Math-Net.Ru

Общероссийский математический портал

Ю. Н. Штейников, Оценки тригонометрических сумм по подгруппам и некоторые их приложения, *Матем. заметки*, 2015, том 98, выпуск 4, 606–625

DOI: <https://doi.org/10.4213/mzm10629>

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

Параметры загрузки:

IP: 54.224.187.69

26 апреля 2023 г., 17:41:33

Оценки тригонометрических сумм по подгруппам и некоторые их приложения

Ю. Н. Штейников

В работе получены новые верхние оценки тригонометрических сумм по подгруппам $\Gamma \subset \mathbb{Z}_p^*$, размер которых принадлежит $[p^{28/95}, p^{182/487}]$. Используя подход Ю. В. Малыхина, мы уточняем оценки таких сумм в $\mathbb{Z}_{p^\Gamma}^*$ и применяем их к задаче делимости частных Ферма.

Библиография: 13 названий.

DOI: 10.4213/mzm10629

1. Введение

Через p будем обозначать достаточно большое простое число; $\mathbb{Z}_q$ – кольцо вычетов из q элементов.

В работе мы будем рассматривать следующую задачу. Пусть Γ – подгруппа $\mathbb{Z}_p^*$, $a \in \mathbb{Z}_p^*$, $e_p(x) := e^{2\pi i x/p}$. Требуется нетривиально оценить модуль суммы

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

Положим

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

Важной задачей является установление нетривиальных по порядку верхних оценок для $S(\Gamma)$:

$$S(\Gamma) = o(|\Gamma|).$$

Известны применения этих оценок, например для распределения элементов подгрупп [1] некоторых аддитивных задач по простому модулю.

Для мультипликативной группы $\Gamma \subset \mathbb{Z}_p^*$ введем по определению величину

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

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

Работа выполнена при поддержке Российского научного фонда (грант № 14-11-00433).

ЛЕММА 1. Для произвольных натуральных k, l справедливо неравенство

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

Оценки такого вида установлены И. М. Виноградовым для тригонометрических сумм Вейля. Доказательство леммы 1 можно найти в [2].

Условимся обозначать $t := |\Gamma|$.

Гарсиа и Волох [3] установили, что при $t \ll p^{3/4}$ и при любом $a \in \mathbb{Z}_p^*$ сравнение $g + g' \equiv a \pmod{p}$ имеет не более $4t^{2/3}$ решений относительно $g, g' \in \Gamma$. Из этого следует нетривиальная оценка $T_2(\Gamma) \ll t^{8/3}$. Развивая идеи работы Д. Хиф-Брауна и Конягина, основываясь на методе С. А. Степанова, Конягиным были получены нетривиальные оценки $T_k(\Gamma)$ для всех натуральных k (см. [4]). Сформулируем соответствующее утверждение из этой работы.

ЛЕММА 2. Для любого натурального m существует такое $C(m)$, что для любых p, Γ таких, что

$$t = |\Gamma| < p^{2/3} \quad \text{при} \quad m = 2 \quad \text{и} \quad t = |\Gamma| < p^{1/2} \quad \text{при} \quad m > 2,$$

имеет место оценка

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

Это позволяет доказать с помощью установленной в работе [4] леммы 1, что для подгрупп при $t > p^{1/4+\varepsilon}$ выполнено неравенство

$$S(\Gamma) < C(\varepsilon)tp^{-\delta(\varepsilon)}$$

для некоторых функций $C(\varepsilon)$, $\delta(\varepsilon) > 0$. Используя другой подход, Бургейн и Конягин [5] доказали оценку такого типа и при $t > p^\varepsilon$.

Относительно недавно Шкредов [6], [7] усилил оценку как для величины $T_2(\Gamma)$, так и для соответствующей тригонометрической суммы. Также приведем из этих работ соответствующие утверждения.

ТЕОРЕМА 3. При $t < p^{2/3}$ справедлива оценка

$$S(\Gamma) \ll p^{1/6}t^{1/2}(\log t)^{1/6},$$

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

Это утверждение усиливает ранее полученные оценки сумм по подгруппам, чей размер находится в определенном интервале. В данной работе мы будем развивать идеи указанных работ и получим новую оценку для величины $T_3(\Gamma)$. Как следствие, используя лемму 1, мы также усилим оценки сумм по подгруппам, чей порядок находится в интервале $[p^{28/95}, p^{182/487}]$. Отметим, что

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

В этом пункте мы будем обозначать через Γ подгруппу. Мы предполагаем, если не оговорено противное, следующее ограничение на t : $t < p^{1/2}$.

ТЕОРЕМА 4. При $t < p^{1/2}$ справедлива оценка

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

Как следствие теоремы 4 и леммы 1 мы получаем теорему 5.

ТЕОРЕМА 5. *Справедливы неравенства*

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

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

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

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

В п. 3 работы мы получим оценку тригонометрической суммы по модулю p^3 для подгруппы G , $|G| = p - 1$. Для этого мы будем использовать современные оценки на величины $S(G)$, $T_2(G)$ по квадрату простого числа p и метод Малыхина получения таких оценок по произвольной степени простого числа. Мы применим этот результат для задачи делимости частных Ферма на квадрат простого числа.

В п. 4 работы, следуя работе [8], мы докажем оценку числа решений специального сравнения, включающего интервал натуральных чисел и множества с малым мультипликативным удвоением по произвольному модулю.

2. Оценка $T_3(\Gamma)$ и расстояния между соседними элементами подгрупп

2.1. Предварительные утверждения. Пусть $\mathbb{Z}_p^*$ – множество обратимых элементов кольца $\mathbb{Z}_p$.

Также обозначим через $\Gamma(x)$ характеристическую функцию множества Γ на $\mathbb{Z}_p$. По определению для двух функций f, g на $\mathbb{Z}_p$ полагаем

$$f \circ g(x) := \sum_{k,l: k-l=x} f(k)g(l), \quad f * g(x) := \sum_{k,l: k+l=x} f(k)g(l).$$

Пусть $g: \mathbb{Z}_p \mapsto \mathbb{R}$ – некоторая функция. Введем матрицу, предложенную 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 [6] (предложение 3) и [4] (следствие 16).

ТЕОРЕМА 6. Пусть $g_1, g_2: \mathbb{Z}_p \mapsto \mathbb{R}$ – четные функции и $\{f_\alpha\}$ – собственные функции оператора T^{g_1} . Тогда выполнено равенство

$$\sum_{x,y,z \in \Gamma} g_1(x-y)g_1(x-z)g_2(y-z) = \sum_{\alpha} \mu_{\alpha}^2(T^{g_1}) \langle T^{g_2} f_{\alpha}, f_{\alpha} \rangle.$$

ТЕОРЕМА 7. Пусть $\Gamma_1, S_2, S_3 \subseteq \mathbb{Z}_p^*$ – Γ -инвариантные множества, причем Γ_1 – смежный класс по Γ и $|S_2||S_3| \leq t^4/16$. 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 $\Gamma_1, \Gamma_2, \dots$ обозначим смежные классы группы $\mathbb{Z}_p^*$ по подгруппе Γ . Будем считать Γ_0 – это класс, состоящий из нулевого элемента. Соответственно, пусть ξ_i – представители этих классов. Обозначим также

$$\begin{aligned} N_4(y) &= |\{x_1 + x_2 - x_3 - x_4 \equiv y \pmod{p}, x_i \in \Gamma\}|, \\ N_3(y) &= |\{x_1 + x_2 - x_3 \equiv y \pmod{p}, x_i \in \Gamma\}|, \\ a_{i,j} &= |\{g_i - g \equiv \xi_j \pmod{p}, g_i \in \Gamma_i, g \in \Gamma, \xi_j \in \Gamma_j \text{ фиксированы}\}|. \end{aligned}$$

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

ЛЕММА 8. Пусть $\{\xi_j\}$, $j \leq t$, принадлежат различным ненулевым смежным классам Γ_{σ_j} и $N_4(\xi_j)$ не возрастают 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:

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

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 Γ_i (и нулевому тоже). Далее,

$$\sum_{1 \leq j \leq J} N_4(\xi_j) = \sum_i N_3(x_i)s_i, \quad \text{где} \quad s_i = \sum_{1 \leq j \leq J} a_{i,\sigma_j}.$$

Разберемся со слагаемым, соответствующим $i = 0$. 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

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

Будем разбивать сумму $\sum_i N_3(x_{i_r})s_{i_r}$ на две части: $1 \leq i \leq i_0$, $i \geq i_0$. Обозначим эти суммы через σ_1 , σ_2 . Разберемся с первой суммой σ_1 :

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

Применяя преобразование Абеля к этой сумме, мы получаем

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

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

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

Если $ij \leq t^2/16$, то заявленная оценка следует из теоремы 7. Пусть теперь $iJ > t^2/16$. Вспоминаем, что $J \leq t$. Тогда в этом случае из простых соображений S_i оценить можно так:

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

Тем самым, оценка на S_i верна всегда при ограничении $J < t$. Для первой суммы σ_1 мы получаем оценку $\sigma \ll T_3^{1/2}t^{1/6}J^{2/3}i_0^{1/6}$.

Теперь разберемся с суммой σ_2 :

$$\sigma_2 \leq \sum_{i > i_0} \left(\frac{t^2}{i} \right) s_i.$$

Опять применяя преобразование Абеля, получаем

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

Выбирая параметр $i_0 := t^5/T_3(\Gamma)$, мы завершаем доказательство леммы 8.

2.2. Доказательство теоремы 4. Пусть ненулевые смежные классы C_j по подгруппе Γ расположены таким образом, что числа $t_j := N_4(y)$, $y \in C_j$, образуют невозрастающую последовательность.

Прежде всего, мы можем считать, что

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

где M – некоторая константа. Справедливость этой оценки для $j \leq t$ следует из леммы 8. Пусть теперь $j \geq t$. Тогда

$$t_j \leq \frac{t^3}{j}.$$

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

Далее, по данному натуральному i положим по определению $S_i(x)$ – характеристическая функция множества

$$S_i := \left\{ \bigcup_j C_j : \frac{MtT_3^{1/3}(\Gamma)}{2^i} < t_j \leq \frac{MtT_3^{1/3}(\Gamma)}{2^{i-1}} \right\},$$

а также определим функции

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

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. Будем вместо $T_3^{(i)}(\Gamma)$ иногда писать просто $T_3^{(i)}$.

С другой стороны, $T_3^{(i)}(\Gamma)$ можно “выразить через оператор”:

$$\begin{aligned} \langle T^{g_i} \Gamma, \Gamma \rangle &= \sum_{x, y \in \Gamma} (\Gamma * \Gamma) \circ (\Gamma * \Gamma)(x - y) S_i(x - y) \\ &= \sum_{z \in S_i} ((\Gamma * \Gamma) \circ (\Gamma * \Gamma))(z) (\Gamma \circ \Gamma)(z) = T_3^{(i)}. \end{aligned}$$

Далее, имеем $T_3^{(i)} = \langle T^{g_i} \Gamma, \Gamma \rangle \leq \mu_0(T^{g_i})t$. Итак, $T_3^{(i)}/t \leq \mu_0(T^{g_i})$.

Наша цель – оценить величину $\mu_0(T^{g_i})$. Для этого воспользуемся теоремой 6 и неотрицательностью оператора T^g . Получим (f_α – собственные функции оператора T^{g_i}):

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

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

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

где

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

Итак, мы заключаем, что

$$\left(\frac{T_3^{(i)}}{t}\right)^3 \leq \sum_{\alpha, \beta} g_i(\alpha) g_i(\beta) g(\beta - \alpha) C_3(\alpha, \beta).$$

Оценим сверху вклад слагаемых (α, β) , для которых $g(\beta - \alpha) \leq d$ (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 Γ . Сумма $\sum_{x \in \Gamma} (\Gamma * g_i)(x)$, как можно заметить, равна $T_3^{(i)}$. Поэтому $(\Gamma * g_i)^2(x) = (T_3^{(i)}/t)^2$.

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

$$\left(\frac{T_3^{(i)}}{t}\right)^3 \ll \sum_{\alpha, \beta: g(\beta - \alpha) \geq T_3^{(i)}/(2t^2)} g_i(\alpha) g_i(\beta) g(\beta - \alpha) C_3(\alpha, \beta).$$

Обозначим последнюю сумму через σ и оценим ее по неравенству Коши:

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

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 следующая оценка этой суммы [6]:

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

Оценим теперь первую сумму. Мы разбиваем сумму на части, определенные следующим образом: при $\alpha \in S_i$, $\beta \in S_i$, $\beta - \alpha \in S_k$ (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

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

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 7. Мы указывали на то, что можно считать $t_j \leq CT_3^{1/3}(\Gamma)j^{-1/3}$. 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 $|S_i| > t^2/4$ эту величину 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

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

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 есть в точности аддитивная энергия группы Γ ,

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

Известна оценка на нее – см., например, [4]: $T_2(\Gamma) \ll t^{5/2}$ при $t < p^{2/3}$.

Несложно показать, что $|S_i| \ll t^{2^{3i}}$, поэтому,

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

Мы можем считать, что

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

В противном случае получаем

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

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

В итоге мы выводим оценку

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

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

$$2^k \ll \frac{t^3 (\log t)^{1/3}}{T_3^{(i)2/3}}.$$

Итак, собирая все вместе, мы выводим, что

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

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

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

Отсюда получаем оценку

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

Значит, имеется оценка

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

Тем самым оценку на $T_3(\Gamma)$ мы показали.

2.3. Приложение тригонометрических сумм и величин T_k для оценки наибольшего расстояния между соседними элементами смежных классов по подгруппе. Для мультипликативной группы $\Gamma \subseteq \mathbb{Z}_p^*$ порядка t введем как в [1] 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 [1] (теорема 3).

ТЕОРЕМА 9. Для $t \geq p^{1/2}$ имеет место оценка

$$H_p(t) \leq p^{463/504+o(1)}, \quad p \rightarrow \infty.$$

Новые оценки для T_k и для тригонометрических сумм по подгруппам позволяют усилить этот результат. А именно, имеет место такая

ТЕОРЕМА 10. Для $t \geq p^{1/2}$ выполнена оценка

$$H_p(t) \leq p^{5977/6552+o(1)}, \quad p \rightarrow \infty.$$

Заметим,

$$\frac{463}{504} = 0.91865\dots, \quad \frac{5977}{6552} = 0.91224\dots$$

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

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

Здесь первая и вторая величины – это соответственно смежный класс и тригонометрическая сумма по нему.

Связь между $H_p(t)$, $N_{j,t}$, $S_j(t)$ дается следующим утверждением (лемма 7.1) [2], которое мы приводим ниже.

ТЕОРЕМА 11. Если для некоторого $h \geq 1$ неравенство

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

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

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

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

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

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

Оценка этой величины нам понадобится для доказательства теоремы 10. Приведем ниже теорему 1 работы [1] для оценки $N(\Gamma, h)$.

ТЕОРЕМА 12. Пусть $\nu \geq 1$ – фиксированное целое, $|\Gamma| \gg p^{1/2}$, $p \rightarrow \infty$. Тогда справедлива оценка

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

Теперь мы готовы вывести теорему 10.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 10. Как и ранее, $t := |\Gamma|$. Для случая $t > 0.7p^{2/3}$ в работе [1] показано, что

$$H_p(t) \leq p^{5/6+o(1)}.$$

Остаются случаи, когда $p^{1/2} \leq t \leq 0.7p^{2/3}$. Вновь рассмотрим случай, когда $p^{49/78} \leq t \leq 0.7p^{2/3}$. Будем пользоваться теоремой 11. Применим оценку на тригонометрическую сумму по подгруппе Γ из теоремы 3 и оценим так:

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

Поэтому h можно взять $[p^{23/156-\varepsilon}]$ для некоторого малого $\varepsilon > 0$. В этом случае по теореме 11:

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

Поэтому при $p^{49/78} \leq t \leq 0.7p^{2/3}$ теорема 10 верна.

Теперь рассмотрим последний случай

$$p^{1/2} \leq t \leq p^{49/78}.$$

Вновь пользуемся теоремой 11 и неравенством Гёльдера. Имеем

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

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

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

Для оценки второй суммы воспользуемся теоремой 12 с $\nu = 6$. Несложно убедиться, что при выбранном h и $p^{1/2} \leq t \leq p^{49/78}$ первое слагаемое в неравенстве теоремы 12 доминирует. Итак, получаем

$$\begin{aligned} \sum_{1 \leq j \leq n} N_{j,t}(h)^2 &= N(\Gamma, h) \leq ht^{13/84} p^{-1/14+o(1)}, \\ \sum_{1 \leq j \leq n} |S_j(t)|^4 &< \frac{p}{t} T_2(\Gamma) < pt^{19/13+o(1)}. \end{aligned}$$

В последнем неравенстве мы применили оценку на $T_2(\Gamma)$ из теоремы 3.

Собирая все вместе, получим

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

Несложно убедиться, что при $t \geq p^{1/2}$ и для выбранного h правая часть меньше $0.5t$. Этим завершается доказательство теоремы 10.

3. Оценки тригонометрических сумм по модулю p^3 и их применение к задаче делимости частных Ферма

3.1. Оценка тригонометрической суммы по модулю p^3 . Пусть G – подгруппа $\mathbb{Z}_q^*$. Тригонометрическими суммами по подгруппе G называются суммы вида $S(a, G) := \sum_{x \in G} e_q(ax)$. Наша задача состоит в оценке величины

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

для подгруппы G порядка $p-1$. Обозначим через G_r подгруппы в $\mathbb{Z}_{p^r}^*$ порядка $p-1$.

Метод, описанный в работе [9], позволяет получать нетривиальные оценки для $S(G_r)$. В частности, было отмечено, что $T_k(G_{r+1}) \leq T_k(G_r)$ выполняется для всех k . С помощью леммы 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 13. *Имеет место оценка*

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

Для доказательства нам будут нужны следующие результаты Шкрёдова из работ [6], [10] соответственно.

ТЕОРЕМА 14. *Имеют место оценки*

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

Теперь дадим доказательство теоремы 13.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 13. Получим сначала такую оценку:

$$T_3(G_2) < p^{4(5/39)+o(1)}.$$

Мы имеем

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

Разберемся со вторым слагаемым. Лемма 11 работы [11] 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

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

Поэтому

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

Теперь разберемся с первым слагаемым. Имеем

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

Известно [2], 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 14, мы получим

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

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

$$T_3(G_3) \leq T_3(G_2) < p^{4(5/39)+o(1)}.$$

Теперь, применяя неравенство леммы 1 при $k = l = 3$, мы получим

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

3.2. Постановка задачи делимости частных Ферма. Для простого p и целого a , $(a, p) = 1$, определяется *частное Ферма*:

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

В ряде работ изучается условие делимости $q_p(a)$ на p . Нас будет интересовать наименьшее a , для которого не выполнено сравнение

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

Для простого p обозначим это число $l_p^{(3)}$.

В ряде работ рассматривалось свойство делимости частных Ферма на p . Обозначим через $l_p^{(2)}$ наименьшее a , для которого не выполнено сравнение $q_p(a) \equiv 0 \pmod{p}$. Приведем некоторые недавние результаты из работы Шкредова [10].

ТЕОРЕМА 15. *Выполнено неравенство*

$$l_p^{(2)} \leq (\log p)^{7829/4284+o(1)}, \quad p \rightarrow \infty.$$

Более старый показатель 463/252 был улучшен до 7829/4284 благодаря новой оценке энергии соответствующей подгруппы, полученной Шкредовым.

Одна из наших целей доказать теорему о делимости частных Ферма на квадрат простого числа, а также вывести ряд вспомогательных утверждений.

ТЕОРЕМА 16. *Имеет место неравенство*

$$l_p^{(3)} \leq (\log p)^{2077/1404+o(1)}.$$

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, $p^2 \mid q_p(a)$ тогда и только тогда, когда $a \in G$.

Напомним определение из работы [1]. Пусть дана произвольная мультипликативная подгруппа G в $\mathbb{Z}_n^*$. Для целого K и натурального k мы определяем

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

Мы будем пользоваться утверждением, доказанным в [1].

ЛЕММА 17. *Пусть имеется подгруппа G порядка t группы $\mathbb{Z}_n^*$. Тогда для любого $\varepsilon > 0$ мы имеем неравенство*

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

где

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

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

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

3.3. Доказательство теоремы 16. 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 [14]

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

Предположим, что $l_p^{(3)} = (\log p)^\alpha$ и также $k = p^\beta$, α, β – некоторые значения. Мы предположили, что все числа $[1, l_p^{(3)}]$ принадлежат нашей подгруппе G . Мы замечаем, что

$$N_p(k) \geq \psi(k, l_p^{(3)}) = p^{\beta(1-1/\alpha)+o(1)}, \quad p \rightarrow \infty.$$

Оценим теперь $N_p(k)$ сверху, используя теорему 15:

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

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

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

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 Шкредов.

Для обратимых элементов по теореме 12 тригонометрическую сумму можно оценить величиной $p^{673/702+o(1)}$.

Итак,

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

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

Значит,

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

Теперь берем $k = p^{2(673/702)+2\varepsilon}$, $\beta = 2(673/702)$. В таком случае получаем

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

Отсюда и в силу произвольности $\varepsilon > 0$ мы заключаем, что

$$\alpha \leq \frac{2077}{1404} + o(1), \quad p \rightarrow \infty.$$

Теорема 16 доказана.

4. Соотношения, включающие произведение интервалов и множеств с малым мультипликативным удвоением по произвольному модулю

4.1. Формулировка результата. Целью этого пункта является получение точной верхней оценки для второго момента величины $M_m(\omega, Z, G)$, где G – произвольное множество с малым мультипликативным удвоением, $|G|$, Z связаны некоторыми ограничениями, а m – некоторое целое число.

Несложно заметить, что

$$\sum_{\omega} M_m^2(\omega, Z, G) = t |\{ux \equiv y \pmod{m}, 0 < |x|, |y| \leq Z, u \in G\}|.$$

Подобная величина уже встречалась в задаче об оценке $H_p(t)$ – там сравнение было по простому модулю. Величина $N(n, G, Z)$ и ее приложения изучались в работах [1] и [8]. Рассматривались соответственно случаи, когда G – подгруппа и множество с малым мультипликативным удвоением. Приведем соответствующую теорему 1, часть (i) из работы [8].

ТЕОРЕМА 18. Пусть $U \subseteq \mathbb{Z}_p^*$ и n, H – натуральные числа такие, что

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

Тогда число решений J сравнения

$$ux \equiv y \pmod{p}, \quad 1 \leq x, y \leq H, \quad u \in U,$$

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

Как замечено в работе [8], условие $|U * U| < 10|U|$ можно ослабить до $|U * U| < |U|^{1+o(1)}$. Следуя работе [8], мы можем показать справедливость следующей теоремы.

ТЕОРЕМА 19. Пусть $U \subseteq \mathbb{Z}_m^*$ и n, H – натуральные числа такие, что

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

Тогда число решений J сравнения

$$ux \equiv y \pmod{m}, \quad 1 \leq x, y \leq H, \quad u \in U,$$

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

4.2. Вспомогательные утверждения. Нам понадобится следующая лемма, доказанная в [1].

ЛЕММА 20. Пусть

$$A = \left\{ \frac{r}{s} : 1 \leq r, s \leq Q, \gcd(r, s) = 1 \right\}$$

и k – натуральное число. Тогда для достаточно большого Q верно

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

где $C(k)$ – некоторая функция, зависящая только от k .

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

Для следующей леммы потребуются некоторые определения. Пусть дана решетка Γ 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 λ такое, что λD содержит i линейно независимых векторов решетки Γ . Известно [12], что верно такое утверждение.

ЛЕММА 21. Справедливо неравенство

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

Для доказательства также будет нужна следующая лемма.

ЛЕММА 22. Для произвольного $s_0 \in \mathbb{Z}_m$ количество решений J сравнения

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

оценивается величиной $O(1 + XY/m)$.

Лемма 22 доказывается абсолютно аналогично лемме 2 работы [8]. Для полноты картины мы приведем полное доказательство леммы 22.

ДОКАЗАТЕЛЬСТВО. Определим решетку Γ и тело D

$$\Gamma = \{(u, v) \in \mathbb{Z}^2, u \equiv s_0 v \pmod{m}\}, \quad D = \{(u, v) \in \mathbb{R}^2, |u| \leq X, |v| \leq Y\}.$$

Пусть числа λ_1, λ_2 являются последовательными минимумами тела D решетки Γ . Если $\lambda_2 > 1$, то $J \leq 1$. В этом случае все доказано.

Пусть теперь $\lambda_2 \leq 1$. Тогда по лемме 21 мы имеем

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

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 Γ . Несложно заметить, что каждый смежный класс есть совокупность $(u, v) \in \mathbb{Z}^2$ для которых фиксированно значение $u - s_0 v \pmod{m}$. Таким образом, этих смежных классов ровно m .

Итак,

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

Отсюда следует исходная оценка на величину J . Лемма 22 доказана.

Для доказательства теоремы 19 нам будет удобно еще одно утверждение сформулировать в виде отдельной леммы. Ее вывод приведен в доказательстве теоремы 1 [8].

ЛЕММА 23. Пусть u, h, m, n – натуральные числа такие, что

$$u < m^{n/(2n+1)}, \quad uh^n < m.$$

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

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

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

4.3. Доказательство теоремы 19. Рассмотрим 2 случая.

1) 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

$$\left| \left\{ ux \equiv y \pmod{m} : 1 \leq x, y \leq \frac{H}{d}, \gcd(x, y) = 1 \right\} \right|.$$

Обозначим эту величину $J_d(H)$. Достаточно доказать, что для любого $\delta > 0$ существует такое $c(\delta) > 0$, что выполняется

$$J_d(H) \leq c(\delta) \frac{H}{d} m^\delta \quad \text{для любого } d.$$

Фиксируем какое-нибудь $\delta > 0$. Так как $J_d(H) \leq (H/d)^2$, то мы можем считать, что $H/d \geq m^\delta$. Согласно лемме 23 для $h' := H/d$ существует такое натуральное $k \leq 1/\delta$, что

$$|U| \leq \left(\frac{H}{d}\right)^k \leq \frac{m}{|U|}.$$

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

$$J_d := \left\{ \frac{y}{x} : 1 \leq x, y \leq \frac{H}{d}, \gcd(x, y) = 1, \gcd(m, xy) = 1, \frac{y}{x} \pmod{m} \in U \right\}.$$

Теперь

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

Так как $|U * U| < |U|^{1+o(1)}$, то, пользуясь неравенством Плюннеке [13] (теорема 7.7), получаем $|U^{(k)}| < |U|^{1+o(1)}$. Используя это и лемму 22, оценим сверху размер множества $J_d^{(k)}$. Имеем

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

С другой стороны, по лемме 20 $|J_d^{(k)}| m^{o(1)} \geq |J_d|^k$, причем множитель $m^{o(1)}$ можно выбрать одинаковым для всех d таких, что $H/d > m^\delta$. Поэтому существует такая $c(\delta) > 0$, что для всех d выполнено

$$|J_d| = J_d(H) \leq c(\delta) \left(\frac{H}{d}\right) m^\delta.$$

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 $c(\delta) > 0$ такое, что для произвольного $m' | m$ число решений сравнения

$$ux \equiv y \pmod{m}, \quad 1 \leq x, y \leq H, \quad \gcd(x, m) = \gcd(y, m) = m', \quad u \in U, \quad (1)$$

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

Обозначим

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

В этом случае число решений (1) равно

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

где

$$N(u') := \left| \left\{ u \in Uu \equiv u' \left(\bmod \frac{m}{m'} \right) \right\} \right|,$$

$$M(u') := \left| \left\{ (x, y) : \gcd\left(xy, \frac{m}{m'}\right) = 1, 1 \leq x, y \leq \frac{H}{m'}, \frac{y}{x} \equiv u' \left(\bmod \frac{m}{m'} \right) \right\} \right|.$$

Пусть

$$U' = \bigcup_{j \in \mathbb{N}: 2^{j-1} \leq m'} U'_j, \quad \text{где } U'_j = \{u' \in U' : N(u') \in [2^{j-1}; 2^j)\}.$$

Тогда

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

Нам достаточно показать существование $c(\delta)$ такой, что для любых допустимых m', j выполняется неравенство

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

Если обозначить

$$J_{m',j} := \left\{ (x, y) : 1 \leq x, y \leq \frac{H}{m'}, \gcd\left(xy, \frac{m}{m'}\right) = 1, \frac{y}{x} \in U'_j \left(\bmod \frac{m}{m'} \right) \right\},$$

то условие (2) переписывается так:

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

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

$$J_{m',j,d} := \left\{ \frac{y}{x} : 1 \leq x, y \leq \frac{H}{m'd}, \gcd\left(xy, \frac{m}{m'}\right) = 1, \gcd(y, x) = 1, \frac{y}{x} \in U'_j \left(\bmod \frac{m}{m'} \right) \right\}.$$

Достаточно показать, что существует $c(\delta)$ такая, что для любых рассматриваемых m', j, d выполняется

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

Так как $|J_{m',j,d}| \leq (H/m'd)^2$, то можно считать, что $H/m'd \geq m^\delta$.

Возьмем произвольное натуральное k . Имеем

$$J_{m',j,d}^{(k)} \subseteq \left\{ \frac{u}{v} : \gcd\left(uv, \frac{m}{m'}\right) = 1, \right.$$

$$\left. \gcd(u, v) = 1, 1 \leq u, v \leq \left(\frac{H}{m'd}\right)^k, \frac{u}{v} \in U_j'^{(k)} \left(\bmod \frac{m}{m'} \right) \right\}.$$

Пользуясь леммой 21, получаем

$$|J_{m',j,d}^{(k)}| \ll \sum_{r \in U_j'^{(k)}} \left(1 + \frac{(H/m'd)^{2k}}{m/m'} \right) \leq |U_j'^{(k)}| \left(1 + \frac{(H/m'd)^{2k}}{m/m'} \right).$$

Покажем, что

$$|U_j'^{(k)}| \ll \frac{|U|^{1+o(1)}}{2^j}. \quad (3)$$

Для каждого $u' \in U_j'^{(k)}$ имеется представление $u' = u'_1 * \dots * u'_k$, $u'_i \in U_j'$. Для каждого u'_i имеется не менее 2^{j-1} элементов $u \in U$ таких, что $u \equiv u'_i \pmod{m/m'}$. Так как U состоит только из обратимых элементов, то для u' имеется не менее 2^{j-1} элементов $u \in U^{(k)}$ таких, что $u \equiv u' \pmod{m/m'}$. Ранее было показано, что $|U^{(k)}| \leq |U|^{1+o(1)}$. Отсюда получаем неравенство (3).

Теперь мы выберем k . Согласно лемме 23 для $h' := H/dm'$ существует такое натуральное $k \leq 1/\delta$, что

$$|U| \leq \left(\frac{H}{dm'} \right)^k \leq \frac{m}{|U|}.$$

Таким образом, мы получаем, что для такого k

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

С другой стороны по лемме 20 мы имеем $|J_{m',j,d}^{(k)}| \geq |J_{m',j,d}|^k m^{o(1)}$, причем множитель $m^{o(1)}$ может быть выбран одним и тем же для всех параметров m', j, d с условием $H/(m'd) > m^\delta$. Сопоставляя последние оценки, мы получаем, что неравенство

$$|J_{m',j,d}| \leq c(\delta) \left(\frac{H}{d2^j} \right) m^\delta$$

выполняется для всех рассматриваемых m', j, d . Таким образом, второй случай мы полностью рассмотрели. Теорема 19 доказана.

4.4. Комментарии к теореме 19. Мы отмечаем, что условие $1 \leq x, y \leq H$ можно заменить на такое: $1 \leq |x|, |y| \leq H$.

Получим оценку снизу на число решений сравнения

$$ux \equiv y \pmod{m}, \quad 1 \leq |x|, |y| \leq H, \quad u \in U. \quad (4)$$

Фиксируем произвольное $u \in U$ и рассмотрим величины $ux - y \pmod{m}$, когда $1 \leq x, y \leq H$. Всего таких различных пар (x, y) найдется H^2 . Будем считать, что $H^2 \geq 10m$. Поэтому найдется s пар (x, y) , $s \geq H^2/m$, таких, что выражение $ux - y \pmod{m}$ принимает одно и то же значение. Обозначим эти пары $(x_1, y_1), \dots, (x_s, y_s)$. Несложно заметить, что пары $(v_i, w_i) = (x_i - x_1, y_i - y_1)$, $i = 2, \dots, s$, удовлетворяют сравнению $uv_i \equiv w_i \pmod{m}$. Таким образом, у нас имеется не менее $|U|H^2/(2m)$ решений сравнения (4).

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

$$|U|H < m$$

нельзя ослабить до

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

ни для какого фиксированного $\delta > 0$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] J. Bourgain, S. V. Konyagin, I. E. Shparlinski, “Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm”, *Int. Math. Res. Not. IMRN*, 2008, rnn090.
- [2] S. V. Konyagin, I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Tracts in Math., **136**, Cambridge Univ. Press, Cambridge, 1999.
- [3] A. García, J. F. Voloch, “Fermat curves over finite fields”, *J. Number Theory*, **30**:3 (1988), 345–356.
- [4] 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, Изд-во Моск. ун-та, 2002, 86–114.
- [5] J. Bourgain, S. V. 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), 75–80.
- [6] I. D. Shkredov, “On exponential sums over multiplicative subgroups of medium size”, *Finite Fields Appl.*, **30** (2014), 72–87.
- [7] I. D. Shkredov, “Some new inequalities in additive combinatorics”, *Mosc. J. Comb. Number Theory*, **3**:3-4 (2013), 189–239.
- [8] J. Cilleruelo, M. Z. Garaev, *Congruences Involving Product of Intervals and Sets with Small Multiplicative Doubling Modulo a Prime and Applications*, arXiv: 1404.5070.
- [9] Ю. В. Мальхин, “Оценки тригонометрических сумм по модулю p^r ”, *Матем. заметки*, **80**:5 (2006), 793–796.
- [10] I. D. Shkredov, “On Heilbronn’s exponential sum”, *Q. J. Math.*, **64**:4 (2013), 1221–1230.
- [11] J. Bourgain, K. Ford, S. V. Konyagin, I. E. Shparlinskii, “On the divisibility of Fermat quotients”, *Michigan Math. J.*, **59**:2 (2010), 313–328.
- [12] U. Betke, M. Henk, J. M. Wills, “Successive-minima-type inequalities”, *Discrete Comput. Geom.*, **9**:2 (1993), 165–175.
- [13] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math., **165**, Springer, New York, 1996.
- [14] S. Konyagin, C. Pomerance, “On primes recognizable in deterministic polynomial time”, *The Mathematics of Paul Erdős*, Vol. I, Algorithms Combin., **13**, Springer-Verlag, Berlin, 176–198.

Ю. Н. Штейников

Математический институт им. В. А. Стеклова

Российской академии наук

E-mail: yuriisht@yandex.ru

Поступило

18.11.2014

Исправленный вариант

18.03.2015