ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2018. Том 25, № 4. С. 97–111

УДК 519.1 DOI: 10.17377/daio.2018.25.608

ЧИСЛО k-СУММ В АБЕЛЕВОЙ ГРУППЕ *)

А. А. Сапоженко[a], *В. Г. Саргсян*[b]

Московский гос. университет им. М. В. Ломоносова,
Ленинские горы, 1, 119991 Москва, Россия

E-mail: [a]sapozhenko@mail.ru, [b]vahe_sargsyan@ymail.com

Аннотация. Сумма подмножеств $A_1, \ldots, A_k$ абелевой группы G определяется как совокупность всех сумм k элементов из множеств $A_1, \ldots, A_k$, т. е. $A_1 + \cdots + A_k = \{a_1 + \cdots + a_k \mid a_1 \in A_1, \ldots, a_k \in A_k\}$. Подмножество, представимое в виде суммы k подмножеств абелевой группы G, назовём *k-суммой*. Рассматривается задача о числе k-сумм в абелевой группе G. Очевидно, что любое подмножество A абелевой группы G является k-суммой, так как подмножество A можно представить в виде суммы $A = A_1 + \cdots + A_k$, где $A_1 = A$ и $A_2 = \cdots = A_k = \{0\}$. Тем самым число k-сумм равно количеству всех подмножеств абелевой группы G. Однако если ввести ограничение на мощность слагаемых $A_1, \ldots, A_k$, то число k-сумм становится существенно меньше. Получены нижняя и верхняя асимптотические оценки на число k-сумм в абелевых группах при условии, что существует слагаемое A_i такое, что $|A_i| \geqslant n \log^q n$ и $|A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| \geqslant n \log^q n$, где $q = -1/8$ и $i \in \{1, \ldots, k\}$. Библиогр. 8.

Ключевые слова: множество, характеристическая функция, группа, прогрессия, смежный класс.

Введение

Пусть G — абелева группа порядка n, а k — натуральное число, $k \geqslant 2$. Сумма подмножеств $A_1, \ldots, A_k$ абелевой группы G определяется следующим образом:

$$A_1 + \cdots + A_k = \{a_1 + \cdots + a_k \mid a_1 \in A_1, \ldots, a_k \in A_k\}.$$

Подмножество, представимое в виде суммы k подмножеств абелевой группы G, назовём *k-суммой*. Заметим, что число подмножеств в абелевой

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 16–01–00593а).

группе G порядка n равно 2^n и любое из них является *k-суммой,* так как $A = A + \underbrace{\{0\} + \cdots + \{0\}}_{k-1}$ для любого $A \subseteq G$. Однако если ввести ограничение на мощность слагаемых, то число k-сумм становится существенно меньше.

В [7] показано, что в группе простого порядка p число различных подмножеств $A + A$ равно $2^{p/3+\bar{o}(p)}$ (здесь и далее запись $\bar{o}(p)$ означает «о-малое от p»). Аналогичная оценка получена в [1] для числа различных подмножеств $A - A$ в группе простого порядка p. Для конечной абелевой группы G определим $D(G)$ как мощность наибольшей по мощности собственной подгруппы группы G, $\varphi(n)$ — функция Эйлера. В [2] доказано, что в абелевой группе G порядка n и экспоненты ν имеется по меньшей мере $\nu\varphi(\nu)2^{\nu/3}$ различных подмножеств как типа $A + A$, так и $A - A$. Кроме того, число таких подмножеств не превышает $2^{n/3+D(G)/3+\bar{o}(n)}$.

Обозначим циклическую группу порядка n через Z_n. Пусть p — простое число. Обозначим через $f(p)$ максимальное целое число такое, что любое подмножество $B \subseteq Z_p$ мощности не меньше $p - f(p)$ можно представить в виде $B = A + A$ для некоторого $A \subseteq Z_p$.

Грин (см. [5, 6]) доказал, что существует целое число p_0 такое, что для всех $p > p_0$ справедливо

$$f(p) \geqslant \frac{1}{9}\log p.$$

Здесь и далее логарифмы берутся по основанию два.

В [6] доказано, что существует абсолютная положительная константа c такая, что для всех p имеет место

$$f(p) \leqslant cp^{2/3}\log^{1/3} p.$$

В [3] доказано, что существуют две положительные константы c_1, c_2 и целое число p_0 такие, что для всех $p > p_0$ верно

$$c_1\frac{\sqrt{p}}{\sqrt{\log p}} \leqslant f(p) \leqslant c_2\frac{p^{2/3}}{\log^{1/3} p}.$$

В [4] доказано, что в группе простого порядка p имеется $2^{p/2+\bar{o}(p)}$ различных подмножеств $A+B$ при условии, что $|A|, |B| \to \infty$ при $n \to \infty$.

Обозначим через $S(G)$ семейство различных подмножеств $A_1 + \cdots + A_k$ при условии, что существует A_i такое, что $|A_i| \geqslant n(\log n)^{-1/8}$ и $|A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| \geqslant n(\log n)^{-1/8}$, $i \in \{1, \ldots, k\}$. Основным результатом этой работы является

Теорема 1. *Пусть G — абелева группа порядка n и экспоненты ν. Тогда при $n, \nu \to \infty$ справедливы неравенства*

$$2^{\nu/2+\bar{o}(\nu)} \leqslant |S(G)| \leqslant 2^{n/2+D(G)/2+\bar{o}(n)}.$$

1. Нижняя оценка числа k-сумм в абелевой группе

При доказательстве нижней оценки будут использованы следующие леммы.

Лемма 1. *Пусть G — абелева группа. Тогда следующие утверждения эквивалентны:*

(i) *экспонента группы G делится на d;*

(ii) *существует подгруппа H группы G такая, что фактор-группа G/H изоморфна циклической группе порядка d.*

Доказательство следующей леммы можно найти в [8, лемма 3.4].

Лемма 2. *Пусть n — достаточно большое натуральное число, M — множество мощности n, а ρ — вещественное число, меньшее некоторой абсолютной положительной константы. Тогда число подмножеств множества M мощности, не превышающей ρn, не превосходит $2^{n\sqrt{\rho}}$.*

Лемма 3. *При $n \to \infty$ справедливо неравенство*

$$|S(Z_n)| \geqslant 2^{n/2+\bar{o}(n)}.$$

Доказательство. Для каждого s положим

$$A_1 = \{0, \lfloor (n-s)/2 \rfloor + 1, \lfloor (n-s)/2 \rfloor + 2, \ldots, \lfloor (n-s)/2 \rfloor + s - 1\} \subseteq Z_n$$

(здесь и далее $\lfloor x \rfloor, \lceil x \rceil$ — округление вещественного числа x до ближайшего целого в меньшую и большую стороны соответственно).

Положим

$$A_3 = \cdots = A_k = \{0\}.$$

Заметим, что для каждого подмножества $A_2 \subseteq \{0, 1, \ldots, \lfloor (n-s)/2 \rfloor\}$ справедливо

$$A_2 = (A_1 + \cdots + A_k) \cap \{0, 1, \ldots, \lfloor (n-s)/2 \rfloor\}.$$

Отсюда следует, что все множества $A_1 + \cdots + A_k$ попарно различны. Следовательно, в группе Z_n существует по меньшей мере $2^{\lfloor (n-s)/2 \rfloor + 1}$ различных подмножеств вида $A_1 + \cdots + A_k$. Положим $s = \lceil n(\log n)^{-1/8} \rceil$.

Из леммы 2 следует, что число подмножеств, мощность которых не превышает $n(\log n)^{-1/8}$, не больше чем $2^{n\sqrt{(\log n)^{-1/8}}}$. Стало быть, число различных подмножеств $A_1 + \cdots + A_k$ таких, что существует A_i такое, что $|A_i| \geqslant n(\log n)^{-1/8}$ и $|A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| \geqslant n(\log n)^{-1/8}$, $i \in \{1, \ldots, k\}$, не меньше $2^{\lfloor (n-s)/2 \rfloor + 1} - 2^{n\sqrt{(\log n)^{-1/8}}}$. Тем самым

$$|S(Z_n)| \geqslant 2^{n/2+\bar{o}(n)} \quad \text{при } n \to \infty.$$

Лемма 3 доказана.

Теорема 2. *Пусть G — абелева группа экспоненты ν, а k — натуральное число, $k \geqslant 2$. Тогда при $\nu \to \infty$ справедлива оценка*

$$|S(G)| \geqslant 2^{\nu/2+\bar{o}(\nu)}.$$

Доказательство. Из леммы 1 следует, что существует подгруппа H абелевой группы G такая, что фактор-группа G/H изоморфна Z_ν. Представим группу G следующим образом:

$$G = H \cup (g + H) \cup \cdots \cup ((\nu - 1)g + H),$$

где $g \in G$, $\operatorname{ord}(g) = \nu$ — порядок элемента g.

Пусть A' — подмножество фактор-группы G/H. Тогда

$$A' = \{(i_1 g + H), \ldots, (i_{|A'|} g + H) \mid \{i_1, \ldots, i_{|A'|}\} \subseteq \{0, \ldots, (\nu - 1)\}\}.$$

Построим множество $A(A')$ следующим образом:

$$A(A') = \{i_1 g, \ldots, i_{|A'|} g \mid \{i_1, \ldots, i_{|A'|}\} \subseteq \{0, \ldots, (\nu - 1)\}\} \subseteq G.$$

Иными словами, $A(A')$ является множеством представителей смежных классов A'.

Нетрудно убедиться, что если $A'_1, A'_2 \subseteq G/H$ различны, то различны и $A_1(A'_1), A_2(A'_2) \subseteq G$, где $A_1(A'_1), A_2(A'_2)$ — множества представителей смежных классов множеств A'_1 и A'_2 соответственно.

Пусть B' — любое подмножество фактор-группы G/H. Предположим, что B' является k-суммой в фактор-группе G/H, т. е. $B' = A'_1 + \cdots + A'_k$ для некоторых $A'_1, \ldots, A'_k \subseteq G/H$. Определим множество $B(B')$ как множество представителей смежных классов множества $A'_1 + \cdots + A'_k$. Несложно заметить, что $B(B') = A_1(A'_1) + \cdots + A_k(A'_k)$, другими словами, $B(B')$ равно сумме множеств представителей смежных классов множеств $A'_1, \ldots, A'_k$. В силу леммы 1 фактор-группа G/H изоморфна Z_ν. Отсюда и из леммы 3 вытекает справедливость теоремы 2.

2. Гранулирование

Обозначим множества вещественных и комплексных чисел через $\mathbb{R}$ и $\mathbb{C}$ соответственно. Пусть G — абелева группа порядка n, k — натуральное число, $k \geqslant 2$ и $f_1, \ldots, f_k \colon G \to \mathbb{R}$. *Свёрткой функций* $f_1, \ldots, f_k$ называется функция $(f_1 * \cdots * f_k)(x)$, определяемая равенством

$$(f_1 * \cdots * f_k)(x) = \sum_{x_1 \in G} \cdots \sum_{x_{k-1} \in G} f_1(x_1) \ldots f_{k-1}(x_{k-1}) f_k(x - x_1 - \cdots - x_{k-1}).$$

Характером группы G называется отображение $\gamma \colon G \to \mathbb{C}$ такое, что $|\gamma(x)| = 1$ и $\gamma(x+y) = \gamma(x)\gamma(y)$ для любых $x, y \in G$. Обозначим через Γ множество всех характеров группы G. Несложно заметить, что Γ образует группу с операцией $\gamma_1 \star \gamma_2(x) = \gamma_1(x)\gamma_2(x)$. *Преобразование Фурье* $\widehat{f} \colon \Gamma \to \mathbb{C}$ функции $f \colon G \to \mathbb{R}$ определяется равенством $\widehat{f}(\gamma) = \sum\limits_{x \in G} f(x)\gamma(x)$.

Следующая лемма доказана в [2, лемма 6].

Лемма 4. *Для любого $\gamma \in \Gamma$ выполняется равенство*

$$\widehat{(f_1 * \cdots * f_k)}(\gamma) = \widehat{f}_1(\gamma) \ldots \widehat{f}_k(\gamma).$$

Рассмотрим непустые подмножества $A_1, \ldots, A_k$ абелевой группы G, при этом пусть $A_1(x), \ldots, A_k(x)$ — характеристические функции множеств $A_1, \ldots, A_k$ соответственно. Тогда $(A_1 * \cdots * A_k)(x)$ есть число наборов $(x_1, \ldots, x_k) \in A_1 \times \cdots \times A_k$ таких, что $x = x_1 + \cdots + x_k$. Определим

$$S_h(A_1, \ldots, A_k) = \{x \in G \mid (A_1 * \cdots * A_k)(x) \geqslant h\}.$$

Доказательство следующей леммы можно найти в [8, следствие 6.2].

Лемма 5. *Пусть G — абелева группа порядка n, A, B — непустые подмножества группы G и $h > 0$ такое, что $\sqrt{hn} \leqslant \min(|A|, |B|)$. Тогда справедлива оценка*

$$|S_h(A, B)| \geqslant \min(n, |A| + |B| - D(G)) - 3\sqrt{hn}.$$

L-гранулой типа смежного класса называется объединение смежных классов группы G по некоторой подгруппе порядка не меньше L.

Пусть L — целое число и $d \in G$, причём $\operatorname{ord}(d) \geqslant L$. Пусть H — подгруппа группы G, порождённая элементом d. Разобьём каждый смежный класс подгруппы H на $\lfloor \operatorname{ord}(d)/L \rfloor$ прогрессий вида $\{x + id \mid 0 \leqslant i \leqslant$

$L-1\}$ и одно «остаточное» множество мощности менее L. Для каждого $d \in G$ фиксируем одно такое разбиение. Объединение полученных прогрессий (в объединение не входят «остаточные» множества) называется *L-гранулой типа прогрессии*.

Отметим, что в определении L-гранулы типа смежного класса (прогрессии) речь идёт об объединении произвольных смежных классов (прогрессий).

Следующая лемма доказана в [8, лемма 3.3].

Лемма 6. *Пусть n — достаточно большое натуральное число, G — абелева группа порядка n и $L \leqslant \sqrt{n}$. Тогда в группе G имеется не более $2^{3n/L}$ L-гранул обоих типов (прогрессии и смежного класса).*

Лемма 7. *Пусть n — достаточно большое натуральное число, G — абелева группа порядка n, $A_1, \dots, A_k$ — произвольные подмножества группы G, $0 < \varepsilon < 1/2$, $0 < \delta = \delta(k) < 1$, L и L' — положительные числа, удовлетворяющие неравенству*

$$n > L'(4L/\varepsilon)^{4\delta^{-2}}.$$

Тогда существует подмножество $P \subseteq G$ такое, что

(i) *P — либо прогрессия вида $\{id \mid -(L-1) \leqslant i \leqslant L-1\}$, причём $\operatorname{ord}(d) \geqslant 2L/\varepsilon$, либо подгруппа группы G порядка не менее L';*

(ii) *для любого $\gamma \in \Gamma$ имеют место неравенства $|\widehat{A}_i(\gamma)(1-g(\gamma))| \leqslant \delta n$, где $i = 1, \dots, k$, $g(\gamma) = |P|^{-1} \sum\limits_{p \in P} \gamma(p)$, а $A_1(x), \dots, A_k(x)$ — характеристические функции множеств $A_1, \dots, A_k$ соответственно.*

Доказательство. Рассмотрим R — множество характеров γ таких, что $\bigl|\widehat{A}_i(\gamma)\bigr| > \delta n/2$, $i = 1, \dots, k$, и пусть Γ_1 — подгруппа группы Γ, порождённая множеством R. Пусть G_1 — подгруппа абелевой группы G

$$G_1 = \{x \in G \mid \gamma(x) = 1 \ \forall \gamma \in \Gamma_1\}.$$

Рассмотрим два случая.

1. Пусть $|G_1| \geqslant L'$. Положим $P = G_1$. Так как $g(\gamma) \in [-1, 1]$, при $\gamma \in \Gamma \setminus \Gamma_1$ получим

$$|\widehat{A}_i(\gamma)(1-g(\gamma))| \leqslant 2|\widehat{A}_i(\gamma)| < 2\delta n/2 = \delta n, \quad i = 1, \dots, k,$$

а при $\gamma \in \Gamma_1$ справедливо равенство $|\widehat{A}_i(\gamma)(1-g(\gamma))| = 0$, $i = 1, \dots, k$.

2. Пусть $|G_1| < L'$. Будем выбирать такое d, что если в качестве P возьмём прогрессию $P = \{id \mid -(L-1) \leqslant i \leqslant L-1\}$, то требования пп. (i)

и (ii) будут удовлетворены. Отметим, что при $\gamma \in \Gamma \setminus \Gamma_1$ п. (ii) выполнен. Оценим величину $1 - g(\gamma)$. Фиксируем $\gamma \in \Gamma$ и через β обозначим $\arg \gamma(d) \in [-\pi, \pi)$. Имеем

$$\begin{aligned} 0 \leqslant 1 - g(\gamma) &= 1 - \frac{1}{2L-1} \sum_{j=-L-1}^{L-1} (\cos j\beta + i \sin j\beta) \\ &= 1 - \frac{1}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta = \frac{2L-2}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta \\ &= \frac{2}{2L-1} \sum_{j=1}^{L-1} (1 - \cos j\beta) \leqslant \frac{1}{2L-1} \sum_{j=1}^{L-1} (j\beta)^2 = \frac{L(L-1)}{6} \beta^2 \leqslant \frac{(L\beta)^2}{6}. \end{aligned}$$

Нетрудно убедиться, что если для всех $\gamma \in R$ имеет место

$$|\arg \gamma(d)| \leqslant L^{-1} \min(\sqrt{6\delta n / |\widehat{A}_1(\gamma)|}, \ldots, \sqrt{6\delta n / |\widehat{A}_k(\gamma)|}),$$

то п. (ii) выполнен. Также отметим, что для выполнения условия

$$\operatorname{ord}(d) \geqslant 2L/\varepsilon$$

достаточно того, чтобы при некотором $\gamma \in \Gamma$ имело место неравенство

$$0 < |\arg \gamma(d)| < 2\pi \cdot \frac{\varepsilon}{2L} = \frac{\pi\varepsilon}{L}.$$

Покажем, что можно выбрать такое $d \notin G_1$, что при всех $\gamma \in R$ справедливо

$$|\arg \gamma(d)| \leqslant L^{-1} \min(\pi\varepsilon, \sqrt{6\delta n / |\widehat{A}_1(\gamma)|}, \ldots, \sqrt{6\delta n / |\widehat{A}_k(\gamma)|}).$$

Нетрудно убедиться, что если $d_1, d_2 \in G$ принадлежат различным смежным классам G по G_1, т. е. $d_1 - d_2 \notin G_1$, то существует характер $\gamma \in R$ такой, что $\gamma(d_1) \neq \gamma(d_2)$. Таким образом, для существования $d = d_1 - d_2$ с ограничением $\big|\arg(\gamma(d))\big| < \eta_\gamma$ достаточно того, что количество смежных классов по G_1 превосходит $\prod\limits_{\gamma \in R} (1 + \lfloor 2\pi/\eta_\gamma \rfloor)$, т. е.

$$|G/G_1| > \prod_{\gamma \in R} \left(1 + L \max\left(\frac{2}{\varepsilon}, 2\pi \sqrt{\frac{|\widehat{A}_1(\gamma)|}{6\delta n}}, \ldots, 2\pi \sqrt{\frac{|\widehat{A}_k(\gamma)|}{6\delta n}}\right)\right).$$

Нетрудно убедиться, что имеют место неравенства

$$\prod_{\gamma\in R}\left(1+L\max\left(\frac{2}{\varepsilon},2\pi\sqrt{\frac{|\widehat{A}_1(\gamma)|}{6\delta n}},\dots,2\pi\sqrt{\frac{|\widehat{A}_k(\gamma)|}{6\delta n}}\right)\right)$$
$$\leqslant\prod_{\gamma\in R}\left(1+(2\pi/\sqrt{6})L\max\left(\frac{1}{\varepsilon},\sqrt{\frac{|\widehat{A}_1(\gamma)|}{\delta n}},\dots,\sqrt{\frac{|\widehat{A}_k(\gamma)|}{\delta n}}\right)\right)$$
$$\leqslant(4L)^{|R|}\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon},\sqrt{\frac{|\widehat{A}_1(\gamma)|}{\delta n}},\dots,\sqrt{\frac{|\widehat{A}_k(\gamma)|}{\delta n}}\right).$$

Из равенства Парсеваля получим

$$\sum_{\gamma\in\Gamma}|\widehat{A}_i(\gamma)|^2=n\sum_{x\in G}|A_i(x)|^2=n|A_i|\leqslant n^2,$$

где $i=1,\dots,k$. Отсюда вытекает, что $|R|\leqslant 4\delta^{-2}$. Отметим также , что справедливо неравенство $\max(x,y)\leqslant x^y$ при $x\geqslant 1$ и $y\geqslant e^{1/e}$. Таким образом, имеем

$$(4L)^{|R|}\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon},\sqrt{\frac{|\widehat{A}_1(\gamma)|}{\delta n}},\dots,\sqrt{\frac{|\widehat{A}_k(\gamma)|}{\delta n}}\right)$$
$$\leqslant(4L)^{4\delta^{-2}}\left(\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon^4},\left(\frac{|\widehat{A}_1(\gamma)|}{\delta n}\right)^2,\dots,\left(\frac{|\widehat{A}_k(\gamma)|}{\delta n}\right)^2\right)\right)^{1/4}$$
$$\leqslant(4L)^{4\delta^{-2}}(\varepsilon^{-4})^{(4\delta^2n^2)^{-1}\max(\sum_{\gamma\in R}|\widehat{A}_1(\gamma)|^2,\dots,\sum_{\gamma\in R}|\widehat{A}_k(\gamma)|^2)}$$
$$\leqslant(4L)^{4\delta^{-2}}\varepsilon^{-\delta^{-2}}\leqslant(4L/\varepsilon)^{4\delta^{-2}}<\frac{n}{L'}\leqslant|G/G_1|.$$

Итак, существование подмножества $P\subseteq G$, удовлетворяющего требованиям пп. (i) и (ii), доказано. Лемма 7 доказана.

Лемма 8 (гранулирование)**.** *Пусть n — достаточно большое натуральное число, G — абелева группа порядка n, $0<\varepsilon<1/2$, $A_1,\dots,A_k$ — произвольные подмножества группы G, $|A_1|,\dots,|A_k|\geqslant\varepsilon n$, и L и L' — положительные числа, удовлетворяющие неравенству*

$$n>L'\,(4L/\varepsilon)^{k^2 4^{2k+1}\varepsilon^{-(2k+3)}}.$$

Тогда существуют подмножества $A'_1,\dots,A'_k\subseteq G$ такие, что

(i) $A'_1, \dots, A'_k$ — *либо* L*-гранулы типа прогрессии, либо* L'*-гранулы типа смежного класса;*

(ii) $\bigl|A_1 \setminus A'_1\bigr| \leqslant \varepsilon n, \dots, \bigl|A_k \setminus A'_k\bigr| \leqslant \varepsilon n$;

(iii) *множество* $A_1 + \dots + A_k$ *содержит все элементы* $x \in G$ *такие, что* $(A'_1 * \dots * A'_k)(x) \geqslant \varepsilon n^{k-1}$, *за исключением не более* εn *элементов.*

Доказательство. Построим множество P по лемме 7 при $\delta = \delta(k) = \varepsilon^{(2k+3)/2} k^{-1} 4^{-k}$. Поскольку P — подгруппа или прогрессия, симметричная относительно 0, то $g(\gamma) = |P|^{-1} \sum\limits_{p \in P} \gamma(p)$ есть вещественное число из отрезка $[-1, 1]$.

Построим множества $A'_1, \dots, A'_k$. Рассмотрим два случая.

1. Если P — подгруппа, то в качестве A'_i возьмём объединение смежных классов G по P, содержащих не менее $\varepsilon|P|$ элементов множества A_i, $i = 1, \dots, k$. Так как $|A_1|, \dots, |A_k| \geqslant \varepsilon n$, эти объединения смежных классов непустые. Тогда

$$|A_1 \setminus A'_1|, \dots, \bigl|A_k \setminus A'_k\bigr| \leqslant \varepsilon|P| \cdot \frac{n}{|P|} = \varepsilon n.$$

2. Если P — прогрессия с разностью d, то рассмотрим структуру гранул типа прогрессии с разностью d, а в качестве A'_i возьмём объединение прогрессий, содержащих не менее $\varepsilon L/2$ элементов множества A_i, $i = 1, \dots, k$. Так как $|A_1|, \dots, |A_k| \geqslant \varepsilon n$, эти объединения прогрессий непустые. Заметим также, что не более чем $nL/\operatorname{ord}(d)$ элементов из «остаточных» множеств не входят ни в одну из гранул. Тогда с учётом того, что $\operatorname{ord}(d) \geqslant 2L/\varepsilon$, получим

$$|A_1 \setminus A'_1|, \dots, |A_k \setminus A'_k| \leqslant \frac{\varepsilon L}{2} \cdot \frac{n}{L} + \frac{nL}{\operatorname{ord}(d)} \leqslant \varepsilon n.$$

Требования пп. (i) и (ii) леммы выполнены в обоих случаях.

Докажем справедливость п. (iii). Определим функции

$$a_i(x) = |P|^{-1} |A_i \cap (P + x)|, \quad i = 1, \dots, k.$$

Нетрудно убедиться, что для преобразования Фурье функций $a_i(x)$ имеет место равенство $\widehat{a}_i(\gamma) = g(\gamma)\widehat{A}_i(\gamma)$, $i = 1, \dots, k$. Действительно, с учётом того, что $P = -P$, получаем

$$\widehat{a}_i(\gamma) = \sum_{x \in G} a_i(x)\gamma(x) = \frac{1}{|P|} \sum_{x \in G} |A_i \cap (P + x)|\gamma(x)$$

$$= \frac{1}{|P|}\sum_{c\in A_i}\sum_{p\in P}\gamma(c-p) = \frac{1}{|P|}\Big(\sum_{c\in A_i}\gamma(c)\Big)\Big(\sum_{p\in P}\gamma(-p)\Big)$$
$$= \frac{1}{|P|}\Big(\sum_{c\in A_i}\gamma(c)\Big)\Big(\sum_{p\in P}\gamma(p)\Big) = g(\gamma)\widehat{A}_i(\gamma).$$

Нетрудно убедиться, что для любого $\gamma \in \Gamma$ и любого целого m справедливо неравенство $1-(g(\gamma))^m \leqslant m(1-g(\gamma))$. Отсюда в силу равенства Парсеваля и лемм 4 и 7 вытекает, что

$$\sum_{x\in G}|(A_1 * \cdots * A_k)(x) - (a_1 * \cdots * a_k)(x)|^2$$
$$= n^{-1}\sum_{\gamma\in\Gamma}|\widehat{(A_1 * \cdots * A_k)}(\gamma) - \widehat{(a_1 * \cdots * a_k)}(\gamma)|^2$$
$$= n^{-1}\sum_{\gamma\in\Gamma}|\widehat{A}_1(\gamma)\ldots\widehat{A}_k(\gamma) - \widehat{a}_1(\gamma)\ldots\widehat{a}_k(\gamma)|^2$$
$$= n^{-1}\sum_{\gamma\in\Gamma}|\widehat{A}_1(\gamma)|^2\ldots|\widehat{A}_k(\gamma)|^2|1-(g(\gamma))^k|^2$$
$$\leqslant \frac{1}{n}k^2\max_{\gamma\in\Gamma}(|\widehat{A}_1(\gamma)||1-g(\gamma)|)^2\cdot\sum_{\gamma\in\Gamma}|\widehat{A}_2(\gamma)|^2\ldots|\widehat{A}_k(\gamma)|^2$$
$$\leqslant \frac{1}{n}k^2\max_{\gamma\in\Gamma}(|\widehat{A}_1(\gamma)||1-g(\gamma)|)^2\max_{\gamma\in\Gamma}(|\widehat{A}_3(\gamma)|^2\ldots|\widehat{A}_k(\gamma)|^2)\cdot\sum_{\gamma\in\Gamma}|\widehat{A}_2(\gamma)|^2$$
$$\leqslant \frac{1}{n}k^2\max_{\gamma\in\Gamma}(|\widehat{A}_1(\gamma)||1-g(\gamma)|)^2 n^{2(k-2)}\cdot n^2$$
$$\leqslant k^2 n^{2k-3}(\delta n)^2 = k^2\delta^2 n^{2k-1}. \quad (1)$$

Рассмотрим два случая: $x \in A'_i$ и $x \notin A'_i$, $i = 1,\ldots,k$.

Пусть $x \in A'_i$. Если P — подгруппа, то $x+P$ содержит не менее $\varepsilon|P|$ элементов множества A_i, а если P — прогрессия, то $x+P$ содержит гранулу, включающую x, и поэтому $|(x+P)\cap A_i| \geqslant \varepsilon|P|/4$. Таким образом, $a_i(x) \geqslant \varepsilon/4 = \varepsilon A'_i(x)/4$ для всех $x \in G$. Если $x \notin A'_i$, то верно неравенство $a_i(x) \geqslant 0 = \varepsilon A'_i(x)/4$.

Из этих неравенств и леммы 4 вытекает, что для всех $x \in G$ имеет место неравенство

$$(a_1 * \cdots * a_k)(x) \geqslant \varepsilon^k(A'_1 * \cdots * A'_k)(x)/4^k. \quad (2)$$

При условии, что

$$(A'_1 * \cdots * A'_k)(x) \geqslant \varepsilon n^{k-1},$$

из (2) получаем

$$(a_1 * \cdots * a_k)(x) \geqslant \varepsilon^{k+1} n^{k-1}/4^k.$$

Покажем, что число элементов $x \in G$, удовлетворяющих условиям $(A_1 * \cdots * A_k)(x) = 0$ и $(A'_1 * \cdots * A'_k)(x) \geqslant \varepsilon n^{k-1}$, не превосходит εn. Семейство таких элементов обозначим через F. Несложно убедиться, что для всякого $x \in F$ выполняется неравенство

$$|(A_1 * \cdots * A_k)(x) - (a_1 * \cdots * a_k)(x)|^2 \geqslant \varepsilon^{2(k+1)} n^{2(k-1)}/4^{2k}. \qquad (3)$$

Из (1) и (3) следует, что

$$k^2\delta^2 n^{2k-1} \geqslant \sum_{x\in G} |(A_1 * \cdots * A_k)(x) - (a * \cdots * a_k)(x)|^2$$
$$\geqslant \sum_{x\in F} |(A_1 * \cdots * A_k)(x) - (a_1 * \cdots * a_k)(x)|^2 \geqslant |F|\varepsilon^{2(k+1)} n^{2(k-1)}/4^{2k}.$$

Отсюда, полагая $\delta = \varepsilon^{(2k+3)/2} k^{-1} 4^{-k}$, получаем $|F| \leqslant \varepsilon n$. Лемма 8 доказана.

3. Верхняя оценка числа k-сумм в абелевой группе

Теорема 3. *Пусть G — абелева группа порядка n, а k — натуральное число, $k \geqslant 2$. Тогда при $n \to \infty$ справедлива оценка*

$$|S(G)| \leqslant 2^{n/2 + D(G)/2 + \bar{o}(n)}.$$

Доказательство. Пусть $A_1, \ldots, A_k \subseteq G$ такие, что существует A_i такое, что $|A_i| \geqslant n(\log n)^{-1/8}$ и $|A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| \geqslant n(\log n)^{-1/8}$, $i \in \{1, \ldots, k\}$. Без ограничения общности будем считать, что

$$|A_1| \geqslant n(\log n)^{-1/8}, \quad |A_2 + \cdots + A_k| \geqslant n(\log n)^{-1/8}.$$

Положим $L = L' = \lfloor \log n \rfloor$ и $\varepsilon = (\log n)^{-1/8}$. Для каждого набора таких подмножеств $(A_1, \ldots, A_k)$, применяя лемму 8, построим пару множеств $(A'(A_1), B'(A_2 + \ldots + A_k))$. Нетрудно убедиться, что при достаточно большом n такой выбор параметров удовлетворяет условию леммы 8. Оценим величину $|S(G)|$ путём подсчёта количества соответствующих пар $((A'(A_1), B'(A_2 + \cdots + A_k)), A_1 + \cdots + A_k)$.

Пусть A', B' — гранулы типа прогрессии или смежного класса. Для каждой фиксированной пары (A', B') рассмотрим два случая:

- $|A'| + |B'| > n/2 + D(G)/2$,
- $|A'| + |B'| \leqslant n/2 + D(G)/2$.

Пусть $|A'| + |B'| > n/2 + D(G)/2$. Из п. (iii) леммы 8 следует, что

$$\overline{A_1 + \cdots + A_k} \subseteq (\overline{S_{\varepsilon n}(A', B')} \cup Q_1),$$

где Q_1 — некоторое подмножество абелевой группы G, $|Q_1| \leqslant \varepsilon n$.

Из леммы 5 получаем

$$|S_{\varepsilon n}(A', B')| \geqslant \min(n, |A'| + |B'| - D(G)) - 3\sqrt{\varepsilon n^2} \geqslant |A'| + |B'| - D(G) - 3\sqrt{\varepsilon n^2}.$$

Из условия $|A'| + |B'| > n/2 + D(G)/2$ вытекает, что

$$|\overline{S_{\varepsilon n}(A', B')}| \leqslant n/2 + D(G)/2 + 3\sqrt{\varepsilon n^2}.$$

Несложно убедиться, что множество $\overline{A_1 + \cdots + A_k}$ однозначно определяет множество $A_1 + \cdots + A_k$. Отсюда и из леммы 2 следует, что число способов выбора $A_1 + \cdots + A_k$ при заданной паре множеств (A', B'), для которых справедливо $|A'| + |B'| > n/2 + D(G)/2$, не превосходит

$$2^{n/2 + D(G)/2 + 4n\sqrt{\varepsilon}}.$$

Рассмотрим случай, когда $|A'| + |B'| \leqslant n/2 + D(G)/2$. Из п. (ii) леммы 8 имеем $A_1 \subseteq (A_1' \cup Q_2)$, где Q_2 — некоторое подмножество абелевой группы G, $|Q_2| \leqslant \varepsilon n$. Аналогично получаем, что $(A_2 + \ldots + A_k) \subseteq (B' \cup Q_3)$, где Q_3 — некоторое подмножество абелевой группы G, $|Q_3| \leqslant \varepsilon n$. В силу леммы 2 и того, что каждый набор множеств $(A_1, A_2 + \cdots + A_k)$ порождает ровно одно множество вида $A_1 + \cdots + A_k$, следует, что число способов выбора $A_1 + \cdots + A_k$ при заданной паре множеств (A', B'), для которых справедливо $|A'| + |B'| \leqslant n/2 + D(G)/2$, не превосходит

$$2^{n/2 + D(G)/2 + 2n\sqrt{\varepsilon}}.$$

В силу вышесказанного и леммы 6 с учётом того, что $6n/L \leqslant n\sqrt{\varepsilon}$ при достаточно большом n, следует справедливость теоремы 3.

ЛИТЕРАТУРА

1. **Саргсян В. Г.** Число разностей в группах простого порядка // Дискрет. математика. 2013. Т. 25, № 1. С. 152–158.
2. **Саргсян В. Г.** Число сумм и разностей в абелевой группе // Дискрет. анализ и исслед. операций. 2015. Т. 22, № 2. С. 73–85.

3. Alon N. Large sets in finite fields are sumsets // J. Number Theory. 2007. Vol. 126. P. 110–118.

4. Alon N., Granville A., Ubis A. The number of sumsets in a finite field // Bull. Lond. Math. Soc. 2010. Vol. 42, No. 5. P. 784–794.

5. Croot E., Lev V. F. Open problems in additive combinatorics // Additive Combinatorics. Providence, RI: Amer. Math. Soc., 2007. P. 207–233. (CRM Proc. Lect. Notes, Vol. 43).

6. Green B. Essay submitted for the Smith's Prize. Cambridge: Camb. Univ., 2001.

7. Green B., Ruzsa I. Z. Counting sumsets and sum-free sets modulo a prime // Stud. Sci. Math. Hung. 2004. Vol. 41, No. 3. P. 285–293.

8. Green B., Ruzsa I. Z. Sum-free sets in abelian groups // Isr. J. Math. 2005. Vol. 147. P. 157–188.

Сапоженко Александр Антонович,
Саргсян Ваге Гнелович

Статья поступила
29 января 2018 г.

Исправленный вариант —
13 июня 2018 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2018. Volume 25, No. 4. P. 97–111

UDC 519.1 DOI: 10.17377/daio.2018.25.608

THE NUMBER OF k-SUMSETS IN AN ABELIAN GROUP

A. A. Sapozhenko[a] and *V. G. Sargsyan*[b]
Lomonosov Moscow State University,
1 Leninskie Gory, 119991 Moscow, Russia
E-mail: [a]sapozhenko@mail.ru, [b]vahe_sargsyan@ymail.com

Abstract. Let G be an Abelian group of order n. The sum of subsets $A_1, \dots, A_k$ of G is defined as the collection of all sums of k elements from $A_1, \dots, A_k$; i. e., $A_1 + \dots + A_k = \{a_1 + \dots + a_k \mid a_1 \in A_1, \dots, a_k \in A_k\}$. A subset representable as the sum of k subsets of G is a *k-sumset*. We consider the problem of the number of k-sumsets in an Abelian group G. It is obvious that each subset A in G is a k-sumset since A is representable as $A = A_1 + \dots + A_k$, where $A_1 = A$ and $A_2 = \dots = A_k = \{0\}$. Thus, the number of k-sumsets is equal to the number of all subsets of G. But, if we introduce a constraint on the size of the summands $A_1, \dots, A_k$ then the number of k-sumsets becomes substantially smaller. A lower and upper asymptotic bounds of the number of k-sumsets in Abelian groups are obtained provided that there exists a summand A_i such that $|A_i| \geqslant n \log^q n$ and $|A_1 + \dots + A_{i-1} + A_{i+1} + \dots + A_k| \geqslant n \log^q n$, where $q = -1/8$ and $i \in \{1, \dots, k\}$. Bibliogr. 8.

Keywords: set, characteristic function, group, progression, coset.

REFERENCES

1. **V. G. Sargsyan,** The number of differences in groups of prime order, *Diskretn. Mat.,* **25**, No. 1, 152–158, 2013 [Russian]. Translated in *Discrete Math. Appl.,* **23**, No. 2, 195–201, 2013.
2. **V. G. Sargsyan,** Counting sumsets and differences in abelian group, *Diskretn. Anal. Issled. Oper.,* **22**, No. 2, 73–85, 2015 [Russian].
3. **A. Alon,** Large sets in finite fields are sumsets, *J. Number Theory,* **126**, 110–118, 2007.
4. **A. Alon, A. Granville** and **A. Ubis,** The number of sumsets in a finite field, *Bull. Lond. Math. Soc.,* **42**, No. 5, 784–794, 2010.
5. **E. Croot** and **V. F. Lev,** Open problems in additive combinatorics, in *Additive Combinatorics,* pp. 207–233, AMS, Providence, 2007 (CRM Proc. Lect. Notes, Vol. 43).

6. B. Green, Essay submitted for Smith's Prize, Camb. Univ., Cambridge, 2001.

7. B. Green and **I. Z. Ruzsa,** Counting sumsets and sum-free sets modulo a prime, *Stud. Sci. Math. Hung.,* **41**, No. 3, 285–293, 2004.

8. B. Green and **I. Z. Ruzsa,** Sum-free sets in abelian groups, *Isr. J. Math.,* **147**, 157–188, 2005.

Aleksandr A. Sapozhenko,
Vahe G. Sargsyan

Received
29 January 2018
Revised
13 June 2018