исторической судьбе их имеется две замечательных общих черты. Во-первых, все три задачи решены самыми элементарными арифметическими методами (не надо только смешивать элементарности с простотой: решения всех трёх задач, как Вы увидите, не очень просты, и Вам придётся затратить немало усилий, чтобы хорошо их понять и усвоить). Во-вторых, все три задачи, после ряда безуспеш-

ных атак со стороны «маститых» учёных, были решены совсем молодыми, начинающими математиками, юнцами едва ли не Вашего возраста. Правда, какой это многообещающий стимул для начинающих учёных вроде Вас, какой замечательный призыв к научному дерзанию?

Работа над изложением этих теорем заставила меня глубже вникнуть в структуру их великолепных доказательств и принесла мне большую радость.

Это была моя третья радость.

Желаю Вам самых лучших успехов — боевых и научных.

Ваш *А. Хинчин.*

24 марта 1945 г.

ГЛАВА I.

ТЕОРЕМА ВАН ДЕР ВАРДЕНА ОБ АРИФМЕТИЧЕСКИХ ПРОГРЕССИЯХ.

§ 1.

Летом 1928 г. я провёл несколько недель в Геттингене. По обыкновению, на летний семестр туда съехалось довольно много иностранных учёных. Со многими из них я познакомился, а с некоторыми даже сдружился. Злобой дня в момент моего прибытия был эффектный результат молодого голландца Ван дер Вардена — теперь известного учёного, а тогда ещё только начинающего юношу. Результат этот был получен тут же, в Геттингене, и всего за несколько дней до моего приезда; о нём мне с увлечением рассказывали почти все математики, с которыми я встречался.

История дела была такова. Один местный математик (имени его я не помню) в ходе своей научной работы был приведён к следующей проблеме: представьте себе, что множество всех натуральных чисел каким угодно способом разбито на две части (например, на числа чётные и нечётные, или на числа простые и составные, или любым другим способом); можно ли тогда утверждать, что по меньшей мере в одной из этих двух частей найдутся арифметические прогрессии сколь угодно длинные (длиною арифметической прогрессии я здесь и в дальнейшем буду называть просто число её членов)? Всем, кому ставили этот вопрос, задача на первый взгляд казалась совсем простой; положительное решение её представлялось почти очевидным. Однако первые попытки её преодоления ни к чему не привели. А так как геттингенские математики и их иностранные гости находились по традиции в постоянном общении друг с другом, то эта дразнящая своим сопротив-

лением проблема вскоре сделалась предметом всеобщего увлечения; за неё взялись все, от маститых учёных до начинающих студентов; после нескольких недель напряжённых усилий задача, наконец, уступила натиску приехавшего в Геттинген учиться юноши — голландца Ван дер Вардена. Я познакомился с ним и от него самого услышал найденное им решение; оно было элементарно, но далеко не просто; задача оказалась глубокой, видимость простоты была обманчивой.

Совсем недавно М. А. Лукомская (Минск) прислала мне найденное ею новое, значительно более простое и прозрачное доказательство теоремы Ван дер Вардена, которое я и изложу Вам в дальнейшем с любезного разрешения автора.

§ 2.

В сущности, Ван дер Варден доказал несколько больше, чем требовалось. Во-первых, он предполагает, что натуральные числа разбиты не на два, а на любое число k классов (множеств); во-вторых, чтобы гарантировать наличие по меньшей мере в одном из этих классов арифметической прогрессии данной (сколь угодно большой) длины l, как оказалось, нет необходимости разбивать весь натуральный ряд, а достаточно взять для этой цели лишь некоторый отрезок его; длина этого отрезка $n(k, l)$ есть функция чисел k и l; само собою понятно, что совершенно безразлично, где мы возьмём этот отрезок, лишь бы это были $n(k, l)$ последовательных натуральных чисел.

Таким образом, теорема Ван дер Вардена имеет следующую формулировку.

Пусть k и l — произвольные натуральные числа. Тогда существует такое натуральное число $n(k, l)$, что при разбиении любого отрезка ряда натуральных чисел длины $n(k, l)$ любым способом на k классов (среди которых могут быть и пустые), по крайней мере в одном из этих классов найдётся арифметическая прогрессия длины l.

Очевидно, эта теорема тривиальным образом верна при $l = 2$; чтобы в этом убедиться, достаточно положить $n(k, 2) = k + 1$; в самом деле, при разбиении $k + 1$ чисел на k классов, по крайней мере один из этих классов будет содержать более одного числа; но любая пара чисел образует арифметическую прогрессию длины 2, чем теорема и доказана. Мы докажем теорему методом полной индукции, при-

менённым к числу l. Таким образом, во всём дальнейшем мы будем считать, что теорема уже установлена для некоторого числа $l \geqslant 2$ и для любых значений k, и покажем, что в таком случае она остаётся верной и для числа $l+1$ (и также, разумеется, для любых значений k).

§ 3.

Итак, согласно нашему предположению, для любого натурального числа k существует такое натуральное число $n(k, l)$, что при разбиении любого отрезка натурального ряда длины $n(k, l)$ любым способом на k классов, по крайней мере в одном из этих классов найдётся арифметическая прогрессия длины l. Наша задача — доказать, что для любого натурального k существует и $n(k, l+1)$. Эту задачу мы решим прямым определением числа $n(k, l+1)$. С этой целью положим

$$q_0 = 1, \quad n_0 = n(k, l),$$

и затем последовательно определим числа q_1, q_2, ..., n_1, n_2, ... следующим образом: если для какого-нибудь $s > 0$ уже определены q_{s-1} и n_{s-1}, то мы полагаем

$$q_s = 2n_{s-1}q_{s-1}, \quad n_s = n(k^{q_s}, l) \quad (s = 1, 2, \ldots); \qquad (1)$$

очевидно, что тем самым числа n_s, q_s определены для любого $s \geqslant 0$. Мы утверждаем теперь, что за $n(k, l+1)$ можно принять число q_k. Мы должны, следовательно, доказать, что если отрезок натурального ряда длины q_k любым способом разбить на k классов, то по меньшей мере в одном из этих классов найдётся арифметическая прогрессия длины $l+1$. Этому доказательству и будет посвящена вся остающаяся часть настоящей главы.

Во всём дальнейшем мы для краткости положим $l+1 = l'$.

§ 4.

Итак, пусть отрезок Δ натурального ряда длины q_k разбит любым способом на k классов. Два числа a и b этого отрезка мы будем называть *однотипными* и писать $a \backsim b$, если a и b принадлежат одному и тому же классу. Два отрезка $\delta(a, a+1, \ldots, a+r)$ и $\delta'(a', a'+1, \ldots, a'+r)$ равной длины, принадлежащих отрезку Δ, мы будем называть

однотипными и писать $\delta \backsim \delta'$, если $a \backsim a'$, $a+1 \backsim a'+1$, $\ldots$, $a+r \backsim a'+r$. Очевидно, что число различных возможных типов, которым могут принадлежать числа отрезка Δ, равно k; для отрезков вида $(a, a+1)$ (т. е. для отрезков длины 2) число возможных типов равно k^2, и вообще, для отрезков длины m число возможных типов равно k^m (само собою разумеется, что некоторые из этих типов могут фактически отсутствовать в отрезке Δ).

Так как $q_k = 2n_{k-1}q_{k-1}$ (см. (1)), то отрезок Δ можно рассматривать как последовательность $2n_{k-1}$ отрезков длины q_{k-1}. Такие отрезки могут иметь, как мы только что видели, $k^{q_{k-1}}$ различных типов; но левая половина отрезка Δ содержит n_{k-1} таких отрезков, причём в силу (1) $n_{k-1} = n(k^{q_{k-1}}, l)$. Мы можем поэтому, по самому смыслу числа $n(k^{q_{k-1}}, l)$, утверждать следующее: левая половина отрезка Δ содержит арифметическую прогрессию из l однотипных между собою отрезков

$$\Delta_1, \Delta_2, \ldots, \Delta_l$$

длины q_{k-1}; при этом мы для краткости говорим, что равные между собою отрезки Δ_i образуют арифметическую прогрессию, если такую прогрессию образуют их первые числа. Разностью d_1 прогрессии $\Delta_1, \Delta_2, \ldots, \Delta_l$ мы будем называть разность первых чисел двух соседних отрезков этой прогрессии. Само собою разумеется, что разность вторых (или третьих, четвёртых и т. д.) чисел двух таких соседних отрезков также равна d_1.

К этой прогрессии из отрезков мы присоединим теперь ещё следующий, $l+1$-й член $\Delta_{l'}$, (вспомним, что $l' = l+1$), который, может быть, выйдет уже за пределы левой половины отрезка Δ, но во всяком случае будет ещё целиком принадлежать самому отрезку Δ; тогда отрезки $\Delta_1, \Delta_2, \ldots, \Delta_l, \Delta_{l'}$ образуют арифметическую прогрессию длины $l' = l+1$ и разности d_1 из отрезков длины q_{k-1}, причём $\Delta_1, \Delta_2, \ldots, \Delta_l$ между собою однотипны, а относительно типа последнего отрезка $\Delta_{l'}$ мы ничего не знаем. Этим завершается первый шаг нашей конструкции. Продумайте его как следует ещё раз, прежде чем итти дальше.

§ 5.

Теперь переходим ко второму шагу. Возьмём любой из l первых членов только что построенной прогрессии отрезков; пусть это будет Δ_{i_1}, так что $1 \leqslant i_1 \leqslant l$. Δ_{i_1} есть отрезок длины q_{k-1}. Мы поступим с ним в точной аналогии с тем, как только

что поступили с отрезком Δ. Так как $q_{k-1} = 2n_{k-2}q_{k-2}$, то левая половина отрезка Δ_{i_1} может рассматриваться как последовательность n_{k-2} отрезков длины q_{k-2}; но для отрезков этой длины возможно всего $k^{q_{k-2}}$ различных типов, а, с другой стороны, в силу (1) $n_{k-2} = n(k^{q_{k-2}}, l)$. Поэтому левая половина Δ_{i_1} должна содержать прогрессию из l однотипных отрезков $\Delta_{i_1 i_2} (1 \leqslant i_2 \leqslant l)$ длины q_{k-2}. Пусть разность этой прогрессии (т. е. расстояние между первыми числами двух её соседних отрезков) равна d_2. К этой прогрессии отрезков мы присоединим ещё её $l+1$-ый член $\Delta_{i_1 l'}$, про тип которого мы, конечно, ничего не знаем; отрезок $\Delta_{i_1 l'}$ может уже не принадлежать левой половине отрезка Δ_{i_1}, но, очевидно, должен принадлежать самому отрезку Δ_{i_1}.

Мы провели нашу конструкцию пока только в одном из отрезков Δ_{i_1}. Но теперь мы конгруэнтно перенесём её во все другие отрезки Δ_{i_1} $(1 \leqslant i_1 \leqslant l')$. Таким образом, мы получим семейство $\Delta_{i_1 i_2} (1 \leqslant i_1 \leqslant l', \ 1 \leqslant i_2 \leqslant l')$ отрезков уже с двумя индексами. При этом очевидно, что два любых отрезка этого семейства с индексами, не превосходящими l, будут однотипны между собою:

$$\Delta_{i_1 i_2} \backsim \Delta_{i'_1 i'_2} \quad (1 \leqslant i_1, \ i_2, \ i'_1, \ i'_2 \leqslant l).$$

Вам теперь уже несомненно ясно, что этот процесс мы можем продолжать и дальше. Мы проведём его k раз. Продуктами конструкции при нашем первом шаге были отрезки длины q_{k-1}, при втором — длины q_{k-2} и т. д. После k-го шага, таким образом, продуктами конструкции окажутся отрезки длины $q_0 = 1$, т. е. просто числа нашего первоначального отрезка Δ; тем не менее мы будем обозначать эти числа по-прежнему через

$$\Delta_{i_1 i_2 \ldots i_k} \quad (1 \leqslant i_1, \ i_2, \ \ldots, \ i_k \leqslant l').$$

При этом для $1 \leqslant s \leqslant k$ и $1 \leqslant i_1, \ \ldots, \ i_s, \ i'_1, \ \ldots, \ i'_s \leqslant l$

$$\Delta_{i_1 i_2 \ldots i_s} \backsim \Delta_{i'_1 i'_2 \ldots i'_s}. \tag{2}$$

Сделаем теперь два важных для дальнейшего замечания.

1) Если в соотношении (2) $s < k$ и если $i_{s+1}, i_{s+2}, \ldots, i_k$ — любые индексы, взятые из ряда 1, 2, ..., l, l', то число $\Delta_{i_1 i_2 \ldots i_{s+1} \ldots i_k}$ занимает в отрезке $\Delta_{i_1 \ldots i_s}$ такое же место,

как число $\Delta_{i_1 i_2 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k}$ в отрезке $\Delta_{i'_1 \ldots i'_s}$; а так как эти два отрезка в силу (2) однотипны, то отсюда следует, что

$$\Delta_{i_1 i_2 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k} \backsim \Delta_{i'_1 i'_2 \ldots i'_s i_{s+1} \ldots i_k}, \tag{3}$$

если $1 \leqslant i_1, \ldots, i_s, i'_1, \ldots, i'_s \leqslant l$,
$1 \leqslant i_{s+1}, i_{s+2}, \ldots, i_k \leqslant l'$ $(1 \leqslant s \leqslant k)$.

2) При $s \leqslant k$, $i'_s = i_s + 1$ отрезки $\Delta_{i_1 \ldots i_{s-1} i_s}$ и $\Delta_{i_1 \ldots i_{s-1} i'_s}$ будут, очевидно, соседними отрезками s-го шага нашей конструкции. Поэтому, каковы бы ни были индексы $i_{s+1}, \ldots, i_k$, числа $\Delta_{i_1 \ldots i_{s-1} i_s i_{s+1} \ldots i_k}$ и $\Delta_{i_1 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k}$ будут занимать одинаковые места в двух таких соседних отрезках, так что (при $i'_s = i_s + 1$)

$$\Delta_{i_1 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k} - \Delta_{i_1 \ldots i_{s-1} i_s i_{s+1} \ldots i_k} = d_s. \tag{4}$$

§ 6.

Мы теперь уже недалеки от нашей цели. Рассмотрим следующие $k+1$ чисел отрезка Δ:

$$\left.\begin{aligned} a_0 &= \Delta_{i'i'i' \ldots i'}, \\ a_1 &= \Delta_{1i'i' \ldots i'}, \\ a_2 &= \Delta_{11i' \ldots i'}, \\ &\ldots \quad \ldots \\ a_k &= \Delta_{11 \ldots 1}. \end{aligned}\right\} \tag{5}$$

Так как число классов, на которые разбит отрезок Δ, равно k, а чисел (5) мы имеем $k+1$, то среди этих чисел найдутся два, принадлежащих одному и тому же классу; пусть это будут числа a_r и a_s $(r < s)$, так что

$$\Delta_{\underbrace{1 \ldots 1}_{r} \underbrace{i' \ldots i'}_{k-r}} \backsim \Delta_{\underbrace{1 \ldots 1}_{s} \underbrace{i' \ldots i'}_{k-s}}. \tag{6}$$

Рассмотрим тогда $l+1$ чисел

$$c_i = \Delta_{\underbrace{1 \ldots 1}_{r} \underbrace{i \ldots i}_{s-r} \underbrace{i' \ldots i'}_{k-s}} \quad (1 \leqslant i \leqslant l'). \tag{7}$$

Первые l чисел этой группы (т. е. те, где $i < l'$) принадлежат

одному и тому же классу в силу (3). Что же касается последнего ($i = l'$), то оно однотипно с первым в силу (6). Таким образом, все $l+1$ чисел (7) однотипны между собою. Поэтому для доказательства нашего утверждения остаётся только убедиться, что эти числа образуют арифметическую прогрессию, т. е. что разность $c_{l+1} - c_l \; (1 \leqslant l \leqslant l)$ не зависит от i.

Положим для краткости $l+1 = i'$; положим, далее,

$$c_{i,m} = \Delta_{\underbrace{1\ldots1}_{r}\,\underbrace{i'\ldots i'}_{m}\,\underbrace{l\ldots l}_{s-r-m}\,\underbrace{i'\ldots i'}_{k-s}} \qquad (0 \leqslant m \leqslant s-r),$$

так что $c_{i,0} = c_l$, $c_{l,s-r} = c_{l+1}$ и, следовательно,

$$c_{l+1} - c_1 = \sum_{m=1}^{s-r} (c_{l,m} - c_{l,m-1}).$$

Но в силу (4)

$$c_{i,m} - c_{i,m-1} = \Delta_{\underbrace{1\ldots1}_{r}\,\underbrace{i'\ldots i'\,l\ldots l}_{m\quad s-r-m}\,\underbrace{i'\ldots i'}_{k-s}} - \Delta_{\underbrace{1\ldots1}_{r}\,\underbrace{i'\ldots i'}_{m-1}\,\underbrace{l\ldots l}_{s-r-m+1}\,\underbrace{i'\ldots i'}_{k-s}} = d_{r+m}$$

и, значит,

$$c_{l+1} - c_l = d_{r+1} + d_{r+2} + \ldots + d_s$$

и действительно не зависит от i, чем доказательство нашего утверждения полностью завершено.

Вы видите, сколь сложным может быть подчас совершенно элементарное построение. Однако это ещё не предел; в следующей главе Вы встретитесь с построением столь же элементарным, которое будет ещё значительно сложнее. Впрочем, мы вовсе на можем быть уверены в том, что теорема Ван дер Вардена не допускает ещё более простого доказательства, и всякие поиски в этом направлении можно только приветствовать.

ГЛАВА II.

ГИПОТЕЗА ЛАНДАУ-ШНИРЕЛЬМАНА И ТЕОРЕМА МАННА.

§ 1.

Может быть, Вам приходилось слышать о замечательной теореме Лагранжа: ***каждое натуральное число есть сумма не более чем четырёх квадратов.*** Другими словами, каждое натуральное число либо само есть квадрат другого числа, либо есть сумма двух, либо трёх, либо четырёх таких квадратов. Сейчас нам будет полезно представить себе содержание этой теоремы в несколько новой форме. Напишем ряд полных квадратов, начиная с нуля:

$$0,\ 1,\ 4,\ 9,\ 16,\ 25,\ \ldots; \qquad (Q)$$

это — некоторая последовательность целых чисел; обозначим её через Q и представим себе, что она выписана у нас в четырёх экземплярах Q_1, Q_2, Q_3, Q_4, ничем не отличающихся друг от друга. Теперь выберем любое число a_1^2 из Q_1, любое число a_2^2 из Q_2, любое число a_3^2 из Q_3 и любое число a_4^2 из Q_4 и сложим эти четыре числа между собою; полученная сумма

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2 \qquad (*)$$

может быть:

1) нулём (если $a_1 = a_2 = a_3 = a_4 = 0$);

2) квадратом натурального числа (если из чисел a_1, a_2, a_3, a_4 в каком-либо представлении (*) числа n три равны нулю, а четвёртое — не нуль);

3) суммой двух квадратов натуральных чисел (если в каком-либо представлении (*) числа n два из чисел a_1, a_2, a_3, a_4 равны нулю, а два других — не нули);

4) суммою трёх квадратов натуральных чисел (если в каком-либо представлении (*) числа n одно из чисел a_1, a_2, a_3, a_4 равно нулю, а три остальных — не нули);

5) суммою четырёх квадратов натуральных чисел (если в каком-либо представлении (*) числа n все четыре числа a_1, a_2, a_3, a_4 отличны от нуля).

Таким образом, полученное число n есть либо нуль, либо натуральное число, представимое в виде суммы не более чем четырёх квадратов, и ясно, что, обратно, всякое такое натуральное число может быть получено описанным нами процессом.

Теперь мы все натуральные числа n, которые могут быть получены нашим процессом (т. е. сложением четырёх чисел, взятых соответственно из последовательностей Q_1, Q_2, Q_3, Q_4), расположим по величине в последовательность

$$0,\ n_1,\ n_2,\ n_3,\ \ldots \qquad (A)$$

(причём $0 < n_1 < n_2 < n_3 < \ldots$, так что если среди построенных чисел имеются равные между собою, то из них в (A) входит только одно). Теорема Лагранжа тогда утверждает просто, что последовательность (A) содержит все натуральные числа, т. е. что $n_1 = 1$, $n_2 = 2$, $n_3 = 3$ и т. д.

Обобщим теперь наш процесс. Пусть мы имеем k возрастающих последовательностей целых чисел, начинающихся с нуля:

$$0,\ a_1^{(1)},\ a_2^{(1)},\ \ldots,\ a_m^{(1)},\ \ldots, \qquad (A^{(1)})$$

$$0,\ a_1^{(2)},\ a_2^{(2)},\ \ldots,\ a_m^{(2)},\ \ldots, \qquad (A^{(2)})$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$0,\ a_1^{(k)},\ a_2^{(k)},\ \ldots,\ a_m^{(k)},\ \ldots; \qquad (A^{(k)})$$

выберем по произволу по одному числу в каждой последовательности $A^{(i)}$ $(1 \leqslant i \leqslant k)$ и сложим между собою эти k чисел; совокупность всех построенных таким образом чисел образует, если мы расположим их в порядке возрастания, новую последовательность того же типа

$$0,\ n_1,\ n_2,\ \ldots,\ n_m,\ \ldots, \qquad (A)$$

которую мы будем называть *суммою* данных последовательностей $A^{(1)}$, $A^{(2)}$, ..., $A^{(k)}$:

$$A = A^{(1)} + A^{(2)} + \ldots + A^{(k)} = \sum_{i=1}^{k} A^{(i)}.$$

Содержание теоремы Лагранжа состоит в том, что сумма $Q+Q+Q+Q$ охватывает весь натуральный ряд.

Может быть, Вы слышали и о знаменитой теореме Ферма: *сумма $Q+Q$ охватывает все простые числа, которые при делении на 4 дают в остатке* 1 (т. е. числа 5, 13, 17, 29...). А, может быть, Вы знаете и о том, что знаменитый советский учёный Иван Матвеевич Виноградов доказал следующую замечательную теорему, над которой до этого двести лет безуспешно трудились многие из величайших математиков; *обозначая через P последовательность*

$$0,\ 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ldots, \qquad (P)$$

состоящую из нуля и всех простых чисел, можно утверждать, что сумма $P+P+P$ содержит все достаточно большие нечётные числа.

Все эти примеры я привёл здесь только с одной, и притом весьма скромной целью: познакомить Вас с понятием суммы числовых последовательностей и показать, как с помощью этого понятия можно просто и удобно формулировать некоторые классические теоремы теории чисел.

§ 2.

Как Вы, конечно, заметили, во всех приведённых примерах мы стремимся установить, что сумма определённого числа последовательностей представляет собою последовательность, охватывающую целиком или почти целиком тот или другой класс чисел (например, все натуральные числа, все достаточно большие нечётные числа и т. п.). Во всех других подобных задачах целью исследования является установление того, что сумма данных числовых последовательностей представляет собою множество чисел, в том или ином смысле *густо* расположенное в натуральном ряду. При этом часто речь идёт о том, что это множество охватывает весь натуральный ряд (как мы это имели в нашем первом примере). Теорема Лагранжа утверждает, что сумма четырёх последовательностей Q охватывает весь натуральный ряд. Вообще, если сумма k оди-

наковых последовательностей A охватывает все натуральные числа, то принято называть последовательность A *базисом* (натурального ряда) *порядка* k. Так, теорема Лагранжа утверждает, что последовательность Q точных квадратов есть базис четвёртого порядка. Позднее было установлено, что последовательность точных кубов образует базис девятого порядка. Как легко сообразить, всякий базис порядка k есть вместе с тем и базис порядка $k+1$.

Во всех этих и многих других примерах доказываемая «густота» суммы обусловлена особыми свойствами слагаемых последовательностей, т. е. специальной арифметической природой входящих в эти последовательности чисел (это — либо полные квадраты, либо простые числа, и т. п.). Замечательный советский учёный Лев Генрихович Шнирельман впервые поставил шестнадцать лет тому назад вопрос о том, в какой мере густота суммы нескольких последовательностей может быть обусловлена одною только густотою слагаемых, независимо от арифметической природы их? Эта задача оказалась не только глубокой и интересной, но и полезной при обработке некоторых классических проблем; за протекшие пятнадцать лет она привлекла к себе усилия многих выдающихся исследователей и породила богатую литературу.

Чтобы мы могли ставить в этой области точные задачи и слово «густота» писать без кавычек, мы, очевидно, должны прежде всего условиться, каким числом (или какими числами) мы будем измерять «густоту» наших последовательностей (подобным образом в физике слова «тёплый» и «холодный» получают точный научный смысл только после того, как мы научимся измерять температуру).

Очень удобная мера «густоты» числовой последовательности, принятая теперь в науке для всех проблем рассматриваемого нами типа, была предложена Л. Г. Шнирельманом. Пусть

$$0,\ a_1,\ a_2,\ \ldots,\ a_n,\ \ldots \qquad (A)$$

— числовая последовательность, в которой, как обычно, все a_n — натуральные числа и $a_n < a_{n+1}$ $(n = 1, 2, \ldots)$. Обозначим через $A(n)$ число натуральных чисел последовательности (A), не превосходящих n (нуль при этом не считается), так что $0 \leqslant A(n) \leqslant n$, вследствие чего

$$0 \leqslant \frac{A(n)}{n} \leqslant 1.$$

Очевидно, дробь $\frac{A(n)}{n}$, которая, конечно, для разных n имеет разные значения, может рассматриваться как некая средняя плотность последовательности (A) на отрезке натурального ряда от 1 до n. *Нижнюю границу* всех значений этой дроби Шнирельман предложил называть *плотностью* последовательности (A) (на всём натуральном ряду); мы будем обозначать эту плотность через $d(A)$.

Чтобы усвоить сразу элементарные черты этого понятия, я рекомендую Вам самостоятельно установить следующие предложения:

1. Если $a_1 > 1$ (т. е. если последовательность (A) не содержит единицы), то $d(A) = 0$.

2. Если $a_n = 1 + r(n-1)$ (т. е. последовательность (A), начиная с a_1, есть арифметическая прогрессия с первым членом 1 и разностью r), то

$$d(A) = \frac{1}{r}.$$

3. Плотность всякой геометрической прогрессии равна нулю.

4. Плотность ряда точных квадратов равна нулю.

5. Для того чтобы последовательность (A) содержала весь натуральный ряд ($a_n = n$, $n = 1, 2, \ldots$), необходимо и достаточно, чтобы $d(A) = 1$.

6. Если $d(A) = 0$ и A содержит число 1, то при любом $\varepsilon > 0$ можно найти сколь угодно большое число N, для которого

$$A(N) < \varepsilon N.$$

Если Вы всё это доказали, то Вы ознакомились с понятием плотности достаточно, чтобы работать с ним. Теперь я хочу познакомить Вас с доказательством следующей замечательной, хотя и очень простой леммы Шнирельмана:

$$d(A+B) \geqslant d(A) + d(B) - d(A)\,d(B). \qquad (1)$$

Смысл этого неравенства понятен: плотность суммы любых двух числовых последовательностей не меньше, чем сумма их плотностей, уменьшенная на произведение этих плотностей. Это «неравенство Шнирельмана» представляет собой первое, пока ещё грубое орудие для оценки плотности суммы по плотностям слагаемых. Вот его доказательство. Обозначим

через $A(n)$ число натуральных чисел, входящих в последовательность A и не превосходящих n, и через $B(n)$ — аналогичное число для последовательности B и положим для краткости $d(A)=\alpha$, $d(B)=\beta$, $A+B=C$, $d(C)=\gamma$. Отрезок $(1, n)$ натурального ряда содержит $A(n)$ чисел последовательности A, каждое из которых входит и в последовательность C. Пусть a_k и a_{k+1} — два последовательных числа этой группы; между ними лежит $a_{k+1}-a_k-1=l$ чисел, не принадлежащих A; это — числа

$$a_k+1,\ a_k+2,\ldots,\ a_k+l=a_{k+1}-1;$$

некоторые из них будут входить в C, например, все числа вида a_k+r, где r входит в B (что мы кратко будем записывать так: $r\in B$); но чисел этого последнего вида будет столько, сколько в отрезке $(1, l)$ содержится чисел, принадлежащих B, т. е. $B(l)$. Таким образом, всякий отрезок длины l, заключённый между двумя соседними числами последовательности A, содержит не менее чем $B(l)$ чисел, принадлежащих C. Отсюда следует, что число $C(n)$ чисел отрезка $(1, n)$, входящих в C, не меньше чем

$$A(n)+\sum B(l),$$

где сумма распространяется на все отрезки, свободные от чисел, входящих в A. Но $B(l)\geqslant\beta l$ по определению плотности, так что

$$C(n)\geqslant A(n)+\beta\sum l=A(n)+\beta\{n-A(n)\},$$

так как $\sum l$ есть сумма длин всех отрезков, свободных от чисел, входящих в A, т. е. просто число $n-A(n)$ чисел отрезка $(1, n)$, не входящих в A. Но $A(n)\geqslant\alpha n$, и следовательно,

$$C(n)\geqslant A(n)(1-\beta)+\beta n\geqslant\alpha n(1-\beta)+\beta n,$$

откуда

$$\frac{C(n)}{n}\geqslant\alpha+\beta-\alpha\beta;$$

а так как это неравенство выполняется для любого натурального n, то

$$\gamma=d(C)\geqslant\alpha+\beta-\alpha\beta,$$

что и требовалось доказать.

Неравенство Шнирельмана (1) может быть записано в эквивалентном виде:

$$1 - d(A + B) \leqslant \{1 - d(A)\}\{1 - d(B)\},$$

и в этом виде легко поддаётся обобщению на случай любого числа слагаемых:

$$1 - d(A_1 + A_2 + \ldots + A_k) \leqslant \prod_{i=1}^{k} \{1 - d(A_i)\}.$$

Доказательство проводится простой индукцией; Вы без труда с ним справитесь сами. Если записать последнее неравенство в виде

$$d(A_1 + A_2 + \ldots + A_k) \geqslant 1 - \prod_{i=1}^{k} \{1 - d(A_i)\}, \qquad (2)$$

то оно снова даёт возможность оценить плотность суммы по плотностям слагаемых. Л. Г. Шнирельман извлёк из своего элементарного неравенства ряд весьма замечательных следствий и прежде всего — следующую важную теорему:

Всякая последовательность положительной плотности есть базис натурального ряда.

Другими словами, если $\alpha = d(A) > 0$, то сумма достаточно большого числа последовательностей A охватывает весь натуральный ряд. Доказательство этой теоремы настолько просто, что мне хочется рассказать его Вам, хотя это немного и отвлечёт нас от нашей прямой задачи.

Если мы условимся для краткости обозначать через A_k сумму k последовательностей, каждая из которых совпадает с A, то в силу неравенства (2)

$$d(A_k) \geqslant 1 - (1 - \alpha)^k;$$

так как $\alpha > 0$, то при достаточно большом k

$$d(A_k) > \frac{1}{2}. \qquad (3)$$

Теперь легко показать, что последовательность A_{2k} охватывает весь натуральный ряд. Это просто вытекает из следующего общего предложения.

Лемма. *Если $A(n) + B(n) > n - 1$, то n входит в $A + B$.*

В самом деле, если n входит в A или в B, то всё доказано. Поэтому мы можем предположить, что n не входит ни

в A, ни в B; тогда $A(n)=A(n-1)$ и $B(n)=B(n-1)$ и, следовательно,

$$A(n-1)+B(n-1)>n-1.$$

Пусть $a_1, a_2, \ldots, a_r$ и $b_1, b_2, \ldots, b_s$ означают числа отрезка $(1, n-1)$, входящие соответственно в A и B, так что $r=A(n-1)$, $s=B(n-1)$; тогда все числа

$$a_1, a_2, \ldots, a_r,$$
$$n-b_1, n-b_2, \ldots, n-b_s$$

принадлежат отрезку $(1, n-1)$; число этих чисел равно $r+s=A(n-1)+B(n-1)>n-1$; поэтому одно из чисел верхнего ряда равно одному из чисел нижнего ряда; пусть $a_i=n-b_k$; тогда $n=a_i+b_k$, т. е. n входит в $A+B$.

Возвращаясь теперь к нашему рассуждению, мы в силу (3) имеем для любого n:

$$A_k(n)>\frac{1}{2}n>\frac{1}{2}(n-1),$$

и значит

$$A_k(n)+A_k(n)>n-1,$$

откуда в силу только что доказанной леммы n входит в $A_k+A_k=A_{2k}$. Но n — любое натуральное число, и следовательно, наша теорема доказана.

Эта простая теорема получила в работах Л. Г. Шнирельмана ряд важных приложений. Так, им впервые установлено, что последовательность, состоящая из единицы и всех простых чисел, есть базис натурального ряда. Правда, эта последовательность P, как показал ещё Эйлер, имеет плотность нуль, так что непосредственно применить к ней только что доказанную нами теорему нельзя. Но Шнирельману удалось доказать, что $P+P$ имеет положительную плотность; значит, $P+P$, а следовательно и P, действительно образует базис. Из этого легко заключить, что при достаточно большом k любое натуральное число, кроме 1, может быть представлено как сумма не более чем k простых чисел. Для своего времени (1930 г.) этот результат был фундаментальным и вызвал величайший интерес в научном мире. В наши дни, как я уже сообщал Вам в начале этой главы, мы благодаря замечательным исследованиям И. М. Виноградова знаем в этом направлении значительно больше.

§ 3.

Во всём предшествующем мне хотелось возможно более коротким путём ввести Вас в проблематику той своеобразной и интересной области теории чисел, разработке которой положили начало замечательные работы Л. Г. Шнирельмана. Однако непосредственной целью настоящей главы будет служить одна определённая задача этой области; к постановке этой задачи я теперь и перехожу.

Осенью 1931 года, вернувшись из заграничной командировки, Л. Г. Шнирельман, рассказывая нам о своих беседах с Ландау в Геттингене, сообщил, между прочим, что в ходе этих бесед они установили следующий интересный факт: для всех конкретных примеров, какие им удавалось придумать, неравенство

$$d(A+B) \geqslant d(A)+d(B)-d(A)\,d(B),$$

которое мы установили в § 2, можно было заменить более сильным (и более простым) неравенством

$$d(A+B) \geqslant d(A)+d(B), \tag{4}$$

т. е. плотность суммы всегда оказывалась не менее суммы плотностей слагаемых (при само собою разумеющемся условии, что $d(A)+d(B) \leqslant 1$). Они поэтому, естественно, предположили, что неравенство (4) является общим законом; но доказательство этой гипотезы при первых попытках не удавалось; сразу стало ясно, что если высказанная ими гипотеза и верна, то путь к её доказательству во всяком случае будет очень нелёгким. Отметим тут же, что если гипотетическое неравенство (4) действительно является общим законом, то закон этот с помощью элементарной индукции немедленно переносится на случай любого числа слагаемых, т. е. при $\sum_{i=1}^{k} d(A_i) \leqslant 1$ мы имеем

$$d\left(\sum_{i=1}^{k} A_i\right) \geqslant \sum_{i=1}^{k} d(A). \tag{5}$$

Поставленная таким образом задача, помимо простоты и изящества гипотетического общего закона (4), естественно-

должна была привлечь к себе внимание исследователей также и острым контрастом между элементарностью проблемы и выяснившейся уже с первых шагов трудностью её решения. Я сам тогда очень ею увлёкся и оставил ради неё все другие свои исследования. После нескольких месяцев напряжённой работы мне в начале 1932 г. удалось доказать неравенство (4) для важнейшего частного случая $d(A)=d(B)$ (этот случай должен быть признан важнейшим потому, что в большинстве конкретных задач все слагаемые просто совпадают между собою). Одновременно я доказал и общее неравенство (5) в предположении, что $d(A_1)=d(A_2)=\ldots=d(A_k)$ (этот результат, как легко видеть, не может быть получен простой индукцией из предыдущего и требует особого доказательства). Метод, которым я пользовался, был вполне элементарным, но очень сложным; позднее мне удалось несколько упростить доказательство.

Как бы то ни было, это был всего лишь частный случай! Довольно долго мне казалось, что не очень хитрое усовершенствование моего метода должно привести к полному решению задачи; однако все мои усилия в этом направлении остались бесплодными.

Между тем, опубликование моей работы привлекло к гипотезе Ландау-Шнирельмана внимание весьма широких кругов исследователей во всех странах. Было получено много незначительных частных результатов, создалась целая литература. Некоторыми авторами проблема была перенесена из области натуральных чисел в другие области. Словом, проблема стала «модной»; учёные общества предлагали её на премию; мои друзья из Англии в 1935 г. писали мне, что добрая половина английских математиков, отложив все очередные дела, занялась решением этой задачи. Ландау в своей книге, посвящённой последним достижениям аддитивной теории чисел, писал, что хотел бы «запечатлеть эту задачу в сердце читателя». Но она оказалась очень упорной, и целый ряд лет не поддавалась усилиям самых искусных исследователей. Только в 1942 г., наконец, с нею справился молодой американский математик Манн: он нашёл полное доказательство неравенства (4) (а значит и неравенства (5)). Его метод вполне элементарен и по стилю близок к методу моей работы, хотя и основан совсем на другой идее. Доказательство очень сложно и длинно, и я не решился бы предложить его Вам здесь. Но год спустя, в 1943 г., Артин и Шерк опубликовали

новое доказательство той же теоремы, основанное совсем на другой мысли и значительно более прозрачное и короткое, хоть и попрежнему совершенно элементарное. Вот это доказательство я и хочу Вам рассказать; ради него я стал писать эту главу, и оно составит собою содержание всех последующих её параграфов.

§ 4.

Итак, пусть A и B — две последовательности; положим $A+B=C$; пусть $A(n)$, $d(A)$, и т. д. имеют обычный смысл. Напомним, что все наши последовательности начинаются с нуля, но при подсчёте $A(n)$, $B(n)$, $C(n)$ принимаются во внимание только натуральные числа, входящие в эти последовательности. Требуется доказать, что при условии $d(A)+d(B)\leqslant 1$ мы имеем

$$d(C)\geqslant d(A)+d(B). \tag{6}$$

В дальнейшем мы для краткости положим $d(A)=\alpha$, $d(B)=\beta$.

Основная лемма. *Для любого натурального числа n существует такое число m $(1\leqslant m\leqslant n)$, что*

$$C(n)-C(n-m)\geqslant(\alpha+\beta)m.$$

Другими словами, существует такой «конец» $(n-m+1, n)$ отрезка $(1, n)$, в котором средняя плотность последовательности C не меньше, чем $\alpha+\beta$.

В дальнейшем перед нами две задачи: 1) доказать основную лемму и 2) показать, что из основной леммы вытекает неравенство (6). Из этих задач вторая несравненно легче первой, поэтому мы с неё начнём.

Итак, пусть основная лемма установлена. В некотором «конце» $(n-m+1, n)$ отрезка $(1, n)$ средняя плотность последовательности C не меньше, чем $\alpha+\beta$. Но отрезок $(1, n-m)$, в силу основной леммы, снова имеет некоторый «конец» $(n-m-m'+1, n-m)$, в котором средняя плотность C не меньше, чем $\alpha+\beta$. Продолжая это рассуждение, мы, очевидно, в конечном счёте разобьём отрезок $(1, n)$ на конечное число отрезков, в каждом из которых средняя плотность C

не меньше, чем $\alpha+\beta$. Значит, и на всём отрезке $(1, n)$ средняя плотность последовательности C не меньше, чем $\alpha+\beta$. А так как число n произвольно, то

$$d(C)\geqslant\alpha+\beta,$$

что и требовалось доказать.

Таким образом, задача сводится к доказательству основной леммы. К этому доказательству, которое будет длинным и сложным, мы теперь и переходим.

§ 5.

Нормальные последовательности.

Во всём дальнейшем мы будем считать число n твёрдо закреплённым, и все последовательности, которые мы будем рассматривать, будут состоять из числа 0 и некоторых чисел отрезка $(1, n)$. Условимся называть такую последовательность H ***нормальной***, если она обладает следующим свойством: для любых чисел f и f' отрезка $(1, n)$, не входящих в H, число $f+f'-n$ также не входит в H (при этом не исключается случай $f=f'$).

Если число n принадлежит последовательности C, то

$$C(n)-C(n-1)=1\geqslant(\alpha+\beta)\cdot 1,$$

так что основная лемма тривиальным образом верна ($m=1$). Поэтому во всём дальнейшем — прошу Вас твёрдо запомнить это — мы будем предполагать, что n не входит в C.

Убедимся прежде всего, что основная лемма может быть очень легко установлена в случае, когда последовательность C нормальна. В самом деле, обозначим через m наименьшее положительное число, не входящее в C ($m\leqslant n$, так как по предположению n не входит в C). Пусть s — любое число, заключённое между $n-m$ и n, $n-m<s<n$; тогда $0<s+m-n<m$. Я утверждаю, что $s\in C$; в самом деле, если бы это было не так, то по свойству нормальности число $s+m-n$ не входило бы в C; но мы только что видели, что это число меньше m, между тем как m по определению есть ***наименьшее*** положительное число, не входящее в C.

Итак, все числа s отрезка $n-m < s < n$ входят в C, откуда

$$C(n) - C(n-m) = m - 1.$$

С другой стороны, так как m не входит в $C = A + B$, то, в силу леммы стр. 20, $A(m) + B(m) \leqslant m - 1$. Следовательно,

$$C(n) - C(n-m) \geqslant A(m) + B(m) \geqslant (\alpha + \beta)\, m, \qquad (7)$$

что и составляет собою утверждение основной леммы.

§ 6.

Канонические расширения.

Мы обращаемся теперь к случаю, когда последовательность $C = A + B$ не обладает свойством нормальности. В этом случае мы будем добавлять к множеству B по совершенно определённому правилу новые, не содержащиеся в нём числа, переходя таким образом от B к расширенному множеству B_1; множество $A + B_1 = C_1$, очевидно, будет тогда некоторым расширением множества C. Как я уже указал, это расширение множеств B и C (причём множество A остаётся неизменным) будет строго, единственным образом определённым; оно возможно тогда и только тогда, если множество C не нормально. Мы будем называть это расширение ***каноническим расширением*** множеств B и C. В дальнейшем мы установим несколько важных свойств канонических расширений и с помощью них завершим доказательство основной леммы.

Я перехожу к определению канонического расширения множеств B и C. Если C не обладает нормальностью, то в отрезке $(0, n)$ существуют два числа c и c', такие, что

$$c \notin C,\ c' \notin C,\ c + c' - n \in C.$$

Так как $C = A + B$, то отсюда

$$c + c' - n = a + b \quad (a \in A,\ b \in B). \qquad (8)$$

Пусть β_0 есть наименьшее число множества B, могущее выступать в роли числа b в равенстве (8); другими словами, β_0 есть наименьшее число $b \in B$, для которого выполняется соотношение (8) при надлежащем выборе чисел отрезка $(0, n)$

$c \notin C$, $c' \notin C$, $a \in A$. Это число β_0 мы будем называть *базой* нашего расширения.

Уравнение

$$c + c' - n = a + \beta_0, \tag{9}$$

таким образом, обязательно имеет решения в числах c, c', a, удовлетворяющие требованиям

$$c \notin C,\ c' \notin C,\ a \in A,$$

причём все три числа принадлежат отрезку $(0, n)$. Все удовлетворяющие уравнению (9) и перечисленным требованиям числа c и c' мы объединяем в множество C^*. Очевидно, что множества C и C^* не имеют ни одного общего элемента. Соединение их (т. е. совокупность всех чисел, входящих либо в C, либо в C^*)

$$C \cup C^* = C_1\ ^{1})$$

мы и назовём каноническим расширением множества C.

Рассмотрим теперь выражение $\beta_0 + n - c$; если заставить в нём c пробегать все числа только что построенного нами множества C^*, то значения этого выражения образуют некоторое множество B^*; при этом в силу уравнения (9) каждое такое число $\beta_0 + n - c$ $(c \in C^*)$ может быть представлено в виде $c' - a$, где $c' \in C^*$, $a \in A$.

Пусть b^* — любое число, входящее в B^*; имея форму $\beta_0 + n - c$, оно $\geqslant \beta_0 \geqslant 0$; имея же форму $c' - a$ $(c' \in C^*$, $a \in A)$, оно $\leqslant c' \leqslant n$; таким образом, все числа множества B^* принадлежат отрезку $(0, n)$. Кроме того, если $b^* \in B^*$, то $b^* \notin B$, так как в противном случае из $b^* = c' - a$ следовало бы $c' = a + b^* \in A + B = C$, что неверно.

Итак, множество B^* расположено на отрезке $(0, n)$ и не имеет общих элементов с множеством B. Мы положим

$$B \cup B^* = B_1$$

и будем называть множество B_1 каноническим расширением множества B.

Убедимся, прежде всего, что

$$A + B_1 = C_1.$$

---

1) Мы здесь и в дальнейшем для соединения множеств пользуемся знаком $\cup$, так как знак $+$ имеет у нас другой смысл.

Пусть, во первых, $a \in A$, $b_1 \in B_1$; покажем, что $a + b_1 \in C_1$. Из $b_1 \in B_1$ следует, что либо $b_1 \in B$, либо $b_1 \in B^*$; если $b_1 \in B$, то $a + b_1 \in A + B = C \subset C_1$; если же $b_1 \in B^*$, то $a + b_1$ либо входит в C, а значит и в C_1, либо $a + b_1 \notin C$; но в этом случае (так как b_1, будучи элементом множества B^*, имеет вид $\beta_0 + n - c'$, $c' \notin C$) мы получаем

$$c = a + b_1 = a + \beta_0 + n - c' \notin C;$$

таким образом,

$$c + c' - n = a + \beta_0 \in A + B = C,$$

причём $c \notin C$ и $c' \notin C$; но тогда по определению множества C^* мы находим

$$c = a + b_1 \in C^* \subset C_1,$$

что и требовалось доказать. Итак, мы доказали, что $A + B_1 \subset C_1$.

Чтобы доказать обратное соотношение, допустим, что $c \in C_1$, откуда либо $c \in C$, либо $c \in C^*$. Если $c \in C$, то $c = a + b$, $a \in A$, $b \in B \subset B_1$. Если же $c \in C^*$, то число $b^* = c - a$, как мы знаем, при некотором $a \in A$ входит в B^*. Мы находим $c = a + b^* \in A + B^* \subset A + B_1$. Таким образом, $C_1 \subset A + B_1$; а так как, по ранее доказанному, и $A + B_1 \subset C_1$, то, значит, $C_1 = A + B_1$.

Теперь я напомню Вам, что, по нашему предположению, $n \notin C$; легко видеть — и это важно для нас — что число n не входит и в расширенное множество C_1; в самом деле, в случае $n \in C^*$ мы, по определению C^*, могли бы положить в соотношении (9) $c' = n$, что дало бы $c = a + \beta_0 \in A + B = C$, между тем как $c \notin C$ по смыслу соотношения (9).

Если расширенная последовательность C_1 всё ещё не нормальна, то в силу $A + B_1 = C_1$ и $n \notin C_1$ мы в лице множеств A, B_1 и C_1 имеем тройку со всеми свойствами тройки A, B, C, необходимыми для нового канонического расширения.

Мы находим новую базу β_1 этого расширения, аналогично предыдущему определяем добавочные множества B_1^*, C_1^*, полагаем

$$B_1 \cup B_1^* = B_2, \quad C_1 \cup C_1^* = C_2$$

и можем снова утверждать, что $A+B_2=C_2$ и $n\in C_2$. Этот процесс можно, очевидно, продолжать до тех пор, покуда одно из расширенных множеств C_h не окажется нормальным. Такой момент, очевидно, обязательно должен наступить, так как при каждом расширении мы вводим в множества B_μ и C_μ новые числа, не выходя при этом за пределы отрезка $(0, n)$.

Мы получаем таким образом конечный ряд множеств

$$B=B_0\subset B_1\subset\ldots\subset B_h,$$
$$C=C_0\subset C_1\subset\ldots\subset C_h,$$

причём всякое $B_{\mu+1}$ (соответственно $C_{\mu+1}$) содержит числа, не входящие в B_μ (C_μ) и образующие множество B_μ^* (C_μ^*), так что

$$B_{\mu+1}=B_\mu\cup B_\mu^*,\ G_{\mu+1}=C_\mu\cup C_\mu^*\ (0\leqslant\mu\leqslant h-1).$$

При этом мы обозначим через β_μ базу расширения, переводящего (B_μ, C_μ) в $(B_{\mu+1}, C_{\mu+1})$. Мы имеем

$$A+B_\mu=C_\mu,\quad n\notin C_\mu\quad(0\leqslant\mu\leqslant h);$$

наконец, множество C_h нормально, в то время как множества $C_\mu\,(0\leqslant\mu\leqslant h-1)$ этим свойством не обладают.

§ 7.

Свойства канонических расширений.

Нужные нам для дальнейшего свойства канонических расширений мы теперь сформулируем и докажем в виде трёх лемм, из которых только последняя найдёт себе дальше применение; леммы же 1 и 2 нужны лишь для доказательства леммы 3.

Лемма 1. $\beta_\mu>\beta_{\mu-1}\,(1\leqslant\mu\leqslant h-1)$, *т. е. базы последовательных канонических расширений образуют возрастающую последовательность.*

В самом деле, так как $\beta_\mu\in B_\mu=B_{\mu-1}\cup B_{\mu-1}^*$, то либо $\beta_\mu\in B_{\mu-1}^*$, и тогда β_μ имеет вид

$$\beta_\mu=\beta_{\mu-1}+n-c,$$

где $c \in C^*_{\mu-1} \subset C_\mu$ и потому $c < n$, так что $\beta_\mu > \beta_{\mu-1}$, и лемма 1 доказана; либо $\beta_\mu \in B_{\mu-1}$; в этом случае мы замечаем, что, по определению числа β_μ, существуют числа $a \in A$, $c \notin C_\mu$, $c' \notin C_\mu$, связанные соотношением

$$c + c' - n = a + \beta_\mu \in C_\mu;$$

но при $\beta_\mu \in B_{\mu-1}$

$$c + c' - n = a + \beta_\mu \in A + B_{\mu-1} = C_{\mu-1}, \qquad (10)$$

причём $c \notin C_{\mu-1}$, $c' \notin C_{\mu-1}$; поэтому $\beta_\mu \geqslant \beta_{\mu-1}$ по свойству минимальности $\beta_{\mu-1}$; но при $\beta_\mu = \beta_{\mu-1}$ мы по определению множества $C^*_{\mu-1}$ имели бы из (10)

$$c \in C^*_{\mu-1} \subset C_\mu, \quad c' \in C^*_{\mu-1} \subset C_\mu;$$

так как то и другое неверно, то $\beta_\mu > \beta_{\mu-1}$.

Во всём дальнейшем мы через m будем обозначать наименьшее положительное число, не входящее в C_h.

Лемма 2. *Если* $c \in C^*_\mu$, $0 \leqslant \mu \leqslant h-1$ и $n - m < c < n$, *то* $c > n - m + \beta_\mu$, *т. е. все числа с множества* C^*_μ, *лежащие в отрезке* $n - m < c < n$, *заключены в части этого отрезка, характеризуемой неравенствами* $n - m + \beta_\mu < c < n$.

Мы должны доказать соотношение

$$c + m - n > \beta_\mu.$$

Из $n - m < c < n$ следует

$$0 < m + c - n < m,$$

откуда, по определению числа m,

$$m + c - n \in C_h.$$

Но

$$C_h = C_\mu \cup C^*_\mu \cup C^*_{\mu+1} \cup \ldots \cup C^*_{h-1};$$

поэтому мы в дальнейшем будем различать два случая.

1) Если $m + c - n \in C_\mu$, то

$$m + c - n = a + b_\mu, \quad a \in A, \quad b_\mu \in B_\mu,$$

но $m \notin C_\mu$ и $c \notin C_\mu$ (последнее в силу $c \in C_\mu^*$), а потому по свойству минимальности β_μ мы должны иметь $b_\mu \geqslant \beta_\mu$; но при $b_\mu = \beta_\mu$ мы по определению множества C_μ^* имели бы $m \in C_\mu^*$, что неверно, ибо $C_\mu^* \subset C_\mu \subset C_h$, а $m \notin C_h$; поэтому $b_\mu > \beta_\mu$, а значит

$$m + c - n = a + b_\mu \geqslant b_\mu > \beta_\mu,$$

и лемма 2 доказана.

2) Если $c' = m + c - n \in C_\nu^*$, $\mu \leqslant \nu \leqslant h-1$, то, по определению множества C_ν^*, c' удовлетворяет уравнению типа (9)

$$c' - a = \beta_\nu + n - c'',$$

где $a \in A$, $c'' \in C_\nu^*$; отсюда $c' \geqslant c' - a > \beta_\nu \geqslant \beta_\mu$ (последнее в силу леммы 1), и лемма 2 снова доказана.

Лемма 3.

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \quad (0 \leqslant \mu \leqslant h-1),$$

т. е. число чисел $c \in C_\mu^*$ в отрезке $n-m < c < n$ в точности равно числу чисел $b \in B_\mu^*$ в отрезке $0 < b < m$ (той же длины).

Рассмотрим соотношение

$$b = \beta_\mu + n - c; \tag{11}$$

по самому определению множеств B_μ^* и C_μ^*, из $c \in C_\mu^*$ следует $b \in B_\mu^*$, и обратно; при этом, если $n - m + \beta_\mu < c < n$, то $\beta_\mu < b < m$, и обратно; таким образом

$$C_\mu^*(n) - C_\mu^*(n - m + \beta_\mu) = B_\mu^*(m-1) - B_\mu^*(\beta_\mu).$$

Но в силу леммы 2, $C_\mu^*(n - m + \beta_\mu) = C_\mu^*(n-m)$; с другой стороны, всякое $b \in B_\mu^*$ выражается в виде (11), где $c < n$, и потому превосходит β_μ, так что $B_\mu^*(\beta_\mu) = 0$.

Поэтому

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1),$$

что и требовалось доказать.

§ 8.

Доказательство основной леммы.

Исходя из результатов § 5 и опираясь на только что доказанную лемму 3, мы можем теперь уже совсем легко доказать основную лемму.

Применяя к последовательностям A, B_h и C_h результат § 5 в форме неравенства (7) (что возможно ввиду нормальности C_h), мы находим:

$$C_h(n) - C_h(n-m) \geqslant A(m) + B_h(m), \qquad (12)$$

где m — наименьшее положительное число, не входящее в C_h; очевидно, $m \notin A$ и $m \notin B_h$, так что вместо $A(m)$ и $B_h(m)$ мы можем писать соответственно $A(m-1)$ и $B_h(m-1)$.

Мы имеем:

$$C_h = C \cup C^* \cup C_1^* \cup \ \dots \ \cup C_{h-1}^*,$$
$$B_h = B \cup B^* \cup B_1^* \cup \ \dots \ \cup B_{h-1}^*,$$

причём множества, входящие в какое-либо из этих двух соединений, попарно не имеют общих элементов, так что

$$C_h(n) - C_h(n-m) =$$
$$= C(n) - C(n-m) + \sum_{\mu=0}^{h-1} \{C_\mu^*(n) - C_\mu^*(n-m)\},$$

$$B_h(m) = B_h(m-1) = B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1),$$

где, конечно, положено $C_0^* = C^*$, $B_0^* = B^*$. В силу (12) мы отсюда имеем:

$$C(n) - C(n-m) + \sum_{\mu=0}^{h-1} \{C_\mu^*(n) - C_\mu^*(n-m)\} \geqslant$$
$$\geqslant A(m) + B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1);$$

но в силу леммы 3

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \quad (0 \leqslant \mu \leqslant h-1),$$

так что предыдущее неравенство даёт:

$$C(n) - C(n-m) \geqslant A(m) + B(m-1) = \\ = A(m) + B(m) \geqslant (\alpha + \beta)\, m,$$

что и доказывает основную лемму.

Тем самым, как мы видели в § 4, полностью доказана теорема Манна, решающая основную метрическую задачу аддитивной теории чисел.

Не правда ли, конструкция Артина и Шерка оставляет впечатление великолепного мастерского произведения? Для меня особенно чарующим является это замечательное сочетание структурной тонкости и предельной элементарности метода.

ГЛАВА III.

ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ПРОБЛЕМЫ ВАРИНГА.

§ 1.

Вы помните теорему Лагранжа, о которой я говорил Вам в начале предыдущей главы: всякое натуральное число может быть представлено как сумма не более чем четырёх точных квадратов. Я говорил Вам и о том, что теорема эта может быть выражена совсем в другой терминологии: последовательность

$$0,\ 1^2,\ 2^2,\ \ldots,\ k^2,\ \ldots, \qquad (A_2)$$

будучи четыре раза сложена с самой собою, даёт такую последовательность, которая охватывает все натуральные числа. Или, ещё короче: последовательность (A_2) есть базис (натурального ряда) порядка 4. Я упомянул совсем кратко и о том, что, как было доказано позже, последовательность точных кубов

$$0,\ 1^3,\ 2^3,\ \ldots,\ k^3,\ \ldots \qquad (A_3)$$

есть базис девятого порядка. Все эти факты, естественно, приводят к предположению, что для любого натурального числа n последовательность

$$0,\ 1^n,\ 2^n,\ \ldots,\ k^n,\ \ldots \qquad (A_n)$$

представляет собою базис (порядок которого, конечно, зависит от n). И действительно, эта гипотеза была высказана Варингом уже в XVIII столетии; однако задача оказалась очень нелёгкой, и только в начале нашего столетия Гильберт (1907) доказал во всей полноте справедливость гипотезы Варинга.

Доказательство Гильберта не только очень громоздко в формальном отношении и опирается на сложные аналитические теории (кратные интегралы), но и в идейном смысле весьма мало прозрачно. Известный французский математик Пуанкаре в своём обзоре научного творчества Гильберта писал, что если когда-нибудь будут поняты основные движущие пружины этого доказательства, то, вероятно, арифметические результаты большого значения посыплются, как из рога изобилия. И в известном смысле он оказался прав: 10—15 лет спустя Харди и Литльвудом в Англии и И. М. Виноградовым в СССР были даны новые доказательства теоремы Гильберта; эти доказательства попрежнему были аналитическими и формально громоздкими, но выгодно отличались от доказательства Гильберта методологической ясностью и идейной простотой, которые не оставляли желать ничего лучшего. И действительно, оба метода сделались в силу этого мощными источниками новых арифметических теорем.

Но когда наша наука имеет дело с такой совершенно элементарной задачей, как проблема Варинга, она продолжает добиваться такого её решения, которое не нуждалось бы в понятиях и методах, выходящих за пределы элементарной арифметики. Разыскание такого элементарного доказательства гипотезы Варинга и есть та третья задача, о которой я хочу Вам рассказать. Такое вполне элементарное доказательство теоремы Гильберта лишь в 1942 г. удалось молодому советскому учёному Ю. В. Линнику.

Вы уже привыкли теперь к тому, что элементарность ещё не означает простоты. Элементарное решение проблемы Варинга, найденное Линником, тоже, как Вы увидите, очень не просто, и Вам придётся порядочно потрудиться, чтобы понять и усвоить его. Я постараюсь своим изложением по возможности облегчить Вам эту задачу. Но Вы должны помнить, что в математике (как, вероятно, и во всякой другой науке) усвоение всего действительно ценного и значительного требует напряжённых усилий.

В доказательстве Линника весьма существенную роль играют идеи Шнирельмана, которые я изложил Вам в начале второй главы. Вспомните (я там кратко говорил об этом), как Шнирельман доказал свою знаменитую теорему о том, что последовательность P, состоящая из нуля, единицы и всех простых чисел, является базисом натурального ряда: он показал, что последовательность $P+P$ имеет положительную

плотность; а так как всякая последовательность положительной плотности есть, согласно доказанной нами на стр. 25—27 общей теореме Шнирельмана, базис натурального ряда, то отсюда сразу вытекает всё требуемое. Этот же приём лежит в основе и доказательства теоремы Гильберта, найденного Линником. Всё сводится к доказательству того, что сумма достаточно большого числа последовательностей (A_n) есть последовательность положительной плотности; как только это сделано, мы можем считать теорему Гильберта доказанной, в силу той же общей теоремы Шнирельмана.

§ 2.

Основная лемма.

Если мы сложим по правилу главы II k последовательностей, совпадающих с A_n, то мы, очевидно, получим последовательность $A_n^{(k)}$, содержащую нуль и все те натуральные числа, которые могут быть представлены в виде суммы не более чем k слагаемых вида x^n, где x — любое натуральное число; другими словами, число m принадлежит последовательности $A_n^{(k)}$, если уравнение

$$x_1^n + x_2^n + \ldots + x_k^n = m \qquad (1)$$

может быть решено в целых неотрицательных числах x_i $(1 \leqslant i \leqslant k)$. Нашей целью является, как мы это выяснили в § 1, доказательство того, что при достаточно большом k последовательность $A_n^{(k)}$ имеет положительную плотность.

Уравнение (1) при данных k и m, вообще говоря, может быть решено различными способами. Обозначим во всём дальнейшем через $r_k(m)$ число этих способов, т. е. число систем неотрицательных целых чисел $x_1, x_2, \ldots, x_k$, удовлетворяющих уравнению (1). Очевидно, число m входит в $A_n^{(k)}$ тогда и только тогда, если $r_k(m) > 0$.

В дальнейшем мы будем считать число n неизменно установленным, и потому все числа, зависящие только от n, будем называть постоянными. Такие постоянные мы будем обозначать буквою c или $c(n)$, причём такая постоянная c может в различных частях одного и того же рассуждения иметь разные значения, лишь бы только все эти значения были

постоянными числами. Может быть, Вам несколько непривычна такая «вольность» в обозначениях; но Вы скоро с ней освоитесь — она всё чаще встречается в современных исследованиях и показала себя как очень удобный внешний приём.

Основная лемма. *Существуют такое натуральное число* $k=k(n)$, *зависящее только от* n, *и такая постоянная* c, *что для любого натурального числа* N

$$r_k(m) < cN^{\frac{k}{n}-1} \qquad (1 \leqslant m \leqslant N). \tag{2}$$

Снова, как и в предыдущей главе, перед нами две задачи: во-первых, доказать основную лемму и, во-вторых, из основной леммы вывести нужное нам заключение, что последовательность $A_n^{(k)}$ имеет положительную плотность. И снова, как там, вторая задача значительно легче первой, и потому мы с неё начнём.

Из определения числа $r_k(m)$ непосредственно вытекает, что сумма

$$r_k(0)+r_k(1)+\ldots+r_k(N)=R_k(N)$$

представляет собою число всех таких систем $(x_1, x_2, \ldots, x_k)$ из k неотрицательных чисел, для которых

$$x_1^n+x_2^n+\ldots+x_k^n \leqslant N. \tag{3}$$

Но этому требованию, очевидно, удовлетворяет всякая группа чисел, для которых

$$0 \leqslant x_i \leqslant \left(\frac{N}{k}\right)^{\frac{1}{n}} \qquad (1 \leqslant i \leqslant k).$$

Так как для осуществления этих неравенств каждое x_i может быть, очевидно, выбрано более чем $\left(\frac{N}{k}\right)^{\frac{1}{n}}$ различными способами $\left(x_i=0, 1, \ldots, \left[\left(\frac{N}{k}\right)^{\frac{1}{n}}\right]\right)$, и эти k выборов (т. е. выборы чисел $x_1, x_2, \ldots, x_k$) можно произвольным образом комбинировать между собою, то для всей системы чисел $x_i\,(1 \leqslant i \leqslant k)$ мы имеем более чем $\left(\frac{N}{k}\right)^{\frac{k}{n}}$ различных выбо-

ров, каждый из которых удовлетворяет условию (3). Это показывает, что

$$R_k(N) \geqslant \left(\frac{N}{k}\right)^{\frac{k}{n}}. \tag{4}$$

Мы предполагаем основную лемму установленной и неравенство (2) выполненным при любом N. Теперь нам остаётся убедиться, что неравенство (2) совместимо с доказанным нами неравенством (4) лишь при том условии, что последовательность $A_n^{(k)}$ имеет положительную плотность. Идея последующего рассуждения очень проста: в сумме $R_k(N)$ отличны от нуля только те слагаемые $r_k(m)$, для которых m входит в $A_n^{(k)}$. Если бы $A_n^{(k)}$ имела плотность нуль, то при больших N число таких слагаемых было бы относительно мало; а так как каждое слагаемое в силу (2) не может быть очень большим, то и сумма их $R_k(N)$ была бы относительно малой, между тем как в силу (4) она должна быть достаточно большой.

Остаётся произвести подсчёты. Если бы было $d(A_n^{(k)}) = 0$, то для сколь угодно малого $\varepsilon > 0$ мы имели бы при надлежаще выбранном N

$$A_n^{(k)}(N) < \varepsilon N;$$

при этом мы могли бы предполагать число N как угодно большим, так как $A_n^{(k)}$ содержит (при любом k) число 1 (вспомните задачу 6 на стр. 18, которую Вы решили!).

Применяя оценку (2), мы поэтому нашли бы:

$$R_k(N) = \sum_{m=0}^{N} r_k(m) =$$

$$= r_k(0) + \sum_{m=1}^{N} r_k(m) < 1 + cN^{\frac{k}{n}-1} A_n^{(k)}(N) < 1 + c\varepsilon N^{\frac{k}{n}},$$

и, значит, для достаточно большого N

$$R_k(N) < 2c\varepsilon N^{\frac{k}{n}}.$$

Так как при достаточно малом ε

$$2c\varepsilon < \left(\frac{1}{k}\right)^{\frac{k}{n}},$$

то мы получили бы

$$R_k(N) < \left(\frac{N}{k}\right)^{\frac{k}{n}},$$

в противоречие с неравенством (4). Таким образом, мы необходимо имеем

$$d(A_n^{(k)}) > 0,$$

а это, как мы уже знаем, доказывает теорему Гильберта.

Вы видите, как просто всё это выходит. Но нам остаётся доказать основную лемму, а для этого нам, как и в предшествующей главе, придётся пройти длинный и трудный путь.

§ 3.

Леммы о линейных уравнениях.

Нам придётся начать издалека. Поэтому Вы сделаете лучше всего, если на время совсем забудете о той задаче, которую мы себе поставили; потом, когда мы вернёмся к ней, я Вам её напомню.

А сейчас нам нужно будет в первую очередь установить некоторые оценки для числа решений систем линейных уравнений. Леммы этого параграфа представляют, пожалуй, и самостоятельный интерес, независимо от той проблемы, для решения которой мы их приводим здесь.

Лемма 1. *Пусть в уравнении*

$$a_1 z_1 + a_2 z_2 = m \tag{5}$$

числа a_1, a_2, m — *целые,* $|a_2| \leqslant |a_1| \leqslant A$ *и числа* a_1 *и* a_2 — *взаимно простые. Тогда число решений уравнения* (5), *удовлетворяющих неравенствам* $|z_1| \leqslant A$, $|z_2| \leqslant A$, *не превосходит* $\frac{3A}{|a_1|}$.

Доказательство. Мы можем допустить, что $a_1 > 0$, так как в противном случае мы просто в каждом решении заменили бы z_1 на $-z_1$.

Пусть (z_1, z_2) и (z_1', z_2') — два различных решения уравнения (5). Тогда из

$$a_1 z_1 + a_2 z_2 = m,$$
$$a_1 z_1' + a_2 z_2' = m$$

мы с помощью вычитания находим:

$$a_2(z_2' - z_2) = a_1(z_1 - z_1');$$

левая часть этого равенства должна, таким образом, делиться на a_1; но [1]) $(a_1, a_2) = 1$, и следовательно, $z_2' - z_2$ должно делиться на a_1; но $z_2' \neq z_2$, и значит $|z_2' - z_2|$, будучи кратным a_1, не меньше чем a_1. Итак, в двух различных решениях (z_1, z_2) и (z_1', z_2') уравнения (5) мы обязательно имеем $|z_2' - z_2| \geqslant a_1$.

Условимся в каждом решении (z_1, z_2) уравнения (5) называть z_1 первым, а z_2 — вторым членом. Очевидно, число решений уравнения (5), удовлетворяющих условиям $|z_1| \leqslant A$, $|z_2| \leqslant A$, не больше чем число t вторых членов, попадающих в отрезок $(-A, A)$. Так как мы доказали, что два таких вторых члена отстоят друг от друга не меньше чем на a_1, то разность между наибольшим и наименьшим вторыми членами, попадающими в отрезок $(-A, A)$, будет не меньше чем $a_1(t-1)$; а так как эта разность, с другой стороны, не превосходит $2A$, то

$$a_1(t-1) \leqslant 2A,$$

$$t - 1 \leqslant \frac{2A}{a_1},$$

$$t \leqslant \frac{2A}{a_1} + 1 \leqslant \frac{3A}{a_1}$$

$\left(\text{так как по условию } a_1 \leqslant A, \text{ и значит } 1 \leqslant \frac{A}{a_1}\right)$. Этим лемма 1 доказана.

Лемма 2. *Пусть в уравнении*

$$a_1z_1 + a_2z_2 + \ldots + a_lz_l = m \qquad (6)$$

числа a_i и m — целые,

$$|a_i| \leqslant A \quad (1 \leqslant i \leqslant l), \quad (a_1, a_2, \ldots, a_l) = 1\ ^2).$$

Тогда число решений этого уравнения, удовлетворяющих

---

[1]) (a_1, a_2) означает наибольший общий делитель чисел a_1 и a_2.

[2]) $(a_1, a_2, \ldots a_l)$ означает наибольший общий делитель чисел, стоящих в скобках.

неравенствам $|z_i| \leqslant A\ (1 \leqslant i \leqslant l)$, *не превосходит*

$$c(l)\frac{A^{l-1}}{H},$$

где H *— наибольшее из чисел* $|a_1|, |a_2|, \ldots, |a_l|$, *а* $c(l)$ *— постоянная, зависящая только от* l.

Доказательство. Очевидно, что при $l=2$ лемма 2 обращается в лемму 1 (при $c(2)=3$). Таким образом, при $l=2$ лемма 2 уже доказана. Допустим поэтому, что $l \geqslant 3$ и что для случая $l-1$ неизвестных лемма 2 уже установлена. Так как порядок нумерации безразличен, то мы можем допустить, что $|a_l|$ есть наибольшее из чисел $|a_1|, |a_2|, \ldots, |a_l|$, т. е. $H=|a_l|$.

Будем различать два случая.

1) $a_1=a_2=\ldots=a_{l-1}=0$. В силу $(a_1, a_2, \ldots, a_l)=1$ мы должны иметь $|a_l|=H=1$, так что данное уравнение получает вид $\pm z_l = m$. Очевидно, в этом уравнении каждое из неизвестных $z_1, z_2, \ldots, z_{l-1}$ может принимать любое целое значение в отрезке $(-A, A)$, т. е. всего не более чем $2A+1 \leqslant 3A$ значений; что же касается z_l, то оно принимает не более одного значения; поэтому число решений данного уравнения, удовлетворяющих неравенствам $|z_i| \leqslant A\ (1 \leqslant i \leqslant l)$, не превосходит

$$(3A)^{l-1} = c(l)\,A^{l-1} = c(l)\frac{A^{l-1}}{H},$$

чем лемма 2 для этого случая и доказана.

2) Если по меньшей мере одно из чисел $a_1, a_2, \ldots, a_{l-1}$ отлично от нуля, то существует

$$(a_1, a_2, \ldots, a_{l-1}) = \delta.$$

Обозначим через H' наибольшее из чисел

$$\frac{|a_l|}{\delta} \qquad (1 \leqslant i \leqslant l-1).$$

Пусть теперь числа $z_1, z_2, \ldots, z$, удовлетворяют данному уравнению (6) и неравенствам $|z_i| \leqslant A\ (1 \leqslant i \leqslant l)$. Положим

$$\frac{a_1}{\delta}z_1 + \frac{a_2}{\delta}z_2 + \ldots + \frac{a_{l-1}}{\delta}z_{l-1} = m', \qquad (7)$$

откуда

$$a_1z_1 + a_2z_2 + \ldots + a_{l-1}z_{l-1} = \delta m';$$

при этом, очевидно,

$$\delta m' + a_l z_l = m, \tag{8}$$

и

$$|\delta m'| \leqslant \sum_{i=1}^{l-1} |a_i| z_i \leqslant l\delta H' A,$$

откуда

$$|m'| \leqslant lH' A.$$

Итак, если числа $z_1, z_2, \ldots, z_l$ удовлетворяют уравнению (6) и неравенствам $|z_i| \leqslant A$ $(1 \leqslant i \leqslant l)$, то существует целое число m', которое вместе с этими числами удовлетворяет уравнениям (7) и (8), причём $m' | \leqslant lH'A$. Но в уравнении (8), очевидно, $\delta \leqslant |a_l|$ и $(\delta, a_l) = 1$ (в противном случае мы имели бы $(a_1, a_2, \ldots, a_{l-1}, a_l) > 1$); поэтому число решений уравнения (8) (в неизвестных m', z_l), для которых $|m'| \leqslant lH' A$, $|z_i| \leqslant A < lH' A$, в силу леммы 1, не превосходит $\frac{3lH'A}{|a_l|}$. При том же m' уравнение (7), в силу леммы 2 для уравнений с $l-1$ неизвестными, имеет не более чем $c(l)\frac{A^{l-2}}{H'}$ решений в целых z_i, $|z_i| \leqslant A$.

Из всего сказанного, очевидно, вытекает, что число решений $(z_1, z_2, \ldots, z_l)$ уравнения (6), подчинённых неравенствам $z_i | \leqslant A$, $1 \leqslant i \leqslant l$ не превосходит

$$\frac{3lH'A}{|a_l|} c(l) \frac{A^{l-2}}{H'} = c(l) \frac{A^{l-1}}{|a_l|} = c(l) \frac{A^{l-1}}{H},$$

что и доказывает лемму 2 [1]).

Рассмотрим теперь семейство всех уравнений вида

$$a_1 z_1 + a_2 z_2 + \ldots + a_l z_l = 0, \tag{9}$$

где $|a_i| \leqslant A$ $(1 \leqslant i \leqslant l)$ и, как всегда, все a_i — целые числа. Пусть B — положительное число, связанное с числом A неравенствами $1 \leqslant A \leqslant B \leqslant c(l) A^{l-1}$, и пусть $l > 2$. Мы хотим оценить сумму чисел решений z_i $(|z_i| \leqslant B$, $1 \leqslant i \leqslant l)$ всех уравнений (9) этого семейства.

1°. Сначала рассмотрим отдельно уравнение (9) при $a_1 = a_2 = \ldots = a_l = 0$ (оно входит в наше семейство!) и оце-

[1]) Вы, вероятно, обратили внимание на то, что в последней цепи равенств символ $c(l)$ в разных местах имел разные значения; я предупреждал Вас на стр. 36 о таком употреблении этого символа.

ним число его решений, удовлетворяющих неравенствам $|z_i| \leqslant B$ $(1 \leqslant i \leqslant l)$. Очевидно, нашему уравнению удовлетворяет любая система чисел $z_1, z_2, \ldots, z_l$, и мы должны только подсчитать, сколько существует таких систем, удовлетворяющих неравенствам $|z_1| \leqslant B$, $|z_2| \leqslant B, \ldots, |z_l| \leqslant B$. Так как отрезок $(-B, +B)$ содержит не более $2B+1$ целых чисел, то каждое z_i может принимать не более $2B+1$ различных значений; следовательно, число систем $(z_1, z_2, \ldots, z_l)$ интересующего нас типа не превосходит $(2B+1)^l \leqslant (3B)^l = c(l) B^l$; а так как в силу наших предположений $B \leqslant c(l) A^{l-1}$, то $c(l) B^l = c(l) B^{l-1} B \leqslant c(l) (AB)^{l-1}$. Таким образом, в случае $a_1 = a_2 = \ldots = a_l = 0$ уравнение (9) имеет не более чем $c(l)(AB)^{l-1}$ решений интересующего нас типа.

2°. Если хоть один из коэффициентов a_i отличен от нуля, то существует наибольший общий делитель $(a_1, a_2, \ldots, a_l) = \delta$ этих коэффициентов. Пусть сначала $\delta = 1$, и пусть H — наибольшее из чисел $|a_1|, |a_2|, \ldots, |a_l|$. Очевидно, H есть одно из целых чисел отрезка $(1, A)$. Значит, H заключено либо между A и $\frac{A}{2}$, либо между $\frac{A}{2}$ и $\frac{A}{4}$, либо между $\frac{A}{4}$ и $\frac{A}{8}$, и т. д. Вообще найдётся такое целое число $m \geqslant 0$, что

$$\frac{A}{2^{m+1}} < H \leqslant \frac{A}{2^m}. \tag{10}$$

Для одного уравнения вида (9), в котором $\delta = 1$ и H удовлетворяет неравенствам (10), число решений z_i $(|z_i| \leqslant B)$ в силу леммы 2 не превосходит

$$c(l) \frac{B^{l-1}}{H} \leqslant c(l) \frac{B^{l-1}}{A/2^{m+1}} = \frac{c(l) B^{l-1} 2^m}{A}.$$

С другой стороны, из неравенства (10) вытекает

$$|a_i| \leqslant \frac{A}{2^m} \quad (1 \leqslant i \leqslant l), \tag{11}$$

и значит число уравнений типа (9), для которых выполняются неравенства (10), не больше числа уравнений того же типа, подчинённых условиям (11), т. е. не больше чем

$$\left(2\frac{A}{2^m} + 1\right)^l \leqslant \left(3\frac{A}{2^m}\right)^l = c(l) A^l 2^{-m'}.$$

Таким образом, сумма чисел решений $|z_i| \leqslant B$ всех таких уравнений типа (9), для которых $\delta = 1$ и $\frac{A}{2^{m+1}} < H \leqslant \frac{A}{2^m}$, не превосходит

$$c(l)\frac{B^{l-1}2^m}{A} \cdot c(l)A^l 2^{-ml} = c(l)(AB)^{l-1}2^{-(l-1)m}.$$

Суммируя эту оценку по всем $m \geqslant 0$, мы приходим к следующему выводу: сумма чисел решений $|z_i| \leqslant B$ всех уравнений типа (9), для которых $|a_i| \leqslant A\,(1 \leqslant i \leqslant l)$ и $\delta = 1$, не больше чем

$$c(l)(AB)^{l-1}.$$

3°. Нам остаётся подсчитать числа решений требуемого типа для уравнений с $\delta > 1$. В этом случае уравнение (9), очевидно, равносильно уравнению

$$\frac{a_1}{\delta} z_1 + \frac{a_2}{\delta} z_2 + \ldots + \frac{a_l}{\delta} z_l = 0,$$

т. е. уравнению того же типа (9), где только

$$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_l}{\delta}\right) = 1$$

и число A нужно заменить числом $\frac{A}{\delta}$. При данном закреплённом δ сумма чисел решений $|z| \leqslant B$ всех таких уравнений, как мы видели в 2°, не превосходит [1])

$$c(l)\left(\frac{A}{\delta} \cdot B\right)^{l-1} = c(l)\frac{(AB)^{l-1}}{\delta^{l-1}}.$$

Нам остаётся, очевидно, просуммировать это выражение по всем возможным значениям $\delta\,(1 \leqslant \delta \leqslant A)$.

Мы убеждаемся таким образом, что сумма чисел требуемых решений всех уравнений вида (9), где $|a_i| \leqslant A\,(1 \leqslant i \leqslant l)$

---

[1]) Так как вместо A мы имеем теперь меньшее число $\frac{A}{\delta}$, то предпосылка $B \leqslant c(l)A^{l-1}$ может оказаться нарушенной. Но Вы без труда убедитесь, что в рассуждении пункта 2° мы нигде этой предпосылкой не пользовались, и следовательно, результат пункта 2° от неё не зависит.

и не все a_i равны нулю, не превосходит величины

$$c(l)(AB)^{l-1}\sum_{\delta=1}^{A}\frac{1}{\delta^{l-1}}<c(l)(AB)^{l-1}\cdot\frac{l-1}{l-2}\ ^{1})=$$
$$=c(l)(AB)^{l-1}.$$

Сопоставляя это с результатом пункта 1°, где мы получили оценку для случая $a_1=a_2=\ldots=a_i=0$, приходим к следующему выводу:

Лемма 3. *Пусть* $l>2$ *и* $1\leqslant A\leqslant B\leqslant c(l)A^{l-1}$. *Тогда сумма чисел решений* $|z_i|\leqslant B\,(1\leqslant i\leqslant l)$ *для всех уравнений вида*

$$a_1z_1+a_2z_2+\ldots+a_lz_l=0, \tag{9}$$

где $|a_i|\leqslant A\,(1\leqslant i\leqslant l)$, *не превосходит*

$$c(l)(AB)^{l-1}.$$

---

[1]) Мы здесь воспользовались неравенством

$$\sum_{n=1}^{A}\frac{1}{n^{q+1}}<\frac{q+1}{q},$$

которое справедливо для любого натурального числа q и для любого $A\geqslant 1$ (через q мы обозначаем число $l-2$, которое положительно, так как мы предположили $l>2$). Вот простое доказательство: при $n\geqslant 1$

$$\frac{1}{n^q}-\frac{1}{(n+1)^q}=\frac{(n+1)^q-n^q}{n^q(n+1)^q}=$$
$$=\frac{n^q+qn^{q-1}+\ldots+1-n^q}{n^q(n+1)^q}\geqslant\frac{qn^{q-1}}{n^q(n+1)^q}>\frac{q}{(n+1)^{q+1}},$$

откуда

$$\frac{1}{(n+1)^{q+1}}<\frac{1}{q}\left\{\frac{1}{n^q}-\frac{1}{(n+1)^q}\right\};$$

полагая же в этом неравенстве поочерёдно $n=1, 2, \ldots, A-1$ и складывая все полученные неравенства, мы находим:

$$\sum_{n=2}^{A}\frac{1}{n^{q+1}}<\frac{1}{q}\left(1-\frac{1}{A^q}\right)<\frac{1}{q},$$

откуда

$$\sum_{n=1}^{A}\frac{1}{n^{q+1}}<1+\frac{1}{q}=\frac{q+1}{q},$$

что и требовалось доказать.

§ 4.
Ещё две леммы.

Прежде чем перейти к доказательству основной леммы, нам придётся установить ещё два вспомогательных предложения особого типа. Оба они очень просты и в идейном, и в формальном отношении; однако усвоение их всё же может доставить Вам известные трудности, потому что здесь будет итти речь о подсчёте всевозможных комбинаций довольно громоздкого строения; трудность такой абстрактной комбинаторики заключается в том, что она плохо поддаётся математической символизации, здесь больше приходится говорить словами, чем знаками; впрочем, это, конечно, есть трудность изложения, а не трудность самого предмета; и я постараюсь обрисовать Вам все встающие вопросы и их разрешение со всею возможной конкретностью.

Будем обозначать через A конечное множество чисел, среди которых могут быть и равные между собою; если число a встречается λ раз в множестве A, то мы будем говорить, что его кратность равна λ. Пусть $a_1, a_2, \ldots, a_r$ — различные между собою числа, входящие в A, и $\lambda_1, \lambda_2 \ldots, \lambda_r$ — их соответственные кратности (так что множество A всего содержит $\sum_{l=1}^{r} \lambda_l$ чисел). Пусть B — другое множество того же типа, содержащее различные между собою числа $b_1, b_2, \ldots, b_s$ с кратностями $\mu_1, \mu_2, \ldots, \mu_s$. Рассмотрим уравнение

$$x + y = c, \qquad (12)$$

где c — данное число, а x и y — неизвестные. Нас будут интересовать такие решения (x, y) этого уравнения, в которых x есть одно из чисел множества A (мы это коротко будем записывать так: $x \in A$), а y — одно из чисел множества B ($y \in B$). Если числа $x = a_l$, $y = b_k$ удовлетворяют уравнению (12), то это даёт $\lambda_{l\mu k}$ решений требуемого типа, потому что любой из λ_l «экземпляров» числа a_l, имеющихся в множестве A, можно сочетать с любым из μ_k экземпляров числа b_k, имеющихся в множестве B. Но $\lambda_{l\mu k} \leqslant \frac{1}{2}(\lambda_l^2 + \mu_k^2)$ [1]).

---

[1]) «Среднее геометрическое не превосходит среднего арифметического». Вот самое простое доказательство:

$$0 \leqslant (\lambda_l - \mu_k)^2 = \lambda_l^2 + \mu_k^2 - 2\lambda_l\mu_k,$$

откуда

$$2\lambda_l\mu_k \leqslant \lambda_l^2 + \mu_k^2.$$

Значит, число таких решений уравнения (12), где $x=a_i$, $y=b_k$ не превосходит величины $\frac{1}{2}(\lambda_i^2+\mu_k^2)$. Отсюда следует, что число всех решений $x\in A$, $y\in B$ уравнения (12) не превосходит суммы $\sum\frac{1}{2}(\lambda_i^2+\mu_k^2)$. Здесь надо суммировать по всем парам значков (i, k), для которых $a+b_k=c$. Мы ещё увеличим нашу сумму, если просуммируем λ_i^2 по всем i, а μ_k^2 по всем k (ведь каждое b_k может сочетаться не более чем с одним a_i). Таким образом, мы получаем окончательно, что число решений $x\in A$, $y\in B$ уравнения (12) не превосходит

$$\frac{1}{2}\left(\sum_{i=1}^{r}\lambda_i^2+\sum_{k=1}^{s}\mu_k^2\right).$$

С другой стороны, рассмотрим уравнение

$$x-y=0 \tag{13}$$

и подсчитаем число его решений $x\in A$, $y\in A$; очевидно, каждое такое решение имеет вид $x=y=a_i$ $(1\leqslant i\leqslant r)$; для данного i мы получаем λ_i^2 решений, так как числа x и y могут независимо друг от друга совпадать с любым из λ_i экземпляров числа a_i, имеющихся в A. Общее число решений $x\in A$, $y\in A$ уравнения (13) равно, таким образом, $\sum_{i=1}^{r}\lambda_i^2$. Точно так же, конечно, число решений $x\in B$, $y\in B$ того же уравнения равно $\sum_{k=1}^{s}\mu_k^2$. Сопоставляя эти результаты с тем, который мы нашли выше, мы приходим к следующему выводу:

Лемма 4. *Число решений уравнения*

$$x+y=c,\ x\in A,\ y\in B$$

не превосходит полусуммы чисел решений уравнений

$$x-y=0,\quad x\in A,\quad y\in A$$

и

$$x-y=0,\quad x\in B,\quad y\in B.$$

В частном случае, когда множества A и B совпадают между собою, мы получаем

Следствие. *Число решений уравнения*

$$x+y=c, \quad x\in A, \quad y\in A$$

не превосходит числа решений уравнения

$$x-y=0, \quad x\in A, \quad y\in A.$$

Пусть теперь k и s — произвольные натуральные числа. Положим $k\cdot 2^s=l$ и будем рассматривать уравнение

$$x_1+x_2+\ldots+x_l=c.$$

Пусть A_1, A_2, ... , A_l — конечные множества чисел; пусть множество $A_i\,(1\leqslant i\leqslant l)$ содержит различные между собою числа a_{i1}, a_{i2}, ... с кратностями λ_{i1}, λ_{i2}, ... Нас будет интересовать число решений уравнения

$$x_1+x_2+\ldots+x_l=c, \quad x_i\in A_i \ (1\leqslant i\leqslant l). \tag{14}$$

Если положить

$$x_1+x_2+\ldots+x_{l/2}=x, \quad x_{(l/2)+1}+\ldots+x_l=y$$

($l/2$ есть, конечно, целое число), то данное уравнение можно переписать в виде

$$x+y=c$$

и применить к нему только что доказанную лемму 4. Надо только разобраться в том, каким множествам должны принадлежать числа x и y. Так как $x_i\in A_i\,(1\leqslant i\leqslant l)$, то x может быть любым числом вида $z_1+z_2+\ldots+z_{l/2}$, где $z_i\in A_i\,(1\leqslant i\leqslant l/2)$; точно так же y может быть любым числом того же вида, где только $z_i\in A_{(l/2)+i}\,(1\leqslant i\leqslant l/2)$.

В силу леммы 4 поэтому число решений уравнения (14) не превосходит полусуммы чисел решений уравнения

$$x-y=0 \tag{15}$$

в следующих двух предположениях:

1) $$x=z_1+z_2+\ldots+z_{l/2},$$
$$y=z'_1+z'_2+\ldots+z'_{l/2},$$

где

$$z_i\in A_i, \quad z'_i\in A_i, \quad 1\leqslant i\leqslant l/2. \tag{16}$$

2) x и y имеют ту же форму, но

$$z_l \in A_{(l/2)+l}, \quad z'_l \in A_{(l/2)+l}, \quad 1 \leqslant l \leqslant l/2. \tag{17}$$

В обоих случаях уравнение (15) может быть переписано в виде

$$(z_1 - z'_1) + (z_2 - z'_2) + \ldots + (z_{l/2} - z'_{l/2}) = 0. \tag{18}$$

Мы приходим таким образом к выводу, что число решений уравнения (14) не превосходит полусуммы чисел решений уравнения (18) в предположениях (16) и (17), т. е. не превосходит полусуммы чисел решений уравнений

$$\sum_{l=1}^{l/2} (z_l - z'_l) = 0, \quad z_l \in A_l, \quad z'_l \in A_i, \quad 1 \leqslant i \leqslant \frac{l}{2} \tag{18a}$$

и

$$\sum_{l=1}^{l/2} (z_l - z'_l) = 0, \quad z_l \in A_{(l/2)+l}, \quad z'_l \in A_{(l/2)+i}, \quad 1 \leqslant i \leqslant \frac{l}{2}. \tag{18b}$$

Уравнение (18) имеет в левой части $l/2$ слагаемых, т. е. вдвое меньше, чем первоначальное уравнение (14). Полагая

$$\sum_{l=1}^{l/4} (z_l - z'_l) = x, \qquad \sum_{l=(l/4)+1}^{l/2} (z_l - z'_l) = y,$$

мы приводим уравнение (18) к виду

$$x + y = 0$$

и можем снова применить к нему лемму 4. Совершенно тем же путём, как мы от уравнения (14) пришли к уравнению (18), мы теперь от уравнения (18) придём, очевидно, к уравнению

$$\sum_{l=1}^{l/4} (u_l + u'_l - u''_l - u'''_l) = 0, \tag{19}$$

причём нам придётся рассматривать сумму чисел решений этого уравнения в следующих (уже четырёх) предположениях:

$$1)\ u_l, u'_l, u''_l, u'''_l \in A_l,$$
$$2)\ u_l, u'_l, u''_l, u'''_l \in A_{(l/4)+l},$$
$$3)\ u_l, u'_l, u''_l, u'''_l \in A_{(l/2)+l},$$
$$4)\ u_l, u'_l, u''_l, u'''_l \in A_{(3l/4)+l}$$
$$\left(1 \leqslant l \leqslant \frac{l}{4}\right).$$

Так как $l = k \cdot 2^s$, то мы можем повторить этот процесс s раз. В результате мы, очевидно, придём к уравнению

$$\sum_{l=1}^{k} \{y_l^{(1)} + y_l^{(2)} + \ldots + y_l^{(2^{s-1})} - y_l^{(2^{s-1}+1)} - \ldots \\ \ldots - y_l^{(2^s)}\} = 0, \qquad (20)$$

причём нам придётся рассматривать сумму чисел решений этого уравнения в 2^s различных предположениях, а именно:

$$\left.\begin{array}{l} 1)\ y_1^{(j)} \in A_1,\ y_2^{(j)} \in A_2,\ \ldots,\ y_k^{(j)} \in A_k, \\ 2)\ y_1^{(j)} \in A_{k+1},\ y_2^{(j)} \in A_{k+2},\ \ldots,\ y_k^{(j)} \in A_{2k}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 2^s)\ y_1^{(j)} \in A_{k2^s-k+1},\ \ldots,\ y_k^{(j)} \in A_{k\cdot 2^s}. \end{array}\right\} \quad (1 \leqslant j \leqslant 2^s)$$

Если мы положим

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)} \quad (1 \leqslant j \leqslant 2^s),$$

то уравнение (20) примет простой вид

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0. \qquad (21)$$

При этом речь идёт о сумме чисел решений уравнения (21) в следующих 2^s предположениях, отличаемых друг от друга значениями параметра m $(0 \leqslant m \leqslant 2^s - 1)$:

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)},$$

где

$$y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2},\ \ldots,\ y_k^{(j)} \in A_{(m+1)k} \\ (j = 1, 2, \ldots, 2^s).$$

Таким образом, мы можем формулировать окончательный результат нашего вывода в виде следующего предложения:

Лемма 5. *Число решений уравнения*

$$x_1 + x_2 + \ldots + x_l = c, \quad x_i \in A_i, \quad 1 \leqslant i \leqslant l \qquad (14)$$

не превосходит суммы чисел решений уравнения

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0, \qquad (21)$$

$$\left.\begin{array}{c} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)}, \\ y_1^{(j)} \in A_{mk+1},\ y_2^{(j)} \in A_{mk+2},\ \ldots,\ y_k^{(j)} \in A_{(m+1)k} \end{array}\right\} \ (j = 1, 2, \ldots, 2^s)$$

в предположениях $m = 0, 1, \ldots, 2^s - 1$. При этом $l = k \cdot 2^s$.

Очевидно, лемма 4 представляет собою частный случай леммы 5, соответствующий $k=s=1$, $l=2$.

Теперь наша подготовка закончена, и мы можем приступить к прямой атаке основной леммы.

§ 5.

Доказательство основной леммы.

Мы будем доказывать основную лемму методом индукции, от $n-1$ к n. При индуктивных доказательствах часто бывает, что, усиливая доказываемое утверждение, мы существенно облегчаем (иногда даже прямо впервые создаём возможность) его обоснования данным методом. Легко понять, почему это происходит: в индуктивном доказательстве утверждение предполагается верным для числа $n-1$ и доказывается для числа n; поэтому, чем сильнее утверждение, тем больше нам дано в случае числа $n-1$; правда, тем больше и требуется доказать для числа n; но во многих задачах первое обстоятельство оказывается важнее второго.

Так и в данном случае. Непосредственно нас интересует число решений уравнения $x_1^n+x_2^n+\ldots+x_k^n=m$ $(1\leqslant m\leqslant N)$ (причём по самому смыслу задачи здесь $0\leqslant x_i\leqslant m^{\frac{1}{n}}\leqslant N^{\frac{1}{n}}$); но есть простейший частный случай многочлена n-й степени

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n;$$

и нам будет выгодно заменить данное уравнение (1) более общим уравнением

$$f(x_1)+f(x_2)+\ldots+f(x_k)=m \qquad (22)$$

с наложением на неизвестные более широких условий $|x_i|\leqslant N^{\frac{1}{n}}$, $1\leqslant i\leqslant k$. Доказав наше утверждение для уравнения (22), мы будем иметь больше, чем нам непосредственно нужно; однако это усиление нашего утверждения как раз и создаёт, как мы увидим, возможность индукции. Итак, для $m\leqslant N$ мы теперь будем обозначать через $r_k(m)$ число решений уравнения (22), удовлетворяющих условиям $|x_i|\leqslant N^{\frac{1}{n}}$, $1\leqslant i\leqslant k$; при этом в интересах проводимой индукции мы вольны ещё, конечно, произвольным образом распорядиться коэффициентами многочлена $f(x)$ (лишь бы налагаемые усло-

вия выполнялись в случае $f(x)=x^n$). Мы докажем следующее предложение.

Пусть в выражении многочлена $f(x)$

$$|a_i| \leqslant c(n) N^{\frac{i}{n}} \quad (0 \leqslant i \leqslant n); \tag{23}$$

тогда при надлежаще выбранном $k=k(n)$

$$r_k(m) < c(n)\, N^{\frac{k}{n}-1} \quad (1 \leqslant m \leqslant N).$$

Так как в случае $f(x)=x^n$ неравенства (23) очевидно выполнены с $c(n)=1$, то это предложение действительно есть усиление нашей основной леммы.

Рассмотрим сначала случай $n=1$, $f(x)=a_0x+a_1$. Положим $k(1)=2$, так что уравнение (22) получает вид

$$a_0(x_1+x_2)=m-2a_1,$$

причём речь идёт о решениях этого уравнения, удовлетворяющих требованиям $|x_1| \leqslant N$, $|x_2| \leqslant N$. Таким образом, для x_1 возможны не более чем $2N+1 \leqslant 3N$ значений; но каждому x_1 соответствует не более одного x_2, так что

$$r_2(m) \leqslant 3N,$$

чем наше предложение и доказано для $n=1$ ($k=2$).

Пусть теперь $n>1$ и наше утверждение установлено для показателя $n-1$. Положим $k(n-1)=k'$ и выберем

$$k=k(n)=2n \cdot 2^{[4\lg_2 k']},$$

где показатель означает наибольшее целое число, не превосходящее $4\lg_2 k'$. В дальнейшем мы для краткости положим $[4\lg_2 k']-1=s$, так что

$$k=2n \cdot 2^{s+1}. \tag{24}$$

Для оценки числа $r_k(m)$ решений уравнения (22) мы прежде всего применим к нему лемму 4, полагая

$$x=\sum_{i=1}^{k/2} f(x), \quad y=\sum_{i=\frac{k}{2}+1}^{k} f(x_i).$$

Множество A (и совпадающее с ним в данном случае множество B) состоит из всех сумм вида

$$\sum_{i=1}^{k/2} f(x), \quad \text{где} \quad |x_i| \leqslant N^{\frac{1}{n}} \left(1 \leqslant i \leqslant \frac{k}{2}\right).$$

В силу следствия леммы 4, $r_k(m)$ не превосходит числа решений уравнения $x - y = 0$, где $x \in A$, $y \in A$, т. е.

$$x = \sum_{i=1}^{k/2} f(x_i), \quad y = \sum_{i=1}^{k/2} f(y_i),$$

$$|x_i| \leqslant N^{\frac{1}{n}}, \quad |y_i| \leqslant N^{\frac{1}{n}}, \quad 1 \leqslant i \leqslant \frac{k}{2}.$$

Иначе говоря, $r_k(m)$ не превосходит числа решений уравнения

$$\sum_{i=1}^{k/2} \{f(x_i) - f(y_i)\} = 0, \tag{25}$$

где $|x_i| \leqslant N^{\frac{1}{n}}$, $|y_i| \leqslant N^{\frac{1}{n}} \left(1 \leqslant i \leqslant \frac{k}{2}\right)$. Положим теперь $x_i - y_i = h_i \left(1 \leqslant i \leqslant \frac{k}{2}\right)$ и заменим систему неизвестных (x_i, y_i) системою (y_i, h_i); при этом мы будем допускать для y_i и $h_i \left(1 \leqslant i \leqslant \frac{k}{2}\right)$ всевозможные целые значения в отрезке $(-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}})$, что может только увеличить число решений нашего уравнения. При этом в уравнении (25) каждое слагаемое $f(x_i) - f(y_i)$ заменится выражением

$$f(y_i + h_i) - f(y_i) = \sum_{v=0}^{n} a_v \{(y_i + h_i)^{n-v} - y_i^{n-v}\} =$$

$$= \sum_{v=0}^{n} a_v \sum_{t=1}^{n-v} \binom{n-v}{t} h_i^t y_i^{n-v-t}.$$

Преобразуем здесь переменные суммирования, полагая

$$v + t = u,$$

так что

$$n - v - t = n - u, \quad t = u - v;$$

мы получим:

$$f(y_i+h_l)-f(y_l)=h_i\sum_{v=0}^{n}a_v\sum_{u=v+1}\binom{n-v}{u-v}h_l^{u-v-1}y_l^{n-u}=$$

$$=h_i\sum_{u=1}^{n}y_l^{n-1}\sum_{v=0}^{u-1}a_v\binom{n-v}{u-v}h_l^{u-v-1}=$$

$$=h_i\sum_{u=1}^{n}a_{i,u}\ y_i^{n-u}=h_i\varphi_i(y_i),$$

где

$$\varphi_l(y)=\sum_{n=1}^{n}a_{i,u}\,y^{n-u}$$

есть многочлен степени $n-1$ с коэффициентами

$$a_{i,u}=\sum_{v=0}^{u-1}a_v\binom{n-v}{u-v}h_l^{u-v-1}\left(1\leqslant i\leqslant\frac{k}{2}\right),$$

зависящими от чисел h_i.

Уравнение (25) в новых переменных $(y_l,\ h_i)$ получает таким образом вид

$$h_1\varphi_1(y_1)+h_2\varphi_2(y_2)+\ldots+h_{\frac{k}{2}}\varphi_{\frac{k}{2}}(y_{\frac{k}{2}})=0. \qquad (26)$$

В этом уравнении числа h_l и y_l могут принимать любые целые значения в отрезке $(-2N^{\frac{1}{n}},\ +2N^{\frac{1}{n}})$, причём необходимо помнить, что коэффициенты многочленов $\varphi_\cdot(y)$ (степени $n-1$) зависят от чисел h.

Запомним твёрдо, что на данном этапе мы доказали следующее: *оцениваемое нами число* $r_k(m)$ *не превосходит суммы чисел решений в целых* y_l, $|y_i|\leqslant 2N^{\frac{1}{n}}\left(1\leqslant i\leqslant\frac{k}{2}\right)$, *всех уравнений вида* (26), *получаемых при всевозможных значениях чисел* h_l, $|h_i|\leqslant 2N^{\frac{1}{n}}\left(1\leqslant i\leqslant\frac{k}{2}\right)$.

§ 6.

Продолжение.

Теперь мы рассмотрим одно из уравнений (26), т. е. на длительное время будем считать числа $h_i \left(1 \leqslant i \leqslant \frac{k}{2}\right)$ закреплёнными. К этому уравнению мы применим лемму 5. При этом роль неизвестных x_i будут играть числа $h_i\varphi_i(y_i)$, а роль числа l — число $\frac{k}{2} = 2n \cdot 2^s$, причём ради краткости мы положим $2n = k_0$. Напомним ещё раз: числа h_i входят в уравнение (26) не только явно, но и через посредство коэффициентов многочленов $\varphi_i(y)$. Множество A_i, которому должны принадлежать числа $x_i = h_i\varphi_i(y_i)$, состоит в данном случае из всех чисел вида $h_i\varphi_i(y_i)$, где числа h_i имеют данные постоянные значения, а числа y_i пробегают отрезок $(-2N^{\frac{1}{n}},\ +2N^{\frac{1}{n}})$.

Согласно лемме 5, число решений уравнения (26), удовлетворяющих только что описанным требованиям, не превосходит суммы чисел решений уравнения

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0 \quad (21)$$

в следующих 2^s предположениях, соответствующих значениям параметра $m = 0,\ 1,\ \ldots,\ 2^s - 1$:

$$\left.\begin{array}{l} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_{k_0}^{(j)}, \\ y_i^{(j)} \in A_{mk_0+i} \quad (1 \leqslant i \leqslant k_0) \end{array}\right\} \quad (1 \leqslant j \leqslant 2^s),$$

где, напомним, A_r $(1 \leqslant r \leqslant 2^s)$ есть множество чисел вида $h_r\varphi_r(y_r)$ с данным h_r и произвольным y_r, $|y_r| \leqslant 2N^{\frac{1}{n}}$.

В развёрнутом виде уравнение (21) выглядит для случая $m = 0$ (который мы выбираем просто для примера) следующим образом:

$$\{y_1^{(1)} + y_2^{(1)} + \ldots + y_{k_0}^{(1)}\} + \{y_1^{(2)} + y_2^{(2)} + \ldots + y_{k_0}^{(2)}\} + \ldots$$
$$\ldots + \{y_1^{(2^{s-1})} + y_2^{(2^{s-1})} + \ldots + y_{k_0}^{(2^{s-1})}\} -$$
$$- \{y_1^{(2^{s-1}+1)} + y_2^{(2^{s-1}+1)} + \ldots + y_{k_0}^{(2^{s-1}+1)}\} - \ldots$$
$$\ldots - \{y_1^{(2^s)} + y_2^{(2^s)} + \ldots + y_{k_0}^{(2^s)}\} = 0.$$

или, меняя порядок слагаемых,

$$\{y_1^{(1)}+y_1^{(2)}+\ldots+y_1^{(2^{s-1})}-y_1^{(2^{s-1}+1)}-\ldots-y_1^{(2^s)}\}+$$
$$+\{y_2^{(1)}+y_2^{(2)}+\ldots+y_2^{(2^{s-1})}-y_2^{(2^{s-1}+1)}-\ldots-y_2^{(2^s)}\}+\ldots$$
$$\ldots+\{y_{k_0}^{(1)}+y_{k_0}^{(2)}+\ldots+y_{k_0}^{(2^{s-1})}-y_{k_0}^{(2^{s-1}+1)}-\ldots-y_{k_0}^{(2^s)}\}=0;$$

каждое из чисел $y_i^{(j)}$ есть здесь число вида $h_i\varphi_i(v_i^{(j)})$, где $|v_i^{(j)}|\leqslant 2N^{\frac{1}{n}}$; поэтому последнее уравнение может быть переписано в виде

$$h_1\{\varphi_1(v_1^{(1)})+\varphi_1(v_1^{(2)})+\ldots+\varphi_1(v_1^{(2^{s-1})})-$$
$$-\varphi_1(v_1^{(2^{s-1}+1)})-\ldots-\varphi_1(v_1^{(2^s)})\}+$$
$$+h_2\{\varphi_2(v_2^{(1)})+\ldots-\varphi_2(v_2^{(2^s)})\}+\ldots$$
$$\ldots+h_{k_0}\{\varphi_{k_0}(v_{k_0}^{(1)})+\ldots-\varphi_{k_0}(v_{k_0}^{(2^s)})\}=0.$$

Полагая для краткости

$$\varphi_i(v_i^{(1)})+\varphi_i(v_i^{(2)})+\ldots+\varphi_i(v_i^{(2^{s-1})})-$$
$$-\varphi_i(v_i^{(2^{s-1}+1)})-\ldots-\varphi_i(v_i^{(2^s)})=z_i\quad(1\leqslant i\leqslant k_0),$$

мы можем переписать это уравнение совсем кратко:

$$h_1z_1+h_2z_2+\ldots+h_{k_0}z_{k_0}=0. \tag{27}$$

Уравнений такого типа мы всего будем иметь 2^s, и совокупность их можно кратко записать в виде

$$\sum_{i=1}^{k_0}h_{mk_0+i}z_{mk_0+i}=0\quad(0\leqslant m\leqslant 2^s-1).$$

Однако, мы пока ограничиваемся рассмотрением одного уравнения (27), которое мы можем, конечно, рассматривать как типичное. Для оценки числа интересующих нас решений этого уравнения мы должны прежде всего посмотреть, в каких пределах может изменяться величина $\varphi_i(v_i^{(j)})$. С этой целью вспомним, что (стр. 62)

$$\varphi_i(y)=\sum_{u=1}^{n}a_{i,u}y^{n-u},$$

где

$$c_{i,u}=\sum_{v=0}^{u-1}a_v\binom{n-v}{u-v}h_i^{u-v-1}\qquad\left(1\leqslant i\leqslant\frac{k}{2}\right).$$

Поэтому из принятых нами предпосылок $|a_v| < c(n) N^{\frac{v}{n}}$ и $|h_l| \leqslant 2N^{\frac{1}{n}}$ следует

$$|a_{l,u}| < \sum_{v=0}^{u-1} c(n) N^{\frac{v}{n}} \binom{n-v}{u-v} c(n) N^{\frac{u-v-1}{n}} =$$

$$= c(n) N^{\frac{u-1}{n}} \sum_{v=0}^{n-1} \binom{n-v}{u-v},$$

т. е. ввиду $u \leqslant n$

$$|a_{l,u}| < c(n) N^{\frac{u-1}{n}}. \qquad (28)$$

Но, с другой стороны, в силу $|v_i^{(j)}| \leqslant 2N^{\frac{1}{n}}$ мы имеем $|v_i^{(j)}|^{n-u} \leqslant c(n) N^{\frac{n-u}{n}}$, вследствие чего

$$|a_{i,u}| \cdot |v_i^{(j)}|^{n-u} \leqslant c(n) N^{\frac{u-1}{n}} N^{\frac{n-u}{n}} = c(n) N^{\frac{n-1}{n}}.$$

Эта же граница (с другим $c(n)$) имеет место и для всего $\varphi_l(v_l^{(j)})$, так как число членов этого многочлена равно n. Таким образом,

$$|\varphi_l(v_l^{(j)})| < c(n) N^{\frac{n-1}{n}}, \quad 1 \leqslant i \leqslant k_0 2^s, \quad 1 \leqslant f \leqslant 2^s.$$

Но каждое z_l есть сумма $2^s = c(n)$ слагаемых вида $\pm \varphi_l(v_i^{(j)})$, и следовательно,

$$|z_i| < c(n) N^{\frac{n-1}{n}} \quad (1 \leqslant i \leqslant 2^s)$$

(конечно, с другим $c(n)$). Таким образом, в уравнении (27) каждое z_i может принимать только значения, заключённые в отрезке $(-c(n) N^{\frac{n-1}{n}}, +c(n) N^{\frac{n-1}{n}})$.

Пусть m — одно из этих чисел; равенство $z_i = m$ осуществимо, вообще говоря, не одним, а несколькими способами, так как определение числа z_i (стр. 64) таково, что одно и то же значение z_l может получиться при различных выборах чисел $v_l^{(j)}$ $(1 \leqslant j \leqslant 2^s)$. Мы должны теперь оценить число ре-

шений соотношения $z_l = m$, т. е. уравнения

$$\varphi_i(v_i^{(1)}) + \ldots + \varphi_i(v_i^{(2^s-1)}) - \\ - \varphi_i(v_i^{(2^{s-1}+1)}) - \ldots - \varphi_i(v_i^{(2^s)}) = m; \qquad (29)$$

именно в этом пункте мы и применим давно возвещённую нами индукцию. Вот как мы это сделаем.

Прежде всего перепишем уравнение (29) в виде

$$\varphi_i(v_i^{(1)}) + \varphi_i(v_i^{(2)}) + \ldots + \varphi_i(v_i^{(k')}) = \\ = m - \varphi_i(v_i^{(k'+1)}) - \ldots + \varphi_i(v_i^{(2^{s-1}+1)}) + \ldots + \varphi_i(v_i^{(2^s)});$$

это можно сделать потому, что при $k' = k(n-1) > 1$ (а мы видели, что уже $k(1) = 2$) мы имеем

$$2^{s-1} = 2^{[4\lg_2 k']-2} > k' \text{ *});$$

обозначая правую часть последнего уравнения через m', имеем

$$\varphi_i(v_i^{(1)}) + \ldots + \varphi_i(v_i^{(k')}) = m'; \qquad (30)$$

выберем для чисел

$$v_i^{(j)} \quad (k'+1 \leqslant j \leqslant 2^s)$$

какие-нибудь определённые значения (конечно, в отрезке $[-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}}]$); тогда и m' получит определённое значение. К уравнению (30) мы и применим доказываемое предложение, так как $\varphi_i(y)$ — многочлен степени $n-1$. Убедимся для этого, что все необходимые предпосылки выполнены; мы имеем

$$\varphi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u},$$

причём в силу (28)

$$|a_{i,u}| < c(n) N^{\frac{u-1}{n}} = c(n) (N^{\frac{n-1}{n}})^{\frac{u-1}{n-1}} \qquad (31)$$

и, как легко видеть,

$$|m'| < c(n) N^{\frac{n-1}{n}}$$

(ибо m и каждое $\varphi_i(y_i^{(j)})$ подчиняются этому неравенству).

---

*) Подробно: $k' \geqslant 2$, $\lg_2 k' \geqslant 1$, $3\lg_2 k' \geqslant 3$, $[4\lg_2 k'] - 2 > 4\lg_2 k' - 3 \geqslant \lg_2 k'$, $2^{s-1} = 2^{[4\lg_2 k']-2} \geqslant k'$.

В силу последнего неравенства роль N здесь может играть число $c(n)N^{\frac{n-1}{n}}$; а тогда условия (31), которым подчинены коэффициенты многочлена $\varphi_l(y)$, представляют собою как раз условия (23) с заменой n на $n-1$. Таким образом, все предпосылки действительно выполнены, и мы можем утверждать, что число решений уравнения (30), для которых $|v_l^{(j)}| \leqslant 2N^{\frac{1}{n}} = 2(N^{\frac{n-1}{n}})^{\frac{1}{n-1}}$, не превосходит числа

$$c(n)N^{\frac{n-1}{n}\cdot\frac{k'}{n-1}-1} = c(n)N^{\frac{k'-n+1}{n}}. \qquad (32)$$

Эта оценка получена для фиксированных значений $v_l^{(k'+1)}, \ldots, v_l^{(2^s)}$; очевидно, мы имеем не более чем

$$(2N^{\frac{1}{n}}+1)^{2^s-k'} < c(n)N^{\frac{2^s-k'}{n}} \qquad (33)$$

таких систем значений; общее число решений требуемого типа для уравнения (29) не превосходит поэтому произведения правых частей (32) и (33), т. е. не превосходит

$$c(n)N^{\frac{2^s-n+1}{n}} \qquad (34)$$

Вернёмся теперь к уравнению (27). Мы видели раньше (стр. 65), что каждое z_i может принимать только значения, лежащие в отрезке $(-c(n)N^{\frac{n-1}{n}}, +c(n)N^{\frac{n-1}{n}})$; теперь мы видим, что «кратность» каждого из этих значений (т. е. число способов выбора $y_l^{(j)}$, которыми оно может быть осуществлено) не превосходит числа (34).

Этот результат позволяет нам свести всю проблему к подсчёту чисел решений линейных уравнений. В самом деле, в конце § 5 оценка $r_k(m)$ была сведена нами к оценке чисел решений уравнений вида (26); но число решений уравнения (26), для которых $|y_i| \leqslant 2N^n$, как мы доказали применением леммы 5, не больше, чем сумма чисел решений 2^s уравнений типа (27), т. е. уже линейных уравнений; при этом для неизвестных z_l нами получены границы, в которых они могут изменяться. Некоторая новая трудность (этой ценою мы за-

платили за переход к линейным уравнениям) заключается в том, что новые неизвестные z_l мы должны рассматривать с определёнными кратностями (для которых мы также установили границы).

Наконец, мы не должны забывать, что все эти подсчёты ведутся в предположении, что числа h_l выбраны и зафиксированы. Результат, к которому мы придём, мы должны будем поэтому ещё помножить на число всех таких возможных выборов.

Заключительный вывод этого параграфа, который мы должны запомнить, гласит: *оцениваемое нами число* $r_k(m)$ *не превосходит суммы чисел решений в целых* z_i, $|z_l| \leqslant c(n) N^{\frac{n-1}{n}}$, *с кратностями* $\lambda_l \leqslant c(n) N^{\frac{2^s-n+1}{n}}$, *уравнений вида*

$$\sum_{i=1}^{k_0} h_{mk_0+i} z_{mk_0+l} = 0, \tag{35}$$

где m *пробегает значения* $0, 1, \ldots, 2^s-1$, *а числа* $h_r (1 \leqslant r \leqslant 2^s k_0)$ *независимо друг от друга пробегают все целые числа отрезка* $(-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}})$.

Мы видим таким образом, что для $r_k(m)$ мы получили теперь такую оценку, в формулировку которой совсем не входит данный многочлен $f(x)$, что придаёт этой оценке весьма общий характер.

§ 7.

Окончание.

После того как мы свели задачу к оценке числа решений линейных уравнений, не зависящих от специального вида многочлена $f(x)$, мы уже легко приходим к цели с помощью леммы 3.

Обозначим через Γ какую-нибудь определённую комбинацию чисел h_l ($|h_i| \leqslant 2N^{\frac{1}{n}}$, $1 \leqslant i \leqslant \frac{k}{2}$) и через $U_m(\Gamma)$ — число решений уравнения (35) при этой фиксированной комбинации Γ и при некотором данном m, причём имеются в виду решения z_i, удовлетворяющие неравенствам $|z_i| \leqslant c(n) N^{\frac{n-1}{n}}$

с кратностями $\lambda_l \leqslant c(n) N^{\frac{2^s-n+1}{n}}$. Тогда, согласно заключению предыдущего параграфа,

$$r_k(m) \leqslant \sum_{\Gamma} \left\{ \sum_{m=0}^{2^s-1} U_m(\Gamma) \right\},$$

где суммирование по Γ распространяется на все допустимые комбинации Γ чисел h_l. Иначе,

$$r_k(m) \leqslant \sum_{m=0}^{2^s-1} \left\{ \sum_{\Gamma} U_m(\Gamma) \right\}.$$

Но непосредственно очевидно, что суммы $\sum_{\Gamma} U_m(\Gamma)$ для различных m ничем не отличаются друг от друга (ибо ничем друг от друга не отличаются уравнения (35) для различных m); поэтому мы можем написать

$$r_k(m) \leqslant 2^s \sum_{\Gamma} U_0(\Gamma) = c(n) \sum_{\Gamma} U_0(\Gamma).$$

Здесь $U_0(\Gamma)$ есть число решений уравнения

$$h_1 z_1 + h_2 z_2 + \ldots + h_{k_0} z_{k_0} = 0 \qquad (36)$$

при данной комбинации Γ чисел h_l $\left(|h_l| \leqslant 2N^{\frac{1}{n}},\ 1 \leqslant i \leqslant \frac{k}{2} \right)$, причём $|z_l| \leqslant c(n) N^{\frac{n-1}{n}}$ и z_l имеет кратность $\lambda_l \leqslant$ $\leqslant c(n) N^{\frac{2^s-n+1}{n}}$. Если мы обозначим через $U_0^*(\Gamma)$ число решений того же уравнения в предположении, что все z_l однократны, то очевидно

$$U_0(\Gamma) \leqslant \{c(n) N^{\frac{2^s-n+1}{n}}\}^{k_0} U_0^*(\Gamma),$$

или, помня, что $k_0 = 2n$,

$$U_0(\Gamma) \leqslant c(n) N^{2(2^s-n+1)} U_0^*(\Gamma),$$

и, следовательно,

$$r_k(m) \leqslant c(n) N^{2(2^s-n+1)} \sum_{\Gamma} U_0^*(\Gamma). \qquad (37)$$

Теперь заметим следующее. Каждое Γ представляет собою некоторую допустимую комбинацию значений в с е х h_i $\left(1 \leqslant i \leqslant \frac{k}{2}\right)$; между тем число $U_0^*(\Gamma)$ полностью определяется значениями первых $k_0 = 2n$ из этих чисел ($1 \leqslant i \leqslant 2n$), ибо только они входят в уравнение (36). Выбрав некоторую определённую комбинацию Γ, мы тем самым, конечно, однозначно определяем и некоторую комбинацию Γ' значений чисел $h_1, h_2, \ldots, h_{2n}$. Но если, обратно, выбрана определённая комбинация Γ' чисел $h_1, h_2, \ldots, h_{2n}$, то ей соответствует не одна комбинация Γ, а столько, сколькими способами можно «довыбрать» остальные h_i $\left(2n < i \leqslant \frac{k}{2}\right)$; так как каждое h_i должно принадлежать отрезку $(-2N^{\frac{1}{n}}, +2N^{\frac{1}{n}})$, то очевидно, что одной комбинации Γ' соответствует не более чем

$$c(n)(N^{\frac{1}{n}})^{\frac{k}{2}-2n} = c(n)N^{\frac{k}{2n}-2}$$

комбинаций Γ. Поэтому

$$\sum_{\Gamma} U_0^*(\Gamma) \leqslant c(n) N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma').$$

Здесь $U_0^*(\Gamma')$ есть число решений в целых z_i, $|z_i| \leqslant c(n) N^{\frac{n-1}{n}}$, $1 \leqslant i \leqslant 2n$, уравнения (36) при данной комбинации Γ' чисел h_i, $|h_i| \leqslant 2N^{\frac{1}{n}}$, $1 \leqslant i \leqslant 2n$, и суммирование производится по всем таким комбинациям. Из (37) мы получаем поэтому

$$r_k(m) \leqslant c(n) N^{2(2^s - n + 1)} N^{\frac{k}{2n}-2} \sum_{\Gamma'} U_0^*(\Gamma') = *)$$

$$= c(n) N^{2(2^{s+1}-n)} \sum_{\Gamma'} U_0^*(\Gamma'). \qquad (38)$$

Наконец, $\sum_{\Gamma'} U_0^*(\Gamma')$ непосредственно оценивается с помощью леммы 3, где надо положить $l = 2n$, $A = 2N^{\frac{1}{n}}$, $B = c(n) N^{\frac{n-1}{n}}$.

*) Вспомните, что $k = 2n \cdot 2^{s+1}$.

Вы легко проверите сами, что все предпосылки леммы 3 при этом выполнены; применяя её, мы находим

$$\sum_{\Gamma'} U_0^*(\Gamma') \leqslant c(n)(AB)^{2n-1} = c(n) N^{2n-1}.$$

Наконец, неравенство (38) даёт нам

$$r_k(m) \leqslant c(n) N^{2(2^s+1-1)} \cdot N^{2n-1} =$$

$$= c(n) N^{2 \cdot 2^s+1-1} = c(n) N^{\frac{k}{n}-1},$$

чем и завершено доказательство основной леммы, а вместе с тем и теоремы Гильберта.

Доказательство это, прекрасное по своей элементарности, несомненно покажется Вам очень сложным. Но Вам стоит поработать над ним 2—3 недели с бумагой и карандашом в руках, чтобы полностью понять и усвоить его. Именно на преодолении такого рода трудностей растёт и развивается математик.

ОГЛАВЛЕНИЕ