Math-Net.Ru

Общероссийский математический портал

И. В. Вьюгин, И. Д. Шкредов, Об аддитивных сдвигах мультипликативных подгрупп, *Матем. сб.*, 2012, том 203, номер 6, 81–100

DOI: <https://doi.org/10.4213/sm7857>

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: 18.208.226.222

26 апреля 2023 г., 15:06:37

УДК 511.218+511.336

И. В. Вьюгин, И. Д. Шкредов

Об аддитивных сдвигах мультипликативных подгрупп

В работе доказано, что для произвольной подгруппы $R \subseteq \mathbb{Z}/p\mathbb{Z}$ и любых различных ненулевых элементов $\mu_1, \dots, \mu_k$ имеем

$$|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \ll_k |R|^{1/2 + \alpha_k}$$

при условии, что $1 \ll_k |R| \ll_k p^{1-\beta_k}$, где $\{\alpha_k\}$, $\{\beta_k\}$ – некоторые последовательности положительных чисел и $\alpha_k, \beta_k \rightarrow 0$, $k \rightarrow \infty$. Кроме того, показано, что для любой подгруппы R , $|R| \ll p^{1/2}$, справедливо неравенство $|R \pm R| \gg |R|^{5/3} \log^{-1/2} |R|$.

Библиография: 25 названий.

Ключевые слова: мультипликативные подгруппы, метод Степанова, аддитивная комбинаторика.

§ 1. Введение

Пусть p – простое, $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ – группа всех обратимых элементов поля $\mathbb{Z}_p$ и $R \subseteq \mathbb{Z}_p^*$ – его мультипликативная подгруппа. Свойства мультипликативных подгрупп изучались различными авторами (см., например, [1]–[15]). Так, А. Гарсиа и Дж. Ф. Волох [7], используя глубокие алгебраические идеи, доказали, что для любой подгруппы R , $|R| < (p-1)/((p-1)^{1/4} + 1)$, и произвольного ненулевого μ имеет место оценка

$$|R \cap (R + \mu)| \leq 4|R|^{2/3}. \quad (1)$$

Д. Р. Хиф-Браун и С. В. Конягин передоказали и обобщили этот результат в статье [8] (см. также [12]). Их подход использует известный метод С. А. Степанова [16]. В настоящей статье мы обобщаем результат Гарсиа–Волоха, а также аналогичные теоремы из [8], [12] на случай нескольких аддитивных сдвигов. Сформулируем один из наших основных результатов.

ТЕОРЕМА 1.1. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа, $k \geq 1$ – целое число, $|R| > k2^{2k+4}$. Пусть также $\mu_1, \dots, \mu_k$ – различные ненулевые вычеты и $Q = RQ$ – некоторое R -инвариантное множество, $0 \notin Q$, $|Q| < ((|R|/k)^{1/2k} - 1)^{2k+1}$, $p \geq 4k|R|(|Q|^{1/(2k+1)} + 1)$. Тогда

$$\sum_{\lambda \in Q} |R \cap (R + \lambda \cdot \mu_1) \cap \dots \cap (R + \lambda \cdot \mu_k)| \leq 4(k+1)(|Q|^{1/(2k+1)} + 1)^{k+1}|R|. \quad (2)$$

Работа первого автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 11-01-00384), Программ Президента РФ поддержки ведущих научных школ (грант № НШ-8508.2010.1) и поддержки молодых ученых (грант № МК-4270.2011.1); работа второго автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (гранты № 06-01-00383, 11-01-00759), Программы Президента РФ поддержки ведущих научных школ (грант № НШ-8684.2010.1) и гранта Правительства РФ по постановлению № 220 (договор № 11.G34.31.0053).

Из теоремы 1.1 легко вытекает утверждение о максимальной мощности пересечения k аддитивных сдвигов подгруппы.

СЛЕДСТВИЕ 1.2. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа, $k \geq 1$ – целое число и $\mu_1, \dots, \mu_k$ – различные ненулевые элементы. Пусть также

$$32k2^{20k \log(k+1)} \leq |R|, \quad p \geq 4k|R|(|R|^{1/(2k+1)} + 1).$$

Тогда

$$|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \leq 4(k+1)(|R|^{1/(2k+1)} + 1)^{k+1}.$$

Иными словами, следствие 1.2 утверждает, что

$$|R \cap (R + \mu_1) \cap \dots \cap (R + \mu_k)| \ll_k |R|^{1/2 + \alpha_k},$$

если $1 \ll_k |R| \ll_k p^{1-\beta_k}$, где $\{\alpha_k\}$, $\{\beta_k\}$ – некоторые последовательности положительных чисел и $\alpha_k, \beta_k \rightarrow 0$, $k \rightarrow \infty$.

Наш подход развивает метод из [8], [12].

Рассмотрим теперь другую аддитивную характеристику мультипликативных подгрупп, а именно мощность их сумм или разностей. Из оценки (1) вытекает (см. [7]), что

$$|R \pm R| \gg |R|^{4/3}$$

для любой подгруппы R , для которой выполнено $|R| \ll p^{3/4}$. Д. Р. Хиф-Браун и С. В. Конягин в работе [8] (см. также [12]) доказали неравенство

$$|R \pm R| \gg |R|^{3/2} \quad (3)$$

для всех подгрупп R с условием $|R| \ll p^{2/3}$. Используя одну комбинаторную идею из работы [17] (см. также статьи [18]–[21], развивающие этот метод), мы усиливаем неравенство (3) (см. теорему 5.5) следующим образом:

$$|R \pm R| \gg \frac{|R|^{5/3}}{\log^{1/2} |R|} \quad (4)$$

для подгрупп R с условием $|R| \ll p^{1/2}$.

Скажем несколько слов о структуре настоящей статьи. Во вспомогательном § 2 мы даем необходимые определения и подробно обсуждаем обобщения обычных сверток, естественно возникающих, когда нам приходится иметь дело с несколькими аддитивными сдвигами. В § 3 мы доказываем предварительные утверждения о линейной зависимости некоторых систем многочленов в $\mathbb{Z}_p[x]$. Применяя метод Степанова и используя независимость рассматриваемых многочленов, мы получаем теорему 1.1 в § 4. Последний § 5 посвящен перечислению следствий полученных результатов, а также их приложению к задачам комбинаторной теории чисел. В частности, в нем мы доказываем оценку (4).

Сделаем несколько замечаний об обозначениях. Пусть $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ и $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Если A – некоторое множество, то будем писать $A(x)$ для его характеристической функции. Иными словами, $A(x) = 1$, если $x \in A$, и нуль иначе. Символ $|A|$ используется для обозначения мощности множества A . Запись $\log$ означает логарифм по основанию два. Знаки $\ll$ и $\gg$ суть обычные символы Виноградова. Если n – натуральное число, то будем писать $[n]$ для отрезка натурального ряда $\{1, 2, \dots, n\}$.

Авторы выражают благодарность С. В. Конягину за полезные замечания и советы, а также ИППИ РАН за создание прекрасных условий для работы.

§ 2. Метод Каца–Коестера и старшие свертки

Напомним необходимые определения. Пусть $\mathbf{G}$ – конечная абелева группа. Хорошо известно (см. [22]), что дуальная группа $\widehat{\mathbf{G}}$ абелевой группы изоморфна ей самой. Пусть f – произвольная функция из $\mathbf{G}$ в $\mathbb{C}$. Преобразование Фурье $\widehat{f}$ функции f задается формулой

$$\widehat{f}(\xi) = \sum_{x \in \mathbf{G}} f(x) e(-\xi \cdot x), \quad (5)$$

где $e(x) = e^{2\pi i x}$. Определим две свертки функций f и g :

$$(f * g)(x) := \sum_{y \in \mathbf{G}} f(y) g(x - y) \quad \text{и} \quad (f \circ g)(x) := \sum_{y \in \mathbf{G}} f(y) g(y + x).$$

Величина $E(A, B)$ называется *аддитивной энергией* двух множеств $A, B \subseteq \mathbf{G}$ (см., например, [23])

$$E(A, B) = |\{a_1 + b_1 = a_2 + b_2 : a_1, a_2 \in A, b_1, b_2 \in B\}|.$$

Если $A = B$, то мы будем писать, для краткости, $E(A)$ вместо $E(A, A)$. Ясно, что

$$E(A, B) = \sum_x (A * B)(x)^2 = \sum_x (A \circ B)(x)^2 = \sum_x (A \circ A)(x) (B \circ B)(x). \quad (6)$$

Рассмотрим обобщение операции $\circ$.

ОПРЕДЕЛЕНИЕ 2.1. Пусть $k \geq 1$ – натуральное число и $f_1, \dots, f_k : \mathbf{G} \rightarrow \mathbb{C}$ – произвольные функции. Тогда функция $C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1})$ задается формулой

$$C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1}) = \sum_z f_1(z) f_2(z + x_1) \cdots f_k(z + x_{k-1}).$$

Таким образом,

$$C_2(f_1, f_2)(x) = (f_1 \circ f_2)(x).$$

Положим также $C_1(f) = \sum_z f(z)$.

В случае, когда $f_1 = \dots = f_k = A$, $A \subseteq \mathbf{G}$ – некоторое множество, мы пишем $C_k(A)(x_1, \dots, x_{k-1})$ вместо $C_k(f_1, \dots, f_k)(x_1, \dots, x_{k-1})$.

ОПРЕДЕЛЕНИЕ 2.2. Пусть $A, B \subseteq \mathbf{G}$ – произвольные множества и $l \geq 1$ – положительное целое число. Тогда

$$A \otimes_l B = \bigcup_{b \in B} (A - b)^l \subseteq \mathbf{G}^l. \quad (7)$$

В частности, $A \otimes_1 B = A \otimes B = A - B$.

Ясно, что

$$\text{supp } C_k(B, A, \dots, A) = \bigcup_{a \in B} (A - a)^{k-1} = A \otimes_{k-1} B \subseteq \mathbf{G}^{k-1}.$$

Имеем $|A|^{k-1} \leq |A \otimes_{k-1} B| \leq |B| |A|^{k-1}$. В частности, множество $A \otimes_{k-1} B$ всегда непусто. Пусть

$$E_k(f_1, \dots, f_k) = \sum_{x_1, \dots, x_{k-1}} C_k^2(f_1, \dots, f_k)(x_1, \dots, x_{k-1}).$$

Тогда $E_2(A, B) = E(A, B)$. Пишем $E_k(A)$ для величины $E_k(A, \dots, A)$. Между величинами $|A \otimes_{k-1} A|$ и $E_k(A)$ существует очевидная связь.

ЛЕММА 2.3. Пусть $A, B \subseteq \mathbf{G}$ – некоторые множества и $k \geq 2$ – произвольное число. Тогда

$$|A|^{2k-2} |B|^2 \leq E_k(A, \dots, A, B) \cdot |A \otimes_{k-1} B|.$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$\sum_{x_1, \dots, x_{k-1}} C_k(B, A, \dots, A)(x_1, \dots, x_{k-1}) = |A|^{k-1} |B|.$$

Применяя неравенство Коши–Буняковского, получаем требуемую оценку.

Пусть $B \subseteq A$ – некоторое множество и $(x_1, \dots, x_k) := \vec{x} \in A \otimes_{k-1} B$ – произвольный вектор. Положим $B_{\vec{x}} = B \cap (A - x_1) \cap (A - x_2) \cap \dots \cap (A - x_k)$. Ясно, что множество $B_{\vec{x}}$ непусто. Кроме того, $|B_{\vec{x}}| = C_k(B, A, \dots, A)(x_1, \dots, x_{k-1})$. В терминах множеств $B_{\vec{x}}$ легко описать строение множества $A \otimes_{k-1} B$.

ЛЕММА 2.4. Пусть $B \subseteq A \subseteq \mathbf{G}$ – произвольные множества и $l \geq 1$ – некоторое число. Тогда

$$A \otimes_l B = \{(x_1, \dots, x_l) : A_{x_1, \dots, x_l} \cap B \neq \emptyset\}.$$

СЛЕДСТВИЕ 2.5. Пусть $B \subseteq A \subseteq \mathbf{G}$ – произвольные множества и $l \geq 2$, $m \geq 1$ – некоторые числа, $m \leq l$. Тогда

$$A \otimes_l B = \bigcup_{(x_1, \dots, x_m) \in A \otimes_m B} \{(x_1, \dots, x_m)\} \times (A \otimes_{l-m} B_{x_1, \dots, x_m}). \quad (8)$$

В частности,

$$A \otimes_l A = \bigcup_{(x_1, \dots, x_{l-1}) \in A \otimes_{l-1} A} \{(x_1, \dots, x_{l-1})\} \times (A - A_{x_1, \dots, x_{l-1}}). \quad (9)$$

Нам понадобятся верхние оценки на мощность множества $A \otimes_{k-1} A$. Пусть для целых положительных l и m , $m \leq l$, для произвольного множества $E \subseteq [l]$, $E = \{j_1, \dots, j_m\}$ и любого вектора $x = (x_1, \dots, x_l)$ символ x^E есть вектор $(x_{j_1}, \dots, x_{j_m})$. Следующая лемма следует из определений.

ЛЕММА 2.6. Пусть $A \subseteq \mathbf{G}$ – произвольное множество и $l \geq 1$ – некоторое число. Пусть также $S = A - A$. Тогда

$$(A \otimes_l A)(x_1, \dots, x_l) \leq \prod_{E \subseteq [l], |E|=m} (A \otimes_m A)(x^E). \quad (10)$$

Кроме того,

$$(A \otimes_2 A)(x, y) \leq S(x)S(y)S(x - y) \quad (11)$$

и

$$(A \otimes_l A)(x_1, \dots, x_l) \leq \prod_{i,j=0, i \neq j}^k S(x_i - x_j), \quad (12)$$

где $x_0 = 0$.

Ясно, что (12) вытекает из (10) и (11).

СЛЕДСТВИЕ 2.7. Пусть $A \subseteq \mathbf{G}$ – произвольное множество и $l \geq 1$ – некоторое число. Пусть также $S = A - A$. Тогда

$$|A \otimes_l A| \leq \sum_{x \in S} |A - A_x|^{l-1} \leq \sum_{x \in S} (S \circ S)^{l-1}(x). \quad (13)$$

ДОКАЗАТЕЛЬСТВО. Первое неравенство в (13) вытекает из формулы (8), если взять $m = 1$. Оценка $|A \otimes_l A| \leq \sum_{x \in S} (S \circ S)^{l-1}(x)$ немедленно следует из леммы 2.6. Наконец, внутреннее неравенство вытекает из включения Каца–Коестера [17]

$$A_{\vec{s}} - A_{\vec{t}} \subseteq S_{\vec{u}}, \quad (14)$$

где $\vec{s} = (s_1, \dots, s_m)$, $\vec{t} = (t_1, \dots, t_n)$ – произвольные векторы длины m , n соответственно, $\vec{s} \in A \otimes_m A$, $\vec{t} \in A \otimes_n A$, а вектор $\vec{u}$ имеет длину $(n+1)(m+1) - 1$ и состоит из ненулевых сумм $s_i + t_j$, $i = 0, 1, \dots, m$, $j = 0, 1, \dots, n$.

Докажем обобщение леммы 3.1 из [13].

ЛЕММА 2.8. Пусть $A \subseteq \mathbf{G}$ – произвольное множество, $l \geq 1$, $k \geq 2$ – целые числа. Тогда

$$\sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^l(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) = \sum_{x_1, \dots, x_{l-1}} C_l^{\|\vec{s}\|+k}(A)(x_1, \dots, x_{l-1}), \quad (15)$$

где $\|\vec{s}\| = \sum_{j=1}^k |\vec{s}_j|$. В частности,

$$\sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) = |A|^{\|\vec{s}\|+k} \quad (16)$$

и

$$\begin{aligned} & \sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^2(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) \\ &= \sum_{\vec{s}_1, \dots, \vec{s}_k} E_k(A_{\vec{s}_1}, \dots, A_{\vec{s}_k}) = E_{\|\vec{s}\|+k}(A). \end{aligned} \quad (17)$$

ДОКАЗАТЕЛЬСТВО. Имеем (снова считаем, что $z_0 = 0$)

$$\begin{aligned}
 & \sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} C_k^l(A_{\vec{s}_1}, \dots, A_{\vec{s}_k})(z_1, \dots, z_{k-1}) \\
 &= \sum_{\vec{s}_1, \dots, \vec{s}_k} \sum_{z_1, \dots, z_{k-1}} \sum_{w_1, \dots, w_l} \prod_{j=1}^l \prod_{i=1}^k A_{\vec{s}_i}(w_j + z_{i-1}) \\
 &= \sum_{w_1, \dots, w_l} \sum_{z_1, \dots, z_{k-1}} C_k^{\|\vec{s}\|}(A)(w_2 - w_1, \dots, w_l - w_1) \prod_{j=1}^l \prod_{i=1}^k A(w_j + z_{i-1}) \\
 &= \sum_{w_1, \dots, w_l} C_k^{\|\vec{s}\|+k-1}(A)(w_2 - w_1, \dots, w_l - w_1) A(w_1) \cdots A(w_l) \\
 &= \sum_{x_1, \dots, x_{l-1}} C_l^{\|\vec{s}\|+k}(A)(x_1, \dots, x_{l-1}), \tag{18}
 \end{aligned}$$

поскольку каждая компонента произвольного вектора $\vec{s}_i$ встречается в формуле (18) в точности l раз. Лемма доказана.

§ 3. О линейной независимости одной системы многочленов

В работе [12] была доказана

ЛЕММА 3.1. Пусть $\alpha_1 \in \mathbb{Z}_p^*$ – произвольный вычет. Пусть также t, B, D – некоторые целые числа, p – простое число и

$$t \geq BD, \quad p \geq tB. \tag{19}$$

Тогда многочлены семейства

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}}, \tag{20}$$

где $a_i < D$, $b_{0,i}, b_{1,i} < B$, в совокупности линейно независимы над $\mathbb{Z}_p[x]$.

В этом параграфе мы обобщим лемму 3.1 на случай систем многочленов с большим числом множителей, хотя зависимость между параметрами у нас хуже.

Будем использовать понятие производной полиномов с коэффициентами из $\mathbb{Z}_p$ формально. Под производной полинома будем понимать формальную производную суммы, т.е. другой полином, получающийся по правилу

$$\left(\sum_{i=0}^n c_i x^i \right)' = \sum_{i=1}^n i c_i x^{i-1}.$$

Будем рассматривать производные только многочленов степени не выше чем $p - 1$. Для формальной производной таких многочленов выполняется правило Лейбница. Отметим, что операция дифференцирования корректно определена не для функций, а только для формальных сумм.

ПРЕДЛОЖЕНИЕ 3.2. Пусть n, t, B, D – некоторые целые числа и p – простое число. Пусть также $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_p^*$ – различные ненулевые вычеты и

$$t \geq \frac{1}{2}(n-1)B^{2n} + DB^n, \quad p \geq (2nB+2)t. \quad (21)$$

Тогда многочлены семейства

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}}, \quad (22)$$

где $a_i < D$, $b_{0,i}, b_{1,i}, \dots, b_{n,i} < B$, в совокупности линейно независимы над $\mathbb{Z}_p[x]$.

ДОКАЗАТЕЛЬСТВО. Допустим, что имеется нетривиальная линейная комбинация многочленов (22), тождественно равная нулю,

$$\sum_{i=1}^m C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \equiv 0. \quad (23)$$

Поделим равенство (23) на $(x - \alpha_n)^{ts}$, где $s = \min_i b_{n,i}$. Рассмотрим только те члены суммы (23), у которых $b_{n,i}$ минимальны, т.е. равны s . Будем считать, что это первые l_0 членов. Тогда многочлен

$$\Phi(x) = \sum_{i=1}^{l_0} C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}} \quad (24)$$

делится нацело на $(x - \alpha_n)^t$. Обозначим сумму многочленов из (24) с одинаковым множителем $x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}$ через

$$\Phi_i(x) = H_i(x) x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}, \quad i = 1, \dots, l.$$

Ясно, что $\deg H_i < D$ и $l < B^n$. Рассмотрим определитель Вронского

$$W(\Phi_1, \dots, \Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi_1'(x) & \Phi_2'(x) & \dots & \Phi_l'(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l-1)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}. \quad (25)$$

Это многочлен от x (назовем его $P(x)$) степени не выше чем

$$\deg P(x) \leq \sum_{i=1}^l \sum_{j=0}^{n-1} tb_{j,i} + l(D-1) - \frac{1}{2}l(l-1).$$

Нетрудно заметить, что $P(x)$ делится без остатка на следующие многочлены:

$$\Psi_0(x) = x^{\sum_{i=1}^l tb_{0,i} - \frac{1}{2}l(l-1)},$$

$$\Psi_k(x) = (x - \alpha_k)^{(t \sum_{i=1}^l b_{k,i} - \frac{1}{2}l(l-1))}, \quad k = 1, \dots, n-1,$$

которые мы будем называть $\Psi_0(x), \dots, \Psi_{n-1}(x)$. Имеем, что $P(x)$ делится на

$$\Psi(x) = \prod_{k=0}^{n-1} \Psi_k(x).$$

При этом

$$\deg \Psi(x) = \sum_{i=1}^l t b_{0,i} + t \sum_{k=1}^{n-1} \sum_{i=1}^l b_{k,i} - \frac{1}{2} n l (l-1) = \deg P(x) - \frac{1}{2} (n-1) l (l-1) - l(D-1).$$

Теперь осталось заметить, что если $P(x)$ делится на $(x - \alpha_n)^C$, то и $P(x)/\Psi(x)$ делится на него, а степень

$$\deg \left(\frac{P(x)}{\Psi(x)} \right) \leq \frac{1}{2} (n-1) l (l-1) + l(D-1),$$

следовательно, $C \leq \frac{1}{2} (n-1) l (l-1)$ (либо $P(x) \equiv 0$, но тогда многочлены $\Phi_1(x), \dots, \Phi_l(x)$ линейно зависимы (см. лемму 3.4 ниже) и мы можем перейти к той же задаче, но с меньшим числом скобок).

Теперь вернемся к исходному предположению, по которому сумма $\Phi(x)$ из (24) делится нацело на $(x - \alpha_n)^t$. При этом предположении вронскиан $P(x) = W(\Phi_1, \dots, \Phi_l)$ должен делиться на $(x - \alpha_n)^{t-(l-1)}$, так как $\Phi(x), \dots, \Phi^{(l-1)}(x)$ делятся на $(x - \alpha_n)^{t-(l-1)}$. Таким образом, получается, что

$$t \leq (l-1) + \frac{1}{2} (n-1) l (l-1) + l(D-1) < \frac{1}{2} (n-1) l (l-1) + lD,$$

но общее количество многочленов l в сумме (24) ограничено, $l < B^n$. Следовательно,

$$t < \frac{1}{2} (n-1) B^{2n} + D B^n,$$

а это противоречит условию предложения. Мы получили, что исходное предположение неверно, и значит, предложение доказано.

Приведем две леммы о линейной зависимости. Лемма 3.3 относится к общей ситуации, а лемма 3.4 позволяет получить лучшее соотношение между параметрами p , t , n и B .

ЛЕММА 3.3. Пусть имеют место все обозначения предложения 3.2. Если вронскиан $P(x) = W(\Phi_1(x), \dots, \Phi_l(x))$, $\deg P < p$, тождественно равен нулю в поле $\mathbb{Z}_p$, то существует нетривиальная линейная комбинация многочленов $\Phi_1(x), \dots, \Phi_l(x)$ с коэффициентами из $\mathbb{Z}_p$, тождественно равная нулю

$$\mu_1 \Phi_1(x) + \dots + \mu_l \Phi_l(x) \equiv 0, \quad \mu_1, \dots, \mu_l \in \mathbb{Z}_p.$$

Доказательство леммы совпадает с началом доказательства леммы 3.4.

ЛЕММА 3.4. Пусть вронскиан $P(x) = W(\Phi_1(x), \dots, \Phi_l(x))$ тождественно равен нулю

$$P(x) \equiv 0$$

в поле $\mathbb{Z}_p$, тогда существует нетривиальная линейная комбинация многочленов $\Phi_1(x), \dots, \Phi_l(x)$ с коэффициентами $\mu_i \in \mathbb{Z}_p$, $i = 1, \dots, l$, тождественно равная нулю

$$\mu_1 \Phi_1(x) + \dots + \mu_l \Phi_l(x) \equiv 0,$$

если $p \geq (2nB + 2)t$.

ДОКАЗАТЕЛЬСТВО. Так как вронсиан $P(x)$ тождественно равен нулю, то существует нетривиальная тождественно нулевая линейная комбинация его строк, тождественно равная нулю, т.е. комбинация

$$\lambda_1 \Phi_k(x) + \lambda_2 \Phi'_k(x) + \cdots + \lambda_l \Phi_k^{(l-1)}(x) \equiv 0, \quad k = 1, \dots, l, \quad (26)$$

с коэффициентами $\lambda_i = \lambda_i(x)$, вообще говоря, зависящими от x , и не равными нулю одновременно. Докажем, что коэффициенты λ_i могут быть выбраны постоянными и не равными нулю одновременно. Линейную комбинацию (26) можно рассматривать как формальное линейное дифференциальное уравнение порядка не выше $l - 1$

$$\lambda_1 u(x) + \lambda_2 u'(x) + \cdots + \lambda_l u^{(l-1)}(x) = 0. \quad (27)$$

Полиномы $u(x)$, удовлетворяющие этому уравнению, образуют линейное пространство. Нетрудно показать, что решение этого уравнения, первые $l - 1$ производная которого в некоторой точке равны нулю, является тождественно нулевым. Действительно, положив $x = 0$, получим из уравнения (27) линейное соотношение, выражающее $u^{(l-1)}(0)$ через производные $u^{(l-2)}(0), \dots, u(0)$ меньшего порядка. Формально продифференцировав уравнение (27), получим аналогичное соотношение для $u^{(l)}(0)$ и т.д., тем самым получим выражения для старших производных. В случае, если первые $l - 1$ производных нулевые при $x = 0$, то нулевые и все остальные производные, так как они линейно выражаются через первые $l - 1$ производных и саму функцию $u(x)$. Обоснуем ниже возможность дифференцирования функций $\lambda_i(x)$; для этого достаточно показать, что функции $\lambda_i(x)$ и формальная линейная комбинация (27) является полиномами степени меньше p .

Теперь рассмотрим линейную комбинацию столбцов, равную нулю при $x = 0$. По нашему предположению, найдутся $\mu_1, \dots, \mu_l$ такие, что

$$\mu_1 \Phi_1^{(k)}(0) + \mu_2 \Phi_2^{(k)}(0) + \cdots + \mu_l \Phi_l^{(k)}(0) = 0, \quad k = 0, 1, \dots, l - 1.$$

Рассмотрим решение

$$u(x) = \mu_1 \Phi_1(x) + \mu_2 \Phi_2(x) + \cdots + \mu_l \Phi_l(x)$$

уравнения (27), оно и его первые $l - 1$ производная равны нулю при $x = 0$, тогда по доказанному выше $u(x)$ – тождественно нулевой многочлен. Следовательно, линейная комбинация полиномов $\Phi_1(x), \dots, \Phi_l(x)$ с коэффициентами $\mu_1, \dots, \mu_l$ тождественно равна нулю, что и требовалось доказать.

Теперь покажем, что левая часть уравнения (27) – формальный полином степени меньше p .

ЛЕММА 3.5. *Степень выражения*

$$\lambda_1 u(x) + \lambda_2 u'(x) + \cdots + \lambda_l u^{(l-1)}(x)$$

как полинома от x не выше $2(nB + 1)t$.

ДОКАЗАТЕЛЬСТВО. Коэффициенты $\lambda_1, \dots, \lambda_l$ являются решениями однородной системы линейных уравнений (26). Уравнения системы (26) линейно зависимы при всех x , а следовательно, она имеет ненулевое решение. Для того чтобы найти решения этой системы, воспользуемся правилом Крамера. Пусть среди l уравнений имеется l_1 линейно независимых, без ограничения общности можно считать, что это первые l_1 уравнений. Существуют l_1 столбцов матрицы системы (26) таких, что матрица составленная из элементов, стоящих в первых l_1 строках и этих l_1 столбцах невырожденная хотя бы при одном x ; обозначим номера этих столбцов через $i_1, \dots, i_{l_1}$, а номера остальных столбцов – через $j_1, \dots, j_{l-l_1}$. Найдем решения системы (26), переписанной в виде

$$\lambda_{i_1} \Phi_k^{(i_1-1)}(x) + \dots + \lambda_{i_{l_1}} \Phi_k^{(i_{l_1}-1)}(x) = - \sum_{s=1}^{l-l_1} \lambda_{j_s} \Phi_k^{(j_s-1)}(x) = \widehat{\Phi}_k(x),$$

$$k = 1, \dots, l_1,$$

при введенном обозначении

$$\widehat{\Phi}_k(x) = - \sum_{s=1}^{l-l_1} \lambda_{j_s} \Phi_k^{(j_s-1)}(x), \quad k = 1, \dots, l_1.$$

Решения этой системы составляют линейное пространство размерности $l - l_1$. Положим свободные неизвестные $\lambda_{j_1}, \dots, \lambda_{j_{l-l_1}}$ равными

$$\lambda_{j_s} = \frac{x^{D+tB} \prod_{j=1}^{n-1} (x - \alpha_j)^{tB}}{\widehat{\Psi}(x)} \begin{vmatrix} \Phi_1^{(i_1-1)}(x) & \dots & \Phi_{l_1}^{(i_1-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{l_1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{l_1}-1)}(x) \end{vmatrix}, \quad s = 1, \dots, l - l_1,$$

где

$$\widehat{\Psi}(x) = x^{\sum_{q=1}^{l_1} (c_q + t b_{0,q}) - \sum_{q=1}^{l_1} (i_{l_1} - i_q)} \prod_{j=1}^{n-1} (x - \alpha_j)^{(t \sum_{q=1}^{l_1} b_{j,q}) - \sum_{q=1}^{l_1} (i_{l_1} - i_q)},$$

где $c_q = \deg H_q < D$. Тогда по формулам Крамера при $i = 1, \dots, l - 1$ получаем

$$\lambda_{i_s} = \frac{x^{D+tB} \prod_{j=1}^{n-1} (x - \alpha_j)^{tB}}{\Psi(x)} \begin{vmatrix} \Phi_1^{(i_1-1)}(x) & \dots & \Phi_{l_1}^{(i_1-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{s-1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{s-1}-1)}(x) \\ \widehat{\Phi}_1^*(x) & \dots & \widehat{\Phi}_{l_1}^*(x) \\ \Phi_1^{(i_{s+1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{s+1}-1)}(x) \\ \dots & \dots & \dots \\ \Phi_1^{(i_{l_1}-1)}(x) & \dots & \Phi_{l_1}^{(i_{l_1}-1)}(x) \end{vmatrix}, \quad s = 1, \dots, l_1,$$

где

$$\widehat{\Phi}_k^*(x) = - \sum_{s=1}^{l-l_1} \Phi_k^{(j_s-1)}(x), \quad k = 1, \dots, l_1.$$

Нетрудно проверить, что формулы для всех $\lambda_1, \dots, \lambda_l$ являются полиномиальными, т.е. знаменатели сокращаются с числителями. Оценим сверху степени этих полиномов:

$$\deg \lambda_i(x) \leq \frac{1}{2}l(l-1)(n-1) + (l+1)D + nBt < (nB+1)t, \quad i = 1, \dots, l.$$

Степени полиномов $\Phi_k(x)$ не превосходят

$$\deg \Phi_k(x) < nBt + D,$$

следовательно,

$$\deg(\lambda_1 \Phi_k(x) + \lambda_2 \Phi'_k(x) + \dots + \lambda_l \Phi_k^{(l-1)}(x)) < 2ntB + t + D - 1 < (2nB+2)t,$$

что и требовалось доказать.

ЗАМЕЧАНИЕ 3.6. Предложение 3.2 можно доказать с помощью соотношения Фукса для левелевского базиса (см. формулировку в [24]). Тем не менее, мы предпочитаем использовать более простой подход, связанный с подсчетом степени вронскиана системы многочленов вида (22).

Аналогично доказывается

ПРЕДЛОЖЕНИЕ 3.7. Пусть $n, t, B, D, D < t$ – некоторые целые числа и p – простое число. Пусть также T – некоторое множество, $T \subseteq \mathbb{Z}_p^*$, $T > n-1$. Предположим, наконец, что

$$t \geq DB^n + \frac{\frac{n}{2}D^2B^{2n}}{|T| - n + 1}, \quad p \geq \min\{tnDB^{n+1}, B^2t^2n^2\}. \quad (28)$$

Тогда найдется набор $\alpha_1, \dots, \alpha_n \in T$ такой, что многочлены семейства

$$x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}}, \quad (29)$$

где $a_i < D$, $b_{0,i}, b_{1,i}, \dots, b_{n,i} < B$, в совокупности линейно независимы над $\mathbb{Z}_p[x]$.

ДОКАЗАТЕЛЬСТВО. Можно считать, что для некоторых $\alpha_1, \dots, \alpha_{n-1} \in T$ соответствующие многочлены из (29) линейно независимы над $\mathbb{Z}_p[x]$, иначе мы имеем задачу с меньшим числом скобок. Таким образом, зафиксируем $\alpha_1, \dots, \alpha_{n-1} \in T$, и пусть α_n пробегает непустое множество $T \setminus \{\alpha_1, \dots, \alpha_{n-1}\}$. Дальше действуем почти так же, как в предложении 3.2. Допустим, что имеется нетривиальная линейная комбинация многочленов (29), тождественно равная нулю,

$$\sum_{i=1}^m C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_n)^{tb_{n,i}} \equiv 0. \quad (30)$$

Поделим равенство (30) на $(x - \alpha_n)^{ts}$, где $s = \min_i b_{n,i}$. Рассмотрим только те члены суммы (30), у которых $b_{n,i}$ минимальны, т.е. равны s . Тогда

$$\Phi(x) = \sum_{i=1}^l C_i x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}} \quad (31)$$

делится нацело на $(x - \alpha_n)^t$. Обозначим многочлены из суммы (31) через

$$\Phi_i(x) = x^{a_i} x^{tb_{0,i}} (x - \alpha_1)^{tb_{1,i}} \dots (x - \alpha_{n-1})^{tb_{n-1,i}}, \quad i = 1, \dots, l.$$

Рассмотрим определитель Вронского

$$W(\Phi_1, \dots, \Phi_l) = \begin{vmatrix} \Phi_1(x) & \Phi_2(x) & \dots & \Phi_l(x) \\ \Phi'_1(x) & \Phi'_2(x) & \dots & \Phi'_l(x) \\ \vdots & \vdots & \ddots & \vdots \\ \Phi_1^{(l-1)}(x) & \Phi_2^{(l-1)}(x) & \dots & \Phi_l^{(l-1)}(x) \end{vmatrix}. \quad (32)$$

Это многочлен от x (назовем его $P(x)$) степени не выше чем

$$\deg P(x) \leq \sum_{i=1}^l \left(a_i + t \sum_{j=0}^{n-1} b_{j,i} \right) - \frac{1}{2} l(l-1).$$

Нетрудно заметить, что $P(x)$ делится без остатка на следующие многочлены:

$$\begin{aligned} \Psi_0(x) &= x^{\sum_{i=1}^l (a_i + tb_{0,i}) - \frac{1}{2} l(l-1)}, \\ \Psi_k(x) &= (x - \alpha_k)^{\left(t \sum_{i=1}^l b_{k,i} \right) - \frac{1}{2} l(l-1)}, \quad k = 1, \dots, n-1, \end{aligned}$$

которые мы будем называть $\Psi_0(x), \dots, \Psi_{n-1}(x)$. Имеем, что $P(x)$ делится на

$$\Psi(x) = \prod_{k=0}^{n-1} \Psi_k(x).$$

При этом

$$\deg \Psi(x) = \sum_{i=1}^l (a_i + tb_{0,i}) + t \sum_{k=1}^{n-1} \sum_{i=1}^l b_{k,i} - \frac{1}{2} nl(l-1) = \deg P(x) - \frac{1}{2} (n-1)l(l-1).$$

Теперь осталось заметить, что если $P(x)$ делится на $(x - \alpha_n)^C$, то и $P(x)/\Psi(x)$ делится на него, а степень

$$\deg \left(\frac{P(x)}{\Psi(x)} \right) \leq \frac{1}{2} (n-1)l(l-1),$$

следовательно, $C \leq \frac{1}{2} (n-1)l(l-1)$. При этом многочлен $P(x)$ не тождественный нуль, поскольку в таком случае многочлены $\Phi_1(x), \dots, \Phi_l(x)$ линейно зависимы, а эту ситуацию мы исключили (см. лемму 3.3 или лемму 3.4).

Теперь вернемся к исходному предположению, по которому сумма $\Phi(x)$ из (31) делится нацело на $(x - \alpha_n)^t$. При этом предположении вронсиан $P(x) = W(\Phi_1, \dots, \Phi_l)$ должен делиться на $(x - \alpha_n)^{t-(l-1)}$, так как $\Phi(x), \dots, \Phi^{(l-1)}(x)$ делятся на $(x - \alpha_n)^{t-(l-1)}$. Значит, для каждого α_n вронсиан $P(x) = W(\Phi_1, \dots, \Phi_l)$ должен делиться на $(x - \alpha_n)^{t-(l-1)}$. Таким образом, получается, что

$$(|T| - n + 1)(t - (l-1)) \leq (l-1) + \frac{1}{2} (n-1)l(l-1) + l(D-1) < \frac{1}{2} (n-1)l(l-1) + lD.$$

Общее количество многочленов l в сумме (31) равно DB^n . Следовательно,

$$t < DB^n + \frac{\frac{n}{2} D^2 B^{2n}}{|T| - n + 1},$$

а это противоречит условию предложения. Отметим еще неравенство

$$\deg P(x) \leq \min\{tnDB^{n+1}, B^2 t^2 n^2\} < p.$$

Мы получили, что исходное предположение неверно, и значит, предложение доказано.

§ 4. Доказательство основного результата

Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа и $t = |R|$. Пусть $k \geq 1$ – целое число и $\mu_1, \dots, \mu_k$ – фиксированные попарно различные ненулевые элементы. Пусть также $\xi_0, \xi_1, \dots, \xi_k$ – некоторые ненулевые вычеты и $A_{\vec{\xi}, \lambda}$, $\vec{\xi} = (\xi_0, \xi_1, \dots, \xi_k)$, $\lambda \in \mathbb{Z}_p^*$, – произвольное подмножество множества $\xi_0 R \cap (\xi_1 R + \lambda \cdot \mu_1) \cap \dots \cap (\xi_k R + \lambda \cdot \mu_k)$. Предположим, наконец, что задано целое семейство множеств $A_{\vec{\xi}_1, \lambda_1}, \dots, A_{\vec{\xi}_s, \lambda_s}$. При этом у множеств $A_{\vec{\xi}_l, \lambda_l}$ рассматриваемого семейства могут быть и одинаковые λ_l .

С помощью метода Степанова докажем одну из основных лемм этого параграфа. Мы будем следовать работе [12] (см. также [8]).

ЛЕММА 4.1. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа и $t = |R|$. Пусть $k \geq 2$, s и B – произвольные натуральные числа такие, что

$$kB^{2k} < t, \quad ts < B^{2k+1}, \quad (33)$$

$$p \geq (2kB + 2)t. \quad (34)$$

Пусть также $A_{\vec{\xi}_1, \lambda_1}, \dots, A_{\vec{\xi}_s, \lambda_s}$ – множества из семейства, построенного выше. Тогда

$$\sum_{l=1}^s |A_{\vec{\xi}_l, \lambda_l}| \leq \frac{(k+1)tB}{[t/(2B^k)]}. \quad (35)$$

ДОКАЗАТЕЛЬСТВО. Пусть $D = [t/(2B^k)]$. Поскольку $2B^k \leq kB^{2k} < t$, то $D \geq 1$. Пусть также $\mathcal{E}$ – объединение всех множеств $A_{\vec{\xi}_l, \lambda_l}$. Можно считать, что множества $A_{\vec{\xi}_l, \lambda_l}$ не пересекаются и для всех них выполнено $\lambda = 1$. Нам нужно оценить мощность множества $\mathcal{E}$. Пусть $\Phi(X, Y, Z_1, \dots, Z_k) \in \mathbb{Z}_p[X, Y, Z_1, \dots, Z_k]$ – произвольный многочлен такой, что

$$\deg_X \Phi < D, \quad \deg_Y \Phi < B, \quad \deg_{Z_j} \Phi < B, \quad j \in [k].$$

Имеем

$$\Phi(X, Y, Z_1, \dots, Z_k) = \sum_{a, b, \vec{c}} \lambda_{a, b, \vec{c}} X^a Y^b Z^{\vec{c}}, \quad (36)$$

где $\vec{c} = (c_1, \dots, c_k) \in \mathbb{Z}_p^k$ и $Z^{\vec{c}} = Z_1^{c_1} \dots Z_k^{c_k}$. Пусть также

$$\Psi(X) = \Phi(X, X^t, (X - \mu_1)^t, \dots, (X - \mu_k)^t). \quad (37)$$

Ясно, что

$$\deg \Psi \leq D - 1 + (k + 1)t(B - 1).$$

Если мы выберем коэффициенты $\lambda_{a,b,\vec{c}}$ так, чтобы, во-первых, многочлен Ψ был бы ненулевым, а, во-вторых, чтобы Ψ имел корень порядка не менее D в каждой точке множества $\mathcal{E}$, то

$$|\mathcal{E}| \leq \frac{D - 1 + (k + 1)t(B - 1)}{D} < \frac{(k + 1)tB}{\lfloor t/2B^k \rfloor},$$

и лемма будет доказана. Итак, необходимо проверить, что

$$\left(\frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0 \quad \forall n < D, \quad \forall x \in \mathcal{E}.$$

Поскольку для всех $x \in \mathcal{E}$ имеем $x \neq 0$ и $x \neq \mu_j$, $j \in [k]$, то последнее условие эквивалентно

$$[X(X - \mu_1) \cdots (X - \mu_k)]^n \left(\frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} = 0 \quad \forall n < D, \quad \forall x \in \mathcal{E}. \quad (38)$$

Легко видеть, что для всех $q \geq m$ и любого μ выполнено

$$(X - \mu)^m \left(\frac{d}{dX} \right)^m (X - \mu)^q = \frac{q!}{(q - m)!} (X - \mu)^q.$$

Если же $m > q$, то левая часть равна нулю. Значит, корректно определены многочлены $P_{n,a,b,\vec{c}}(X)$ такие, что

$$\begin{aligned} & [X(X - \mu_1) \cdots (X - \mu_k)]^n \left(\frac{d}{dX} \right)^n X^a X^{tb} (X - \mu_1)^{tc_1} \cdots (X - \mu_k)^{tc_k} \\ &= P_{n,a,b,\vec{c}}(X) X^{tb} (X - \mu_1)^{tc_1} \cdots (X - \mu_k)^{tc_k}. \end{aligned}$$

Здесь $a, b, c_1, \dots, c_k$ — целые неотрицательные числа, причем многочлен $P_{n,a,b,\vec{c}}$ может быть нулевым. Ясно, что $\deg P_{n,a,b,\vec{c}} \leq a + n$. По определению множеств $A_{\vec{\xi}_l, \vec{\mu}_l}$ имеем

$$\begin{aligned} & [X(X - \mu_1) \cdots (X - \mu_k)]^n \left(\frac{d}{dX} \right)^n X^a X^{tb} (X - \mu_1)^{tc_1} \cdots (X - \mu_k)^{tc_k} \Big|_{X=x} \\ &= y_0^b(l) y_1^{c_1}(l) \cdots y_1^{c_k}(l) P_{n,a,b,\vec{c}}(X), \quad x \in A_{\vec{\xi}_l, \vec{\mu}_l}, \end{aligned}$$

где вычеты $y_0^b(l), y_1^{c_1}(l), \dots, y_1^{c_k}(l)$ не зависят от выбора элемента $x \in A_{\vec{\xi}_l, \vec{\mu}_l}$. По формулам (36), (37)

$$\begin{aligned} & [X(X - \mu_1) \cdots (X - \mu_k)]^n \left(\frac{d}{dX} \right)^n \Psi(X) \Big|_{X=x} \\ &= \sum_{a,b,\vec{c}} \lambda_{a,b,\vec{c}} \cdot y_0^b(l) y_1^{c_1}(l) \cdots y_1^{c_k}(l) P_{n,a,b,\vec{c}}(x) := P_{n,l}(x), \quad x \in A_{\vec{\xi}_l, \vec{\mu}_l}. \end{aligned}$$

Коэффициенты многочленов $P_{n,l}(X)$ являются линейными формами от $\lambda_{a,b,\vec{c}}$. Путем надлежащего выбора $\lambda_{a,b,\vec{c}}$ сделаем многочлены $P_{n,l}(X)$ тождественно

нулевыми для всех $n < D$ и всех $l \in [s]$. Тогда равенство (38) будет выполнено для всех $x \in \mathcal{E}$. Поскольку $\deg P_{n,l} < 2D$, то неравенство

$$2sD^2 \leq \frac{2sDt}{2B^k} < DB^{k+1}, \quad (39)$$

вытекающее из (33), гарантирует, что найдется такой набор коэффициентов $\lambda_{a,b,\bar{c}}$, не равных нулю одновременно, для которых $P_{n,l}(X) \equiv 0$, $n < D$, $l \in [s]$.

Нам осталось убедиться в том, что многочлен $\Psi(X)$ ненулевой. Имеем $D = \lfloor t/(2B^k) \rfloor$ и $kB^{2k} < t$. Отсюда $t \geq \frac{1}{2}(k-1)B^{2k} + DB^k$. Кроме того, справедливо неравенство (34). Применяя предложение 3.2 с $n = k$, получаем, что многочлен $\Psi(X)$ не тождественный нуль. Лемма доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1.1. Пусть $|R| = t$, $s = |Q|/t$. Пусть B – наименьшее целое число такое, что $B^{2k+1} > ts$. Тогда $B \leq (ts)^{1/(2k+1)} + 1$. Используя оценку

$$|Q| < \left(\left(\frac{t}{k} \right)^{1/2k} - 1 \right)^{2k+1},$$

находим

$$kB^{2k} \leq k((ts)^{1/(2k+1)} + 1)^{2k} < t,$$

и условие (33) леммы 4.1 выполнено. Так как $t > k2^{2k+4}$ и

$$|Q| < \left(\left(\frac{t}{k} \right)^{1/2k} - 1 \right)^{2k+1} < \left(\frac{t}{k} \right)^{(2k+1)/2k},$$

то $t/(2B^k) \geq 2$. Наконец, неравенство (34) той же леммы вытекает из оценки $p \geq 4tk(|Q|^{1/(2k+1)} + 1)$. Применяя лемму и используя неравенства $t/(2B^k) \geq 2$, $B \leq |Q|^{1/(2k+1)} + 1$, находим

$$\begin{aligned} \sum_{\lambda \in Q} |R \cap (R + \lambda \cdot \mu_1) \cap \dots \cap (R + \lambda \cdot \mu_k)| &\leq t \frac{(k+1)tB}{\lfloor t/(2B^k) \rfloor} \\ &\leq 4(k+1)B^{k+1}t \leq 4(k+1)(|Q|^{1/(2k+1)} + 1)^{k+1}t. \end{aligned}$$

Теорема доказана.

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ 1.2. Достаточно проверить, что для всех $|R| \geq 32k2^{20k \log(k+1)} > k2^{2k+4}$ выполнено

$$|R| < \left(\left(\frac{|R|}{k} \right)^{1/2k} - 1 \right)^{2k+1}.$$

Легко видеть, что при данных ограничениях на мощность R последнее неравенство справедливо.

Используя предложение 3.7 вместо предложения 3.2, получаем

УТВЕРЖДЕНИЕ 4.2. Пусть $k \geq 2$ – натуральное число и $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа. Пусть также $T \subseteq \mathbb{Z}_p^*$ – любое множество, $2k \leq |T| \leq |R|k/2$, а s и B – произвольные натуральные числа такие, что

$$2kB^{2k} \leq |R||T|, \quad 2s \left(\frac{|R||T|}{2k} \right)^{1/2} < B^{2k+1}, \quad (40)$$

$$p \geq (2kB + 2)t. \quad (41)$$

Тогда найдутся попарно различные элементы $\mu_j \in T$, $j \in [k]$, такие, что для любых построенных по ним множеств $A_{\xi_1, \lambda_1}, \dots, A_{\xi_s, \lambda_s}$ выполнено

$$\sum_{l=1}^s |A_{\xi_l, \lambda_l}| \leq \frac{(k+1)|R|B}{[(|R||T|/(2kB^{2k}))^{1/2}]}. \quad (42)$$

ДОКАЗАТЕЛЬСТВО. Пусть $t = |R|$ и $D = \lceil (t|T|/(2kB^{2k}))^{1/2} \rceil$. Поскольку $2kB^{2k} \leq t|T|$, то $D \geq 1$. Кроме того, $D < t$, ибо $|T| \leq tk/2$. Пусть $\mathcal{E}$ – объединение всех множеств A_{ξ_l, λ_l} . Рассуждая как в лемме 4.1, строим многочлен Ψ , имеющий корень кратности не менее D в каждой точке множества $\mathcal{E}$. Если многочлен Ψ ненулевой, то имеем оценку сверху на мощность множества $\mathcal{E}$:

$$|\mathcal{E}| \leq \frac{D-1+(k+1)t(B-1)}{D} < \frac{(k+1)tB}{[(t|T|/(2kB^{2k}))^{1/2}]}. \quad (43)$$

Кроме того, аналог неравенства (39) выглядит теперь следующим образом:

$$2sD^2 \leq 2sD \left(\frac{t|T|}{2kB^{2k}} \right)^{1/2} < DB^{k+1}, \quad (43)$$

что справедливо по второму неравенству из (40). Из (40) и оценки $|T| \leq tk/2$ вытекает, что

$$t \geq DB^k + \frac{kD^2B^{2k}}{2(|T| - k + 1)}.$$

Используя условие (41) и применяя предложение 3.7 с $n = k$, получаем, что для некоторых попарно различных $\mu_j \in T$, $j \in [k]$, многочлен $\Psi(X)$ не тождественный нуль. Утверждение доказано.

ЗАМЕЧАНИЕ 4.3. Хотя в утверждении 4.2 сумма (42) оценивается для специфического набора элементов μ_j , зависимость между параметрами B , t и T (см. первое неравенство в (40)) не такая обременительная, как соответствующая оценка (33) из леммы 4.1.

СЛЕДСТВИЕ 4.4. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа, $k \geq 1$ – целое число. Пусть также $T \subseteq \mathbb{Z}_p^*$ – любое множество, $2k \leq |T| \leq |R|k/2$ и $Q = RQ$ – некоторое R -инвариантное множество, $0 \notin Q$,

$$|Q| < \left(\frac{k|R|}{2|T|} \right)^{1/2} \left(\left(\frac{|R||T|}{8k} \right)^{1/2k} - 1 \right)^{2k+1}, \quad (44)$$

$$p \geq \left(\frac{k|R|^3|T|}{2} \right)^{1/2} \left(\left(|Q| \left(\frac{2|T|}{k|R|} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right). \quad (45)$$

Тогда

$$\begin{aligned} & \min_{\mu_1, \dots, \mu_k \in T, \mu_i \neq \mu_j} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k) \\ & \leq (32k^3)^{1/2} \left(\frac{|R|}{|T|} \right)^{1/2} \left(\left(|Q| \left(\frac{2|T|}{k|R|} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{k+1}. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Пусть $t = |R|$, $s = |Q|/t$. Пусть B – наименьшее целое такое, что $B^{2k+1} > 2s(t|T|/(2k))^{1/2}$. Тогда

$$B \leq \left(2s \left(\frac{t|T|}{2k} \right)^{1/2} \right)^{1/(2k+1)} + 1.$$

Так как

$$|Q| < \left(\frac{kt}{2|T|} \right)^{1/2} \left(\left(\frac{|R||T|}{8k} \right)^{1/2k} - 1 \right)^{2k+1},$$

то

$$2kB^{2k} \leq 8kB^{2k} \leq 8k \left(\left(2s \left(\frac{t|T|}{2k} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{2k} < t|T|. \quad (46)$$

Следовательно, все условия (40) утверждения 4.2 выполнены. Неравенство (41) той же леммы вытекает из оценки (45). Применяя утверждение 4.2 и (46), находим

$$\begin{aligned} \min_{\mu_1, \dots, \mu_k \in T} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k) \\ \leq \frac{(k+1)tB}{[(t|T|/(2kB^{2k}))^{1/2}]} \leq (8k)^{1/2}(k+1) \left(\frac{t}{|T|} \right)^{1/2} B^{k+1} \\ \leq (32k^3)^{1/2} \left(\frac{t}{|T|} \right)^{1/2} \left(\left(|Q| \left(\frac{2|T|}{k|R|} \right)^{1/2} \right)^{1/(2k+1)} + 1 \right)^{k+1}. \end{aligned}$$

Следствие доказано.

ЗАМЕЧАНИЕ 4.5. Можно несколько обобщить следствие 4.4, рассмотрев сумму $\sum_{\lambda \in Q_1} C_{k+1}(Q, R, \dots, R)(\mu_1, \dots, \mu_k)$, $Q_1 = RQ_1$, как в теореме 1.1.

§ 5. О суммах подгрупп

Мы начнем с простейших следствий, вытекающих из леммы 4.1 и теоремы 1.1.

СЛЕДСТВИЕ 5.1. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа, и пусть $Q, Q_1, Q_2 \subseteq \mathbb{Z}_p^*$ – произвольные R -инвариантные множества. Тогда справедливы следующие утверждения:

1) если $|Q| \ll |R|^3$, $|Q||R|^3 \ll p^3$, то

$$\sum_{x \in Q} (R \circ R)(x) \ll |R||Q|^{2/3}; \quad (47)$$

2) если $|Q||Q_1| \ll |R|^4$, $|Q||Q_1||R|^2 \ll p^3$, то

$$\sum_{x \in Q} (Q_1 \circ R)(x) \ll |R|^{1/3}(|Q||Q_1|)^{2/3}; \quad (48)$$

3) если $|Q||Q_1||Q_2| \ll |R|^5$, $|Q||Q_1||Q_2||R| \ll p^3$, то

$$\sum_{x \in Q} (Q_1 \circ Q_2)(x) \ll |R|^{-1/3}(|Q||Q_1||Q_2|)^{2/3}. \quad (49)$$

ЗАМЕЧАНИЕ 5.2. Ясно, что неравенство (49) можно немного усилить, если известна информация о мощности множества $\bigcup_{q \in Q} (q^{-1}Q_1 \times q^{-1}Q_2)$ – мультипликативного аналога множества из (7).

Из следствия 5.1 вытекает утверждение об аддитивной энергии R -инвариантного множества, которое немного обобщает аналогичный результат из [12]. Используя утверждение 5.3 ниже, легко получить (применяя, например, лемму 2.3), что любое R -инвариантное множество $Q \subseteq \mathbb{Z}_p^*$, для которого выполнено $|Q| \ll |R|^{3/2}$, $|Q||R|^{1/2} \ll p$ обладает свойством расширения, а именно $|Q \pm Q| \gg |Q||R|^{1/2}$.

УТВЕРЖДЕНИЕ 5.3. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа и $Q \subseteq \mathbb{Z}_p^*$ – произвольное R -инвариантное множество. Пусть также $|Q| \ll |R|^{3/2}$ и $|Q||R|^{1/2} \ll p$. Тогда

$$E(Q) \ll \frac{|Q|^3}{|R|^{1/2}}, \quad \max_{\xi \neq 0} |\widehat{Q}(\xi)| \ll |Q|^{7/8} |R|^{-1/4} p^{1/8}. \quad (50)$$

ДОКАЗАТЕЛЬСТВО. Пусть a – некоторый параметр. Имеем

$$E(Q) \leq a|Q|^2 + \sum_{x: (Q \circ Q)(x) \geq a} (Q \circ Q)^2(x).$$

Упорядочим значения $(Q \circ Q)(x)$, $x \in \mathbb{Z}_p/R$, по убыванию. Получим числа $N_1 \geq N_2 \geq \dots$. Из формулы (49) имеем $N_j \ll |Q|^{4/3} |R|^{-2/3} j^{-1/3}$. Отсюда

$$E(Q) \ll a|Q|^2 + |R| \sum_{j: j \ll |Q|^4/(|R|^2 a^3)} j^{-2/3} \cdot \frac{|Q|^{8/3}}{|R|^{4/3}} \ll a|Q|^2 + \frac{|Q|^4}{|R|a}.$$

Полагая $a = |Q|/|R|^{1/2}$, получаем требуемый результат. Второе неравенство в (50) вытекает из первого (см., например, доказательство следствия 2.5 из [13]).

Нам понадобится лемма из [13].

ЛЕММА 5.4. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа, $|R| \ll p^{2/3}$. Тогда

$$E_3(R) \ll |R|^3 \log |R|.$$

Получим теперь новый результат о константах удвоения мультипликативных подгрупп.

ТЕОРЕМА 5.5. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа. Если $|R| \ll p^{1/2}$, то

$$|R \pm R| \gg \frac{|R|^{5/3}}{\log^{1/2} |R|}. \quad (51)$$

ДОКАЗАТЕЛЬСТВО. Пусть $S = (R - R) \setminus \{0\}$ (для $R + R$ доказательство аналогичное) и $t = |R|$. Применяя лемму 2.3 и следствие 2.7, находим

$$|R|^6 \leq E_3(R) \cdot \sum_{x \in S} (S \circ S)(x).$$

Если $|S| \gg |R|^{5/3}$, то утверждение очевидно. В противном случае, имеем $|S|^3|R| \ll p^3$, поскольку $|R| \ll p^{1/2}$ по условию. Используя теперь оценку (49) следствия 5.1 с $Q = Q_1 = Q_2 = S$, а также лемму 5.4, получаем

$$|R|^6 \ll |R|^3 \log |R| \cdot |S|^2 |R|^{-1/3}.$$

Отсюда $|S| \gg |R|^{5/3} \log^{-1/2} |R|$. Теорема доказана.

Неравенство (51) дает ответ на один вопрос из работы [5]. Более слабая оценка для подгрупп с $|R| \ll \sqrt{p}$, но все же лучшая, чем (3), была получена Т. Чоеном и И. Д. Шкредовым в статье [13]. Наиболее сильный результат о мощностях сумм и разностей подгрупп $R \pm R$ с ограничением на мощность $\sqrt{p} \ll |R| \ll p^{2/3}$ содержится в статье [13]. Отметим следствие теоремы 5.5.

СЛЕДСТВИЕ 5.6. Пусть $R \subseteq \mathbb{Z}_p^*$ – мультипликативная подгруппа и действительное число $\kappa > 33/67$. Предположим, что $|R| \geq p^\kappa$. Тогда для всех достаточно больших p выполнено $\mathbb{Z}_p^* \subseteq 6R$.

Следствие 5.6 вытекает из теоремы 5.5 и доказывается аналогично теореме 4.1 из [13], в которой было установлено, что $\mathbb{Z}_p^* \subseteq 6R$ при $\kappa > 41/83$. Заметим, что из одного результата А. А. Глибичука [11] (см. также [25]) следует, что $|4R| > p/2$, если $|R| > \sqrt{p}$.

Список литературы

- [1] J. Bourgain, M.-C. Chang, “Exponential sums estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors”, *Geom. Funct. Anal.*, **16:2** (2006), 327–366.
- [2] J. Bourgain, “Multilinear exponential sums in prime fields under optimal entropy condition on the sources”, *Geom. Funct. Anal.*, **18:5** (2009), 1477–1502.
- [3] J. Bourgain, A. A. Glibichuk, S. V. Konyagin, “Estimates for the number of sums and products and for exponential sums in fields of prime order”, *J. London Math. Soc.* (2), **73:2** (2006), 380–398.
- [4] 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.
- [5] T. Cochrain, C. Pinner, “Sum-product estimates applied to Waring’s problem mod p ”, *Integers*, **8:1** (2008), A46.
- [6] T. Cochrain, C. Pinner, “Stepanov’s method applied to binomial exponential sums”, *Q. J. Math.*, **54:3** (2003), 243–255.
- [7] A. Garcia, J. F. Voloch, “Fermat curves over finite fields”, *J. Number Theory*, **30:3** (1988), 345–356.
- [8] D. R. Heath-Brown, S. Konyagin, “New bounds for Gauss sums derived from k -th powers, and for Heilbronn’s exponential sum”, *Q. J. Math.*, **51:2** (2000), 221–235.
- [9] S. V. Konyagin, I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Math., **136**, Cambridge Univ. Press, Cambridge, 1999.
- [10] A. A. Glibichuk, S. V. Konyagin, “Additive properties of product sets in fields of prime order”, *Additive combinatorics*, CRM Proc. Lecture Notes, **43**, Amer. Math. Soc., Providence, RI, 2007, 279–286.

- [11] А. А. Глибичук, “Комбинаторные свойства множеств вычетов по простому модулю и задача Эрдёша–Грэхэма”, *Матем. заметки*, **79:3** (2006), 384–395; англ. пер.: A. A. Glibichuk, “Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem”, *Math. Notes*, **79:3** (2006), 356–365.
- [12] С. В. Конягин, “Оценки для тригонометрических сумм на подгруппы и для гауссовых сумм”, IV интернац. конф. “Современные проблемы теории чисел и ее приложения”, Актуальные проблемы. Часть 3 (Тула, 2001), Изд-во Моск. ун-та, М., 2002, 86–114.
- [13] T. Schoen, I. D. Shkredov, “Additive properties of multiplicative subgroups of $\mathbb{F}_p$ ”, *Q. J. Math.*, 2011, 1–10.
- [14] И. Д. Шкредов, “О некоторых аддитивных задачах, связанных с показательной функцией”, *УМН*, **58:4** (2003), 165–166; англ. пер.: I. D. Shkredov, “Some additive problems connected with exponential functions”, *Russian Math. Surveys*, **58:4** (2003), 798–799.
- [15] S. Yekhanin, “A note on plane pointless curves”, *Finite Fields Appl.*, **13:2** (2007), 418–422.
- [16] С. А. Степанов, “О числе точек гиперэллиптической кривой над простым конечным полем”, *Изв. АН СССР. Сер. матем.*, **33:5** (1969), 1171–1181; англ. пер.: S. A. Stepanov, “On the number of points of a hyperelliptic curve over a finite prime field”, *Math. USSR-Izv.*, **3:5** (1969), 1103–1114.
- [17] N. H. Katz, P. Koester, “On additive doubling and energy”, *SIAM J. Discrete Math.*, **24:4** (2010), 1684–1693.
- [18] T. Sanders, *On a non-abelian Balog–Szemerédi-type lemma*, arXiv:0912.0306.
- [19] T. Sanders, *Structure in sets with logarithmic doubling*, arXiv:1002.1552.
- [20] T. Sanders, *On Roth’s theorem on progressions*, arXiv:1011.0104.
- [21] T. Schoen, “Near optimal bounds in Freiman’s theorem”, *Duke Math. J.* (to appear).
- [22] W. Rudin, *Fourier analysis on groups*, Wiley, New York, 1990.
- [23] T. Tao, V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006.
- [24] А. А. Болибрух, *Обратные задачи монодромии в аналитической теории дифференциальных уравнений*, МЦНМО, М., 2009.
- [25] M. Rudnev, *An improved estimate on sums of product sets*, arXiv:0805.2696.

И. В. Вьюгин (I. V. Vyugin)

Институт проблем передачи информации РАН, г. Москва
E-mail: vyugin@gmail.com

Поступила в редакцию

22.02.2011

И. Д. Шкредов (I. D. Shkredov)

Математический институт им. В. А. Стеклова РАН;
Лаборатория дискретной и вычислительной геометрии
им. Б. Н. Делоне
Ярославского государственного университета
им. П. Г. Демидова
E-mail: ilya.shkredov@gmail.com