Оценки тригонометрических сумм по модулю p^2

Ю. В. МАЛЫХИН
Московский государственный университет им. М. В. Ломоносова
e-mail: jura05@narod.ru

УДК 511.321

Ключевые слова: тригонометрические суммы, метод Степанова.

Аннотация

В работе рассматриваются тригонометрические суммы по подгруппам $G \subset \mathbb{Z}_q^*$. С помощью метода Степанова получены нетривиальные оценки тригонометрических сумм в случае, когда q есть квадрат простого числа.

Abstract

Yu. V. Malykhin, Bounds for exponential sums modulo p^2, Fundamentalnaya i prikladnaya matematika, vol. 11 (2005), no. 6, pp. 81—94.

In this paper we consider exponential sums over subgroups $G \subset \mathbb{Z}_q^*$. Using Stepanov's method, we obtain nontrivial bounds for exponential sums in the case, where q is a square of a prime number.

1. Введение

1.1. Для натурального q через $\mathbb{Z}_q$ мы будем обозначать кольцо вычетов по модулю q, а через $\mathbb{Z}_q^*$ — мультипликативную группу этого кольца. Для $x \in \mathbb{Z}_q$ обозначим $e_q(x) := e^{2\pi i x/q}$.

Пусть G — подгруппа $\mathbb{Z}_q^*$, $\#G = t$, $a \in \mathbb{Z}_q$. Тригонометрическими суммами по подгруппе G называются суммы вида

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

Положим

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

Наша задача будет состоять в оценке величины $S(G)$ в случае, когда q есть квадрат простого числа: $q = p^2$ (здесь и далее p обозначает простое число, большее 2). Заметим, что в этом случае группа $\mathbb{Z}_q^*$ циклична, так что G однозначно определяется по t.

Фундаментальная и прикладная математика, 2005, том 11, № 6, с. 81—94.

При достаточно больши́х t оценки тригонометрических сумм по подгруппам $G \subset \mathbb{Z}_q^*$ основаны на оценке величин

$$T_k(G) := \#\{(x_1, \ldots, x_{2k})\colon x_1 + \ldots + x_k = x_{k+1} + \ldots + x_{2k} \pmod q,\ x_i \in G\}.$$

Имеет место следующая лемма.

Лемма (основное неравенство). *Для любых натуральных k и l*

$$S(G) \leqslant (qT_k(G)T_l(G))^{1/2kl} t^{1-1/k-1/l}.$$

Оценки такого типа установлены И. М. Виноградовым для тригонометрических сумм Вейля (см. [4, § 15]). Также такие оценки встречались в работах А. А. Карацубы [1, 2]. В явном виде неравенство сформулировано и доказано в [11].

Замечание. $S(G) \leqslant \min(t, \sqrt{q})$. Неравенство $S(G) \leqslant t$ очевидно, неравенство $S(G) \leqslant \sqrt{q}$ получается из основного неравенства при $k = l = 1$ (так как $T_1(G) = t$).

1.2. Наиболее хорошо исследован случай простого $q = p$. Заметим, что в этом случае суммы Гаусса

$$S_n(a, p) := \sum_{x=1}^{p} e_p(ax^n)$$

легко выражаются через суммы по подгруппам. Действительно, взяв $G = \{x^n\colon x \in \mathbb{Z}_p^*\}$, получим, что

$$S_n(a, p) = 1 + (n, p-1)S(a, G).$$

Пользуясь методом С. А. Степанова [5] для оценки T_2, Д. Р. Хиф-Браун и С. В. Конягин [10] получили следующие оценки тригонометрических сумм для $G \subset \mathbb{Z}_p^*$:

$$S(G) \ll \begin{cases} p^{1/8}t^{5/8}, & p^{1/3} < t < p^{1/2}, \\ p^{1/4}t^{3/8}, & p^{1/2} < t < p^{2/3}. \end{cases}$$

Таким образом, при $t > p^{1/3+\varepsilon}$ выполняется неравенство $S(G) \ll tp^{-\delta(\varepsilon)}$, т. е. имеется нетривиальная по порядку оценка на $S(G)$. До этого аналогичное неравенство было известно при $t > p^{3/7+\varepsilon}$ (И. Е. Шпарлинский [6]).

Используя T_k для всех $k \in \mathbb{N}$, С. В. Конягин [3] доказал, что при $t > p^{1/4+\varepsilon}$ выполнено неравенство

$$S(G) < C(\varepsilon)tp^{-\delta(\varepsilon)} \tag{1}$$

(для некоторых функций $C(\varepsilon) > 0$ и $\delta(\varepsilon) > 0$). Существенное продвижение было сделано в работе Ж. Бургейна и С. В. Конягина [8]: используя дополнительные комбинаторные соображения, они доказали (1) при $t > p^{\varepsilon}$.

Оказывается, оценка типа (1) верна и для тригонометрических сумм по произвольному модулю.

Теорема (Бургейн [7]). *Пусть $G \subset \mathbb{Z}_q^*$, $\varepsilon > 0$ таковы, что $t > q^{\varepsilon}$. Тогда*

$$S(G) < C(\varepsilon) t q^{-\delta(\varepsilon)}.$$

Замечание. В [7, 8] показатель δ достаточно мал, так что можно ожидать, что оценки, полученные методом Степанова при достаточно больших t, не перекрываются.

Методы из [3, 10] будут использованы в этой работе для получения аналогичных оценок по модулю p^2.

1.3. Оценки для $q = p^2$ проводились в основном для подгрупп порядка $p-1$, т. е. для $G = \{x^p \colon x \in \mathbb{Z}_{p^2}^*\}$. Точнее, изучалась сумма Хейльбронна

$$H_p(a) := \sum_{x=1}^{p} e_{p^2}(ax^p)$$

(ясно, что $H_p(a) = S(a, G) + 1$). Долгое время было неизвестно, верно ли, что $|H_p(a)| = o(p)$, $p \to \infty$. С помощью оценки $T_2(G)$ Д. Р. Хиф-Браун [9] ответил на этот вопрос, доказав, что $|H_p(a)| \ll p^{11/12}$. В [8] эта оценка была улучшена до $|H_p(a)| \ll p^{7/8}$.

1.4. Пусть теперь G — произвольная подгруппа $\mathbb{Z}_{p^2}^*$, $\#G = t$. Ниже будет показано, что если $t \geqslant p$, то $S(G) = 0$, поэтому нас будет интересовать случай $t < p$. В данной работе доказываются следующие утверждения.

Теорема 1.

$$T_2(G) \ll p^{1/2} t^2 \quad \textit{при} \quad p^{1/2} < t < p.$$

Теорема 2.

$$T_3(G) \ll \begin{cases} p^{3/4} t^{7/2} & \textit{при} \quad p^{1/2} < t < p^{3/4} (\log p)^{-1}, \\ t^{9/2} \log p & \textit{при} \quad p^{3/4} (\log p)^{-1} < t < p. \end{cases}$$

Как следствие этих теорем и основного неравенства получается теорема 3.

Теорема 3.

$$S(G) \ll \begin{cases} (p^7 t^{26})^{1/36} & \textit{при} \quad p^{7/10} < t < p^{3/4} (\log p)^{-1}, \\ p^{1/9} t^{5/6} (\log p)^{1/9} & \textit{при} \quad p^{3/4} (\log p)^{-1} < t < p^{7/9}, \\ (p^5 t^{17})^{1/24} (\log p)^{1/12} & \textit{при} \quad p^{7/9} < t < p^{4/5}, \\ p^{3/8} t^{1/2} & \textit{при} \quad p^{4/5} < t < p. \end{cases}$$

2. Оценка $T_2(G)$

2.1. Пусть G — подгруппа $\mathbb{Z}_{p^2}^*$ порядка t. Тогда $t \mid p(p-1) = \#\mathbb{Z}_{p^2}^*$. Предположим, что $p \mid t$, т. е. $t = t_1 p$, $(p, t_1) = 1$. Рассмотрим подгруппу $G_1 \subset \mathbb{Z}_p^*$ порядка t_1. Ясно, что множество $\{x \in \mathbb{Z}_{p^2} \colon x \bmod p \in G_1\}$ является подгруппой, причём порядка t. Так как порядок однозначно определяет подгруппу, то это

множество и есть G. Поэтому $x \in G$ тогда и только тогда, когда $x + p \in G$, откуда

$$S(a,G) = \sum_{x\in G} e_{p^2}(ax) = \sum_{x\in G} e_{p^2}(a(x+p)) = S(a,G)e_{p^2}(ap).$$

Так как $ap \not\equiv 0 \pmod{p^2}$, получаем $S(a,G) = 0$.

Рассмотрим случай $t \mid p-1$. Пусть $G' := G \bmod p$. Это подгруппа $\mathbb{Z}_p^*$ порядка t, причём $G = \{x^p \colon x \in G'\}$ (поскольку $x = y \pmod p$ тогда и только тогда, когда $x^p = y^p \pmod{p^2}$, то запись корректна). Пусть $g_1, g_2, \ldots, g_d$ — представители смежных классов $G'_1, \ldots, G'_d$ группы $\mathbb{Z}_p^*$ по G' (можно считать $g_1 = 1$).

Пусть R — ассоциативное кольцо с единицей, R^* — его мультипликативная группа. Назовём смежными классами кольца R по подгруппе $H \subset R^*$ множества вида xH, $x \in R$. Ясно, что представители смежных классов $\mathbb{Z}_p$ по G' — это $0, g_1, \ldots, g_d$.

Представителями смежных классов $\mathbb{Z}_{p^2}$ по G являются 0, pg_i, $g_i^p + pj$ ($i = 1, \ldots, d$, $j = 1, \ldots, p$). Для доказательства этого утверждения сначала проверим, что эти элементы лежат в разных смежных классах. Пусть $g \in G$, $g' := g \bmod p$, $g' \in G'$. Имеем

$$(g_i^p + pj)g = (g_k^p + pl) \pmod{p^2} \implies$$
$$\implies g_i g' = g_k \pmod p \implies i = k,\ g' = 1 \implies j = l.$$

Доказательства для остальных представителей аналогичны этому. Теперь заметим, что каждый смежный класс, кроме нулевого, состоит ровно из t элементов. Всего получилось $1 + dt + dpt = 1 + p - 1 + p(p-1) = p^2$ элементов, т. е. всё кольцо.

Исходя из этого, назовём (i,j)-м смежный класс $G_{i,j}$ элемента $g_i^p + pj$. Смежный класс элемента pg_i назовём i-м смежным классом G_i. $\{0\}$ назовём нулевым смежным классом G_0 (здесь и далее i и j обозначают ненулевые числа). В итоге получаем

$$\mathbb{Z}_{p^2} = G_0 \sqcup \bigsqcup_{i=1,\ldots,d} G_i \sqcup \bigsqcup_{\substack{i=1,\ldots,d\\ j=1,\ldots,p}} G_{i,j}, \quad \mathbb{Z}_{p^2}^* = \bigsqcup_{\substack{i=1,\ldots,d\\ j=1,\ldots,p}} G_{i,j}, \quad G = G_{1,p}.$$

2.2. Далее везде будем считать, что $t > p^{1/2}$.

Возьмём фиксированное $u \in G_\beta$ (β может обозначать как один индекс, так и пару). Обозначим

$$n_\beta := N_2(u,G) := \#\{(x_1,x_2) \colon x_1 + x_2 = u \pmod{p^2},\ x_1, x_2 \in G\}$$

(такое определение корректно, т. е. если $u_1, u_2 \in G_\beta$, то $N_2(u_1,G) = N_2(u_2,G)$).

Ясно, что

$$T_2(G) = \sum_{u\in\mathbb{Z}_{p^2}} N_2(u,G)^2 = n_0^2 + t\sum_i n_i^2 + t\sum_{i,j} n_{i,j}^2. \tag{2}$$

Далее мы выразим числа $n_{i,j}$ через мощности некоторых подмножеств $M_{i,j} \subset \subset \mathbb{Z}_p$. Мощность $M_{i,j}$ оценим с помощью метода Степанова.

Легко видеть, что $n_0 \leqslant t$. Покажем, что $n_i = 0$. Пусть $x_1 + x_2 = pg_i \pmod{p^2}$. Возьмём $m, n \in G'$ так, чтобы $x_1 = m^p$, $x_2 = n^p$. Тогда

$$m^p + n^p = pg_i \pmod{p^2} \implies m + n = 0 \pmod{p} \implies m^p = -n^p \pmod{p^2}.$$

Противоречие с условием $g_i \neq 0 \pmod{p}$.

Теперь рассмотрим основной случай. Пусть $u = g_i^p + pj$. Рассмотрим равенство $x_1 + x_2 = u \pmod{p^2}$. Так как $x_1 = m^p$, $x_2 = n^p$, где $m, n \in G'$, получаем $m + n = g_i \pmod{p}$. Решения имеют вид $m = g_i b$, $n = g_i(1-b)$, где $b \in \mathbb{Z}_p$ такие, что $b \in (g_i^{-1})G'$, $1-b \in (g_i^{-1})G'$. Подставляя m и n в исходное равенство, получаем цепочку равенств

$$\begin{aligned} &g_i^p b^p + g_i^p (1-b)^p = g_i^p + pj \pmod{p^2} \iff \\ &\quad \iff 1 + (b-1)^p - b^p = -pjg_i^{-p} \pmod{p^2} \iff \\ &\quad \iff pf(b) = -pjg_i^{-p} \pmod{p^2} \iff f(b) = -jg_i^{-1} \pmod{p}, \end{aligned}$$

где $f(X) = X + \frac{X^2}{2} + \ldots + \frac{X^{p-1}}{p-1}$.

Итак, мы получили, что

$$n_{i,j} = \# M_{i,j},$$

где

$$M_{i,j} := \{b \in \mathbb{Z}_p \colon b \in g_i^{-1}G',\ 1 - b \in g_i^{-1}G',\ f(b) = -jg_i^{-1} \pmod{p}\}.$$

Лемма 1. *Пусть $(i_\sigma, j_\sigma)_{\sigma=1}^s$ — различные пары чисел. Тогда*

$$\sum_{\sigma=1}^{s} n_{i_\sigma, j_\sigma} \ll \min(p^{1/3} t^{1/3} s^{2/3}, t).$$

Доказательство. Ясно, что

$$n_{i,j} = \#\{(x,y) \colon 1 + x = y,\ x \in G,\ y \in G_{i,j}\},$$

откуда

$$\sum_{i,j} n_{i,j} \leqslant t,$$

поэтому при $s > tp^{-1/2}$ неравенство выполнено.

Пусть теперь $s < tp^{-1/2}$. Заметим, что множества $M_{i,j}$ не пересекаются, поэтому

$$\sum_{\sigma=1}^{s} n_{i_\sigma, j_\sigma} = \sum_{\sigma=1}^{s} \# M_{i_\sigma, j_\sigma} = \# \bigcup_{\sigma=1}^{s} M_{i_\sigma, j_\sigma}.$$

Применим метод Степанова для оценки числа элементов

$$M := \bigcup_{\sigma=1}^{s} M_{i_\sigma, j_\sigma}.$$

Рассмотрим полином $\Phi(X,Y,Z)\in\mathbb{Z}_p[X,Y,Z]$. Пусть $\deg_X\Phi<A$, $\deg_Y\Phi<B$, $\deg_Z\Phi<C$. Подберём $\Phi\neq 0$ так, чтобы $\Psi(X)=\Phi(X,f(X),X^t)$ имел нули порядка D в каждой точке $x\in M$ (кроме, возможно, 0 и 1). Отсюда получим $D\#M\ll\deg\Psi(X)<A+pB+Ct$ при условии $\Psi\neq 0$.

Пусть

$$\Phi(X,Y,Z)=\sum\lambda_{a,b,c}X^aY^bZ^c.$$

Тогда

$$\Psi(X)=\sum\lambda_{a,b,c}X^af(X)^bX^{ct}.$$

Заметим, что

$$X^q\frac{d^q}{dX^q}X^a=\frac{a!}{(a-q)!}X^a\qquad(\text{при}\quad q<a),$$
$$X^u\frac{d^u}{dX^u}X^{ct}=\frac{(ct)!}{(ct-u)!}X^{ct}\quad(\text{при}\quad u<ct).$$

Из [9, лемма 2] следует, что для всякого натурального r найдутся многочлены $q_r(X)$ и $l_r(X)$, такие что

$$\{X(1-X)\}^r\frac{d^r}{dX^r}f(X)=q_r(X)+(X^p-X)l_r(X),\quad\deg q_r\leqslant r+1.$$

Отсюда (мы обозначили $\bar r=(r_1,\dots,r_b)$)

$$\{X(1-X)\}^n\frac{d^n}{dX^n}(X^af(X)^bX^{ct})=$$
$$=\{X(1-X)\}^n\sum_{\substack{q+r_1+\ldots+r_b+u=n\\ q,r_i,u\geqslant 0}}C_{q,\bar r,u}\frac{d^q}{dX^q}X^a\frac{d^u}{dX^u}X^{ct}\prod_{j=1}^b\frac{d^{r_j}}{dX^{r_j}}f(X)=$$
$$=(X^p-X)l_{a,b,c}(X)+$$
$$+\sum_{\substack{q+r_1+\ldots+r_b+u=n\\ q,r_i,u\geqslant 0}}C_{a,b,c,q,\bar r,u}X^aX^{ct}(1-X)^{q+u}f(X)^{b-\#\{j\colon r_j\neq 0\}}\prod_{j\colon r_j\neq 0}q_{r_j}(X).$$

Поскольку на M_{i_σ,j_σ} многочлены X^t и $f(X)$ постоянны, то при $x\in M_{i_\sigma,j_\sigma}$

$$\{X(1-X)\}^n\left.\frac{d^n}{dX^n}X^af(X)^bX^{ct}\right|_{X=x}=P_{n,\sigma,a,b,c}(x),$$

где $P_{n,\sigma,a,b,c}(X)$ — многочлен степени ниже $A+2D$. Отсюда при $x\in M_{i_\sigma,j_\sigma}$

$$\{X(1-X)\}^n\left.\frac{d^n}{dX^n}\Psi(X)\right|_{X=x}=P_{n,\sigma}(x),$$

где коэффициенты полиномов $P_{n,\sigma}$ суть линейные функции от коэффициентов Φ и $\deg P_{n,\sigma}(X)<A+2D$. Равенство этих полиномов нулю при всех $n<D$ и $1\leqslant\sigma\leqslant s$ даёт $sD(A+2D)$ линейных уравнений на коэффициенты Φ, поэтому если $sD(A+2D)<ABC$, то найдётся $\Phi\neq 0$ с нужными нам свойствами. Как

следует из [9, доказательство леммы 3], условие $\Psi \neq 0$ будет выполнено, если $AB \leqslant t$. Нам подходят следующие A, B, C, D:

$$A = \lfloor p^{1/3}t^{1/3}s^{-1/3} \rfloor, \quad B = \lfloor p^{-1/3}t^{2/3}s^{1/3} \rfloor, \quad C = \lfloor p^{2/3}t^{-1/3}s^{1/3} \rfloor,$$
$$D = \left\lfloor \frac{1}{8} p^{1/3}t^{1/3}s^{-1/3} \right\rfloor.$$

Остаётся проверить, что $A, B, C, D > 0$, но при достаточно большом p это следует из неравенств $t > p^{1/2}$ и $s < tp^{-1/2}$. □

Замечание к лемме 1. При доказательстве мы использовали в определении множеств $M_{i,j}$ лишь первое и третье условия. Возможно, использовав второе условие, можно будет получить $\#M \ll (ts)^{2/3}$. Впрочем, при $s < p^3t^{-4}$ это неравенство вытекает из первого и второго свойств (см. [10]).

Доказательство теоремы 1. Переупорядочим числа $n_{i,j}$ в порядке убывания: $n_{i_1,j_1} \geqslant n_{i_2,j_2} \geqslant \ldots \geqslant n_{i_{pd},j_{pd}}$. Из леммы 1 следует, что

$$n_{i_s,j_s} \ll \min(p^{1/3}t^{1/3}s^{-1/3}, ts^{-1}). \tag{3}$$

Обозначим $s_0 := tp^{-1/2}$. Имеем

$$\sum n_{i,j}^2 = \sum_{s=1}^{pd} n_{i_s,j_s}^2 = \sum_{s<s_0} n_{i_s,j_s}^2 + \sum_{s>s_0} n_{i_s,j_s}^2 \ll$$
$$\ll p^{2/3}t^{2/3} \sum_{s<s_0} s^{-2/3} + t^2 \sum_{s>s_0} s^{-2} \ll p^{2/3}t^{2/3}s_0^{1/3} + t^2 s_0^{-1} = 2p^{1/2}t.$$

Поскольку $n_0^2 \leqslant t^2 < p^{1/2}t^2$, то нужная оценка T_2 получена. □

3. Оценка $T_3(G)$

3.1. Возьмём фиксированное $u \in G_\beta$. Обозначим

$$a_\alpha^\beta := \#\{(x_1, x_2) \colon x_1 + x_2 = u,\ x_1 \in G,\ x_2 \in G_\alpha\}.$$

Напомним, что α — это 0, i или (i,j). Аналогично β — это 0, i или (i,j). (Как и раньше, i и j обозначают ненулевые числа.) Ясно, что определение корректно. Легко установить следующие свойства.

Свойства.

1. $a_{1,p}^\beta = n_\beta$.
2. *При* $\beta \neq 0$ *имеем*

$$a_\alpha^\beta = \#\{(x,y) \colon 1 + x = y,\ x \in G_\alpha,\ y \in G_\beta\}. \tag{4}$$

3. *Вырожденные случаи*: *пусть* $-1 \in G'_{i_0} \subset \mathbb{Z}_p$, *т. е.* $-1 = g_{i_0}g' \pmod p$ *для* $g' \in G'$, *откуда* $-1 = (-1)^p = g_{i_0}^p (g')^p \pmod{p^2}$, *значит*, $-1 \in G_{i_0,p} \subset \mathbb{Z}_{p^2}$.

Кроме $a_{i,j}^{k,l}$, ненулевыми являются лишь следующие числа:

$$a_{i(l)}^{1,l}=1\ \ (l\neq p),\quad a_{i_0,j}^{k(j)}=1\ \ (j\neq p),\quad a_0^{1,p}=1,\quad a_{i_0,p}^{0}=t \tag{5}$$

(*для некоторых функций* $i(l),k(j)\colon\{1,\dots,p-1\}\to\{1,\dots,d\}$).

Доказательство. Свойства 1 и 2 очевидны. Рассмотрим свойство 3. Найдём, например, чему равны числа вида $a_i^{k,l}$. Если $x_1\in G$, то $x_1=m^p$, где $m\in G'$. Если $x_2\in G_i$, то $x_2=pg_in^p$, где $n\in G'$. Отсюда

$$\begin{aligned}x_1+x_2=g_k^p+pl\ (\mathrm{mod}\ p^2)\ &\Longrightarrow\ m=g_k\ (\mathrm{mod}\ p)\ \Longrightarrow\\ &\Longrightarrow\ pg_in^p=pl\ (\mathrm{mod}\ p^2)\ \Longrightarrow\ g_in=l\ (\mathrm{mod}\ p).\end{aligned}$$

Значит, если $l\notin G_i'$, то последнее равенство невозможно, т. е. $a_i^{k,l}=0$. Если же $l\in G_i'$, что равносильно тому, что $i=i(l)=$ «номер смежного класса l», то n находится однозначно. Так как $m\in G'$, то $k=1$, и m определяется однозначно, и в этом случае получаем $a_i^{k,l}=1$. Аналогично находятся остальные ненулевые a_α^β. □

Рассмотрим теперь невырожденные случаи, т. е. $a_{i,j}^{k,l}$. Если $x\in G_{i,j}$, то $x=(g_i^p+pj)m^p$, $m\in G'$. Поэтому

$$\begin{aligned}&1+x=y\ (\mathrm{mod}\ p^2)\ \Longleftrightarrow\\ &\Longleftrightarrow\ 1+(g_i^p+pj)m^p=(g_k^p+pl)n^p\ (\mathrm{mod}\ p^2)\ \Longrightarrow\ 1+g_im=g_kn\ (\mathrm{mod}\ p).\end{aligned}$$

Решения имеют вид $m=g_i^{-1}(b-1)$, $n=g_k^{-1}b$, где $b\in\mathbb{Z}_p$ такие, что $b\in G_k'$, $b-1\in G_i'$. Подставляя m и n в исходное равенство, получаем цепочку равенств

$$\begin{aligned}&1+(g_i^p+pj)g_i^{-p}(b-1)^p=(g_k^p+pl)g_k^{-p}b^p\ (\mathrm{mod}\ p^2)\ \Longleftrightarrow\\ &\Longleftrightarrow\ 1+(b-1)^p-b^p=plg_k^{-p}b^p-pjg_i^{-p}(b-1)^p\ (\mathrm{mod}\ p^2)\ \Longleftrightarrow\\ &\Longleftrightarrow\ f(b)=(lg_k^{-1}-jg_i^{-1})b+jg_i^{-1}\ (\mathrm{mod}\ p).\end{aligned}$$

Итак, мы получили, что

$$a_{i,j}^{k,l}=\#M_{i,j}^{k,l}:=\#\{b\in\mathbb{Z}_p\colon b\in G_k',\ b-1\in G_i',\ f(b)=ub+v\},$$

где $u=u(i,j,k,l)=lg_k^{-1}-jg_i^{-1}$ и $v=v(i,j,k,l)=jg_i^{-1}$.

Заметим, что теперь $M_{i_1,j_1}^{k_1,l_1}$ и $M_{i_2,j_2}^{k_2,l_2}$ уже могут пересекаться, правда лишь при $i_1=i_2$ и $k_1=k_2$, но и тогда не более чем по одному элементу.

Для оценки чисел $a_{i,j,k,l}$ нам понадобится вспомогательная лемма.

Лемма 2. *Пусть G' — подгруппа в $\mathbb{Z}_p^*$ порядка t, $G_1',\dots,G_d'$ — её смежные классы. Обозначим*

$$K_{i,k}:=\{x\in\mathbb{Z}_p\colon x\in G_k',\ x-1\in G_i'\}.$$

Тогда при всех i,k выполняется неравенство

$$\#K_{i,k}\ll\begin{cases}t^{2/3} & \text{при } p^{1/2}<t<p^{3/4},\\ t^2p^{-1} & \text{при } p^{3/4}<t.\end{cases}$$

Доказательство. Случай $t < p^{3/4}$ рассмотрен в [10, лемма 5]. Разберём случай $t > p^{3/4}$. Как и раньше, пусть $g_1, \dots, g_d$ — представители смежных классов $\mathbb{Z}_p^*$ по группе G'. Ясно, что

$$\#\{x\colon x \in G'_k,\ x-1 \in G'_i\} = \#\{(x,y)\colon x-y=1,\ x \in G'_k,\ y \in G'_i\} = \\ = t^{-1}\#\{(x,y,z)\colon g_k x - g_i y = z,\ x,y,z \in G'\}.$$

Воспользовавшись простым тождеством

$$\frac{1}{p}\sum_{a \in \mathbb{Z}_p} e_p(ax) = \begin{cases} 1, & \text{если } x = 0 \pmod p, \\ 0, & \text{если } x \neq 0 \pmod p, \end{cases}$$

и неравенством

$$\left|\sum_{x \in G'} e_p(ax)\right| \leqslant \sqrt{p} \quad \text{при} \quad (a,p) = 1,$$

получим

$$\#K_{i,k} = (pt)^{-1} \sum_{x,y,z \in G'} \sum_{a \in \mathbb{Z}_p} e_p(a(g_k x - g_i y - z)) = \\ = (pt)^{-1} \sum_{a \in \mathbb{Z}_p} S(ag_k, G')S(-ag_i, G')S(-a, G') \leqslant \\ \leqslant (pt)^{-1}\left(t^3 + \sqrt{p}\sum_{a \in \mathbb{Z}_p^*} |S(ag_k, G')S(ag_i, G')|\right) \leqslant \\ \leqslant t^2 p^{-1} + t^{-1}p^{-1/2}\sum_{a \in \mathbb{Z}_p} |S(a, G')|^2 = t^2 p^{-1} + \sqrt{p}.$$

Последнее равенство имеет место, так как

$$\sum_{a \in \mathbb{Z}_p} |S(a, G')|^2 = \sum_{x,y \in G'} \sum_{a \in \mathbb{Z}_p} e_p(a(x-y)) = pt.$$

Лемма доказана. □

Лемма 3. *Пусть $(i_\sigma, j_\sigma, k_\sigma, l_\sigma)_{\sigma=1}^s$ — различные четвёрки чисел. Тогда при $s < pt^{-1/2}$ выполнено неравенство*

$$\sum_{\sigma=1}^{s} a_{i_\sigma, j_\sigma}^{k_\sigma, l_\sigma} \ll p^{1/3} t^{1/3} s^{2/3}.$$

Доказательство. Пусть сначала $t < p^{3/4}$. Разобьём всю сумму на «пачки» с одинаковыми i, k. По предыдущей лемме для $K_{i,k} := \{b \in \mathbb{Z}_p\colon b \in G'_k,\ b-1 \in G'_i\}$ верно $\#K_{i,k} \ll t^{2/3}$. Поэтому для пачки размера r имеем

$$\sum_{\sigma=1}^{r} a_{i,j_\sigma}^{k,l_\sigma} \leqslant \#\bigcup_{\sigma=1}^{r} M_{i,j_\sigma}^{k,l_\sigma} + r^2 \leqslant \#K_{i,k} + r^2 \ll t^{2/3} + r^2.$$

Следовательно, для пачек размера меньше $t^{1/3}$ справедлива оценка (на сумму элементов) $t^{2/3}$, а для пачек, больших $t^{1/3}$, — оценка $rt^{1/3}$ (достаточно разбить пачку на части размера меньше $t^{1/3}$). Поэтому сумма элементов в больших пачках не больше $st^{1/3}$. Маленькие пачки будем суммировать все вместе. Пусть их h штук, ρ-я пачка размера s_ρ. Обозначим $\sigma_\rho := s_1 + \ldots + s_\rho$. Можно считать, что ρ-я пачка состоит из чисел $a_{i_\rho,j_\sigma}^{k_\rho,j_\sigma}$ с $\sigma \in (\sigma_{\rho-1}, \sigma_\rho]$. Ясно, что

$$\sum_{\rho=1}^{h} \sum_{\sigma_\rho<\sigma\leqslant\sigma_{\rho+1}} a_{i_\rho,j_\sigma}^{k_\rho,l_\sigma} \leqslant \sum_{\rho=1}^{h} \# \bigcup_{\sigma_\rho<\sigma\leqslant\sigma_{\rho+1}} M_{i_\rho,j_\sigma}^{k_\rho,l_\sigma} + \sum_{\rho=1}^{h} s_\rho^2 \leqslant \# \bigcup_{\sigma=1}^{s} M_{i_\sigma,j_\sigma}^{k_\sigma,l_\sigma} + \sum_{\rho=1}^{h} s_\rho^2.$$

Последняя сумма не больше $(\max s_\rho) \sum s_\rho \leqslant st^{1/3}$.

Применим метод Степанова для оценки числа элементов

$$M := \bigcup_{\sigma=1}^{s} M_{i_\sigma,j_\sigma}^{k_\sigma,l_\sigma}.$$

Рассмотрим полином $\Phi(X,Y,Z) \in \mathbb{Z}_p[X,Y,Z]$. Пусть $\deg_X \Phi < A$, $\deg_Y \Phi < B$, $\deg_Z \Phi < C$. Подберём Φ так, чтобы $\Psi(X) = \Phi(X, f(X), X^t)$ имел нули порядка D в каждой точке $x \in M$ (кроме, возможно, 0 и 1). Отсюда получим $D\#M \ll \deg \Psi(X)$, при условии $\Psi \neq 0$. Аналогично доказательству леммы 1 можно показать, что при $x \in M_{i_\sigma,j_\sigma}^{k_\sigma,l_\sigma}$

$$\{X(1-X)\}^n \left.\frac{d^n}{dX^n}\Psi(X)\right|_{X=x} = P_{n,\sigma}(x),$$

где коэффициенты полиномов P суть линейные функции от коэффициентов Φ и $\deg P_{n,\sigma}(X) < A+2D+B$. Равенство этих полиномов нулю даёт $sD(A+2D+B)$ линейных уравнений на коэффициенты Φ, поэтому нам достаточно выполнения неравенства $sD(A+2D+B) < ABC$. Условие $\Psi \neq 0$ будет выполнено, если $AB \leqslant t$. При $s < pt^{-1/2}$ нам подходят те же A, B, C, что и в лемме 1, и D, выбранное так, чтобы

$$p^{1/3}t^{1/3}s^{-1/3} \ll D \ll p^{1/3}t^{1/3}s^{-1/3}.$$

При больши́х p числа A, B, C, D больше нуля, как и в лемме 1. Значит, как и в лемме 1, $\#M \ll p^{1/3}t^{1/3}s^{2/3}$. Остаётся заметить, что при $s < pt^{-1/2}$ выполнено неравенство $st^{1/3} \ll p^{1/3}t^{1/3}s^{2/3}$.

Случай $t > p^{3/4}$ рассматривается аналогично. □

Замечание к лемме 3. При доказательстве мы, как и в лемме 1, использовали в определении множеств $M_{i,j}$ лишь первое и третье условия вместе либо первое и второе условия вместе.

3.2. Возьмём фиксированное $u \in G_\beta$. Обозначим

$$b_\beta := N_3(u,G) := \#\{(x_1,x_2,x_3)\colon x_1+x_2+x_3 = u,\ x_1,x_2,x_3 \in G\}.$$

Докажем, что

$$b_\beta = \sum_\alpha a_{1,p}^\alpha a_\alpha^\beta, \quad T_3(G) = b_0^2 + t\sum_i b_i^2 + t\sum_{i,j} b_{i,j}^2. \tag{6}$$

Действительно, обозначим через z сумму x_2+x_3 в уравнении $x_1+x_2+x_3=u$. Зафиксируем α. Есть ровно a_α^β таких $(x_1,z)\in G\times G_\alpha$, что $x_1+z=u$. Для каждой такой пары получаем $a_{1,p}^\alpha$ пар $(x_2,x_3)\in G\times G$, таких что $x_2+x_3=z$, т. е. $x_1+x_2+x_3=u$. Всего будет как раз $\sum\limits_\alpha a_{1,p}^\alpha a_\alpha^\beta$ троек (x_1,x_2,x_3). Вторая формула следует из того, что $T_3(G)=\sum\limits_{u\in\mathbb{Z}_{p^2}} N_3(u,G)^2$, но при $u_1,u_2\in G_\beta$ будет $N_3(u_1,G)=N_3(u_2,G)$. Остаётся учесть, что $\#G_i=\#G_{i,j}=t$, $\#G_0=1$.

Лемма 4 (о вырожденных случаях).

$$b_0^2+t\sum_i b_i^2\ll p^{2/3}t^{8/3}.$$

Доказательство. Вспомнив свойство (5) и лемму 3, получим

$$b_0=\sum_\alpha a_{1,p}^\alpha a_\alpha^0=a_{1,p}^{i_0,p}a_{i_0,p}^0\leqslant t\max a_{i,j}^{k,l}\ll p^{1/3}t^{4/3}.$$

Значит, $b_0^2\ll p^{2/3}t^{8/3}$. Фиксируем i. Тогда

$$b_i=\sum_\alpha a_{1,p}^\alpha a_\alpha^i\leqslant\sum_\alpha a_{1,p}^\alpha=a_{1,p}^0+\sum_{\beta\neq0}a_{1,p}^\beta.$$

Отсюда и из свойств (4) и (5) следует, что b_i не превосходит $2t$. Значит,

$$t\sum_i b_i^2\ll td\max_i b_i^2\leqslant 4t^2p\ll p^{2/3}t^{8/3},$$

поскольку $t>p^{1/2}$. □

Перейдём к невырожденным случаям, т. е. числам $b_{k,l}$.

Лемма 5. *Пусть $(k_\sigma,l_\sigma)_{\sigma=1}^s$ — различные пары чисел. Если*

$$s<s_0:=\left(\frac{p}{t}\right)^{3/2}(\log p)^{-3},$$

то

$$\sum_{\sigma=1}^s b_{k_\sigma,l_\sigma}\ll p^{1/2}ts^{2/3}.$$

Доказательство. Воспользуемся свойством (6):

$$\sum_{\sigma=1}^s b_{k_\sigma,l_\sigma}=\sum_{\sigma=1}^s\sum_\alpha a_{1,p}^\alpha a_\alpha^{k_\sigma,l_\sigma}=$$

$$=a_{1,p}^0\sum_{\sigma=1}^s a_0^{k_\sigma,l_\sigma}+\sum_{i=1}^d\left(a_{1,p}^i\sum_{\sigma=1}^s a_i^{k_\sigma,l_\sigma}\right)+\sum_{i,j}\left(a_{1,p}^{i,j}\sum_{\sigma=1}^s a_{i,j}^{k_\sigma,l_\sigma}\right).$$

Первая сумма, очевидно, не превосходит t. Так как $a_{1,p}^i=0$ всегда, то вторая сумма равна нулю. Оценим теперь последнюю сумму. Упорядочим набор чисел $\{a_{1,p}^{i,j}\}$ по убыванию: $a_{1,p}^{i_1,j_1}\geqslant a_{1,p}^{i_2,j_2}\geqslant\ldots$. Из (3) следует, что

$a_{1,p}^{i_r,j_r} \ll \alpha_r := \min(p^{1/3}t^{1/3}r^{-1/3}, tr^{-1})$. Поэтому

$$\sum_{i,j}\left(a_{1,p}^{i,j}\sum_{\sigma=1}^{s}a_{i,j}^{k_\sigma,l_\sigma}\right)=\sum_{r=1}^{pd}\left(a_{1,p}^{i_r,j_r}\sum_{\sigma=1}^{s}a_{i_r,j_r}^{k_\sigma,l_\sigma}\right)\ll\sum_{r=1}^{pd}\alpha_r S_r,$$

где

$$S_r=\sum_{\sigma=1}^{s}a_{i_r,j_r}^{k_\sigma,l_\sigma}.$$

Применяя преобразование Абеля, получаем

$$\sum_{r=1}^{pd}\alpha_r S_r=a_{pd+1}\sum_{\rho=1}^{pd}S_\rho+\sum_{r=1}^{pd}(\alpha_r-\alpha_{r+1})\sum_{\rho=1}^{r}S_\rho. \tag{7}$$

Обозначим $r_0 := tp^{-1/2}$, $r_1 := pt^{-1/2}$. Разобьём последнюю двойную сумму на три ($\sum_1$, $\sum_2$, $\sum_3$): в первой $1 \leqslant r < r_0$, во второй $r_0 < r < \frac{r_1}{s}$, в третьей $\frac{r_1}{s} < r \leqslant pd$.

Так как $s < s_0$, то $rs < r_0 s_0 < r_1 = pt^{-1/2}$ и по лемме 3

$$\sum_{\rho=1}^{r}S_\rho\ll p^{1/3}t^{1/3}r^{2/3}s^{2/3}.$$

Поскольку $r < r_0$, то $\alpha_r = p^{1/3}t^{1/3}r^{-1/3}$. Отсюда

$$\sum\nolimits_1\ll p^{2/3}t^{2/3}s^{2/3}\sum_{r<r_0}r^{-2/3}\ll p^{2/3}t^{2/3}s^{2/3}r_0^{1/3}=p^{1/2}ts^{2/3}.$$

Аналогично

$$\sum_{\rho=1}^{r}S_\rho\ll p^{1/3}t^{1/3}r^{2/3}s^{2/3}.$$

Поскольку $r > r_0$, то $\alpha_r = tr^{-1}$. Отсюда

$$\sum\nolimits_2\ll p^{1/3}t^{4/3}s^{2/3}\sum_{r_0<r<\frac{r_1}{s}}(r^{-1}-(r+1)^{-1})r^{2/3}\ll$$
$$\ll p^{1/3}t^{4/3}s^{2/3}\sum_{r_0<r}r^{-4/3}\ll p^{1/3}t^{4/3}s^{2/3}r_0^{-1/3}=p^{1/2}ts^{2/3}.$$

Из леммы 3 следует, что

$$\sum_{\rho=1}^{r}S_\rho\ll rst^{1/2}.$$

Опять $\alpha_r = tr^{-1}$. Поэтому

$$\sum\nolimits_3\ll st^{3/2}\sum_{\frac{r_1}{s}<r\leqslant pd}r^{-1}\ll st^{3/2}\log p.$$

Число s_0 и было выбрано для того, чтобы выполнялось $\sum_3 \ll p^{1/2}ts^{2/3}$, как только $s < s_0$.

Наконец, первое слагаемое в правой части (7) оценивается таким же образом, как $\sum_3$:

$$\alpha_{pd+1}\sum_{\rho=1}^{pd} S_\rho \ll st^{3/2}.$$

Лемма доказана. □

Доказательство теоремы 2. Покажем, что $\sum\limits_{i,j} b_{i,j} \ll t^2$. Ясно, что $\sum\limits_{\beta} a_\alpha^\beta \leqslant 2t$ при фиксированном α. Поэтому

$$\sum_\beta b_\beta = \sum_{\alpha,\beta} a_{1,p}^\alpha a_\alpha^\beta = \sum_\alpha \left(a_{1,p}^\alpha \sum_\beta a_\alpha^\beta \right) \leqslant 2t \sum_\alpha a_{1,p}^\alpha \leqslant 4t^2.$$

Упорядочим числа $b_{i,j}$ по убыванию: $b_{i_1,j_1} \geqslant b_{i_2,j_2} \geqslant \ldots$. Ясно, что $b_{i_s,j_s} \ll \ll t^2 s^{-1}$ при всех s. Используя лемму 5, получаем $b_{i_s,j_s} \ll p^{1/2}ts^{-1/3}$ при $s < < s_0 = \left(\frac{p}{t}\right)^{3/2}(\log p)^{-3}$. Эти оценки совпадают при $s = s_1 := t^{3/2}p^{-3/4}$. Если $t < p^{3/4}(\log p)^{-1}$, то $s_1 < s_0$ и мы получаем

$$\sum_{s=1}^{pd} b_{i_s,j_s}^2 = \sum_{s<s_1} b_{i_s,j_s}^2 + \sum_{s>s_1} b_{i_s,j_s}^2 \ll pt^2 \sum_{s<s_1} s^{-2/3} + t^4 \sum_{s>s_1} s^{-2} \ll$$
$$\ll pt^2 s_1^{1/3} + t^4 s_1^{-1} = 2p^{3/4}t^{5/2}.$$

Если же $t > p^{3/4}(\log p)^{-1}$, то $s_1 > s_0$ и аналогично

$$\sum_{s=1}^{pd} b_{i_s,j_s}^2 = \sum_{s<s_0} b_{i_s,j_s}^2 + \sum_{s>s_0} b_{i_s,j_s}^2 \ll pt^2 s_0^{1/3} + p^{1/2}ts_0^{-1/3} \sum_{s>s_0} b_{i_s,j_s} \ll$$
$$\ll pt^2 s_0^{1/3} + p^{1/2}t^3 s_0^{-1/3} \ll p^{1/2}t^3 s_0^{-1/3} = t^{7/2}\log p.$$

Теперь из (6) и леммы 4 следует оценка $T_3 \ll t^{9/2}\log p$. □

Чтобы доказать теорему 3, нужно применить основное неравенство при $k = 2$ и $l = 2$, при $k = 2$ и $l = 3$, а также при $k = 3$ и $l = 3$.

Можно аналогичным образом оценить $T_k(G)$ для всех натуральных k. Это даст нетривиальную оценку на $S(G)$ при t, несколько меньших $p^{7/10}$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант № 05-01-00066, и программы поддержки ведущих научных школ, грант № НШ-3004.2003.1.

Литература

[1] Карацуба А. А. Дробные доли специального вида // Изв. РАН. Сер. мат. — 1995. — Т. 59, № 4. — С. 93—102.

[2] Карацуба А. А. Двойные суммы Клоостермана // Мат. заметки. — 1999. — Т. 66, № 5. — С. 682—687.

[3] Конягин С. В. Оценки тригонометрических сумм по подгруппам и сумм Гаусса // IV Международная конференция «Современные проблемы теории чисел и её приложения». Актуальные проблемы. Часть III. — М., 2002. — С. 86—114.

[4] Коробов Н. М. Тригонометрические суммы и их приложения. — М.: Наука, 1984.

[5] Степанов С. А. О числе точек гиперэллиптической кривой над простым конечным полем // Изв. АН СССР. Сер. мат. — 1969. — Т. 33. — С. 1171—1181.

[6] Шпарлинский И. Е. Об оценках сумм Гаусса // Мат. заметки. — 1991. — Т. 50, № 1. — С. 122—130.

[7] Bourgain J. Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary. — Preprint.

[8] Bourgain J., Konyagin S. 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. — 2003. — Vol. 337. — P. 75—80.

[9] Heath-Brown D. R. An estimate for Heilbronn's exponential sum // Analytic Number Theory: Proc. Conf. in Honor of Heini Halberstam. — Boston: Birkhäuser, 1996. — P. 451—463.

[10] Heath-Brown D. R., Konyagin S. V. New bounds for Gauss sums derived from k^{th} powers, and for Heilbronn's exponential sums // Quart J. Math. — 2000. — Vol. 51. — P. 221—235.

[11] Konyagin S., Shparlinski I. Character Sums with Exponential Functions. — Cambridge: Cambridge University Press, 1999.