Математический Институт имени В. А. Стеклова

отдел алгебры и теории чисел

На правах рукописи

Штейников Юрий Николаевич

# ТРИГОНОМЕТРИЧЕСКИЕ СУММЫ ПО ПОДГРУППАМ И ЗАДАЧИ ДЕЛИМОСТИ ЧАСТНЫХ ФЕРМА

01.01.06 — математическая логика, алгебра, теория чисел

Диссертация

на соискание ученой степени
кандидата физико–математических наук

Научный руководитель —
доктор физико–математических
наук С. В. Конягин

Москва 2015

# Содержание

# Введение.

Диссертация подготовлена в Математическом институте имени В. А. Стеклова и затрагивает ряд вопросов, относящихся к распределению элементов подгрупп и задач делимости частных Ферма.

**Актуальность темы.** Настоящая диссертация посвящена исследованию оценок тригонометрических сумм по подгруппам, их приложениям к задачам делимости частных Ферма и свойствам распределения элементов полугрупп натуральных чисел.

Постановки задач, связанных с оценками тригонометрических сумм по подгруппам восходят к работам К.Гаусса, Г.Г. Харди, Дж.Е. Литтлвуда. Ими впоследствии занимались такие известные математики как А.А. Карацуба, И.Е. Шпарлинский, Д.Р. Хиф-Браун, С.В. Конягин, Ж. Бургейн, И.Д. Шкредов. Этой и сходным задачам посвящено множество работ, как в России, так и за рубежом. Классическим и новым результатам, связанным с этими вопросами, а также их приложениям уделено внимание в совместной книге С.В Конягина и И.Е. Шпарлинского [26], а также в книге Т.Тау и В.Ву [35].

За последние десятилетия были разработаны существенно новые методы и получены глубокие результаты с многочисленными применениями тригонометрических сумм в различных задачах теории чисел. Оценки этих сумм могут быть получены с использованием оценок на количество решений специальных сравнений. Такой подход, основанный на получении оценок таких сравнений, использовался например в работах Д.Р. Хиф-Брауна, С.В. Конягина [24] [2], Ю.В Малыхина [4] [3], Б. Жоу [37], И.Д. Шкредова [32]. В настоящей диссертации получена новая оценка на число решений определенного сравнения, на основании которой получаются новые оценки тригонометрических сумм по мультипликативным подгруппам, которые принадлежат полю вычетов простого порядка и размер которых лежит в определенном диапазоне.

В диссертации также исследуются задачи о делимости частных Ферма на простое и квадрат простого числа. Данное свойство имеет некоторые теоретико-числовые приложения. Первые нетривиальные результаты в задаче о делимости частного Ферма на простое число появились в работах Х. Ленстры [28], Э. Грэнвиля [21]. В статье [16] с использованием тригонометрических сумм и комбинаторных идей были получены существенные продвижения в этой задаче. В диссертации будет улучшена одна из теорем работы [16].

**Научная новизна.** Полученные результаты являются новыми, полученными автором самостоятельно. Основными результатами данной работы можно считать следующие:

— Получены новые оценки тригонометрических сумм по подгруппам в поле вычетов простого порядка, размер которых есть приблизительно кубический корень из простого числа.

— Получена новая верхняя оценка на первое число, не обладающего свойством делимости частного Ферма на простое число, за исключением множества простых относительно нулевой плотности.

— Получены оценки о количестве элементов полугрупп натуральных чисел на коротких отрезках с заданным степенным распределением на больших интервалах.

**Методы исследования.** В работе используются результаты, полученные методом С.А. Степанова, линейная алгебра, результаты о распределении гладких чисел, некоторые комбинаторные идеи.

**Теоретическая и практическая ценность.** Диссертация носит теоретический характер. Ее результаты могут быть использованы при исследовании распределения конечных множеств.

**Апробация работы.** Результаты настоящей диссертации неоднократно докладывались автором на следующих семинарах:

1. Современные проблемы теории чисел – под руководством С.В. Конягина и И.Д. Шкредова в Математическом институте имени В.А. Стеклова,

2. Ортогональные ряды – под руководством Б.С. Кашина, С.В. Конягина,

а также на международных конференциях

Компьютерная алгебра и информационные технологии (Одесса, 20–26 августа 2012 года),

Лобачевские чтения – 2014 (Казань, 24-29 октября 2014 г.),

Воронежская зимняя математическая школа. Современные методы теории функций и смежные проблемы. (Воронеж, 27 января – 2 февраля 2015 года.)

Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения (Тула, 25–30 мая 2015 года.)

XII Международная Казанская летняя школа-конференция–

Теория функций, ее приложения и смежные вопросы (Казань, 27 июня – 4 июля 2015 г.)

**Публикации.** Результаты диссертации опубликованы в работах [6], [7], [8], [9]. Кроме того, результаты диссертации были также опубликованы в трудах конференций [10], [11], [12], [13], [14].

**Структура и объем работы.** Диссертация изложена на 60 страницах и состоит из введения, 4 глав и списка литературы, включающего 37 наименований.

**Содержание работы.**

Введем некоторые определения, которыми будем пользоваться в дальнейшем. Для натурального $q$ мы будем обозначать через $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$, а через $\mathbb{Z}_q^*$ условимся обозначать множество обратимых элементов кольца $\mathbb{Z}_q$, $p$ – достаточно большое простое число, если не оговорено обратное. Для целого $x$ обозначим $e_q(x) := e^{2\pi ix/q}$. Пусть $\Gamma \subseteq \mathbb{Z}_q^*$ - некоторая подгруппа по умножению. Тригонометрическими суммами по подгруппе $\Gamma$ будут называться суммы вида

$$S(a,\Gamma) = \sum_{x\in\Gamma} e_q(ax).$$

Важной задачей является установление нетривиальных по порядку верхних оценок для $S(\Gamma) := \max_{a\in\mathbb{Z}_q^*} |S(a,\Gamma)|$:

$$S(\Gamma) = o(|\Gamma|), q \to \infty. \tag{0.1}$$

Один из первых результатов в этом направлении принадлежит К. Гауссу. В случае когда $\Gamma$ – это подгруппа квадратичных вычетов, Гаусс установил точное значение величин $S(a,\Gamma)$. Оценками $S(a,\Gamma)$ для случая $\Gamma \subset \mathbb{Z}_p^*$ занимались Г.Г. Харди и Дж. Е. Литллвуд [23]. Из их результата [23] следует соотношение (0.1) для подгрупп $\Gamma$, когда $|\Gamma| > \sqrt{p}$.

По определению пусть

$$T_k(\Gamma) := \{(x_1,\ldots,x_{2k}) \in \Gamma^{(2k)} : x_1+\ldots+x_k = x_{k+1}+\ldots+x_{2k}\}.$$

Верхние оценки для $S(\Gamma)$ могут быть получены с использованием оценок для $T_k(\Gamma)$. Пусть $\Gamma \subseteq \mathbb{Z}_p^*$ - подгруппа мультипликативной группы поля простого порядка $p$ и $t := |\Gamma|$. А. Гарсиа и Дж. Волох [22] установили, что при $t \ll p^{3/4}$ и любого $a \in \mathbb{Z}_p^*$ сравнение $g + g' \equiv a \pmod p$ имеет не более $4t^{2/3}$ решений относительно $g, g' \in \Gamma$. Из этого следует нетривиальная оценка $T_2(\Gamma) \ll t^{8/3}$. На основании метода С.А. Степанова Д.Р. Хиф-Браун и С.В. Конягин установили [24], что при $t < p^{2/3}$ справедлива оценка $T_2(\Gamma) \ll t^{5/2}$. Затем С.В. Конягин получил [2] нетривиальные оценки для $T_k(\Gamma)$ для всех натуральных $k > 1$.

Таким образом, в работе [2] было показано, что для подгрупп при $t > p^{1/4+\varepsilon}$ выполнено неравенство:

$$S(\Gamma) < C(\varepsilon) t p^{-\delta(\varepsilon)},$$

для некоторых функций $C(\varepsilon), \delta(\varepsilon) > 0$. Используя другой подход Ж. Бургейн и С. В. Конягин [17] доказали оценку такого типа и при $t > p^{\varepsilon}$. Ж. Бургейн доказал такой результат для произвольного составного модуля.

Относительно недавно И. Д. Шкредов [33], [31] усилил оценку как для величины $T_2(\Gamma)$, так и для соответствующей тригонометрической суммы для подгрупп $\Gamma$, размер которых лежит в определеных границах.

Используя подход И. Д. Шкредова этих работ, в первой главе получена новая оценка на величину $T_3(\Gamma)$. Это – основной результат первой главы, из которого получаются новые верхние оценки тригонометрических сумм по подгруппам в поле вычетов простого порядка, когда размер подгруппы есть $p^{\alpha}$ и $\alpha$ лежит в окрестности $1/3$. Теорема формулируется так.

**Теорема.** *При $t < p^{1/2}$ справедлива следующая оценка:*

$$T_3(\Gamma) \ll t^{4\frac{3}{14}} (\log t)^{12/7}.$$

Далее в этой главе будут получены с использованием тригонометрических сумм и других величин новые оценки для наибольшего расстояния между соседними элементами подгруппы $\Gamma$, $|\Gamma| \geqslant p^{\frac{1}{2}}$. Также будет получена оценка тригонометрической суммы по специальной подгруппе в кольце вычетов по модулю $p^3$ и этот результат будет использован в четвертой главе для задачи делимости частных Ферма на квадрат простого числа.

В последней части первой главы, следуя работе [20], будет распространена от простого модуля $p$ к произвольному оценка о числе решений $ux \equiv y \pmod p, x, y \in I, u \in U$, включающего интервал натуральных чисел $I$ и множества с малым мультипликативным удвоением $U$.

Во второй главе изучается такая задача. Пусть даны два произвольных множества $G_1$ и $G_2$, причем $G_1 \subseteq \mathbb{Z}_{q_1}, G_2 \subseteq \mathbb{Z}_{q_2}$, $q_1$ и $q_2$ – различные натуральные числа. Для заданного $N$ требуется оценить сверху количество натуральных $n$, что

$$\{n < N, n \in G_1 \pmod{q_1}, n \in G_2 \pmod{q_2}\} \tag{0.2}$$

Подобная величина, когда $G_1$ и $G_2$ являются специальными подгруппами, была оценена в работе [16] и там же использовалась для исследования свойств делимости частных Ферма. Во второй главе рассматривается эта задача в несколько более общей формулировке.

Пусть $q_1$ и $q_2$ по порядку одинаковые, взаимно простые натуральные числа. Пусть также заданы величины $N_1, N_2$, являющиеся соответственно числом решений следующих двух сравнений

$$x_1 - x_2 \equiv kq_2 \pmod{q_1}, x_1, x_2 \in G_1, 0 \leqslant k \leqslant \frac{N}{q_1}$$

и

$$x_1 - x_2 \equiv kq_1 \pmod{q_2}, x_1, x_2 \in G_2, 0 \leqslant k \leqslant \frac{N}{q_1}.$$

Во второй главе получена неулучшаемая по порядку оценка на искомую величину (0.2). Ниже дается основной, но с несколько упрощенной формулировкой, результат второй главы.

**Теорема.** *Пусть, как указано выше, даны $q_1, q_2, N$ множества $G_1 \subseteq \mathbb{Z}_{q_1}, G_2 \subseteq \mathbb{Z}_{q_2}$ и соответственно заданы величины $N_1, N_2$. Тогда справедлива оценка*

$$|\{n < N, n \in G_1 \pmod{q_1}, n \in G_2 \pmod{q_2}\}| \ll (N_1 N_2)^{1/2}$$

Мы отмечаем, что этот результат используется далее в четвертой главе.

В третьей главе рассматривается такая задача. Пусть дано множество $A$ натуральных чисел, замкнутое относительно умножения. То есть, если $a, b \in A$ то и $ab \in A$. Пусть известно, что для некоторого числа $q$ и $\nu \in (0, 1)$ выполняется

$$|\{m \in A; 1 \leqslant m \leqslant q\}| < q^{\nu}.$$

Требуется оценить количество элементов множества $A$ на интервале $[1, n]$, когда $n$ растет медленнее чем любая степень $q$. В этой главе получены верхние оценки для такой величины.

Например, в качестве множества $A$ можно взять все натуральные числа, у которых вычеты по модулю $q$ принадлежат мультипликативной подгруппе $\Gamma \subset \mathbb{Z}_q^*$. Отметим, что в работе [18] получены оценки на количество чисел не превосходящих $n$, которые принадлежат подгруппе порядка $t$ группы $\mathbb{Z}_p^*$. Эти оценки содержательны, когда $t$ мало по сравнению с $p$. Из результата третьей главы вытекают оценки в случае, когда $t$ растет как степень $p$, а $n$ мало.

Для простого $p$ и целого $a$, $(a, p) = 1$, определяется частное Ферма:

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

В четвертой главе исследуются задачи о делимости $q_p(a)$ на $p$ и $p^2$. Нас будет интересовать наименьшее $a$, для которого не выполнено сравнение $q_p(a) \equiv 0 \pmod{p}$. Для простого $p$ обозначим это число $l_p$.

Ленстра доказал следующие неравенства [28]:

$$\begin{cases} p > 3 \Rightarrow l_p \leqslant 4(\log p)^2; \\ p \to \infty \Rightarrow l_p \leqslant (4e^{-2} + o(1))(\log p)^2. \end{cases}$$

Можно, однако, ожидать гораздо более сильную оценку на $l_p$. Например, Ленстра предположил, что $l_p \leqslant 3$. В работе [16] были расмотрены три задачи о верхней оценке $l_p$ :

1)для всех простых $p$,

2) для всех простых на заданном интервале, возможно кроме одного,

3)для большинства простых на заданном интервале.

Основной результат четвертой главы - получение новой верхней оценки для задачи 3). Соответствующий результат формулируется так.

**Теорема.** *Для каждого* $\varepsilon > 0$ *существует такое* $\delta > 0$, *что при достаточно больших* $Q$ *неравенство:*

$$l_p \leqslant (\log p)^{\frac{3}{2}+\varepsilon}$$

*выполнено для всех простых* $p < Q$, *за исключением* $O(Q^{1-\delta})$ *простых.*

Отметим, что в работе [16] в соответствующей теореме вместо показателя $\frac{3}{2}$ стоял показатель $\frac{5}{3}$.

Автор выражает глубокую благодарность своему научному руководителю С. В. Конягину за постановку задач и постоянное внимание к работе.

# Глава 1

# Тригонометрические суммы по подгруппам и некоторые их применения.

## 1.1 Введение

Как и раньше пусть $p$ – простое число, $\Gamma$ – подгруппа $\mathbb{Z}_p^*$, $a \in \mathbb{Z}_p^*$. Требуется нетривиально оценить $S(\Gamma)$:

$$S(\Gamma) := \max_{a \in \mathbb{Z}_p^*} |S(a, \Gamma)|.$$

Одна из основных задач этой главы – получение нетривиальных по порядку верхних оценок для $S(\Gamma)$.

Известны применения этих оценок, например для распределения элементов подгрупп [15], некоторых аддитивных задач по простому модулю. Всюду далее $t := |\Gamma|$.

Для целого $k$ и для мультипликативной группы $\Gamma \subset \mathbb{Z}_p^*$ мы определили величину

$$T_k(\Gamma) := \{(x_1, \dots, x_{2k}) \in \Gamma^{2k} : x_1 + \dots + x_k = x_{k+1} + \dots + x_{2k}\}.$$

Оценки для $S(\Gamma)$ могут быть получены с помощью оценок для $T_k(\Gamma)$. Известна следующая лемма:

**Лемма 1.1.** *Для произвольных натуральных $k, l$ справедливо неравенство:*

$$S(\Gamma) \leqslant (pT_k(\Gamma)T_l(\Gamma))^{\frac{1}{2kl}} t^{1-1/k-1/l}.$$

Оценки такого вида установлены И.М. Виноградовым для тригонометрических сумм Вейля. Доказательство этой леммы можно найти в [26] .

С.В. Конягин получил нетривиальные оценки $T_k(\Gamma)$ для всех натуральных $k$ (см. [2]). Им доказан следующий результат.

**Лемма 1.2.** *Для любого натурального $m$ существует такое $C(m)$, что для любых $p, \Gamma$ таких, что $t < p^{2/3}$ при $m = 2$ и $t < p^{1/2}$ при $m > 2$, имеет место оценка:*

$$T_m(\Gamma) \leqslant C(m) t^{2m-2+1/2^{m-1}}.$$

В работах [33], [31] И.Д. Шкредов доказал оценки как для величины $T_2(\Gamma)$, так и для соответствующей тригонометрической суммы. Ниже приводятся эти результаты.

**Теорема 1.1.** *При $t < p^{2/3}$ справедлива оценка:*

$$S(\Gamma) \ll p^{1/6} t^{1/2} (\log t)^{1/6}, T_2(\Gamma) \ll \min(t^{\frac{32}{13}} (\log t)^{\frac{41}{65}}, t^3 p^{-\frac{1}{3}} \log t + p^{\frac{1}{26}} t^{\frac{31}{13}} (\log t)^{\frac{8}{13}}).$$

Это утверждение усиливает ранее полученные оценки сумм по подгруппам, чей размер находится в определенном интервале. В данной главе мы будем использовать идеи указанных работ и получим новую оценку для величины $T_3(\Gamma)$. Как следствие, используя лемму 1.1, мы также усилим оценки сумм по подгруппам, чей порядок находится в интервале $[p^{\frac{28}{95}}, p^{\frac{182}{487}}]$. Отметим, что

$$\frac{28}{95} = 0.29473..., \frac{182}{487} = 0.37371...$$

Один из основных результатов этой главы такой:

**Теорема 1.2.** *При $t < p^{1/2}$ справедлива следующая оценка:*

$$T_3(\Gamma) \ll t^{4\frac{3}{14}} (\log t)^{12/7}.$$

Как следствие теоремы 1.2 и леммы 1.1 мы получаем теорему 1.3

**Теорема 1.3.** *Справедливы неравенства:*

$$\begin{cases} p^{\frac{182}{515}} < t < p^{\frac{182}{487}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{12}} t^{\frac{1579}{2184}} (\log t)^{\frac{1067}{5460}}; \\ p^{\frac{56}{185}} < t < p^{\frac{182}{515}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{18}} t^{\frac{101}{126}} (\log t)^{\frac{4}{21}}; \\ p^{\frac{28}{95}} < t < p^{\frac{56}{185}} \Rightarrow S(\Gamma) \ll p^{\frac{1}{24}} t^{\frac{1139}{1344}} (\log t)^{\frac{1}{14}} \end{cases}$$

Для сравнения приведем такой пример. Для подгруппы $\Gamma$ у которой $t$ имеет порядок $p^{\frac{1}{3}}$ справедлива оценка $S(\Gamma) < t^{\frac{61}{63}+o(1)}$. В предыдущем результате вместо показателя $\frac{61}{63}$ был $\frac{35}{36}$. Отметим, что

$$\frac{35}{36} = 0.97222..., \frac{61}{63} = 0.96825...$$

Мы применим оценки величин тригонометрических сумм и $T_k(\Gamma)$ для оценки наибольшего расстояния между соседними элементами смежных классов по подгруппе.

В этой главе также мы получим оценку тригонометрической суммы для подгруппы $G$, $G \subseteq \mathbb{Z}^*_{p^3}$, $|G| = p-1$. Для этого мы будем использовать современные оценки на величины $S(G)$ $T_2(G)$ для $G \in \mathbb{Z}^*_{p^2}$ и метод Ю.В. Малыхина получения таких оценок по модулю $p^r$, где $r$ – произвольное.

## 1.2 Предварительные утверждения

Также обозначим через $\Gamma(x)$ – характеристическую функцию множества $\Gamma$ на $\mathbb{Z}_p$. По определению для двух функций $f, g$ на $\mathbb{Z}_p$ полагаем $f \circ g(x) := \sum_{k,l:k-l=x} f(k)g(l)$, $f * g(x) := \sum_{k,l:k+l=x} f(k)g(l)$.

Пусть $g : \mathbb{Z}_p \mapsto R$ - некоторая функция. Введем матрицу, предложенную И.Д. Шкредовым

$$T^g(x,y) := g(x-y)\Gamma(x)\Gamma(y),$$

где $x, y \in \mathbb{Z}_p$. Эту матрицу можно рассматривать как оператор, действующий на пространстве функций. Через $\{\mu_\alpha(T^g)\}$ и $\{f_\alpha\}$ обозначим набор собственных значений и собственных функций этого оператора. Нам понадобятся утверждения, доказанные соответственно в [33] (предложение 3) и [2] (следствие 16).

**Теорема 1.4.** *Пусть $g_1, g_2 : \mathbb{Z}_p \mapsto R$ - четные функции и $\{f_\alpha\}$ - собственные функции оператора $T^{g_1}$. Тогда выполнено равенство:*

$$\sum_{x,y,z\in\Gamma} g_1(x-y)g_1(x-z)g_2(y-z) = \sum_\alpha \mu^2_\alpha(T^{g_1}) < T^{g_2}f_\alpha, f_\alpha > .$$

**Теорема 1.5.** *Пусть $\Gamma_1, S_2, S_3 \subseteq \mathbb{Z}^*_p$ - являются $\Gamma$ - инвариантными множествами, причем $\Gamma_1-$ смежный класс по $\Gamma$ и что: $|S_2||S_3| \leqslant t^4/16$. Тогда имеет место неравенство:*

$$\sum_{x\in\Gamma_1}(S_2 \circ S_3)(x) \ll t^{1/3}(|S_2||S_3|)^{2/3}.$$

Через $\Gamma_1, \Gamma_2, ...$ обозначим смежные классы группы $\mathbb{Z}^*_p$ по подгруппе $\Gamma$. Будем считать $\Gamma_0$ - это класс состоящий из нулевого элемента. Соответственно пусть $\xi_i$ - являются представителями этих классов. Обозначим также

$$N_4(y) = |\{x_1 + x_2 - x_3 - x_4 \equiv y \pmod p, x_i \in \Gamma\}|$$

$$N_3(y) = |\{x_1 + x_2 - x_3 \equiv y \pmod p, x_i \in \Gamma\}|$$

$$a_{i,j} = |\{g_i - g \equiv \xi_j \pmod p, g_i \in \Gamma_i, g \in \Gamma, \xi_j \in \Gamma_j - fixed\}|.$$

$N_m(y), a_{i,j}$ не зависят от выбора в качестве $y$ представителя данного смежного класса по подгруппе $\Gamma$.

**Лемма 1.3.** *Пусть $\{\xi_j\}, j \leqslant t$ принадлежат различным ненулевым смежным классам $\Gamma_{\sigma_j}$ и $N_4(\xi_j)$ невозрастают по $j$. Тогда имеет место неравенство:*

$$N_4(\xi_j) \ll tT_3^{1/3}(\Gamma)j^{-1/3}.$$

Доказательство. Для получения неравенства достаточно получить оценку на сумму этих $J$ слагаемых такого вида:

$$\sum_{1\leqslant j\leqslant J} N_4(\xi_j) \ll tT_3J^{2/3},$$

когда $J < t$. Несложно заметить, что:

$$N_4(\xi_j) = \sum_i N_3(x_i)a_{i,\sigma_j},$$

где $x_i$ принадлежат различным смежным классам $\Gamma_i$(и нулевому тоже). Далее,

$$\sum_{1\leqslant j\leqslant J} N_4(\xi_j) = \sum_i N_3(x_i)s_i,$$

где $s_i = \sum_{1\leqslant j\leqslant J} a_{i,\sigma_j}$.

Разберемся со слагаемым соответствующем $i = 0$. Замечаем, что $a_{0,j}$ равно единице только в одном случае среди всех $j$. Поэтому слагаемое $N_3(0)s_0 \ll t^{5/3}$. Значит, вклад этого слагаемого не существенен для заявленной в утверждении оценки. Оставшиеся в сумме слагаемые перепишем так:

$$\sum_i N_3(x_{i_r})s_{i_r},$$

где индекс $i \in [1, (p-1)/t]$, $i_r$ отличны от нуля и $N_3(x_{i_r})$ неубывают по $i$.

При $i$ отличном от нуля имеем две оценки:

$$N_3(x_{i_r}) \leqslant T_3^{1/2}(\Gamma)(ti)^{-1/2}, N_3(x_{i_r}) \leqslant t^2/i.$$

Будем разбивать сумму $\sum_i N_3(x_{i_r})s_{i_r}$ на две части: $1 \leqslant i \leqslant i_0, i \geqslant i_0$.Обозначим эти суммы через $\sigma_1, \sigma_2$. Разберемся с 1-ой суммой $\sigma_1$:

$$\sum_{1\leqslant i\leqslant i_0} N_3(x_{i_r})s_{i_r} \leqslant \sum_{1\leqslant i\leqslant i_0} T_3^{1/2}(\Gamma)(ti)^{-1/2}s_{i_r}.$$

Применяя преобразование Абеля к этой сумме, мы получаем

$$\sum_{1\leqslant i<i_0}(T_3^{1/2}(\Gamma)(ti)^{-1/2}-T_3^{1/2}(\Gamma)(t(i+1))^{-1/2})S_i+T_3^{1/2}(\Gamma)(ti_0)^{-1/2}S_{i_0},$$

где $S_i=\sum_{k\leqslant i}s_k$. Покажем, что для любого $i$ справедлива оценка

$$S_i\ll(iJt)^{2/3}.$$

Если $ij\leqslant t^2/16$ то заявленная оценка следует из теоремы 1.5. Пусть теперь $iJ>t^2/16$. Вспоминаем, что $J\leqslant t$. Тогда в этом случае из простых соображений оценить можно так

$$S_i\leqslant Jt\leqslant t^2\ll(t^3)^{2/3}\ll(iJt)^{2/3}.$$

Тем самым оценка на $S_i$ верна всегда при ограничении $J<t$. Для первой суммы $\sigma_1$ мы получаем оценку $\sigma\ll T_3^{1/2}t^{1/6}J^{2/3}i_0^{1/6}$.

Теперь разберемся с суммой $\sigma_2$ :

$$\sigma_2\leqslant\sum_{i>i_0}(t^2/i)s_i$$

Опять применяя преобразование Абеля, получаем

$$\sigma_2\leqslant\sum_{i>i_0}(\frac{t^2}{i}-\frac{t^2}{i+1})S_i\ll t^{8/3}J^{2/3}i_0^{-1/3}.$$

Выбирая параметр $i_0:=t^5/T_3(\Gamma)$ мы завершаем доказательство леммы 1.3.

## 1.3 Доказательство теоремы 1.2

Пусть ненулевые смежные классы $C_j$ по подгруппе $\Gamma$ расположены таким образом, что числа $t_j:=N_4(y),y\in C_j$ образуют невозрастающую последовательность.

Прежде всего мы можем считать, что

$$t_j\leqslant MtT_3^{1/3}(\Gamma)j^{-1/3},$$

где $M$- некоторая константа. Справедливость этой оценки для $j\leqslant t$ следует из леммы 1.3. Пусть теперь $j\geqslant t$. Тогда

$$t_j\leqslant t^3/j$$

Если вдруг $\frac{t^3}{j} \geqslant \frac{MtT_3^{1/3}(\Gamma)}{j^{1/3}}$, то это влечет оценку $T_3(\Gamma) \ll t^4$. Поэтому мы можем считать, что для всех $j$ выполнено $t_j \leqslant MtT_3^{1/3}(\Gamma)j^{-1/3}$ с некоторой абсолютной константой $M$.

Далее, по данному натуральному $i$ по определению $S_i(x)$ — характеристическая функция множества:

$$S_i := \{\cup_j C_j : \frac{MtT_3^{1/3}(\Gamma)}{2^i} < t_j \leqslant \frac{MtT_3^{1/3}(\Gamma)}{2^{i-1}}\}$$

и функции $g_i(x) := (\Gamma * \Gamma) \circ (\Gamma * \Gamma)(x)S_i(x)$, $g(x) = (\Gamma * \Gamma) \circ (\Gamma * \Gamma)(x)$.

Для натурального $i$ определим величину $T_3^{(i)}(\Gamma) := |\{x_1, \dots, x_6 \in \Gamma : x_1 + x_2 - x_3 - x_4 = x_5 - x_6 : x_1 + x_2 - x_3 - x_4 \in S_i\}|$. Для $i = 0$ мы полагаем $T_3^{(0)}(\Gamma) := |\{x_1, \dots, x_6 \in \Gamma : x_1 + x_2 - x_3 - x_4 = x_5 - x_6 : x_1 + x_2 - x_3 - x_4 = 0\}|$

Легко видеть, что сумма всех $T_3^{(i)}(\Gamma)$ равна в точности $T_3(\Gamma)$. Далее мы выбираем такое натуральное $i$, что

$$T_3^{(i)}(\Gamma) \gg \frac{T_3(\Gamma)}{(\log p)}$$

и фиксируем его. С другой стороны, $T_3^{(i)}(\Gamma)$ можно «выразить через оператор»:

$$< T^{g_i}\Gamma, \Gamma >= \sum_{x,y \in \Gamma} (\Gamma * \Gamma) \circ (\Gamma * \Gamma)(x - y)S_i(x - y) =$$

$$= \sum_{z \in S_i} ((\Gamma * \Gamma) \circ (\Gamma * \Gamma))(z)(\Gamma \circ \Gamma)(z) = T_3^{(i)}(\Gamma).$$

Далее, $T_3^{(i)}(\Gamma) =< T^{g_i}\Gamma, \Gamma >\leqslant \mu_0(T^{g_i})t$.

Итак, $\frac{T_3^{(i)}(\Gamma)}{t} \leqslant \mu_0(T^{g_i})$

Наша цель оценить величину $\mu_0(T^{g_i})$. Для этого воспользуемся теоремой 1.4 и неотрицательностью оператора $T^g$, получим ($f_\alpha$ - собственные функции оператора $T^{g_i}$):

$$\mu_0^3(T^{g_i}) \leqslant \sum_\alpha \mu_\alpha^2(T^{g_i}) < T^g f_\alpha, f_\alpha >= \sum_{x,y,z \in \Gamma} g_i(x - y)g_i(x - z)g(y - z).$$

Преобразуем последнюю сумму, обозначив $\alpha := x - y, \beta := x - z$

$$\sigma = \sum_{x,y,z \in \Gamma} g_i(x - y)g_i(x - z)g(y - z) = \sum_{\alpha,\beta} g_i(\alpha)g_i(\beta)g(\beta - \alpha)C_3(\alpha, \beta),$$

где

$$C_3(\alpha,\beta) := \{x \in \Gamma : x-\alpha, x-\beta \in \Gamma\}.$$

Итак, мы заключаем: $(\frac{T_3^{(i)}(\Gamma)}{t})^3 \leqslant \sum_{\alpha,\beta} g_i(\alpha)g_i(\beta)g(\beta-\alpha)C_3(\alpha,\beta)$.

Оценим сверху вклад слагаемых $(\alpha,\beta)$, для которых $g(\beta-\alpha) \leqslant d$ (где $d$ определим потом).

Для них имеем оценку:

$$d\sum_{\alpha,\beta} g_i(\alpha)g_i(\beta)C_3(\alpha,\beta) = d\sum_{x\in\Gamma}\sum_{\alpha,\beta} g_i(\alpha)g_i(\beta)\Gamma(x-\alpha)\Gamma(x-\beta) =$$

$$= d\sum_{x\in\Gamma}(\Gamma * g_i)^2(x).$$

Разберемся с величиной $(\Gamma * g_i)(x), x \in \Gamma$. Она равна

$$|\{x_1,x_2,x_3,x_4,x_5 \in \Gamma : x = x_1+x_2-x_3-x_4+x_5, x_1+x_2-x_3-x_4 \in S_i\}|.$$

Далее, величина $(\Gamma * g_i)(x)$ постоянна на $\Gamma$. Сумма $\sum_{x\in\Gamma}(\Gamma * g_i)(x)$, как можно заметить, равна $T_3^{(i)}(\Gamma)$. Поэтому $(\Gamma * g_i)^2(x) = (\frac{T_3^{(i)}(\Gamma)}{t})^2$.

Тем самым вклад маленьких слагаемых не превосходит $d\frac{(T_3^{(i)})^2}{t}$. Поэтому можно просуммировать по таким $(\alpha,\beta)$, что $g(\beta-\alpha) \geqslant \frac{T_3^{(i)}}{2t^2}$, но при этом неравенство примет следующий вид:

$$(\frac{T_3^{(i)}(\Gamma)}{t})^3 \ll \sum_{\alpha,\beta: g(\beta-\alpha)\geqslant\frac{T_3^{(i)}(\Gamma)}{2t^2}} g_i(\alpha)g_i(\beta)g_(\beta-\alpha)C_3(\alpha,\beta).$$

Обозначим последнюю сумму через $\sigma$ и оценим ее по неравенству Коши:

$$\sigma^2 \ll \sum_{\alpha,\beta: g_2(\beta-\alpha)\geqslant\frac{T_3^{(i)}(\Gamma)}{2t^2}} g_i^2(\alpha)g_i^2(\beta)g^2(\beta-\alpha)\sum_{\alpha,\beta} C_3^2(\alpha,\beta).$$

Несложно заметить, что

$$\sum_{\alpha,\beta} C_3^2(\alpha,\beta) = |\{(x_1,\dots,x_6) : x_1-x_2 = x_3-x_4 = x_5-x_6; x_i \in \Gamma\}|.$$

Известна оценка на нее, [33]

$$\sum_{\alpha,\beta} C_3^2(\alpha,\beta) \ll t^3\log t.$$

Оценим теперь первую сумму. Мы разбиваем сумму на такие части. Если $\alpha \in S_i, \beta \in S_i, \beta - \alpha \in S_k$, (здесь $i$ фиксированно, а $k$ меняется). Возможен также случай, когда $\beta - \alpha = 0$ - его мы также рассмотрим. В случае $\beta - \alpha \in S_k$ мы получаем:

$$\sum_{\alpha,\beta} g_i^2(\alpha) g_i^2(\beta) g^2(\beta-\alpha) \ll \sum_k \frac{t^6 T_3^2(\Gamma)}{2^{4i+2k}} \sum_{\alpha \in S_i} |\{\beta \in S_i : \beta - \alpha \in S_k\}| =$$

$$= \sum_k \frac{t^6 T_3^2(\Gamma)}{2^{4i+2k}} \sum_{z \in S_k} (S_i \circ S_i)(z).$$

Для оценки $\sum_{z \in S_k} (S_i \circ S_i)(z)$ разобьем $S_k$ на смежные классы, из которых он состоит. Если $|S_i| < t^2/4$, то далее для каждого смежного класса, входящего в $S_k$ применим теорему 1.5. Мы указывали на то, что можно считать $t_j \leqslant C T_3^{1/3}(\Gamma) j^{-1/3}$. Поэтому $S_k$ состоит из не более $8^k$ смежных классов. Исходя из сказанного, в случае $|S_i| < t^2/4$ получаем:

$$\sum_{z \in S_k} (S_i \circ S_i)(z) \ll 8^k t^{1/3} S_i^{4/3} \ll 8^k 2^{4i} t^{5/3}.$$

Если же $|S_i| > t^2/4$ то отсюда получаем, что $8^i t \gg t^2$ или $t^{1/3} \ll 2^i$. Поэтому в случае $|S_i| > t^2/4$ оцениваем так $\sum_{z \in S_k} (S_i \circ S_i)(z) \ll 8^k t |S_i| \ll 8^k t^{5/3+1/3} 2^{3i} \ll 8^k t^{5/3} 2^{4i}$. Получилась такая же оценка.

Итак, в случае $\beta - \alpha \in S_k$ мы получаем

$$\sum_{\alpha,\beta} g_i^2(\alpha) g_i^2(\beta) g^2(\beta-\alpha) \ll t^{7\frac{2}{3}} T_3^2(\Gamma) 2^k.$$

Теперь рассмотрим случай, когда $\beta = \alpha$. Мы получаем

$$\sum_{\alpha=\beta} g_i^2(\alpha) g_i^2(\beta) g^2(\beta-\alpha) = \sum_\alpha g_i^4(\alpha) g^2(0).$$

Величина $g(0)$ это в точности есть аддитивная энергия группы $\Gamma$ -

$$T_2(\Gamma) = |\{g_1 + g_2 = g_3 + g_4, g_i \in \Gamma\}|.$$

Известна оценка на нее - см. например [2] : $T_2(\Gamma) \ll t^{5/2}$, при $t < p^{2/3}$.

Несложно показать, что:

$$|S_i| \ll t 2^{3i},$$

поэтому,

$$\sum_{\alpha} g_i^4(\alpha) g^2(0) \ll \frac{t^{10} T_3^{4/3}(\Gamma)}{2^i}.$$

Мы можем считать, что:

$$\frac{t^{10} T_3^{4/3}}{2^i} \ll t^{7\frac{2}{3}} T_3^2(\Gamma).$$

В противном случае, получаем,

$$T_3(\Gamma) \ll t^{3.5}.$$

Итак, случай $\alpha = \beta$ мы рассмотрели.

Итого мы выводим,

$$\sum_{\alpha,\beta} g_i^2(\alpha) g_i^2(\beta) g^2(\beta - \alpha) \ll \sum_k t^{7\frac{2}{3}} T_3^2(\Gamma) 2^k.$$

Мы помним,что достаточно суммировать только по тем $\alpha, \beta$, для которых $g(\beta - \alpha) > \frac{T_3^{(i)}(\Gamma)}{2t^2}$. В нашем случае $\beta - \alpha \in S_k$, то есть $tT_3^{1/3}(\Gamma)/2^k > \frac{T_3^{(i)}(\Gamma)}{2t^2}$. Вспоминая оценку $T_3(\Gamma) \ll T_3^{(i)}(\Gamma) \log t$, получаем, что $2^k \ll \frac{t^3 (\log t)^{1/3}}{T_3^{(i)}(\Gamma)^{2/3}}$.

Итак, собирая все вместе мы выводим, что:

$$(\frac{T_3^{(i)}(\Gamma)}{t})^6 \ll t^{13\frac{2}{3}} (\log t)^{4/3} \frac{T_3^2(\Gamma)}{(T_3^{(i)}(\Gamma))^{2/3}}.$$

Опять пользуемся, что $T_3(\Gamma) \ll T_3^{(i)}(\Gamma) \log t$, получаем,

$$(T_3^{(i)}(\Gamma))^{4\frac{2}{3}} \ll t^{19\frac{2}{3}} (\log t)^{3\frac{1}{3}}.$$

Отсюда получаем оценку:

$$T_3^{(i)}(\Gamma) \ll t^{4\frac{3}{14}} (\log t)^{5/7}.$$

Значит имеется оценка $T_3(\Gamma) \ll t^{4\frac{3}{14}} (\log t)^{12/7}$. Тем самым оценку на $T_3(\Gamma)$ мы показали.

## 1.4 Наибольшее расстояние между соседними элементами смежных классов по подгруппе

Для мультипликативной группы $\Gamma \subseteq \mathbb{Z}_p^*$ порядка $t$ введем как в [15] величину

$$H_p(t) = max\{H : \exists a \in \mathbb{Z}_p^*, \exists u \in \mathbb{Z}_p : u + j \in \mathbb{Z}_p \setminus a\Gamma\}$$

Следующий результат был получен в работе [15] (теорема 3)

**Теорема 1.6.** *Для $t \geqslant p^{1/2}$ имеет место оценка:*

$$H_p(t) \leqslant p^{463/504+o(1)}, p \to \infty.$$

Новые оценки для $T_k(\Gamma)$ и для тригонометрических сумм по подгруппам позволяют усилить этот результат. А именно имеет место такая

**Теорема 1.7.** *Для $t \geqslant p^{1/2}$ имеет место оценка:*

$$H_p(t) \leqslant p^{\frac{5977}{6552}+o(1)}, p \to \infty.$$

Заметим, $\frac{463}{504} = 0.91865...; \frac{5977}{6552} = 0.91224...$

Сначала введем необходимые определения. Пусть $g$- первообразный корень $\mathbb{Z}_p$, как и ранее $\Gamma$ - подгруппа порядка $t$, $n = (p-1)/t$. Полагаем

$$\Gamma_j := g^j\Gamma; S_j(t) := S(g^j, \Gamma); N_{j,t}(h) := |\{1 \leqslant |u| \leqslant h : u \in \Gamma_j\}|$$

Здесь первая и вторая величина это смежный класс и тригонометрическая сумма по нему.

Связь между $H_p(t), N_{j,t}(h), S_j(t)$ дается следующим утверждением (лемма 7.1) [26] , которое мы приводим ниже:

**Теорема 1.8.** *Если для некоторого $h \geqslant 1$ неравенство:*

$$\sum_{1 \leqslant j \leqslant n} N_{j,t}(h)|S_{j+k}(t)| \leqslant 0.5t$$

*выполняется для всех $k = 1, \ldots, n$, то для любого $\varepsilon > 0$*

$$H_p(t) \ll p^{1+\varepsilon}h^{-1}.$$

Несложно заметить, что величина $\sum_{1 \leqslant j \leqslant n} N_{j,t}^2(h)$ это число решений сравнений

$$\{ux \equiv y \pmod p, 0 < |x|, |y| \leqslant h, u \in \Gamma\}.$$

Обозначим это число через $N(\Gamma, h)$.

Оценка этой величины нам понадобится для доказательства теоремы 1.7. Приведем ниже теорему 1 работы [15] для оценки $N(\Gamma, h)$.

**Теорема 1.9.** *Пусть $\nu \geqslant 1$ - фиксированное целое, $|\Gamma| \gg p^{1/2}, p \to \infty$. Тогда справедлива оценка:*

$$N(\Gamma, h) \leqslant ht^{\frac{2\nu+1}{2\nu(\nu+1)}+o(1)} + h^2 t^{1/\nu} p^{-1/\nu+o(1)}.$$

Теперь мы готовы вывести теорему 1.7. Как и ранее $t := |\Gamma|$. Для случая $t > 0.7p^{2/3}$ в работе [15] показано, что $H_p(t) \leqslant p^{5/6+o(1)}$.

Остаются случаи, когда $p^{1/2} \leqslant t \leqslant 0.7p^{2/3}$. Вновь рассмотрим случай, когда $p^{\frac{49}{78}} \leqslant t \leqslant 0.7p^{2/3}$. Будем пользоваться теоремой 1.8. Применим оценку на тригонометрическую сумму по подгруппе $\Gamma$ из теоремы 1.1 и оценим так:

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h)|S_{j+k}(t)| \leqslant max_j|S_j(t)| \sum_{1\leqslant j\leqslant n} N_{j,t}(h) \leqslant p^{1/6+o(1)}t^{1/2}h.$$

Поэтому $h$ можно взять $[p^{\frac{23}{156}-\varepsilon}]$ для некоторого малого $\varepsilon > 0$. В этом случае по теореме 1.8:

$$H_p(t) \leqslant p^{\frac{133}{156}+3\varepsilon}.$$

Поэтому при $p^{\frac{49}{78}} \leqslant t \leqslant 0.7p^{2/3}$ теорема 1.7 верна.

Теперь рассмотрим последний случай $p^{\frac{1}{2}} \leqslant t \leqslant p^{\frac{49}{78}}$. Вновь пользуемся теоремой 1.8 и неравенством Гельдера:

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h)|S_{j+k}(t)| \leqslant (\sum_{1\leqslant j\leqslant n} N_{j,t}(h))^{1/2}(\sum_{1\leqslant j\leqslant n} N_{j,t}(h)^2)^{1/4}(\sum_{1\leqslant j\leqslant n} |S_j(t)|^4)^{1/4}.$$

Берем достаточно малое $\varepsilon > 0$ и полагаем $h := [p^{\frac{575}{6552}-\varepsilon}]$.

Мы имеем:

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h) = 2h,$$

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h)^2 = N(\Gamma, h).$$

Для оценки второй суммы воспользуемся теоремой 1.9 с $\nu = 6$. Несложно убедиться, что при выбранном $h$ и $p^{1/2} \leqslant t \leqslant p^{\frac{49}{78}}$ первое слагаемое в неравенстве теоремы 1.9 доминирует. Итак получаем:

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h)^2 = N(\Gamma, h) \leqslant ht^{\frac{13}{84}}p^{\frac{-1}{14}+o(1)},$$

$$\sum_{1\leqslant j\leqslant n} |S_j(t)|^4 < \frac{p}{t}T_2(\Gamma) < pt^{19/13+o(1)}.$$

В последнем неравенстве мы применили оценку на $T_2(\Gamma)$ из теоремы 1.1.

Собирая все вместе получим:

$$\sum_{1\leqslant j\leqslant n} N_{j,t}(h)|S_{j+k}(t)| \leqslant h^{1/2}(ht^{\frac{13}{84}}p^{\frac{-1}{14}+o(1)})^{1/4}(pt^{19/13+o(1)})^{1/4}.$$

Собирая все вместе, несложно убедиться, что при $t \geqslant p^{1/2}$ и для выбранного $h$ правая часть меньше $0.5t$. Этим завершается доказательство теоремы 1.7.

## 1.5 Оценки тригонометрических сумм по модулю $p^3$

Обозначим через $G_r$ - подгруппу $\mathbb{Z}_{p^r}^*$ порядка $p-1$. Наша задача состоит в оценке величины:

$$S(G_3) := max_{a\in\mathbb{Z}_{p^3}^*}|S(a,G_3)|$$

Эту оценку мы применим в 4 главе в задаче делимости частных Ферма на квадрат простого числа.

Метод, описанный в работе [4] позволяет получать нетривиальные оценки для $S(G_r)$. В частности было отмечено, что $T_k(G_{r+1}) \leqslant T_k(G_r)$ выполняется для всех $k$. С помощью леммы 1.1 можно получать оценки для $S(G_r)$, используя оценки величин $T_k(G_{r-1})$. Используя современные оценки на $S(G_2)$ и $T_2(G_2)$ мы получим более точную оценку на $S(G_3)$. Мы покажем такую оценку.

**Теорема 1.10.** *Имеет место оценка*

$$S(G_3) < p^{\frac{673}{702}+o(1)}.$$

Для доказательства нам будут нужны результаты И.Д.Шкредова из работ [33], [32] соответственно:

**Теорема 1.11.** *Имеет место оценка*

$$S(G_2) \ll p^{\frac{5}{6}}(\log p)^{\frac{1}{6}}, T_2(G_2) < p^{\frac{32}{13}+o(1)}.$$

Теперь дадим доказательство теоремы 1.10.

Получим сначала такую оценку: $T_3(G_2) < p^{4\frac{5}{39}+o(1)}$. Мы имеем:

$$p^2T_3(G_2) = \sum_{a\in\mathbb{Z}_{p^2}^*}|S(a,G_2)|^6 + \sum_{a\in\mathbb{Z}_{p^2}\setminus 0, p|a}|S(a,G_2)|^6 + (p-1)^6.$$

Разберемся со вторым слагаемым. Лемма 11 работы [16] утверждает, что все элементы группы $G_2$ принадлежат различным классам вычетов по модулю $p$, за исключением нулевого. Поэтому для $a = lp, (l,p) = 1$ мы имеем:

$$S(a, G_2) = \sum_{g \in G_2} e_{p^2}(ag) = \sum_{1 \leqslant n \leqslant p-1} e_p(ln) = -1.$$

Поэтому,

$$\sum_{a \in \mathbb{Z}_{p^2} \setminus 0, p|a} |S(a, G_2)|^6 = p - 1.$$

Теперь разберемся с первым слагаемым.

$$\sum_{a \in \mathbb{Z}_{p^2}^*} |S(a, G_2)|^6 \leqslant (\sum_{a \in \mathbb{Z}_{p^2}} |S(a, G_2)|^4) max |S(a, G_2)|^2$$

Известно [26], что $\sum_{a \in \mathbb{Z}_{p^2}} |S(a, G_2)|^4 = p^2 T_2(G_2)$. Поэтому применяя оценки на $T_2$ и $S(G_2)$ теоремы 1.11, мы получим

$$\sum_{a \in \mathbb{Z}_{p^2}^*} |S(a, G_2)|^6 \leqslant p^{6\frac{5}{39}+o(1)}.$$

Итак, мы получили: $T_3(G_2) < p^{4\frac{5}{39}+o(1)}$. Значит, $T_3(G_3) \leqslant T_3(G_2) < p^{4\frac{5}{39}+o(1)}$.

Теперь, применяя неравенство леммы 1.1 при $k = l = 3$, мы получим:

$$S(G_3) < p^{\frac{673}{702}+o(1)}.$$

тем самым оценку на $S(G_3)$ мы вывели.

## 1.6 О произведении интервалов и множеств с малым мультипликативным удвоением.

### 1.6.1 Формулировка результата

Целью этого раздела является получение точной верхней оценки для числа решений следующего сравнения

$$\{ux \equiv y \pmod m, 0 < |x|, |y| \leqslant Z; u \in G\},$$

где $G$ - произвольное множество с малым мультипликативным удвоением, $|G|, Z$ связаны некоторыми ограничениями, а $m$ – некоторое число.

Подобная величина уже встречалась в задаче об оценке $H_p(t)$ - там сравнение было по простому модулю. Рассматриваемая величина и ее приложения изучались в работах [15] и [20]. Рассматривались соответственно случаи, когда $G$ подгруппа и множество с малым мультипликативным удвоением. Приведем соответствующую теорему 1, часть (i) из работы [20].

**Теорема 1.12.** *Пусть $U \subseteq \mathbb{Z}_p^*$ и $n, H$ - натуральные числа, что*

$$|U| < p^{n/(2n+1)}; |U * U| < 10|U|; |U|H^n < p.$$

*Тогда число решений $J$ сравнения*

$$ux \equiv y \pmod p; 1 \leqslant x, y \leqslant H; u \in U$$

*удовлетворяет неравенству $J \leqslant Hp^{o(1)}$.*

Как замечено в работе [20], условие $|U * U| < 10|U|$ можно ослабить до $|U * U| < |U|^{1+o(1)}$. Следуя работе [20] мы можем показать справедливость следующей теоремы.

**Теорема 1.13.** *Пусть $U \subseteq \mathbb{Z}_m^*$ и $n, H$ - натуральные числа, что*

$$|U| < m^{n/(2n+1)}; |U * U| < |U|^{1+o(1)}; |U|H^n < m.$$

*Тогда число решений $J$ сравнения*

$$ux \equiv y \pmod m; 1 \leqslant x, y \leqslant H; u \in U$$

*удовлетворяет неравенству $J \leqslant Hm^{o(1)}$.*

### 1.6.2 Вспомогательные утверждения

Нам понадобится лемма доказанная в [15].

**Лемма 1.4.** *Пусть*

$$A = \{\frac{r}{s} : 1 \leqslant r, s \leqslant Q; gcd(r, s) = 1\}$$

*и $k$ - натуральное число. Тогда для достаточно большого $Q$ верно*

$$|A^{(k)}| > exp(-C(k)\frac{\log Q}{(\log\log Q)^{1/2}})|A|^k,$$

*где $C(k)$ - некоторая функция зависящая только от $k$.*

Здесь $A^{(k)} := \{a_1 * \ldots * a_k : a_i \in A\}$.

Для следующей леммы потребуется некоторые определения. Пусть дана решетка $\Gamma$ в $\mathbb{R}^n$ и выпуклое, компактное, симметричное относительно нуля тело $D \subset \mathbb{R}^n$. Последовательные минимумы $\lambda_i(D, \Gamma)$ определяются как наименьшее число $\lambda$, такое что $\lambda D$ содержит $i$ линейно независимых векторов решетки $\Gamma$. Известно [19], что верно такое утверждение.

**Лемма 1.5.** *Справедливо неравенство*

$$\sqcap_{1 \leqslant i \leqslant n} min\{\lambda_i(D, \Gamma), 1\} \leqslant \frac{(2n+1)!!}{|D \cap \Gamma|}.$$

Для доказательства также будет нужна следующая лемма.

**Лемма 1.6.** *Для произвольного $s_0 \in \mathbb{Z}_m$ количество решений $J$ сравнения*

$$s_0 x \equiv y \pmod{m}; 1 \leqslant x \leqslant X; 1 \leqslant y \leqslant Y; gcd(x, y) = 1$$

*оценивается величиной $O(1 + \frac{XY}{m})$.*

Лемма 1.6 доказывается абсолютно аналогично лемме 2 работы [20]. Для полноты картины мы приведем полное доказательство леммы 1.6.

**Доказательство.** Определим решетку $\Gamma$ и тело $D$

$$\Gamma = \{(u, v) \in \mathbb{Z}^2; u \equiv s_0 v \pmod{m}\}$$

$$D = \{(u, v) \in \mathbb{R}^2; |u| \leqslant X, |v| \leqslant Y\}.$$

Пусть числа $\lambda_1, \lambda_2$ являются последовательными минимумами тела $D$ решетки $\Gamma$. Если $\lambda_2 > 1$ то $J \leqslant 1$. В этом случае все доказано.

Пусть теперь $\lambda_2 \leqslant 1$. Тогда по лемме 1.5 мы имеем

$$\lambda_1 \lambda_2 \leqslant \frac{15}{|\Gamma \cap D|} \leqslant \frac{15}{J}.$$

Пусть $r_i = (u_i, v_i) \in \lambda_i D \cap \Gamma, i = 1, 2$ являются линейно независимыми векторами. Понятно, что площадь $S$ параллелограмма, натянутого на эти векторы отлична от нуля. Покажем также, что $S$ делится на $m$. Площадь параллелограмма натянутого на линейно независимые векторы решетки делится на определитель этой решетки. А определитель решетки есть число смежных классов группы $\mathbb{Z}^2$ по подгруппе, которая задается решеткой $\Gamma$. Несложно заметить, что каждый смежный класс есть совокупность $(u, v) \in \mathbb{Z}^2$ для которых фиксированно значение $u - s_o v \pmod{m}$. Таким образом этих смежных классов ровно $m$.

Итак,

$$m \leqslant |u_1 v_2 - u_2 v_1| \leqslant 2\lambda_1 \lambda_2 XY \leqslant \frac{30XY}{J}.$$

Отсюда следует исходная оценка на величину $J$. Лемма 1.6 доказана.

Для доказательства теоремы 1.13 нам будет удобно еще одно утверждение сформулировать в виде отдельной леммы. Ее вывод приведен в доказательстве теоремы 1 [20].

**Лемма 1.7.** *Пусть $u, h, m, n$ - натуральные числа, что*

$$u < m^{n/(2n+1)}; uh^n < m$$

*Тогда для любого целого $h'$, $2 \leqslant h' \leqslant h$ существует такое натуральное $k$, что*

$$u \leqslant (h')^k \leqslant \frac{m}{u}.$$

Для натуральных $m, n$ через $gcd(m, n)$ обозначим наибольший общий делитель чисел $m, n$.

### 1.6.3 Доказательство теоремы 1.13

Рассмотрим 2 случая.

I)Рассмотрим случай когда $x, y$ взаимно просты с $m$: $gcd(m, xy) = 1$. Пусть $d := gcd(x, y)$. Тогда в этом случае при фиксированном $d$ число решений есть

$$|\{ux \equiv y \pmod m : 1 \leqslant x, y \leqslant H/d; gcd(x, y) = 1\}|.$$

Обозначим эту величину $J_d(H)$. Достаточно доказать, что для любого $\delta > 0$ существует $c(\delta) > 0$, что выполняется $J_d(H) \leqslant c(\delta)\frac{H}{d}m^{\delta}$ для любого $d$. Фиксируем какое-нибудь $\delta > 0$. Так как $J_d(H) \leqslant (\frac{H}{d})^2$, то мы можем считать, что $\frac{H}{d} \geqslant m^{\delta}$. Согласно лемме 1.7 для $h' := H/d$ существует такое натуральное $k \leqslant 1/\delta$, что

$$|U| \leqslant (H/d)^k \leqslant m/|U|.$$

Заметим, что $J_d(H)$ есть число элементов множества

$$J_d := \{\frac{y}{x} : 1 \leqslant x, y \leqslant H/d; gcd(x, y) = 1; gcd(m, xy) = 1; \frac{y}{x} \pmod m \in U\}.$$

Теперь

$$J_d^{(k)} \subseteq \{\frac{u}{v} : 1 \leqslant u, v \leqslant (H/d)^k; gcd(u, v) = 1; \frac{u}{v} \pmod m \in U^{(k)}\}.$$

Так как $|U*U| < |U|^{1+o(1)}$, то пользуясь неравенством Плюннеке [29] (теорема 7.7), получаем $|U^{(k)}| < |U|^{1+o(1)}$. Используя это и лемму 1.6 оценим сверху размер множества $J_d^{(k)}$

$$|J_d^{(k)}| \ll \sum_{r \in U^{(k)}} (1 + \frac{(H/d)^{2k}}{m}) \ll |U|^{1+o(1)}(1 + \frac{(H/d)^{2k}}{m}) \leqslant (H/d)^k m^{o(1)}.$$

С другой стороны по лемме 1.4 $|J_d^{(k)}|m^{o(1)} \geqslant |J_d|^k$, причем множитель $m^{o(1)}$ можно выбрать одинаковым для всех $d$, с $\frac{H}{d} > m^\delta$. Поэтому существует такая $c(\delta) > 0$, что для всех $d$ выполнено $|J_d| = J_d(H) \leqslant c(\delta)(H/d)m^\delta$. Таким образом первый случай мы рассмотрели.

II)Рассмотрим второй случай. Пусть $gcd(x,m) = gcd(y,m) = m'$. Достаточно показать, что для любого $\delta > 0$ существует $c(\delta) > 0$, что для произвольного $m'|m$ число решений

$$ux \equiv y \pmod m; 1 \leqslant x, y \leqslant H; gcd(x,m) = gcd(y,m) = m'; u \in U \quad (1.1)$$

не превосходит $c(\delta)Hm^\delta$. Фиксируем $\delta > 0, m'$.

Обозначим $U' := U \pmod{\frac{m}{m'}}$.

В этом случае число решений (1.1) равно

$$\sigma := \sum_{u' \in U'} N(u')M(u'),$$

где

$$N(u') := |\{u \in U : u \equiv u' \pmod{\frac{m}{m'}}\}|,$$

$$M(u') := |\{(x,y) : gcd(xy, \frac{m}{m'}) = 1; 1 \leqslant x, y \leqslant \frac{H}{m'}; \frac{y}{x} \equiv u' \pmod{\frac{m}{m'}}\}|.$$

Пусть $U' = \bigcup_{j \in \mathbb{N}: 2^{j-1} \leqslant m'} U'_j$, где

$$U'_j = \{u' \in U' : N(u') \in [2^{j-1}; 2^j)\}.$$

Тогда

$$\sigma \leqslant \sum_{1 \leqslant j \leqslant \log_2 m'} 2^j (\sum_{u' \in U'_j} M(u')).$$

Нам достаточно показать существование $c(\delta)$, что для любых таких $m', j$ выполнялось:

$$\sum_{u' \in U'_j} M(u') \leqslant c(\delta)\frac{H}{2^j}m^\delta \quad (1.2)$$

Если обозначить

$$J_{m',j} := \{(x,y) : 1 \leqslant x,y \leqslant \frac{H}{m'}; gcd(xy, \frac{m}{m'}) = 1; \frac{y}{x} \in U'_j \pmod{\frac{m}{m'}}\}$$

то условие (1.2) переписывается так

$$|J_{m',j}| \leqslant c(\delta)\frac{H}{2^j}m^{\delta}.$$

Рассмотрим подмножество множества $J_{m',j}$ состоящее из пар $(x,y)$ с дополнительным условием $d = gcd(x,y)$.

Число таких пар есть размер множества несократимых рациональных дробей

$$J_{m',j,d} :=$$

$$= \{\frac{y}{x} : 1 \leqslant x,y \leqslant \frac{H}{m'd}; gcd(xy, \frac{m}{m'}) = 1; gcd(y,x) = 1; \frac{y}{x} \in U'_j \pmod{\frac{m}{m'}}\}.$$

Достаточно показать, что существует $c(\delta)$, что для любых рассматриваемых $m', j, d$ выполнялось $|J_{m',j,d}| \leqslant c(\delta)\frac{H}{2^j d}m^{\delta}$. Так как $|J_{m',j,d}| \leqslant (\frac{H}{m'd})^2$, то можно считать, что $\frac{H}{m'd} \geqslant m^{\delta}$.

Возьмем произвольное натуральное $k$. Имеем

$$J^{(k)}_{m',j,d} \subseteq$$

$$\subseteq \{\frac{u}{v} : gcd(uv, \frac{m}{m'}) = 1; gcd(u,v) = 1; 1 \leqslant u,v \leqslant (\frac{H}{m'd})^k; \frac{u}{v} \in U'^{(k)}_j \pmod{\frac{m}{m'}}\}$$

Пользуясь леммой 1.5, получаем

$$|J^{(k)}_{m',j,d}| \ll \sum_{r \in U'^{(k)}_j} (1 + \frac{(H/m'd)^{2k}}{\frac{m}{m'}}) \leqslant |U'^{(k)}_j|(1 + \frac{(H/m'd)^{2k}}{\frac{m}{m'}}).$$

Покажем, что

$$|U'^{(k)}_j| \ll \frac{|U|^{1+o(1)}}{2^j}. \tag{1.3}$$

Для каждого $u' \in U'^{(k)}_j$ имеется представление $u' = u'_1 * \ldots * u'_k, u'_i \in U'_j$. Для каждого $u'_i$ имеется не менее $2^{j-1}$ элементов $u \in U$ таких, что $u \equiv u'_i \pmod{\frac{m}{m'}}$. Так как $U$ состоит только из обратимых элементов, то для $u'$ имеется не менее $2^{j-1}$ элементов $u \in U^{(k)}$ таких что $u \equiv u' \pmod{\frac{m}{m'}}$. Ранее было показано, что $|U^{(k)}| \leqslant |U|^{1+o(1)}$. Отсюда получаем неравенство (1.3).

Теперь мы выберем $k$. Согласно лемме 1.7 для $h' := \frac{H}{dm'}$ существует такое натуральное $k \leqslant \frac{1}{\delta}$, что

$$|U| \leqslant (\frac{H}{dm'})^k \leqslant \frac{m}{|U|}$$

Таким образом, мы получаем что для такого $k$

$$|J^{(k)}_{m',j,d}| \ll \frac{|U|^{1+o(1)}}{2^j}(1 + \frac{(H/m'd)^{2k}}{\frac{m}{m'}}) \ll (\frac{H}{d2^{j-1}})^k m^{o(1)}.$$

С другой стороны по лемме 1.4 мы имеем $|J^{(k)}_{m',j,d}| \geqslant |J_{m',j,d}|^k m^{o(1)}$, причем множитель $m^{o(1)}$ может быть выбран одим и тем же для всех параметров $m', j, d$ с условием $\frac{H}{m'd} > m^\delta$. Сопоставляя последние оценки мы получаем что неравенство $|J_{m',j,d}| \leqslant c(\delta)(\frac{H}{d2^j})m^\delta$ выполняется для всех рассматриваемых $m', j, d$. Таким образом второй случай мы полностью рассмотрели. Теорема 1.13 доказана.

### 1.6.4 Комментарии к теореме 1.13

Мы отмечаем, что условие $1 \leqslant x, y \leqslant H$ можно заменить на такое $1 \leqslant |x|, |y| \leqslant H$.

Получим оценку снизу на число решений

$$ux \equiv y \pmod m; 1 \leqslant |x|, |y| \leqslant H; u \in U \tag{1.4}$$

Фиксируем произвольное $u \in U$ и рассмотрим величины $ux - y \pmod m$, когда $1 \leqslant x, y \leqslant H$. Всего таких различных пар $(x, y)$ $H^2$. Будем считать, что $H^2 \geqslant 10m$. Поэтому найдется $s$ пар $(x, y)$ ,$s \geqslant \frac{H^2}{m}$, что выражение $ux - y \pmod m$ принимает одно и тоже значение. Обозначим эти пары $(x_1, y_1), \ldots, (x_s, y_s)$. Несложно заметить, что пары $(v_i, w_i) = (x_i - x_1, y_i - y_1)$ $i = 2, \ldots, s$ удовлетворяют сравнению $uv_i \equiv w_i \pmod m$. Таким образом, у нас имеется не менее $|U|H^2/2m$ решений сравнения (1.4).

Отсюда несложно увидеть, что для множеств $U, |U| \leqslant m^{\frac{1}{3}}$ $(n = 1)$ условие

$$|U|H < m$$

нельзя ослабить до

$$|U|H < m^{1+\delta}$$

ни для какого фиксированного $\delta > 0$ в формулировках теорем 1.12, 1.13.

# Глава 2

# Совместные представители вычетов по двум модулям.

## 2.1 Введение в задачу о совместных представителях вычетов

Пусть $p_1, p_2$ - достаточно большие натуральные числа, не обязательно простые и не обязательно взаимно простые: $p_1 < p_2, A := p_2/p_1$. Пусть также имеются множества

$$G_1 \subseteq \mathbb{Z}_{p_1}, G_2 \subseteq \mathbb{Z}_{p_2}.$$

По определению положим

$$\overline{G_1} := \{n \in \mathbb{N} : n \in G_1 \pmod{p_1}\}; \overline{G_2} := \{n \in \mathbb{N} : n \in G_2 \pmod{p_2}\}.$$

Пусть также дано натуральное $z$, и мы хотим нетривиально оценить сверху

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|.$$

Оценка этой величины, когда $p_1 = q_1^2, p_2 = q_2^2$ и $q_1, q_2$ являются простыми числами, а $G_1, G_2$ являются мультипликативными подгруппами групп $\mathbb{Z}_{q_1}^*$ и $\mathbb{Z}_{q_2}^*$ размеров $q_1 - 1$ и $q_2 - 1$ соответственно, рассматривался в работе [16]. Оценка размера $[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}$ была нужна для задачи об оценке первого натурального $a$, не обладающего свойством делимости частного Ферма на простое число. Отметим, если $p_1$ и $p_2$ являются взаимно простыми, то с помощью китайской теоремы об остатках получаем:

$$|[1, p_1 p_2] \bigcap \overline{G_1} \bigcap \overline{G_2}| = |G_1||G_2|.$$

Нам понадобятся такие величины. Для целого $k$ обозначим через $f_1(k)$ - число решений сравнения относительно $x_1, x_2 \in G_1$

$$x_1 - x_2 \equiv k p_2 \pmod{p_1}.$$

Введем по определению

$$N_1 := \sum_{0 \leqslant k \leqslant \frac{z}{A}} f_1(k).$$

Аналогично, через $f_2(k)$ обозначим число решений сравнения относительно $x_1, x_2 \in G_2$

$$x_1 - x_2 \equiv kp_1 \pmod{p_2}.$$

И

$$N_2 := \sum_{0 \leqslant k \leqslant z} f_2(k).$$

Наша цель - оценить размер $|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|$ через $N_1$ и $N_2$.

В работе [16], когда множества $G_1, G_2$ являлись подгруппами, величины $N_1, N_2$ были явно оценены. Нам понадобится такое утверждение.

**Лемма 2.1.** *Существует такая константа $C > 0$, что для любого $n$ имеет место неравенство:*

$$\sum_{0 \leqslant k \leqslant 2n} f_1(k) \leqslant C \sum_{0 \leqslant k \leqslant n} f_1(k) \tag{2.1}$$

**Доказательство.** Для удобства обозначим $q_1 := \frac{p_1}{\gcd(p_1,p_2)}, q_2 := \frac{p_2}{\gcd(p_1,p_2)}$. Функция $f_1$ является четной и неотрицательной. Легко видеть, что для любого $k$ верно $f_1(k + q_1) = f_1(k)$. Поэтому можно считать, что она задана на кольце вычетов по модулю $q_1$. Покажем теперь, что $f_1$ является положительно определенной функцией. Иными словами убедимся, что ее дискретное преобразование Фурье неотрицательно. Отметим сразу, что для неотрицательных, положительно определенных функций справедливость неравенства (2.1) следует из работы [1].

Остается убедиться в неотрицательности преобразования Фурье. Пусть $e_q(k) := exp(2\pi ik/q)$. Известно, что для любого целого $x$: $\sum_{0 \leqslant a \leqslant q-1} e_q(ax) = q$, только если $x \equiv 0 \pmod{p}$, а в остальных случаях $\sum_{0 \leqslant x \leqslant q-1} e_q(ax) = 0$. Поэтому мы можем написать,

$$f_1(k) = \frac{1}{p_1} \sum_{x_1, x_2 \in G_1} \sum_{0 \leqslant a \leqslant p_1 - 1} e_{p_1}(a(x_1 - x_2 - kp_2)) =$$

$$= \frac{1}{p_1} \sum_{0 \leqslant a \leqslant p_1 - 1} e_{p_1}(-akp_2) \sum_{x_1 \in G_1} e_{p_1}(ax_1) \sum_{x_2 \in G_1} e_{p_1}(-ax_2).$$

Обозначим $S(a, G_1) := \sum_{x \in G_1} e_{p_1}(ax)$. Тогда

$$f_1(k) = \frac{1}{p_1} \sum_{0 \leqslant a \leqslant p_1 - 1} |S(a, G_1)|^2 e_{p_1}(-akp_2) =$$

$$= \frac{1}{p_1} \sum_{0 \leqslant a \leqslant p_1 - 1} |S(a, G_1)|^2 e_{q_1}(-akq_2) = \frac{1}{p_1} \sum_{0 \leqslant a \leqslant q_1 - 1} L(a) e_{q_1}(-akq_2),$$

где

$$L(a) := \sum_{0 \leqslant t \leqslant p_1 - 1, t \equiv a \pmod{q_1}} |S(t, G_1)|^2 \geqslant 0.$$

Через $q_2^*$ обозначим обратный элемент к элементу $q_2 \pmod{q_1}$ в кольце вычетов по модулю $q_1$. Таким образом, мы получили

$$f_1(k) = \frac{1}{p_1} \sum_{0 \leqslant a \leqslant q_1 - 1} L(-aq_2^*) e_{q_1}(ak).$$

Отсюда следует, что преобразование Фурье для $f_1$ неотрицательно. Тем самым мы показали справедливость неравенства (2.1). Тем самым мы показали справедливость предложения 2.1.

Введем еще некоторые определения и обозначения.

Пусть $\Lambda_1$ и $\Lambda_2$ есть непустые конечные множества. Для множества $L \subseteq \Lambda_1 \times \Lambda_2$ пусть

$$L(x, .) := \{y \in \Lambda_2 : (x, y) \in L\}; L(., y) := \{x \in \Lambda_1 : (x, y) \in L\}.$$

Всюду в работе выражение $a(n) \ll b(n)$ будет означать, что для всех $n$ выполнено неравенство $|a(n)| \leqslant cb(n)$ для некоторой абсолютной константы $c > 0$.

Теперь приведем одно утверждение из работы [16] и далее покажем, какие оценки на величину $|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|$ можно получить с ее помощью и величин $N_1$ и $N_2$.

**Лемма 2.2.** *[16] Для любого множества $L \subseteq \Lambda_1 \times \Lambda_2$ существуют подмножество $B \subseteq L$ и натуральные $k_1$ и $k_2$, что справедливы неравенства:*

*1)* $|B| \geqslant |L|/2$;

*2)* $|B(x, .)| \leqslant k_1$ *для любого* $x \in \Lambda_1$;

*3)* $|B(., y)| \leqslant k_2$ *для любого* $y \in \Lambda_2$;

*4)* $\sum_{x \in \Lambda_1 : |B(x,.)| > \frac{k_1}{2}} |B(x, .)| \gg \frac{L}{\log(|\Lambda_1| + |\Lambda_2|)}$;

*5)* $\sum_{y \in \Lambda_2 : |B(.,y)| > \frac{k_2}{2}} |B(., y)| \gg \frac{L}{\log(|\Lambda_1| + |\Lambda_2|)}$.

Из этой леммы следует такое утверждение.

**Лемма 2.3.** *Предположим даны достаточно большие $p_1, p_2, z$ причем* $\gcd(p_1, p_2) = 1$ $A := \frac{p_2}{p_1} > 1$,$z < p_2$. *Пусть имеются множества* $G_1 \subseteq \mathbb{Z}_{p_1}, G_2 \subseteq \mathbb{Z}_{p_2}$ *и соответственно заданы величины* $N_1, N_2$. *Тогда справедлива оценка:*

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll \max\{N_1, N_2\} \log p_1.$$

**Доказательство.** Пусть $\Lambda_1 := \mathbb{Z}_{p_1}, \Lambda_2 := \mathbb{Z}_{p_2}$. Каждому элементу

$$m \in [1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}$$

биективно сопоставим пару в $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ по правилу $(m \pmod{p_1}, m \pmod{p_2})$ Обозначим множество таких пар через $L$.

Используя лемму 2.2 для множества $L$, мы получаем существование такого множества

$$B \subseteq [1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2},$$

натуральных $k_1, k_2$ и абсолютной константы $c > 0$, что справедливы следующие утверждения:

1) для каждого вычета по модулю $p_1$ имеется не более $k_1$ чисел из $B$, представляющих этот вычет.

2) для каждого вычета по модулю $p_2$ имеется не более $k_2$ чисел из $B$, представляющих этот вычет.

3) имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|}{k_1 \log p_1}$ вычетов по модулю $p_1$, каждый из которых содержит не менее $k_1/2$ чисел из $B$, представляющих этот вычет.

4) имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|}{k_2 \log p_1}$ вычетов по модулю $p_2$, каждый из которых содержит не менее $k_2/2$ чисел из $B$, представляющих этот вычет.

Будем считать, что $k_2$ не меньше $k_1$. Если какой-то класс вычетов по модулю $p_2$ содержит не менее $k_2/2$ чисел из $B$, то у нас имеется не менее $k_2^2/8$ пар $(a, b) \in B \times B$ таких, что

$$a \geqslant b; a \equiv b \pmod{p_2}$$

Теперь суммируя по всем таким вычетам по модулю $p_2$, можно получить не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|k_2}{8 \log p_1}$ пар $(a, b) \in B \times B$, что

$$a - b = l p_2, 0 \leqslant l \leqslant \frac{z}{A}$$

Так как среди элементов $B$ имеется не более $k_1$ чисел, представляющих любой фиксированный вычет по модулю $p_1$, то мы заключаем, что имеется не менее $\frac{c|[1,p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}|k_2}{8 k_1 \log p_1}$ решений сравнения

$$x_1 - x_2 \equiv l p_2 \pmod{p_1}, 0 \leqslant l \leqslant \frac{z}{A}.$$

Но число решений последнего сравнения есть величина $N_1$. Получаем,

$$\frac{|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|k_2}{k_1\log p_1}\ll N_1.$$

Значит, в случае $k_2\geqslant k_1$ следует неравенство

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll N_1\log p_1.$$

Так как мы не знаем, какое из чисел $k_1,k_2$ является наибольшим, то получаем заявленную оценку

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll \max\{N_1,N_2\}\log p_1.$$

Тем самым лемма 2.3 доказана.

## 2.2 Основное утверждение

Теперь мы готовы сформулировать и доказать главную теорему этой главы в этом пункте. Она является более сильным результатом по сравнению с леммой 2.3.

**Теорема 2.1.** *Предположим даны числа $p_1,p_2,A,z$, $p_1<p_2$, множества $G_1,G_2$ и соответственно заданы величины $N_1,N_2$. Тогда справедлива оценка:*

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\ll (N_1N_2)^{1/2}.$$

**Доказательство.** Так как числа $1,\dots,p_1$ пробегают полную систему вычетов по модулю $p_1$, то множеству $G_1$ можно естественным образом взаимно однозначно сопоставить множество чисел $\overline{G_1}\bigcap[1,p_1]$. Теперь каждый элемент $g\in\overline{G_1}\bigcap[1,p_1]$ отобразим в $\mathbb{Z}_{p_2}$ по правилу

$$g\to g\pmod{p_2}.$$

Обозначим образ этого отображения через $G_1',G_1'\subseteq\mathbb{Z}_{p_2}$. Тем самым у нас имеется взаимно-однозначное соответствие между тремя множествами

$$G_1\to\overline{G_1}\bigcap[1,p_1]\to G_1' \tag{2.2}$$

Таким образом нам необходимо оценить сверху

$$\sum_{0\leqslant k\leqslant z-1}|G_2\bigcap(G_1'+kp_1)|.$$

Прежде всего заметим, что достаточно доказать теорему для $z \leqslant q_2$. Действительно, пусть $z > q_2$.

Обозначим $K := z/q_2 > 1$. Пользуясь тем, что

$$G_1' + q_2 p_1 = G_1'$$

получаем

$$\sum_{0 \leqslant k \leqslant z-1} |G_2 \bigcap G_1' + k p_1| \ll K \sum_{0 \leqslant k \leqslant q_2 - 1} |G_2 \bigcap G_1' + k p_1|.$$

Заметим, что для любого $l$

$$f_1(l + q_1) = f_1(l), f_2(l + q_2) = f_2(l).$$

Поэтому,

$$\sum_{0 \leqslant k \leqslant \frac{z}{A}} f_1(k) = \sum_{0 \leqslant k \leqslant K q_1} f_1(k) \gg K \sum_{0 \leqslant k \leqslant q_1 - 1} f_1(k).$$

Аналогично,

$$\sum_{0 \leqslant k \leqslant z} f_2(k) \gg K \sum_{0 \leqslant k \leqslant q_2 - 1} f_2(k).$$

Поэтому, из этих неравенств убеждаемся, что теорему достаточно доказать для $z \leqslant q_2$. Пусть $z \leqslant q_2$.

Разобьем множество $\mathbb{Z}_{p_2}$ на множества $\{\Delta_i\}, 1 \leqslant i \leqslant \gcd(p_1, p_2)$ следующим образом.

Определим для $1 \leqslant i \leqslant \gcd(p_1, p_2)$ наборы

$$\Delta_i := \{i + l p_1\}_{0 \leqslant l \leqslant q_2 - 1}.$$

Они не пересекаются и покрывают все $\mathbb{Z}_{p_2}$.

Теперь каждый $\Delta_i$ еще разобьем на непересекающиеся множества $\Delta_{i,j}$. Для $1 \leqslant j \leqslant J := [\frac{q_2}{z}]$ по определению полагаем

$$\Delta_{i,j} := \{i + l p_1\}_{(j-1)z \leqslant l \leqslant jz - 1}.$$

Если $\bigcup_{1 \leqslant j \leqslant J} \Delta_{i,j}$ не покрывает весь $\Delta_i$, то положим

$$\Delta_{i,J+1} := \Delta_i \setminus \bigcup_{1 \leqslant j \leqslant J} \Delta_{i,j}.$$

Определим множество

$$S_{i,j} := \Delta_{i,j} \bigcap G_2.$$

Далее введем множество

$$s_{i,j} := \bigcup_{0 \leqslant l \leqslant z-1} \{g \in G_1' : g + lp_1 \in \Delta_{i,j}\}.$$

Тогда

$$|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \leqslant \sum_{i,j} |S_{i,j}||s_{i,j}|.$$

Отметим, что $g + kp_1, 0 \leqslant k \leqslant z-1$ пробегает прогрессию длины $z$ с шагом $p_1$ и поэтому каждый $g \in G_1'$ может принадлежать не более трем множествам $s_{i,j}$. Отсюда следует, что

$$\sum_{i,j} s_{i,j} \ll |G_1|; \sum_{i,j} S_{i,j} = |G_2|.$$

Далее

$$\sum_{i,j} |S_{i,j}||s_{i,j}| \leqslant (\sum_{i,j} |S_{i,j}|^2)^{1/2} (\sum_{i,j} |s_{i,j}|^2)^{1/2}.$$

Сперва оценим первую сумму :

$$\sum_{i,j} |S_{i,j}|^2 = \sum_{i,j} |\{(a,b) \in G_2 \times G_2 : a, b \in \Delta_{i,j}\}| \leqslant$$

$$\leqslant |\{(a,b) \in G_2 \times G_2 : a - b \equiv kp_1 \pmod{p_2}, -z+1 \leqslant k \leqslant z-1\}| \ll N_2.$$

Теперь оценим вторую сумму:

$$\sum_{i,j} |s_{i,j}|^2 = \sum_{i,j} |\{(a,b) \in G_1' \times G_1' : a, b \in s_{i,j}\}|.$$

Так как каждый элемент $g \in G_1'$ может принадлежать не более чем трем множествам $s_{i,j}$, то каждая пара $(a,b) \in G_1' \times G_1'$ которая подсчитывается в последней сумме может быть подсчитана не более трех раз для разных $s_{i,j}$. Значит,

$$\sum_{i,j} |s_{i,j}|^2 \ll |\{(a,b) \in G_1' \times G_1' : \exists (i,j) : a, b \in s_{i,j}\}|.$$

Поймем, что значит условие $a, b \in s_{i,j}$ для некоторых $i, j$. Это означает, что для некоторых $0 \leqslant k, k' \leqslant z-1$ выполнено

$$a + kp_1, b + k'p_1 \in s_{i,j}.$$

Из этого условия следует, что

$$a,b\in G_1'\times G_1' : a-b\equiv kp_1 \pmod{p_2}, -2z+2\leqslant k\leqslant 2z-2.$$

В самом начале мы строили взаимно-однозначное соотвествие (2.2) между $G_1$ и $G_1'$. Для каждого $a\in G_1'$ обозначим через $f(a)$ его прообраз в $G_1$. Можно увидеть, что если

$$a,b\in G_1'\times G_1' : a-b\equiv kp_1 \pmod{p_2}, -2z+2\leqslant k\leqslant 2z-2$$

то

$$f(a),f(b)\in G_1\times G_1 : f(a)-f(b)\equiv kp_2 \pmod{p_1}, -2z/A\leqslant k\leqslant 2z/A.$$

Поэтому мы заключаем, что

$$\sum_{i,j}|s_{i,j}|^2\ll\sum_{0\leqslant k\leqslant\frac{2z}{A}}f_1(k).$$

Пользуясь неравенством (2.1), мы получаем

$$\sum_{0\leqslant k\leqslant\frac{2z}{A}}f_1(k)\ll\sum_{0\leqslant k\leqslant\frac{z}{A}}f_1(k),$$

то есть $\sum_{0\leqslant k\leqslant\frac{2z}{A}}f_1(k)\ll N_1$. Таким образом:

$$|[1,p_1z]\bigcap\overline{G_1}\bigcap\overline{G_2}|\leqslant\sum_{i,j}|S_{i,j}||s_{i,j}|\ll$$

$$\ll(\sum_{i,j}|S_{i,j}|^2)^{1/2}(\sum_{i,j}|s_{i,j}|^2)^{1/2}\ll(N_1N_2)^{1/2}.$$

Этим мы завершаем доказательство теоремы.

## 2.3 Доказательство неулучшаемости теоремы 2.1

Докажем еще одно утверждение, которое показывает некоторую точность оценки в теореме 2.1

**Теорема 2.2.** *Пусть целые числа* $p,m_1,m_2,z,l\to\infty$, *причем*

$$zm_1<p/10, zm_2<pl/10, \sqrt{\frac{\max\{m_1,m_2\}}{\min\{m_1,m_2\}}}=o(z) \qquad (2.3)$$

*Тогда существуют подмножества*

$$G_1 \subseteq \mathbb{Z}_p, G_2 \subseteq \mathbb{Z}_{p+1}$$

*такие, что выполнены следующие условия:*

*1)* $|G_1| \asymp m_1, |G_2| \asymp m_2$,

*2) число решений сравнения относительно* $x_1, x_2, n$

$$x_1 - x_2 \equiv n \pmod{p}, 0 \leqslant n \leqslant z; x_1, x_2 \in G_1$$

*есть* $O(m_1)$.

*3) число решений сравнения относительно* $x_1, x_2, n$

$$x_1 - x_2 \equiv n \pmod{p+1}, 0 \leqslant n \leqslant z; x_1, x_2 \in G_2$$

*есть* $O(lm_2)$.

*4) величина*

$$|[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}|$$

*не может быть оценена величиной* $O(m_1 m_2)^{1/2}$.

**Замечания.**

1)Пусть для примера $p_1$ и $p_2$ взаимно просты и $p_1 \asymp p_2$ и пусть $zm > p_1 l'$, где $l'$ какая-то растущая величина при $p_1 \to \infty$. Тогда можно показать, что для любого подмножества $G_1 \subseteq \mathbb{Z}_{p_1}, |G_1| = m$ число решений сравнения относительно $x_1, x_2, n$

$$x_1 - x_2 \equiv np_2 \pmod{p_1}, 0 \leqslant n \leqslant z; x_1, x_2 \in G_1$$

будет иметь по порядку не меньше $l'm$ решений. Поэтому в условии теоремы 2.2 мы требуем условия $zm_1 < p/10, zm_2 < pl/10$.

2)Пусть $p_1 \asymp p_2$ и

$$z \ll \sqrt{\frac{\max\{m_1, m_2\}}{\min\{m_1, m_2\}}}.$$

Так как для любого целого $k$ справедлива оценка $|[kp_1 + 1, (k+1)p_1] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll \min\{m_1, m_2\}$, то $|[1, p_1 z] \bigcap \overline{G_1} \bigcap \overline{G_2}| \ll z \min\{m_1, m_2\} \ll (m_1 m_2)^{1/2}$. Поэтому условие

$$\sqrt{\frac{\max\{m_1, m_2\}}{\min\{m_1, m_2\}}} = o(z)$$

также является необходимым.

**Доказательство теоремы 2.2** Мы можем считать, что $l$ по порядку меньше чем $m_1, m_2$ а также считать справедливость соотношения

$$l\sqrt{\frac{\max\{m_1,m_2\}}{\min\{m_1,m_2\}}} = o(z).$$

Для удобства обозначим $m := \min\{m_1, m_2\}$.

Каждое из $\mathbb{Z}_p$ и $\mathbb{Z}_{p+1}$ разобьем на подмножества и на них определим $G_1$ и $G_2$.

Пусть для $1 \leqslant i \leqslant [p/z]$

$$\delta_i := \{(i-1)z+1 \pmod p, \dots, iz \pmod p\} \bigcap \mathbb{Z}_p$$

и быть может

$$\delta_{[p/z]+1} := \mathbb{Z}_p \setminus \bigcup_{1\leqslant i\leqslant [p/z]} \delta_i.$$

Тем самым, $\mathbb{Z}_p = \bigcup_i \delta_i$. Из условия следует, что всего множеств $\{\delta_i\}$ не меньше $10m_1$

Так же разобьем $\mathbb{Z}_{p+1}$ на множества $\gamma_i$. Пусть для $1 \leqslant i \leqslant [\frac{p+1}{z}]$

$$\gamma_i := \{(i-1)z+1 \pmod{p+1}, \dots, iz \pmod{p+1}\} \bigcap \mathbb{Z}_{p+1}$$

и быть может

$$\gamma_{[\frac{p+1}{z}]+1} := \mathbb{Z}_{p+1} \setminus \bigcup_{1\leqslant i\leqslant [\frac{p+1}{z}]} \gamma_i.$$

Мы получили $\mathbb{Z}_{p+1} = \bigcup_i \gamma_i$. Из условия (2.3) следует, что всего множеств $\{\gamma_i\}$ не меньше $\frac{10m_2}{l}$.

Определим теперь $G_1, G_2$. Пусть для $1 \leqslant i \leqslant [\frac{m}{l}]$

$$G_1 \bigcap \delta_i := \{(i-1)z+1 \pmod p, \dots, (i-1)z + \left[\sqrt{\frac{m_1 l}{m}}\right] \pmod p\},$$

$$G_2 \bigcap \gamma_i := \{iz - \left[l\sqrt{\frac{m_2}{m}}\right] + 1 \pmod{p+1}, \dots, iz \pmod{p+1}\}.$$

Для $[\frac{m}{l}] + 1 \leqslant i \leqslant [\frac{m}{l}] + m_1$

$$G_1 \bigcap \delta_i := \{(i-1)z+1 \pmod p\}.$$

Для $[\frac{m}{l}]+1 \leqslant i \leqslant [\frac{m}{l}]+[\frac{m_2}{l}]$

$$G_2 \bigcap \gamma_i := \{iz - l + 1 \pmod{p+1}, \ldots, iz \pmod{p+1}\}.$$

Так как $[\frac{m}{l}]+m_1 < 2m_1$, а всего множеств $\{\delta_i\}$ не меньше $10m_1$, поэтому мы можем так определить $G_1$. Аналогично $[\frac{m}{l}]+[\frac{m_2}{l}] \leqslant \frac{2m_2}{l}$ то мы можем так определить и $G_2$.

Убедимся, что $G_1, G_2$ имеют размеры порядка $m_1$ и $m_2$ соответственно. Действительно

$$|G_1| = \sum_{1 \leqslant i \leqslant [\frac{m}{l}]+m_1} |\delta_i \bigcap G_1| = \left[\frac{m}{l}\right] \left[\sqrt{\frac{m_1 l}{m}}\right] + m_1 \asymp m_1.$$

Аналогично проверяется что и $|G_2|$ имеет порядок $m_2$.

Теперь убедимся, что число решений сравнения относительно $x_1, x_2, n$

$$x_1 - x_2 \equiv n \pmod{p+1}, 0 \leqslant n \leqslant z; x_1, x_2 \in G_2$$

есть величина $O(lm_2)$.

Действительно, пусть сравнение выполнено для некоторого $0 \leqslant n \leqslant z$ и элемент $x_2 \in \gamma_i$ для некоторого $i$. Получаем,

$$x_1 \equiv x_2 + n \pmod{p+1}, 0 \leqslant n \leqslant z.$$

Тогда элемент $x_1$ обязан принадлежать либо $\gamma_i$, либо $\gamma_{i+1}$. Если обозначить $v_i := |G_2 \bigcap \gamma_i|$, то число рассматриваемых сравнений оценивается величиной

$$\sum_{1 \leqslant i \leqslant [\frac{m}{l}]+[\frac{m_2}{l}]} v_i(v_i + v_{i+1}) \leqslant 2l^2 \frac{m_2}{m}\frac{m}{l} + 2l^2\frac{m_2}{l} = O(lm_2).$$

Аналогично можно показать, что число решений сравнения относительно $x_1, x_2, n$

$$x_1 - x_2 \equiv n \pmod{p}, 0 \leqslant n \leqslant z; x_1, x_2 \in G_1$$

есть величина $O(m_1)$.

Наконец осталось оценить снизу размер $[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}$. Обозначим также $u_i := |G_1 \bigcap \delta_i|$ По условию (2.3) следует что $u_i, v_i = o(z)$. Поэтому

$$|[1, pz] \bigcap \overline{G_1} \bigcap \overline{G_2}| \geqslant \sum_{1 \leqslant i \leqslant [\frac{m}{l}]-1} v_i u_{i+1} \gg l\sqrt{\frac{m_2}{m}}\sqrt{\frac{m_1 l}{m}}\frac{m}{l}.$$

Последняя величина по-порядку больше чем $(m_1 m_2)^{1/2}$. Этим мы завершаем доказательтсво теоремы 2.2

# Глава 3

# Распределение элементов подмножеств натуральных чисел, замкнутых относительно умножения.

## 3.1 Вспомогательные утверждения

Пусть $q$ – некоторое натуральное число. Также пусть $A \subset \mathbb{N}, A \subseteq [1,q]$ – множество, замкнутое относительно опрерации умножения, то есть если $a_1, a_2 \in A$ и $a_1 a_2 \leqslant q$ то $a_1 a_2 \in A$. Можно считать, что элементы $A$ это те целые числа из отрезка $[1,q]$, которые принадлежат некоторой полугруппе натуральных чисел.

Нас будет интересовать случай, когда для некоторого $0 < \nu < 1$ справедливо неравенство:

$$|A| < q^{\nu}. \tag{3.1}$$

Пусть для $x > 0$ определим :

$$f(x) = |A \cap [1,x]|.$$

Покажем, что верно следующее утверждение.

**Теорема 3.1.** *Пусть $A$ – множество, замкнутое относительно операции умножения и удовлетворяет условию (3.1) и $x = (\log q)^u$.*

*1) если $\log\log x = o(\log\log q)$, то*

$$\frac{f(x)}{x} \leqslant exp\{-(C+o(1))u(1-\nu)^2 \log(u(1-\nu)^2)\}$$

*где $C$ - некоторая абсолютная константа.*

*2) если $\gamma = \frac{\log\log x}{\log\log q}$ и $\log x = o(\log q)$, то*

$$f(x) \leqslant x^{1-max\{L_\gamma, C_\gamma\}+o(1)}, q \to \infty,$$

*где*

$L_\gamma = \gamma(\frac{1-\nu}{1-\gamma+\sqrt{(1-\gamma)^2+\gamma(1-\nu)}})^2$ *и* $C_\gamma = \frac{(1-\nu)^2\gamma}{4(1-\gamma)}$, *если* $\gamma \leqslant \frac{2}{3-\nu}$ *и* $C_\gamma = 2-\nu-\frac{1}{\gamma}$, *если* $\gamma > \frac{2}{3-\nu}$.

Предположим, что задано целое $y$. Каждое натуральное $n$ представим в виде $n = n_1 n_2$, так что если простое $p$ делит $n_1$, то $p \leqslant y$, а если делит $n_2$, то $p > y$. Пусть также даны $x, z$. Определим множество:

$$N(x, y, z) = \{n \leqslant x : n_1 > z\}.$$

Мы хотим оценить сверху количество элементов множества $N(x, y, z)$. На довольно большой области изменения $x, y, z$ была получена ассимптотика $N(x, y, z)$ в работе [34]. Нам нужен будет более грубый результат, но при еще слабых ограничениях на параметры $x, y, z$. Мы будем следовать технике, разработанной в [34].

Нам потребуются оценки для множеств чисел, у которых все простые делители малы либо наоборот, большие. Для натурального $n$ пусть $P^+(n)$ и $P^-(n)$ соответственно наибольший и наименьший простой делитель числа $n$, $P^+(1) = 1, P^-(1) = \infty$. Для $x \geq y \geq 2$ полагаем:

$$\psi(x, y) = |\{n \leq x : P^+(n) \leq y\}|, \phi(x, y) = |\{n \leq x : P^-(n) > y\}|.$$

Также нужны следующие оценки на $\psi(x, y)$ – [25] и также оценки на $\phi(x, y)$ – следствие из теоремы 3, 3 часть, 6 глава [36]. Ниже мы приводим соответствующие утверждения.

**Теорема 3.2.** *[25] Пусть* $x \geqslant y \geqslant 2, v = \frac{\log x}{\log y}$ *Тогда для любого* $\varepsilon > 0$ *на множестве* $v \leqslant y^{1-\varepsilon}$ *имеет место неравенство:*

$$\psi(x, y) = xv^{-v(1+o(1))},$$

*если* $v \to \infty$.

**Теорема 3.3.** *[36] Пусть* $x \geqslant y \geqslant 2$. *Тогда*

$$\phi(x, y) \ll \frac{xw(v)}{\log y},$$

*где* $v = \frac{\log x}{\log y}$, $w()-$ *функция Бухштаба.*

**Лемма 3.1.** *Пусть* $\varepsilon > 0$ *и* $\alpha_0 < \infty$ *фиксированы. Также пусть имеются положительные* $\alpha, \beta, \gamma$, *причем* $0 < \alpha < \alpha_0$, $\beta < 1$, $\gamma < \alpha(1-\varepsilon)$ *и также* $x = (\log q)^u$, $x \leqslant exp\{(\log q)^\gamma\}$, $y = (\log q)^\alpha, z = x^\beta$. *Тогда*

$$|N(x, y, z)| \leqslant xexp\{-\frac{\beta u}{\alpha}(1+o(1))\log(\frac{\beta u}{\alpha})\}, u \to \infty.$$

Доказательство.

$$|N(x,y,z)| = \sum_{z<n_1\leqslant x, P^+(n_1)\leqslant y} \phi(\frac{x}{n_1},y) =$$

$$= \sum_{z<n_1\leqslant \frac{x}{y}, P^+(n_1)\leqslant y} \phi(\frac{x}{n_1},y) + (\psi(x,y) - \psi(\frac{x}{y},y)).$$

Последнее слагаемое несложно оценить:

$$\psi(x,y) - \psi(\frac{x}{y},y) \leqslant \psi(x,y) = xexp\{-\frac{u}{\alpha}(1+o(1))\log\frac{u}{\alpha}\}.$$

Распишем сумму , используя теорему 3.3 :

$$\sum_{z<n_1\leqslant \frac{x}{y}, P^+(n_1)\leqslant y} \phi(\frac{x}{n_1},y) \ll \frac{x}{\log y} \sum_{z<n_1\leqslant \frac{x}{y}, P^+(n_1)\leqslant y} \frac{w(\frac{u}{\alpha} - \frac{\log n_1}{\log y})}{n_1}$$

Применим к последней сумме преобразование Абеля, обозначив через $S(t) = \sum\limits_{z<n_1\leqslant t, P^+(n_1)\leqslant y} \frac{1}{n_1}$. Получаем:

$$\sum_{z<n_1\leqslant \frac{x}{y}, P^+(n_1)\leqslant y} \frac{w(\frac{u}{\alpha} - \frac{\log n_1}{\log y})}{n_1} = S(\frac{x}{y})w(1) + \int_z^{\frac{x}{y}} \frac{w'(\frac{u}{\alpha} - \frac{\log t}{\log y})}{t\log y} S(t)dt \ll$$

$$\ll S(\frac{x}{y}) + \int_{\frac{\beta u}{\alpha}}^{\frac{u}{\alpha}-1} |w'(\frac{u}{\alpha} - s)| S(y^s)ds.$$

Оценим $S(y^s)$, для этого вновь воспользуемся преобразованием Абеля:

$$S(y^s) = \sum_{z<n_1\leqslant y^s, P^+(n_1)\leqslant y} \frac{1}{n_1} = \frac{\psi(y^s,y) - \psi(z,y)}{y^s} + \log y \int_{\frac{\beta u}{\alpha}}^{s} \frac{\psi(y^\tau,y) - \psi(z,y)}{y^\tau} d\tau$$

$$\leqslant \frac{\psi(y^s,y)}{y^s} + \log y \int_{\frac{\beta u}{\alpha}}^{s} \frac{\psi(y^\tau,y)}{y^\tau} d\tau.$$

Теперь воспользуемся теоремой 3.2, условия которой выполнены, получаем,

$$(y^s) \ll exp\{-s(1+o(1))\log s\} + (\log y)\int_{\frac{\beta u}{\alpha}}^{s} exp\{-\tau(1+o(1))\log\tau\}d\tau \ll$$

$$\ll (\log y) exp\{-\frac{\beta u}{\alpha}(1+o(1))\log\frac{\beta u}{\alpha}\}, u \to \infty.$$

Теперь подставляя полученные оценки и используя неравенства на $w(v)$ (см теорема 4, 3 часть, 6 глава [36] )

$$|w'(v)| \leqslant exp\{-v(1+o(1))\log v\},$$

мы получаем требуемый результат.

Теперь докажем еще одну лемму.

**Лемма 3.2.** *Количество делителей числа $n < Q$, не превосходящих $z$, не превосходит $\psi(z, (1+o(1))\log Q), Q \to \infty$..*

Доказательство. Пусть $p_1^{t_1}...p_s^{t_s}$ разложение на простые множители, причем $p_1 < p_2 < \ldots < p_s$.

Рассмотрим отображение делителей числа $n$

$$\sigma : p_1^{l_1}...p_s^{l_s} \to p_{(1)}^{l_1}...p_{(s)}^{l_s},$$

где $p_{(i)}$ - $i-$ простое число в натуральном ряду, то есть $p_{(1)} = 2, p_{(2)} = 3, p_{(3)} = 5, ...$

Это отображение инъективно. Также, $\sigma(d) \leqslant d \leqslant z$.

Известно, что если $n := p_1^{t_1}...p_s^{t_s} < Q$ то $p_{(s)} \leqslant (1+o(1))\log Q$. Отсюда количество чисел в образе отображения $\sigma$, которые не превосходят $z$ не больше $\psi(z, (1+o(1))\log Q)$. А это и есть исходное утверждение. Лемма доказана.

## 3.2 Доказательство теоремы 3.1

Пусть $x = (\log q)^u$. Определим $\varepsilon$ из равенства :

$$|A \cap [1, x]| = \varepsilon x.$$

Введем параметры $\alpha, \beta$ ; $\beta < 1$ и соответственно $y = (\log q)^\alpha, z = x^\beta$. Для каждого натурального $n$, как и раньше, $n = n_1 n_2$, так что если простое $p$ делит $n_1$, то $p \leqslant y$, а если $p$ делит $n_2$, то $p > y$.

Напомним, что $N(x, y, z) = \{n \leqslant x : n_1 > z\}$ . Теперь рассмотрим множество $A' = A \cap [1, x] \backslash N(x, y, z)$. Положим также $|A'| = \varepsilon' x$. Используя лемму 3.1, несложно заметить, что :

$$\varepsilon \leqslant \varepsilon' + exp\{-\frac{\beta u}{\alpha}(1+o(1))\log(\frac{\beta u}{\alpha})\},$$

здесь $o(1)$ по $u \to \infty$.

Рассмотрим $B = \{m_1 \dots m_r\}$, где $r = [\frac{\log q}{\log x}]$ и $m_1, \dots, m_r \in A'$. Оценим сверху размер этого множества, используя, что произведение произвольных $r$ чисел из $A'$ является числом из $A : |B| \leqslant |\{m_1 \dots m_r\}| \leqslant |A| \leqslant q^\nu$. Теперь оценим снизу $|B|$. Пусть каждое $m_i = n_{1,i}n_{2,i}$, так что если простое $p$ делит $n_{1,i}$, то $p \leqslant y$, а если $p$ делит $n_{2,i}$, то $p > y$. Определим из равенства $N_1, N_2 : m = m_1 \dots m_r = n_{1,1} \dots n_{1,r}n_{2,1} \dots n_{2,r} = N_1N_2$, где $N_1 = n_{1,1} \dots n_{1,r}$ и $N_2 = n_{2,1} \dots n_{2,r}$.

Возьмем конкретный представитель, например элемент $m \in A' \dots A'(r$ сомножителей) и оценим сверху число представлений его в виде произведения $A' \dots A'$.

Пусть $m = N_1N_2$, оценим количество представлений для $N_2$ в виде произведения $r$ чисел $n_{2,1} \dots n_{2,r}$ , $N_2 = n_{2,1} \dots n_{2,r} = p_1 \dots p_s$ ,где все $p_i > y$ и являются простыми числами. Видим, что $s \leqslant s_0 = [\frac{\log q}{\log y}]$.

Каждый делитель $p_i, i = 1, \dots, s$ может входить в разложение некоторого $n_{2,j}, j = 1, \dots, r$. Значит количество представлений числа $N_2$ не превосходит $r^s \leqslant r^{s_0}$.

Теперь оценим количество представлений для $N_1$, $N_1 = n_{1,1} \dots n_{1,r}$. Каждое $n_{1,i}$ не превосходит $z$ и является $y-$ гладким числом. Значит для каждого $n_{1,i}$ имеется не более $|\psi(z, y)|$ возможностей. Заметим также, что каждое $n_{1,i} \leqslant z$ является делителем $N_1$. Значит, по лемме 3.2 каждое $n_{1,i}$ может принимать не более $\psi(z, (1 + o(1)) \log q)$ значений. Отсюда получаем, что количество представлений для $N_1$ не превосходит каждого из 2-ух чисел $|\psi(z, y)|^r, |\psi(z, (1 + o(1)) \log q)|^r$. Число же представлений для числа $m$ не превосходит произведения числа представлений для $N_1$ и $N_2$.

Отсюда получается и нижняя оценка для $B$ :

$$|B| \geqslant \frac{(\frac{\varepsilon' x}{|\psi(z,y)|})^r}{r^{s_0}}, |B| \geqslant \frac{(\frac{\varepsilon' x}{|\psi(z,(1+o(1))\log q)|})^r}{r^{s_0}}.$$

Значит должно выпоняться 2 соотношения:

$$\frac{(\frac{\varepsilon' x}{|\psi(z,y)|})^r}{r^{s_0}} \leqslant q^\nu \tag{3.2}$$

$$\frac{(\frac{\varepsilon' x}{|\psi(z,(1+o(1))\log q)|})^r}{r^{s_0}} \leqslant q^\nu \tag{3.3}$$

для любых выбранных параметров $(\alpha, \beta)$. Из этого неравенства можно получить оценку для $\varepsilon'$, а значит и для $\varepsilon$. Теперь найдем соответствующие значения параметров $(\alpha, \beta)$, которые дают наилучшую (наименьшую) оценку для $\varepsilon$.

**Первый случай.** Пусть $\log\log x = o(\log\log p)$. В этом случае, в (2) используя, что $\psi(z,y) \leqslant z$ мы получаем $\frac{(\frac{\varepsilon' x}{z})^r}{r^{s_0}} \leqslant q^\nu$. Распишем левую часть и напишем условие на $\varepsilon'$, предварительно сделав преобразования.

$\frac{(\frac{\varepsilon' x}{z})^r}{r^{s_0}} \geqslant \frac{(\varepsilon' x^{1-\beta})^{\frac{\log q}{\log x}-1}}{(\frac{\log q}{\log x})^{\frac{\log q}{\log y}}} = exp\{(\frac{\log q}{\log x} - 1)(\log\varepsilon' + (1-\beta)\log x) - \frac{\log q}{\alpha\log\log q}(\log\log q - \log\log x)\} \geqslant exp\{\log q(\frac{\log\varepsilon'}{\log x} + 1 - \beta - \frac{1}{\alpha} + \frac{\log\log x}{\alpha\log\log q} - \frac{(1-\beta)\log x}{\log q})\}.$

Отсюда и из (2) получаем соотношение :

$$\frac{\log\varepsilon'}{\log x} + 1 - \beta - \frac{1}{\alpha} + \frac{\log\log x}{\alpha\log\log q} - \frac{(1-\beta)\log x}{\log q} \leqslant \nu,$$

Выразим теперь отсюда $\varepsilon'$ :

$$\log\varepsilon' \leqslant \log x(\frac{1}{\alpha} - 1 + \beta + \nu - \frac{\log\log x}{\alpha\log\log q} + \frac{(1-\beta)\log x}{\log q}).$$

То есть,

$$\varepsilon' \leqslant x^{\frac{1}{\alpha}-1+\beta+\nu-\frac{\log\log x}{\alpha\log\log q}+\frac{(1-\beta)\log x}{\log q}} \tag{3.4}$$

А тогда получаем оценку на $\varepsilon$:

$$\varepsilon \leqslant x^{\frac{1}{\alpha}-1+\beta+\nu-\frac{\log\log x}{\alpha\log\log q}+\frac{(1-\beta)\log x}{\log q}} + exp\{-\frac{\beta u}{\alpha}(1+o(1))\log(\frac{\beta u}{\alpha})\}.$$

Так как $x \leqslant exp\{(\log q)^{\gamma_0}\}, \gamma_0 < 1$, то первое слагаемое в неравенстве для $\varepsilon$ есть:

$$\frac{(x)^{\frac{1}{\alpha}-1+\beta+\nu}}{(\log x)^{\frac{\log x}{\alpha\log\log q}(1+o(1))}} = \frac{(x)^{\frac{1}{\alpha}-1+\beta+\nu}}{(\log x)^{\frac{u}{\alpha}(1+o(1))}},$$

при $q \to \infty$. Значит,

$$\varepsilon \leqslant \frac{(x)^{\frac{1}{\alpha}-1+\beta+\nu}}{(\log x)^{\frac{u}{\alpha}(1+o_q(1))}} + exp\{-\frac{\beta u}{\alpha}(1+o_u(1))\log(\frac{\beta u}{\alpha})\}.$$

Здесь в первом слагаемом $o(1)$ это по $q$, а во втором слагаемом $o(1)$ по $u$.

Берем следующие значения параметров : $\alpha = \frac{2}{1-\nu}, \beta = \frac{1-\nu}{2} - \delta$, где $\delta > 0$ - произвольное фиксированное. Тогда получаем :

$$\varepsilon \leqslant C(x^{-\delta}) + exp\{-Cu(1-\nu)^2\log(Cu(1-\nu)^2)\},$$

где $C$ - некоторая абсолютная константа. Первое слагаемое меньше второго для достаточно больших $q$.

Поэтому, для первого случая мы получили:

$$\frac{f(x)}{x} \leqslant exp\{-(C+o_q(1))u(1-\nu)^2\log(u(1-\nu)^2)\},$$

для некоторой абсолютной константы $C$ и при $q \to \infty$.

**Второй случай.** Рассмотрим случай, когда $\gamma = \frac{\log\log x}{\log\log q}$ и $\log x = o(\log q)$.

Пусть $\alpha \geqslant (1+\varepsilon)\gamma$ для некоторого $\varepsilon > 0$. Вспоминая, что $z = x^\beta = exp\{\beta(\log q)^\gamma\}$, $y = (\log q)^\alpha$ согласно теореме [A], мы получаем:
$|\psi(z,y)| = z^{1-\frac{\gamma}{\alpha}+o(1)}$, $|\psi(z,(1+o(1))\log q)| = z^{1-\gamma+o(1)}$.

Исходя из этого, заменяя $\beta$ на $\beta(1-\frac{\gamma}{\alpha}+o(1))$ в (4) первый раз и $\beta$ на $\beta(1-\gamma+o(1))$ , заключаем 2 неравенства :

$$\varepsilon' \leqslant x^{\frac{1}{\alpha}-1+\beta(1-\frac{\gamma}{\alpha}+o(1))+\nu-\frac{\log\log x}{\alpha\log\log q}+o(1)}$$

$$\varepsilon' \leqslant x^{\frac{1}{\alpha}-1+\beta(1-\gamma+o(1))+\nu-\frac{\log\log x}{\alpha\log\log q}+o(1)}$$

Окончательно получаем,

$$\frac{f(x)}{x} \leqslant x^{\frac{1}{\alpha}-1+\beta-\frac{\beta\gamma}{\alpha}+\nu-\frac{\gamma}{\alpha}+o(1)} + exp\{-\frac{\beta u}{\alpha}(1+o(1))\log(\frac{\beta u}{\alpha})\}.$$

$$\frac{f(x)}{x} \leqslant x^{\frac{1}{\alpha}-1+\beta-\beta\gamma+\nu-\frac{\gamma}{\alpha}+o(1)} + exp\{-\frac{\beta u}{\alpha}(1+o(1))\log(\frac{\beta u}{\alpha})\}.$$

Во втором слагаемом $o(1)$ по $u$. В нашем случае $u = \frac{(\log q)^\gamma}{\log\log q}$, поэтому можно считать, что $o(1)$ зависит от $q$.

Последнее слагаемое это $exp\{-\frac{\beta}{\alpha}\gamma(\log q)^\gamma(1+o(1))\} = x^{-\frac{\beta}{\alpha}\gamma(1+o(1))}$.

Итак, одновременно выполняются

$$\frac{f(x)}{x} \leqslant x^{\frac{1}{\alpha}-1+\beta-\frac{\beta\gamma}{\alpha}+\nu-\frac{\gamma}{\alpha}+o(1)} + x^{-\frac{\beta}{\alpha}\gamma(1+o(1))}.$$

$$\frac{f(x)}{x} \leqslant x^{\frac{1}{\alpha}-1+\beta-\beta\gamma+\nu-\frac{\gamma}{\alpha}+o(1)} + x^{-\frac{\beta}{\alpha}\gamma(1+o(1))}.$$

Будем искать параметры $(\alpha,\beta)$.

Рассмотрим случай, когда $\alpha \geqslant 1$. Тогда будем минимизировать наибольшее из значений : $-\frac{\beta}{\alpha}\gamma$, $\frac{1-\gamma}{\alpha}+\beta-\beta\gamma-1+\nu$. Если $\alpha \geqslant 1$. то берем такие параметры :

$$\begin{cases} \alpha = \frac{1-\gamma+\sqrt{(1-\gamma)^2+\gamma(1-\nu)}}{1-\nu}; \\ \beta = \alpha^{-1} = \frac{1-\nu}{\sqrt{(1-\gamma)^2+\gamma(1-\nu)}+1-\gamma} \end{cases}$$

Подставляя эти параметры получаем : $f(x) \leqslant x^{1-C_\gamma+o(1)}$, где

$$C_\gamma = \gamma(\frac{1-\nu}{1-\gamma+\sqrt{(1-\gamma)^2+\gamma(1-\nu)}})^2$$

Пусть теперь $\gamma < \alpha \leqslant 1$. Тогда будем минимизировать наибольшее из значений : $-\frac{\beta}{\alpha}\gamma$ и $\frac{1-\gamma}{\alpha} + \beta - \frac{\beta}{\alpha}\gamma - 1 + \nu$. В случае если $\gamma \leqslant \frac{2}{3-\nu}$, берем такие параметры: $\beta = \frac{1-\nu}{2}, \alpha = (1+\eta)\frac{2(1-\gamma)}{1-\nu}$, где $\eta > 0-$ произвольное фиксированное. В случае если $\gamma > \frac{2}{3-\nu}$, берем такие параметры: $\beta = 2-\nu-\frac{1}{\gamma}, \alpha = \gamma(1+\eta)$, где также $\eta > 0-$ произвольное фиксированное.

Подставляя такие параметры получаем $f(x) \leqslant x^{1-L_\gamma+\delta+o(1)}$, где $\delta > 0$ - произвольное фиксированное и $L_\gamma = \frac{(1-\nu)^2\gamma}{4(1-\gamma)}$ если $\gamma \leqslant \frac{2}{3-\nu}$, $L_\gamma = 2-\nu-\frac{1}{\gamma}$, если $\gamma > \frac{2}{3-\nu}$. В силу произвольного $\delta$ отсюда следует исходное неравенство:

$$f(x) \leqslant x^{1-L_\gamma+o(1)}, q \to \infty.$$

Отсюда заключаем неравенство :

$$f(x) \leqslant x^{1-max\{L_\gamma, C_\gamma\}+o(1)}, q \to \infty.$$

Теорема доказана.

**Комментарии**

1. Покажем на примере гладких чисел, какие есть оценки снизу на функцию $f((\log q)^u)$. Возьмем любое число $0 < \nu < 1$ и положим $A_q$ – подмножество $y$ - гладких чисел, где

$$y = (\log q)^\lambda,$$

где $\lambda = \frac{1}{1-\nu+\varepsilon}$, где $\varepsilon$ - малое число. Множество $A_q$ являтся множеством, замкнутым относительно операции умножения.

Пользуясь теоремой [A] о количестве гладких чисел при при $q \geqslant q(\nu, \varepsilon)$ получаем,

$$|A_q \bigcap [1, q]| < q^\nu.$$

Тогда выполнено неравенство (1).

Возьмем теперь какое-нибудь $u$, $|A_q \bigcap [1, (\log q)^u]| = (\log q)^u exp\{-u(1-\nu+\varepsilon')(1+o(1))\log u(1-\nu)\}$, по $u \to \infty$, $\varepsilon' > 0$ - некоторое малое число.

Здесь, как видно, линейный порядок по $(1-\nu)$. Теорема дает правильный характер зависимости по $u$. Однако в нижней оценке зависимость от $(1-\nu)$ линейная, а в теореме квадратичная.

2. Если $x$ растет как степень $q$ с показателем, меньшим 1, то нельзя дать нетривиальную оценку на $|A\bigcap[1,x]|$. Для этого возьмем достаточно большое $q$ и рассмотрим множество $A_q \subseteq [1,q]$, которое состоит из любых произведений чисел взятых из $(q^{0.1}, 1.5q^{0.1}]$. Заметим, если $n \in A$ то $n = n_1 \dots n_r, r \leqslant 9$ и $n_1, \dots, n_r \in (q^{0.1}, 1.5q^{0.1}]$. Значит $|A_q| \leqslant \sum\limits_{1\leqslant r\leqslant 9} (0.5q^{0.1})^r \leqslant q^{0.9}$.

Теперь возьмем $x = 1.5q^{0.1}$. Тогда

$$|A_q \bigcap [1,x]| \geqslant \frac{x}{4}.$$

Таким образом, хороших оценок на функцию $f(x)$ при $x$ порядка степени $q$ для произвольных множеств, замкнутых относительно операции умножения, получить не удается.

# Глава 4

# Задачи делимости частных Ферма.

## 4.1 Определение и некоторые результаты.

Для простого $p$ и целого $a$, $(a,p)=1$, мы определили частное Ферма:

$$q_p(a)=\frac{a^{p-1}-1}{p}.$$

Для простого $p$ наименьшее $a$, для которого не выполнено сравнение

$$q_p(a)\equiv 0 \pmod{p}$$

мы обозначили через $l_p$.

Оценки на $l_p$ могут иметь приложения в различных теоретико-числовых задачах [21],[30].

Приведем некоторые недавние результаты из работы [16].

**Теорема 4.1.** *Для каждого $\varepsilon > 0$ существует такое $\delta > 0$, что для достаточно больших $Q$ неравенство*

$$l_p \leqslant (\log p)^{\frac{5}{3}+\varepsilon}$$

*выполнено для всех простых $p<Q$, за исключением $O(Q^{1-\delta})$ простых.*

**Теорема 4.2.** *Для каждого $\varepsilon > 0$ существует такое $\delta > 0$, что для всех, кроме, быть может, одного простого $p \in [Q^{1-\delta};Q]$ выполнено неравенство :*

$$l_p \leqslant (\log p)^{\frac{59}{35}+\varepsilon}$$

В данной главе мы доказываем следущее утверждение.

**Теорема 4.3.** *Для каждого* $\varepsilon > 0$ *существует такое* $\delta > 0$, *что при достаточно больших* $Q$ *неравенство:*

$$l_p \leqslant (\log p)^{\frac{3}{2}+\varepsilon}$$

*выполнено для всех простых* $p < Q$, *за исключением* $O(Q^{1-\delta})$ *простых.*

При доказательстве этой теоремы используются идеи доказательства теоремы 4.2

## 4.2 Вспомогательные утверждения

Нам потребуются нижние оценки для множества гладких чисел, то есть чисел, все простые делители которых малы.

Для натурального $n$ обозначим через $P(n)$ наибольший простой делитель числа $n$, $P(1) = 1$. Для $x \geq y \geq 2$ полагаем

$$S(x,y) = \{n \leq x : P(n) \leq y\}, N(x,y) =\mid S(x,y) \mid$$

Будем использовать результат работы [2].

**Теорема 4.4.** *Пусть* $x \geq 4$, $x \geq y \geq 2$. *Тогда*

$$N(x,y) > x^{1-\log(\log x)/\log y}.$$

Для натурального $n$ определим $\mathbb{Z}_n$ - кольцо вычетов по модулю $n$ и $\mathbb{Z}_n^*$ - множество обратимых элементов $\mathbb{Z}_n$. Множество $\mathbb{Z}_n^*$ образует группу по умножению.

Пусть $p > 2$ простое. Через $G_p$ обозначим группу степеней порядка $p$ элементов группы $\mathbb{Z}_{p^2}^*$. Ясно, что $\mid \mathbb{Z}_{p^2}^* \mid = p(p-1)$. Так как $Z_{p^2}^*$ - циклическая группа, то несложно видеть, что $\mid G_p \mid = p-1$. Пусть $\overline{G_p}$ - множество целых чисел, сравнимых с элементами $G_p$ по модулю $p^2$. Для $v \in \mathbb{Z}_{p^2}^*$ определим $D_p(v) =\mid \{(g_1,g_2) : g_1, g_2 \in G_p, g_1 - g_2 = v\} \mid$. Здесь равенство понимается в кольце $\mathbb{Z}_{p^2}$.

**Лемма 4.1.** *Пусть* $v_1, v_2 \in Z_{p^2}^*$ *и* $\frac{v_1}{v_2} \in G_p$ , *тогда* $D_p(v_1) = D_p(v_2)$.

**Доказательство**. Пусть $\frac{v_1}{v_2} = g \in G_p$, тогда $D_p(v_1) =\mid \{(g_1,g_2) : g_1, g_2 \in G_p, g_1 - g_2 = v_1\} \mid =\mid \{(g_1,g_2) : g_1, g_2 \in G_p, \frac{g_1}{g} - \frac{g_2}{g} = v_2\} \mid =\mid \{(g_1,g_2) : g_1, g_2 \in G_p, g_1 - g_2 = v_2\} \mid = D_p(v_2)$. Лемма доказана.

При доказательстве следующей леммы мы следуем схеме, предложенной в [30].

**Лемма 4.2.** *Пусть дано* $\delta \in (0,1)$, $Q \in \mathbb{R}$ *достаточно большое число. Пусть простые* $p_1, p_2, \ldots, p_l \in (\frac{Q}{\sqrt{2}}, Q]$, $l \gg Q^{1-\delta}$. *Тогда среди элементов* $p_2^2, \ldots, p_l^2$ *найдется* $t$ *элементов, принадлежащих различным классам смежности по подгруппе* $G_{p_1}$, *где* $t \gg Q^{1-2\delta}$.

**Доказательство**. Без ограничения общности можно считать, что в последовательности $p_2^2, \ldots, p_l^2$ первые $k_1$ элементов принадлежат некоторому классу смежности, следующие $k_2$ элементов принадлежат другому классу смежности и т. д., $k_t$ элементов принадлежат последнему классу. Тогда $\sum_{i=1}^{t} k_i = l - 1$.

Если $p_i^2$ и $p_j^2$ принадлежат одному классу, то это равносильно $\frac{p_i^2}{p_j^2} \in G_{p_1}$(деление в понимается в группе $\mathbb{Z}^*_{p_1^2}$). Покажем, что $\frac{p_i^2}{p_j^2} \in G_{p_1}$ эквивалентно $\frac{p_i}{p_j} \in G_{p_1}$.

Пусть $g$ - первообразный корень по модулю $p^2$. Пусть для некоторого целого $k$ выполнено : $\frac{p_i}{p_j} = g^k$(равенство в группе $\mathbb{Z}^*_{p_1^2}$). Тогда $\frac{p_i^2}{p_j^2} = g^{2k}$. А из $\frac{p_i^2}{p_j^2} \in G_{p_1}$ также следует $\frac{p_i^2}{p_j^2} = g^{pk'}$ для некоторого $k'$. Тогда $2k \equiv pk' \pmod{p(p-1)}$. Отсюда следует, что $k$ делится на $p$. А это то, что и требовалось.

Пусть $p_i \neq p_j; p_i' \neq p_j'; (p_i, p_j) \neq (p_i', p_j'); \frac{p_i}{p_j}, \frac{p_i'}{p_j'} \in G_{p_1}$. Покажем теперь, что $\frac{p_i}{p_j}$ и $\frac{p_i'}{p_j'}$ различаются как элементы $\mathbb{Z}^*_{p_1^2}$.

Действительно, в противном случае, $p_i p_j' \equiv p_i' p_j \pmod{p_1^2}$. С учетом того, что все рассматриваемые $\{p_i\} \in (\frac{Q}{\sqrt{2}}; Q]$, получаем численное равенство $p_i p_j' = p_i' p_j$. Но это невозможно. Следовательно, $\frac{p_i}{p_j} \neq \frac{p_i'}{p_j'}$(как элементы $\mathbb{Z}^*_{p_1^2}$).

В $s$-ый смежный класс попадает $k_s$ чисел среди $p_2^2, \ldots, p_l^2$. Тогда из них можно образовать $k_s(k_s - 1)$ пар $(p_i, p_j)$ $p_i \neq p_j$. Каждая пара дает условие $\frac{p_i}{p_j} \in G_{p_1}$ и все такие пары различаются как элементы $G_{p_1}$. Поэтому $\sum_{i=1}^{t} k_i(k_i - 1) \leq p - 1$. Значит, $\sum_{i=1}^{t} k_i^2 \ll Q$.

$$Q^{1-\delta} \ll k_1 + \ldots + k_t \leq \sqrt{t}\sqrt{k_1^2 + \ldots + k_t^2} \ll \sqrt{t}\sqrt{Q}.$$

Отсюда $t \gg Q^{1-2\delta}$. Что и требовалось доказать.

## 4.3 Доказательство основной леммы

Докажем лемму, из которой выведем теорему.

**Лемма 4.3.** *Для каждого* $\varepsilon > 0$ *существует такое* $\delta > 0$, *что при достаточно больших* $Q$ *неравенство*

$$l_p \leqslant (\log p)^{\frac{3}{2}+\varepsilon}$$

*выполнено для всех простых* $p$ :$\frac{Q}{\sqrt{2}} < p \leq Q$ , *за исключением* $O(Q^{1-\delta})$ *простых* $p$.

**Доказательство леммы**. Докажем от противного. Пусть существует такое $\varepsilon_0 \in (0,1)$, что для любого $\delta > 0$ и некоторого большого $Q$ для простых на $(\frac{Q}{\sqrt{2}}; Q]$ в количестве не менее $Q^{1-\delta}$ выполнены неравенства : $l_p > (\log p)^{3/2+\varepsilon_0}$. Пусть $\alpha := 3/2 + \frac{\varepsilon_0}{2}$. Подберем $\gamma$ и $\delta$ из условий :

$$\begin{cases} \gamma \in (\frac{\alpha}{\alpha-1}; 3) \subset (2; 3); \\ \delta \in (0, \frac{3-\gamma}{2}). \end{cases}$$

При условии $\alpha > 3/2$ такие $\delta$ и $\gamma$ можно подобрать.

Введем $x := [Q^\gamma]; y := [(\log \frac{Q}{\sqrt{2}})^{\frac{3}{2}+\varepsilon}]$. Занумеруем простые $\{p_i\}$ $(i = 1, 2, \ldots)$, количество которых не менее $Q^{1-\delta}$, для которых $l_p > (\log p)^{\frac{3}{2}+\varepsilon_0}$.

Далее, $N(x,y) > x^{1-\log(\log x)/\log y} \geq (Q-1)^{\delta(1-\frac{\log\log Q+O(1)}{(\frac{3}{2}+\varepsilon)(\log\log Q+O(1))})} \gg Q^{\gamma(1-\frac{1}{\alpha})} = Q^{1+\mu^2}$, для некоторого $\mu$. Легко заметить, что для любого $i$ выполнено условие : $S(x,y) \subseteq \overline{G_{p_i}}$. Поэтому, для любых $i, j$

$$S(x,y) \subseteq [1,x] \bigcap \overline{G_{p_i}} \bigcap \overline{G_{p_j}}.$$

На множестве $\{p_i\}$ мы определяем ориентированный граф, который удобно трактовать в виде турнира. Среди простых $p_i$ устраиваем турнир. Для $p_i \neq p_j$ ниже будут определено число $N_{i,j}$. Если, например, $N_{i,j} < N_{j,i}$, то считаем, что $p_j$ выиграло у $p_i$, в случае $N_{i,j} = N_{j,i}$, полагаем, что $p_i$ сыграло вничью с $p_j$.

Опишем переход к паре $(N_{i,j}, N_{j,i})$. Воспользуемся теоремой 2.1 для оценки сверху величины $|[1,x] \bigcap \overline{G_{p_i}} \bigcap \overline{G_{p_j}}|$. В условии теоремы положим $z := [\frac{2x}{Q^2}]$. Применив теорему 2.1 и то, что, $|[1,x] \bigcap \overline{G_{p_i}} \bigcap \overline{G_{p_j}}| \geqslant N(x,y) \geqslant Q^{1+\mu^2}$ получим

$$|[1,x] \bigcap \overline{G_{p_i}} \bigcap \overline{G_{p_j}}| \ll max(N_{i,j}, N_{j,i})$$

где величины $N_{i,j}$ определяются так

$$N_{i,j} := \sum_{1 \leqslant k \leqslant z} D_{p_i}(kp_j^2).$$

Среди простых $p_\nu$ ввели турнир. Существует простое $p_l$, которое не проиграло хотя бы половину встреч. Без ограничения общности, $p_1$ не выиграло у $p_2, \dots, p_l$, где $l \gg Q^{1-\delta}$. Тем самым для $\nu = 2, \dots, l$ справедливо неравенство

$$N(x,y) \ll N_{1,\nu} = \sum_{1 \leqslant k \leqslant z} D_{p_1}(kp_\nu^2).$$

Пусть элементы $1, \dots, z$ содержатся в классах $C_1, \dots, C_J$ группы $\mathbb{Z}^*_{p_1^2}$ по подгруппе $G_{p_1}$. Пусть в $C_j$ классе содержится $s_j$ элементов из $1, \dots, Z$. Тогда $p_\nu^2, \dots, zp_\nu^2$ содержатся в $p_\nu^2 C_1, \dots, p_\nu^2 C_J$ классах, причем в классе $p_\nu^2 C_j$ содержится $s_j$ элементов из $1p_\nu^2, \dots, zp_\nu^2$.

Согласно лемме 4.2 среди $p_2^2, \dots, p_l^2$ найдется $t \gg Q^{1-2\delta}$ элементов, принадлежащих различным классам смежности. Выберем те простые из $p_2, \dots, p_l$, что рассмотренные смежные классы попарно различны. Без ограничения общности считаем, что эти простые $p_2, \dots, p_{t+1}$, где $t \gg Q^{1-2\delta}$. Это означает, что для любого $j$ классы $p_2^2 C_j, \dots, p_{t+1}^2 C_j$ попарно различны.

Обозначим

$$f_{j\nu} = D_{p_1}(v),$$

где $v \in p_\nu^2 C_j$. Здесь и далее $\nu = 2, \dots, t+1$.

С одной стороны,

$$\sum_{v \in \mathbb{Z}^*_{p_1^2}} \mid D_{p_1}(v) \mid < p_1(p_1 - 1).$$

С другой стороны, по лемме 4.1

$$\sum_{v \in \mathbb{Z}^*_{p_1^2}} \mid D_{p_1}(v) \mid = \Big( \sum_{v \in \mathbb{Z}^*_{p_1^2}/G_{p_1}} \mid D_{p_1}(v) \mid \Big) p_1.$$

Значит,

$$\sum_{\nu=2}^{t+1} f_{i\nu} \leq \sum_{v \in \mathbb{Z}^*_{p_1^2}/G_{p_1}} \mid D_{p_1}(v) \mid) < p_1 - 1.$$

Далее,

$$\sum_{\nu=2}^{t+1} \Big( \sum_{i=1}^{z} D_{p_1}(ip_\nu^2) \Big) = \sum_{\nu=2}^{t+1} \sum_{j=1}^{J} s_j f_{j\nu} = \sum_{j=1}^{J} s_j \sum_{\nu=2}^{t+1} f_{j\nu} < \Big( \sum_{j=1}^{J} s_j \Big) p_1 \ll p_1 Q^{\gamma-2}.$$

В тоже время,

$$\sum_{\nu=2}^{t+1} \Big( \sum_{i=1}^{z} D_{p_1}(ip_\nu^2) \Big) \geq \sum_{\nu=2}^{t+1} N(x,y) \gg Q^{1-2\delta} Q.$$

Как следствие получим неравенство

$$Q^{2-2\delta} \ll Q^{1+\gamma-2}.$$

Но для достаточно больших $Q$ это противоречит выбору $\delta$ из условия $\gamma-2 < 1-2\delta$.

## 4.4 Завершение доказательства теоремы 4.3

Возьмем любое $\varepsilon > 0$. Тогда существуют такие $Q'$ и $\delta > 0$, что для $Q > Q'$ неравенство

$$l_p \leqslant (\log p)^{\frac{3}{2}+\varepsilon}$$

выполнено для всех простых $p : \frac{Q}{\sqrt{2}} < p \leq Q$ , за исключением быть может не более $(Q^{1-\delta})$ простых $p$.

Разобьчм $(Q';\infty)$ на множества вида $(Q'(\sqrt{2})^{k-1}; Q'(\sqrt{2})^k]$, где $k$-натуральное.

Возьмем $Q > Q'$, пусть $(Q';Q]$ покрывается первыми $s+1$ множествами, где $s \geq 0$. Тогда $Q'(\sqrt{2})^s < Q \leq Q'(\sqrt{2})^{s+1}$

Далее, используя утверждение получаем, что количество простых $p$, что

$$p < Q; l_p \geq (\log p)^{\frac{3}{2}+\varepsilon}$$

не превосходит велиичины $T$, где $T := \pi(Q') + (\sqrt{2}Q')^{1-\delta} + \ldots + ((\sqrt{2})^{s+1}Q')^{1-\delta} = \pi(Q') + (\sqrt{2}Q')^{1-\delta}\frac{(\sqrt{2})^{(1-\delta)(s+1)}-1}{(\sqrt{2})^{1-\delta}-1}$.

Заметим, что $\sqrt{2}^{(1-\delta)(s+1)} \ll Q^{1-\delta}$ при достаточно больших $s$. Следовательно, $T \ll Q^{1-\delta}$.

Получили, что для любого $\varepsilon$ существуют такие $Q(\varepsilon)$ и $\delta > 0$, что при $Q > Q(\varepsilon)$ для всех простых $p < Q$, за исключением не более $O(Q^{1-\delta})$ выполнено неравенство:

$$l_p \leqslant (\log p)^{\frac{3}{2}+\varepsilon}.$$

Теорема доказана.

## 4.5 Делимость частных Ферма на квадрат простого числа.

Нас будет интересовать наименьшее $a$, для которого не выполнено сравнение

$$q_p(a) \equiv 0 \pmod{p^2}.$$

Для простого $p$ обозначим это число $l_p^{'}$.

В работе [16] была получена верхняя оценка на $l_p$. Было доказано следующее утверждение.

**Теорема 4.5.** *Мы имеем неравенство:*

$$l_p \leqslant (\log p)^{\frac{463}{252}+o(1)}, p \to \infty$$

С помощью более сильных результатов об энергии подгрупп, И.Д.Шкредов улучшил этот результат. Ниже мы приводим этот результат [32].

**Теорема 4.6.** *Имеет место оценка:*

$$l_p \leqslant (\log p)^{\frac{7829}{4284}+o(1)}, p \to \infty$$

Новые оценки энергии подгрупп и тригонометрических сумм, полученные И.Д. Шкредовым, позволяют доказать следующую теорему о делимости частных ферма на квадрат простого числа.

**Теорема 4.7.** *Мы имеем неравенство:*

$$l_p^{'} \leqslant (\log p)^{\frac{2077}{1404}+o(1).}$$

В $\mathbb{Z}_{p^3}^*$ имеется подгруппа порядка $p-1$, которую мы обозначим $G$. Несложно заметить, что свойство делимости частных Ферма на $p^2$ связано с данной подгруппой $G$. Действительно, $p^2|q_p(a)$ тогда и только тогда, когда $a \in G$.

Напомним определение из работы [15]. Пусть дана произвольная мультипликативная подгруппа $G$ в $\mathbb{Z}_n^*$. Для целого $K$ и натурального $k$ мы определяем

$$J(n,G,k,K) = |(\{K+1,...,K+k\} \bigcap G)|.$$

Мы будем пользоваться утверждением, доказанном в [15].

**Лемма 4.4.** *Пусть имеется подгруппа $G$ порядка $t$ группы $\mathbb{Z}_n^*$. Тогда для любого $\varepsilon > 0$ мы имеем неравенство:*

$$J(n,G,k,K) \ll \frac{kt}{n} + \frac{k}{tn} \sum_{\omega \in \mathbb{Z}_n} M_n(\omega, Z, G) | \sum_{u \in G} e_n(u\omega)|,$$

*где*

$$Z := min(n^{1+\varepsilon}k^{-1}, n/2)$$

*и* $M_n(\omega, Z, G)$ *есть число решений сравнения*

$$\omega \equiv zu \pmod{n}, 1 \leqslant |z| \leqslant Z, u \in G.$$

Для целого $k < p^3$ пусть $N_p(k)$ обозначает количество элементов $v \in [1, k]$ подгруппы $G$. Положим $\psi(x, y)$ - число $y-$ гладких чисел меньших $x$. Имеет место оценка [27]

$$\psi(x, y) > x^{1-\log\log x/\log y}.$$

Предположим что $l_p^{'} = (\log p)^{\alpha}$ и также $k = p^{\beta}$, $\alpha, \beta$ - некоторые значения. Мы предположили, что все числа $[1, l_p^{'}]$ принадлежат нашей подгруппе $G$. Мы замечаем, что

$$N_p(k) \geqslant \psi(k, l_p^{'}) = p^{\beta(1-1/\alpha)+o(1)}, p \to \infty$$

Оценим теперь $N_p(k)$ сверху используя лемму 4.4

$$N_p(k) \ll \frac{k}{p^2} + \frac{k}{p^4} \sum_{\omega \in \mathbb{Z}_{p^3}} M_{p^3}(\omega, Z, G)|S(w, G)|$$

Рассмотрим вклад необратимых элементов $\omega \in \mathbb{Z}_{p^3}$. Если $\omega = 0$ то $M_{p^3}(\omega, Z, G) = 0$. Для ненулевых $\omega = \tau p$ оценим соответствующую тригонометрическую сумму:

$$|S(w, G)| = \sum_{g \in G} e_{p^3}(\frac{(\tau p)g}{p^3}) = \sum_{g' \in G'} e_{p^2}(\frac{\tau g'}{p^2}),$$

где $G'-$ подгруппа порядка $p-1$ в $\mathbb{Z}_{p^2}^*$.

Поэтому для ненулевых необратимых элементов соответствующую тригонометрическую сумму можно оценить величиной $p^{5/6+o(1)}$. Здесь мы применили оценку тригонометрической суммы, которую получил И.Д. Шкредов.

Для обратимых элементов по теореме 1.10 тригонометрическую суму можно оценить величиной $p^{\frac{673}{702}+o(1)}$.

Итак,

$$\sum_{\omega \in \mathbb{Z}_{p^3}} M_{p^3}(\omega, Z, G)|S(w, G)| \leqslant p^{\frac{673}{702}+o(1)} \sum_{\omega \in \mathbb{Z}_{p^3}} M_{p^3}(\omega, Z, G).$$

Таким образом, эта сумма не превосходит $p^{4\frac{673}{702}+2\varepsilon}/k$, где $\varepsilon > 0$ произвольное достаточно малое.

Значит,

$$N_p(k) \ll \frac{k}{p^2} + p^{\frac{673}{702}+2\varepsilon}.$$

Теперь берем $k = p^{2\frac{673}{702}+2\varepsilon}, \beta = 2\frac{673}{702}$ В таком случае получаем:

$$p^{2\frac{673}{702}(1-\frac{1}{\alpha})+o(1)} \leqslant N_p(k) \ll p^{\frac{673}{702}+2\varepsilon}.$$

Отсюда и в силу произвольности $\varepsilon > 0$ мы заключаем $\alpha \leqslant \frac{2077}{1404}+o(1), p \to \infty$. Теорема 4.7 доказана.

# Список литературы


[1] *Д.В. Горбачев* Некоторые неравенства для дискретных положительно определенных функций, Известия ТулГУ. Естественные науки. 2015. Вып. 2. С. 5–12.

[2] *С. В. Конягин* Оценки тригонометрических сумм по подгруппам и сумм Гаусса, IV Международная конференция – Современные проблемы теории чисел и ее приложения, посвященная 180-летию П. Л. Чебышева и 110-летию И. М. Виноградова: Актуальные проблемы ч. III, МГУ, мехмат 2002, стр. 86–114.

[3] *Ю. В. Малыхин* Оценки тригонометрических сумм по модулю $p^2$, Фундамент. и прикл. матем., 11:6 (2005),с. 81–94.

[4] *Ю. В. Малыхин* Оценки тригонометрических сумм по модулю $p^r$,' Математические заметки, том 80, выпуск 5, 2006, с. 793–796.

[5] *К. Прахар*, Распределение простых чисел, Издательство Мир, 1984.

[6] *Ю.Н. Штейников*, О распределении элементов полугрупп натуральных чисел, Чебышевский сборник, 13:3 (2012), с. 91–99.

[7] *Ю.Н. Штейников*, Делимость частных Ферма, Математические заметки, 92:1 (2012), с. 116–122.

[8] *Ю.Н. Штейников*, Тригонометрические суммы по подгруппам и некоторые их приложения, Математические заметки, 98:4 (2015), с. 606–625.

[9] *Ю.Н. Штейников*, О множестве совместных представителей вычетов по двум модулям, Труды МИАН, том 290, (2015), с. 202–210.

[10] *Ю.Н. Штейников*, О распределении элементов полугрупп натуральных чисел, Материалы конференции – Компьютерная алгебра и информационные технологии, с. 89–90.

[11] *Ю.Н. Штейников*, Оценки тригонометрических сумм по подгруппам, Материалы тринадцатой молодежной школы-конференции – Лобачевские чтения - 2014 , с. 181–183.

[12] *Ю.Н. Штейников*, О произведениях множеств с малым мультипликативным удвоением и интервалов , Материалы конференции – Воронежская зимняя математическая школа - 2015 , с. 151.

[13] *Ю.Н. Штейников*, О множестве совместных представителей вычетов по двум модулям, Материалы конференции – XIII Международная конференция Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения - 2015 , с. 254–255.

[14] *Ю.Н. Штейников*, О плотности распределения полугрупп натуральных чисел , Материалы конференции – XII Международная Казанская летняя школа-конференция – Теория функций, ее приложения и смежные вопросы - 2015 , с. 491–492.

[15] *J. Bourgain, S.V. Konyagin and I.E. Shparlinski* Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm International Math Research Notices 2008, p. 1–29.

[16] *J. Bourgain, K. Ford, S. Konyagin, I. Shparlinski* On the divisibility of Fermat Quotients, Michigan J. Math. 59:2 , 2010 p. 313–328.

[17] *J. Bourgain, S. Konyagin* Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order, C. R. Math. Acad. Sci. Paris, 337:2, 2003, p. 75–80.

[18] *J. Bourgain, S. Konyagin, I. Shparlinski*, Distribution of elements of cosets of small subgroups and applications, International Math Research Notices, 1968–2009, 2012:9 (2012).

[19] *U. Betke, M. Henk, J. M. Wills* Successive-minima-type inequalities, Discr. Comput. Geom., 9, 1993, p. 165–175.

[20] *J. Cilleruelo, M. Z. Garaev* Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications, http://arxiv.org/abs/1404.5070.

[21] *A. Granville* On pairs of coprime integers with no large prime factors, Exposition. Math. 9 1991, p. 335–350.

[22] *A. Garcia, J.F. Voloch* Fernat curves over finite fields, J. Number Theory, 30, 1988, p. 345–356.

[23] *G.H. Hardy and J.E. Littlewood*, Some problems of "Partitio Numerorum": IV The singular series in Waring's problem, Math. Z. 12 (1922), 161-188.

[24] *D. R. Heath-Brown, S. Konyagin* New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Q. J. Math., 51:2 (2000),p. 221–235.

[25] *A. Hildebrand, G. Tenenbaum*, Integers without large prime factors, J Theorie des Nombres de Bordeaux, 5 (1993) no. 2 411–484.

[26] *S. Konyagin, I. Shparlinski* Character sums with exponential functions, Cambridge University Press, Cambridge, 1999.

[27] *S. V. Konyagin, C. Pomerance* On primes recognizable in deterministic polynomial time, The mathematics of Paul Erdős, 1 p. 176–198, Springer, Berlin.

[28] *H. W. Lenstra*, Miller's primality test, Inform. Process. Let.,8 (1979),p. 86–88.

[29] *M. B. Nathanson* Additive number theory. Inverse problems and the geometry of sumsets, Springer, New York, 1996.

[30] *A. Ostafe, I. Shparlinski*, Pseudorandomness and dynamics of Fermat quotients, SIAM J. Discr. Math., 2011, v. 25, p. 50–71.

[31] *I.D. Shkredov* Some new inequalities in additive combinatorics, Moscow journal of combinatorics and number theory 3, 2013 p. 189–239.

[32] *I. D. Shkredov* On Heilbronn's exponential sum Q. J. Math., 64:4, 2013 p. 1221–1230.

[33] *I.D. Shkredov* On exponential sums over multiplicative subgroups of medium size, Finite fields and applications, 30, 2014, p. 72–87.

[34] *I. Shparlinski*, Integers with a large smooth divisor, Electronic journal of combinatorial number theory 7, 2007.

[35] *T. Tao, V. Vu* Additive combinatorics, Cambridge University Press, Cambridge, 2010.

[36] *G. Tenenbaum*, Introduction to analytic and probabilistic number theory, Cambridge Universit Press, Cambridge, UK, 1995.

[37] *B. Zhou* A note on exponential sums over subgroups of $\mathbb{Z}_{p^2}^*$ and their applications, J. Number Theory, 130:11 2010, p. 2467–2479.