С. А. Алешина, И. В. Вьюгин, О полиномиальном варианте задачи сумм-произведений для подгрупп, *Матем. заметки*, 2023, том 113, выпуск 1, 3–10

DOI: 10.4213/mzm13530

Математические заметки

Том 113 выпуск 1 январь 2023

УДК 511

О полиномиальном варианте задачи сумм-произведений для подгрупп

С. А. Алешина, И. В. Вьюгин

Мы обобщаем два результата работ [1], [2] о суммах подмножеств $\mathbb{F}_p$ на более общую ситуацию, когда вместо суммы $x+y$ рассматривается величина $P(x,y)$, где P – многочлен достаточно общего вида. В частности, получена нижняя оценка мощности множества значений многочлена $P(x,y)$, где переменные x и y принадлежат подгруппе G мультипликативной группа поля $\mathbb{F}_p$. Также мы доказываем, что если подгруппа G может быть представлена как множество значений многочлена $P(x,y)$ при $x \in A$, $y \in B$, то мощности множеств A и B по порядку близки к $\sqrt{|G|}$.

Библиография: 7 названий.

Ключевые слова: подгруппа, многочлен, задача сумм-произведений, задача множеств сумм.

DOI: https://doi.org/10.4213/mzm13530

1. Введение. Пусть $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ – поле вычетов по простому модулю p, $\mathbb{F}_p^*$ – мультипликативная группа поля $\mathbb{F}_p$. Рассмотрим множество

$$P(A,B) = \{P(a,b) \mid a \in A,\ b \in B\}, \tag{1}$$

где $P \in \mathbb{F}_p[x,y]$, а A и B – подмножества $\mathbb{F}_p$. Множество $P(A,B)$ будем называть *полиномиальной суммой множеств* A *и* B. В качестве частного случая можно рассмотреть многочлен $P(x,y) = x+y$. Тогда соответствующей ему полиномиальной суммой множеств является

$$A + B = \{a+b \mid a \in A,\ b \in B\}$$

– обыкновенная сумма Минковского в $\mathbb{F}_p$. Пусть $G \subset \mathbb{F}_p^*$ – подгруппа мультипликативной группы поля. Рассмотрим случай, когда $A = B = G$. Для мощности множества $|G+G|$ известны следующие оценки. Как следствие результата работы [3] для подгруппы G, такой, что $|G| \ll p^{3/4}$, выводится следующая нижняя оценка:

$$|G \pm G| \gg |G|^{4/3}.$$

Исследование выполнено за счет гранта Российского научного фонда № 19-11-00001, https://rscf.ru/project/19-11-00001/.

В этой формуле и ниже под “$\ll$” и “$\gg$” понимаются символы Виноградова. Это означает, что неравенство выполняется с точностью до мультипликативной константы, не зависящей от выбора подгруппы.

Д. Р. Хиф-Браун и С. В. Конягин усилили это неравенство (см. [4]):

$$|G \pm G| \gg |G|^{3/2} \tag{2}$$

для подгрупп $|G| \ll p^{2/3}$. Оценка

$$|G \pm G| \gg \frac{|G|^{5/3}}{\log^{1/2}|G|}\,.$$

для таких подгрупп, что $|G| \ll p^{1/2}$, $-1 \in G$, получена в [2]. Другие современные оценки мощностей этих множеств можно посмотреть в [5].

2. Основные результаты. Прежде чем сформулировать первую теорему, введем два определения.

Определение 1. Назовем однородный многочлен $P \in \mathbb{F}_p[x, y]$ *хорошим*, если многочлен $P(x, y)-1$ абсолютно неприводим (неприводим над алгебраическим замыканием $\overline{\mathbb{F}}_p$ поля $\mathbb{F}_p$) и хотя бы один из многочленов $P(x, 0) \in \mathbb{F}_p[x]$, $P(0, y) \in \mathbb{F}_p[y]$ не является нулевым.

Определение 2. Для простого числа p и натурального числа n назовем подгруппу $G \subset \mathbb{F}_p^*$ (n, p)-*допустимой*, если

$$100n^3 < |G| < \frac{1}{3}p^{1/2}.$$

Следующая теорема нашей работы обобщает оценку (2) на случай полиномиальной суммы.

Теорема 1. *Для любого n существует такое $C > 0$, что для любого простого p, (n, p)-допустимой подгруппы $G \in \mathbb{F}_p^*$ и хорошего многочлена $P(x, y)$ степени n выполнена оценка*

$$|P(G, G)| > C|G|^{3/2}.$$

Вторая теорема касается возможности представить подгруппу G в виде полиномиальной суммы

$$G = P(A, B), \tag{3}$$

множеств A и B. Множества $A, B \subset \mathbb{F}_p$ назовем *нетривиальными*, если они содержат не менее двух элементов и не совпадают со всей подгруппой G. Мы доказываем, что если представление (3) возможно, то мощности множеств A и B примерно равны $\sqrt{|G|}$ (см. часть 4). Этот результат обобщает результат И. Е. Шпарлинского (см. теорему 8 в [1]), доказанный им для многочлена $P(x, y) = x + y$, на случай многочленов $P(x, y)$ более общего вида.

Теорема 2. *Для любых k и l найдутся константы $K_1(k, l)$ и $K_2(k, l)$ такие, что для любой подгруппы $G \subset \mathbb{F}_p^*$ и многочлена $P(x, y)$ степеней k и l по переменным x и y, соответственно, и $A, B \subset \mathbb{F}_p$, удовлетворяющих условиями*

$$K_1 < |G| < K_2 p^{1-o(1)}, \qquad G = P(A, B), \qquad |A|, |B| > 1,$$

мощности множеств A и B равны $|G|^{1/2+o(1)}$, $p \to \infty$.

3. Многочлены на подгруппах (доказательство теоремы 1). Теорема 2 из статьи [6] может быть переформулированна для однородного многочлена $P(x,y)$ следующим образом.

Теорема 3. *Для любого n найдутся такие константы $C_1, C_2 > 0$, что для любых простого p, (n,p)-допустимой подгруппы $G \subset \mathbb{F}_p^*$, хорошего многочлена $P(x,y)$ степени n, натурального числа $h < C_2|G|^2$ и чисел $\alpha_1, \dots, \alpha_h \in \mathbb{F}_p^*$, принадлежащих различным смежным классам по подгруппе G, существует не более чем*

$$C_1 h^{2/3}|G|^{2/3}$$

пар (x,y), для которых $P(x,y) = \alpha_k$ для по крайней мере одного $k = 1, \dots, h$.

Значения констант могут быть выбраны следующим образом (см. [6]):

$$C_1 = 24n^4, \qquad C_2 = 40^{-3}n^{-9}.$$

Докажем следующую лемму.

Лемма 1. *Если $P(x,y)$ – хороший многочлен, тогда многочлен $P(x,y) - \alpha$, где $\alpha \in \mathbb{F}_p^*$, абсолютно неприводим.*

Доказательство. Пусть $\alpha \in \mathbb{F}_p^*$. Обозначим через $a = \sqrt[n]{1/\alpha}$ произвольный корень n-го поряка из $1/\alpha$ в алгебраическом замыкании $\overline{\mathbb{F}}_p$. Рассмотрим многочлен

$$P_a(x,y) = P(ax, ay) - 1.$$

Предположим, что $P_a(x,y)$ – приводимый, т.е.

$$P_a(x,y) = P(ax,ay) - 1 = Q_1(x,y)Q_2(x,y), \tag{4}$$

где $Q_1(x,y)$ и $Q_2(x,y)$ не являются константами. Подставим x/a и y/a вместо x и y в уравнении (4). Получим, что

$$P_a\left(\frac{x}{a}, \frac{y}{a}\right) = P(x,y) - 1 = Q_1\left(\frac{x}{a}, \frac{y}{a}\right)Q_2\left(\frac{x}{a}, \frac{y}{a}\right),$$

т.е. $P(x,y) - 1$ тоже приводимый, а это противоречит предположению. Таким образом имеем

$$P_a(x,y) = P(ax,ay) - 1 = a^n P(x,y) - 1 = \frac{P(x,y)}{\alpha} - 1$$

неприводим. Умножив $P_a(x,y)$ на α, получим неприводимый многочлен

$$P(x,y) - \alpha = \alpha P_a(x,y).$$

Доказательство теоремы 1. Предположим противное. Это означает, что существует такое n, что условие теоремы не выполнено, т.е. для любой константы C существуют такие подгруппа G и многочлен $P(x,y)$, что

$$|P(G,G)| \leqslant C|G|^{3/2}.$$

Такие пары (P,G) для константы C мы назовем плохими.

Чтобы придти к противоречию, применим теорему 3. Для заданного n должны найтись константы $C_1, C_2 > 0$, удовлетворяющие условию теоремы 1. Найдем $C > 0$ такое, что

$$C < C_2, \qquad C_1 C^{2/3} < \frac{100n^2 - 1}{100n^2}\,.$$

Смысл этого станет ясен позже.

Возьмем для данного C произвольную плохую пару (P, G). Все возможные значения $P(G,G)$, не превосходящие $C|G|^{3/2}$ и отличные от нуля, можно расположить в виде диаграммы Юнга таким образом, что каждая строка содержит значения из одного G-класса смежности, а в разных строках – из разных классов смежности. Таким образом, каждая строка полученной диаграммы содержит не более $|G|$ элементов. Оценим сверху количество пар (x, y), для которых значение $P(x, y)$ лежит в том или ином столбце.

1) Количество пар, для которых $P(x, y) = 0$, не превышает $n|G|$.

Действительно, многочлен $P(x, y)$ однородный, а это значит, что при $x = x_0 \neq 0$ многочлен $P(x_0, y) \in \mathbb{F}_p[y]$ не равен тождественно нулю. Оно имеет не более n корней. Оценим количество таких пар (x, y), что

$$P(x, y) = 0, \qquad (x, y) \in G \times G. \tag{5}$$

Пусть $x_0 \in G$; это означает, что $x_0 \neq 0$. Тогда количество пар $(x_0, y) \in G \times G$, $P(x_0, y) = 0$ не больше чем n, поэтому общее число пар (5) не больше $n|G|$, так как для каждого $x \in G$ существует не более $n|G|$ пар.

2) Если какой-либо столбец содержит h элементов, то можно заметить, что

$$h \leqslant |P(G,G)| \leqslant C|G|^{3/2} < C_2|G|^{3/2};$$

следовательно, поскольку все элементы столбца лежат в разных смежных классах, согласно теореме 3, существует не более $C_1 h^{2/3}|G|^{2/3}$ пар (x, y), для которых $P(x, y)$ лежит в этом столбце.

Теперь обозначим длины столбцов через $h_1, h_2, \ldots, h_{|G|}$ и оценим общее количество пар:

$$|G|^2 < n|G| + \sum_{k=1}^{|G|} C_1 h_k^{2/3} |G|^{2/3}.$$

С другой стороны, по неравенству для степенных средних имеем

$$\left(\frac{1}{|G|}\sum_{k=1}^{|G|} h_k^{2/3}\right)^{3/2} \leqslant \frac{1}{|G|}\sum_{k=1}^{|G|} h_k.$$

Сумма всех h_k – это общее количество ячеек в таблице, поэтому оно не превосходит $C|G|^{3/2}$, откуда получаем

$$|G|^2 < n|G| + C_1|G|^{2/3}\cdot|G|\left(\frac{C|G|^{3/2}}{|G|}\right)^{2/3} = n|G| + C_1C^{2/3}|G|^2 < n|G| + \frac{(100n^2-1)|G|^2}{100n^2}\,.$$

Неравенство $|G| > 100n^3$ (см. определение 2) в совокупности с полученным выше неравенством приводит нас к противоречию; следовательно, теорема доказана.

Мы имеем следующее значение константы C:

$$C = \min\biggl(\Bigl(\frac{100n^2-1}{100n^2C_1}\Bigr)^{3/2}; C_2\biggr).$$

4. Полиномиальная версия задачи о множестве сумм (доказательство теоремы 2). Рассмотрим подгруппу $G \subset \mathbb{F}_p^*$, классы смежности $G_1, \dots, G_n$ по подгруппе G ($G_i = g_iG$, где $g_i \in \mathbb{F}_p^*$, $1 \leqslant i \leqslant n$, при этом смежные классы могут совпадать), а также рассмотрим отображение

$$f\colon x \mapsto (f_1(x), \dots, f_n(x)) \in \mathbb{F}_p^n, \qquad n \geqslant 2$$

с многочленами $f_1(x), \dots, f_n(x) \in \mathbb{F}_p[x]$.

Определение 3. Назовем множество многочленов $f_1(x), \dots, f_n(x)$ *допустимым*, если каждый из многочленов $f_i(x)$ имеет хотя бы один корень $x_i \neq 0$, принадлежащий алгебраическому замыканию $x_i \in \overline{\mathbb{F}}_p$), несовпадающий ни с одним из корней других многочленов, т.е.

$$f_i(x_i) = 0, \quad f_j(x_i) \neq 0, \quad i \neq j, \quad 1 \leqslant i, j \leqslant n; \qquad x_i \neq x_j, \quad x \neq j,$$

и каждый из f_i имеет ненулевой свободный член $f_i(0) \neq 0$, $i = 1, \dots, n$.

В статье [7] получена верхняя оценка мощности множества

$$M = \{x \mid f_i(x) \in G_i, i = 1, \dots, n\},$$

где $G_i = g_iG$ $(i = 1, \dots, n)$ – смежные классы по подгруппе G.

Теорема 4. *Пусть $G \subset \mathbb{F}_p^*$ – подгруппа (p – простое число), $G_1, \dots, G_n$ – G-классы смежности, $f_1(x), \dots, f_n(x)$ – допустимый набор многочленов степеней соответственно $m_1, \dots, m_n$. Пусть также выполняется неравенство*

$$C_1(m, n) < |G| < C_2(m, n)p^{1-1/(2n+1)},$$

где $C_1(m, n)$, $C_2(m, n)$ – константы, зависящие от n и $m = (m_1, \dots, m_n)$. Тогда имеет место следующая оценка:

$$|M| \leqslant C_3(m, n)|G|^{1/2+1/(2n)},$$

а константы могут быть выбраны следующими:

$$C_1(m, n) = 2^{2n}(\max m_i)^{4n}, \qquad C_2(m, n) = (n+1)^{-2n/(2n+1)}(m_1 \dots m_n)^{-2/(2n+1)},$$
$$C_3(m, n) = 4(n+1)(m_1 \dots m_n)^{1/n}\sum_{i=1}^{n} m_i.$$

Определение 4. Многочлен $P(x, y) \in \mathbb{F}_p[x, y]$ назовем *требуемым*, если он не делится ни на один из многочленов от x или от y, не равных константе, что означает

$$f(x) \mid P(x, y) \Rightarrow f(x) \equiv \mathrm{const},$$
$$g(y) \mid P(x, y) \Rightarrow g(y) \equiv \mathrm{const}.$$

Лемма 2. *Для любого требуемого многочлена* $P(x,y)$, *где* $\deg_x P = k$, $\deg_y P = l$, *среди многочленов* $f_i(x) = P(x,y_i)$, *где* $y_1,\dots,y_h$ – *различные элементы* $\mathbb{F}_p$, *можно найти допустимый набор* $f_{i_1},\dots,f_{i_N}$ *из* $N = [(h-2l)/kl]$ *многочленов.*

Доказательство. Можно заметить, что число $x = r$ может быть корнем не более чем l многочленов $f_i(x) = P(x,y_i)$, $i = 1,\dots,h$. Обратное означало бы, что многочлен $g(y) = P(r,y)$ имеет более l корней, но его степень не выше $\deg_y P(x,y) = l$. Следовательно, он должен быть равен нулю, но в этом случае $P(x,y)$ делился бы на $(x-r)$, что противоречит тому, что $P(x,y)$ – требуемый.

Выделим из множества $y_1,\dots,y_h$ все y_i, которые являются корнями старшего коэффициента $p_k(y)$ и свободного члена $p_0(y)$ многочлена

$$P(x,y) = p_k(y)x^k + \dots + p_0(y), \tag{6}$$

рассматриваемого как многочлена переменной x. Очевидно, что число таких y_i не больше $2l$, так как и старший, и свободный члены являются ненулевыми многочленами переменной y, степень которых не превышает l (свободный член отличен от нуля, так как P – требуемый и, соответственно, не может делиться на x).

Из оставшихся не менее $h-2l$ значений y_i можно выбрать любое такое, что многочлен $f_i(x) = P(x,y_i)$ имеет не более k корней (поскольку старший член (6) отличен от нуля). Выберем все y_j такие, что $f_j(x) = P(x,y_j)$ имеет хотя бы один общий корень с $f_i(x) = P(x,y_i)$. Из вышеизложенного видно, что для каждого многочлена $f_i(x) = P(x,y_i)$, имеющего не более k корней, существует не более l многочленов из множества, имеющих этот корень. Следовательно, существует не более kl многочленов, имеющих общий с $P(x,y_i)$ корень. Повторим этот процесс: из оставшихся y_i можно выбрать одно и вынести не более kl значений y_j таких, что этот многочлен имеет хотя бы один общий корень с рассматриваемым многочленом. В конце можно выбрать как минимум $[(h-2l)/kl]$ многочленов $f_i(x) = P(x,y_i)$, что никакие два из них не имеют общих корней. Также видно, что эти многочлены имеют ненулевой свободный член, так как были удалены все y_i, которые делают его равным нулю. Поэтому взятое множество допустимо.

Доказательство теоремы 2. Пусть $h(n,k,l)$ – минимальное значение h, которое необходимо взять в лемме 2 так, чтобы из множества h значений y было n допустимых многочленов. Он существует по лемме 2 и не превышает $nkl + 2l$. Пусть $\delta > 0$ и $\varepsilon > 0$ – индексы, которые можно взять в формулировке теоремы вместо $o(1)$. Это означает, что

$$|G| < K_2 p^{1-\delta},$$

и требуется доказать, что

$$|G|^{1/2-\varepsilon} < |A|, |B| < |G|^{1/2+\varepsilon}.$$

Возьмем $q \geqslant 2$ такое, что

$$1 - \frac{1}{(2q+1)} > 1 - \delta.$$

Выберем K_2 так, чтобы для каждого p:

$$K_2 p^{1-\delta} < \frac{(p/k)^{1-1/(2q+1)}}{(q+1)}.$$

Пусть $|A|, |B| > h(q,k,l)$. Тогда по лемме 2 из $|B|$ значений y можно выбрать q таких, что при подстановке в P будет допустимое множество из q многочленов. Применим теорему 4 к этому множеству и смежным классам $G_i = g_iG$, $i = 1, \dots, h$. Это можно сделать, поскольку последнее неравенство преобразуется в

$$|G| < \frac{(p/k)^{1-1/(2q+1)}}{(q+1)},$$

вытекающее из первого условия и выбора q, K_2. Константа в теореме 2 зависит только от k и δ, поскольку $m = (\underbrace{k, \dots, k}_{q \text{ штук}})$. Левые неравенства в теореме 2 выполняются, если G достаточно велико и k, l, δ фиксированы. Множество M для таких малых смежных классов включает A. Это означает, что

$$|A| \leqslant C_1(k,\delta)|G|^{1/2+1/(2q)} \leqslant C_1(k,\delta)|G|^{3/4}.$$

Применяя тот факт, что

$$|A|\,|B| \geqslant |G|,$$

так как многочлен P определяет сюръективной отображение $P\colon A \times B \to G$, получаем

$$|B| \geqslant \left(\frac{1}{C_1(k,\delta)}\right)|G|^{1/4}.$$

Отсюда можно доказать, что для любого n существует такая константа $C_2(k,l,n,\delta)$, что

$$|A| < C_2(k,l,n,\delta)|G|^{1/2+1/(2n)}.$$

Если

$$\left(\frac{1}{C_1(k,\delta)}\right)|G|^{1/4} \geqslant h(n,k,l),$$

то из

$$|B| > h(q,k,l)$$

следует, что

$$|B| > h(n,k,l).$$

Применим теорему 4 еще раз, для множества n подстановок y из B и смежных классов, равных G; тогда

$$|A| \leqslant C_2(k,l,n,\delta)|G|^{1/2+1/(2n)}$$

для каждого

$$|G| \geqslant \left(\frac{h(n,k,l)}{C_1(k,\delta)}\right)^4.$$

Правая часть последнего неравенства зависит только от k, l, n, δ, поэтому, увеличивая константу $C_2(k,l,n,\delta)$ еще больше, ее можно получить и в других случаях.

При этом можно получить

$$|B| \leqslant C_3(k,l,n,\delta)|G|^{1/2+1/(2n)},$$

используя условие симметричности. Из

$$|A||B| \geqslant |G|$$

следует, что для другой константы $C_4(k, l, n, \delta)$ имеет место

$$|A|, |B| \geqslant C_4(k, l, n, \delta)|G|^{1/2-1/(2n)}.$$

Поскольку n может быть максимально большим, $1/(2n)$ можно взять меньше ε. Существование таких констант означает, что

$$|G|^{1/2-\varepsilon} < |A|, |B| < |G|^{1/2+\varepsilon}.$$

В заключение авторы выражают благодарность Андрею Волгину и рецензенту за сделанные ими полезные замечания.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] I. E. Shparlinski, “Additive Decompositions of Subgroups of Finite Fields”, *SIAM J. Discrete Math.*, **27**:4 (2013), 1870–1879.

[2] И. В. Вьюгин, И. Д. Шкредов, “Об аддитивных сдвигах мультипликативных подгрупп”, *Матем. сб.*, **203**:6 (2012), 81–100.

[3] A. Garcia, J. Voloch, “Fermat curves over nite elds”, *J. Number Theory*, **30**:3 (1988), 345–356.

[4] D. Heath-Brown, S. Konyagin, “New bounds for Gauss sums derived from k-thpowers, and for Heilbronn’s exponential sum”, *Q. J. Math.*, **51**:2 (2000), 221–235.

[5] B. Murphy, M. Rudnev, I. Shkredov, Y. Shteinikov, *J. Théor. Nombres Bordeaux*, **31**:3 (2019), 573–602.

[6] S. Makarychev, I. Vyugin, “Solutions of polynomial equation over $\mathbb{F}_p$ and new bounds of additive energy”, *Arnold Math J.*, **5**:1 (2019), 105–121.

[7] И. В. Вьюгин, “Оценка числа прообразов полиномиального отображения”, *Матем. заметки*, **106**:2 (2019), 212–221.

С. А. Алешина
University of Malaga, Испания
E-mail: aleshina.sofia@mail.ru

И. В. Вьюгин
Институт проблем передачи информации
им. А.А. Харкевича Российской академии наук,
г. Москва;
Национальный исследовательский университет
“Высшая школа экономики”, г. Москва;
Математический институт им. В.А. Стеклова
Российской академии наук, г. Москва
E-mail: ilyavyugin@yandex.ru

Поступило
06.04.2022
После доработки
19.07.2022
Принято к публикации
20.08.2022