

ЧИСЛО СУММ И РАЗНОСТЕЙ В АБЕЛЕВОЙ ГРУППЕ ^{*)}

В. Г. Саргсян¹

¹Московский гос. университет им. М. В. Ломоносова, Ленинские горы, 1,
119991 Москва, Россия
email: vahe_sargsyan@yandex.ru

Аннотация. Подмножество A группы G называется (k, l) -суммой, если существует подмножество $B \subseteq G$ такое, что $A = kB - lB$, где $kB - lB = \{x_1 + \dots + x_k - x_{k+1} - \dots - x_{k+l} \mid x_1, \dots, x_{k+l} \in B\}$. В частности, $(1, 1)$ -сумма называется *разностью*, а $(2, 0)$ -сумма — просто суммой. Получены нижняя и верхняя оценки числа сумм и разностей в абелевой группе. Библиогр. 4.

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

Введение

Пусть G — абелева группа порядка n , $A \subseteq G$ и

$$A + A = \{x_1 + x_2 \mid x_1, x_2 \in A\},$$

$$A - A = \{x_1 - x_2 \mid x_1, x_2 \in A\}, \quad -A = \{-x \mid x \in A\}.$$

Пусть $k, l \geq 0$ — целые числа, удовлетворяющие условию $k + l \geq 2$. Подмножество $A \subseteq G$ называется (k, l) -суммой, если существует подмножество $B \subseteq G$ такое, что $A = \underbrace{B + \dots + B}_k - \underbrace{B - \dots - B}_l$. В частности, $(1, 1)$ -сумма называется *разностью*, а $(2, 0)$ -сумма — просто суммой. Семейство (k, l) -сумм в G обозначим через $SS_{k,l}(G)$, а группу по модулю n — через Z_n .

В 2004 г. в [3] доказана

Теорема 1. Пусть p — простое число. Тогда справедливы соотношения

$$p^2 2^{p/3} \ll |SS_{2,0}(Z_p)| \leq 2^{p/3 + \kappa(p)},$$

где $\kappa(p)/p \rightarrow 0$ при $p \rightarrow \infty$, причём $\kappa(p) \ll p(\log \log p)^{2/3}(\log p)^{-1/9}$.

^{*)}Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 13-01-00958-а).

Здесь и далее логарифмы берутся по основанию два, а запись $a(p) \ll b(p)$ означает, что $a(p) \in O(b(p))$ при $p \rightarrow \infty$.

В 2013 г. автором в [2] получена асимптотика логарифма числа подмножеств A , представимых в виде $A = B - B$.

Теорема 2. Пусть p — простое число. Тогда справедливы соотношения

$$p^2 2^{p/3} \ll |SS_{1,1}(Z_p)| \leq 2^{p/3 + \kappa(p)},$$

где $\kappa(p)/p \rightarrow 0$ при $p \rightarrow \infty$, причём $\kappa(p) \ll p(\log \log p)^{2/3}(\log p)^{-1/9}$.

Пусть $D(G)$ — размер наибольшей собственной подгруппы группы G , а $\varphi(n)$ — функция Эйлера. В данной работе доказывается

Теорема 3. Пусть G — абелева группа порядка n и экспоненты ν , а k, l — неотрицательные целые числа, $k + l = 2$. Тогда при $n, \nu \rightarrow \infty$ справедливы оценки

$$\nu \varphi(\nu) 2^{\nu/3} \ll |SS_{k,l}(G)| \leq 2^{n/3 + D(G)/3 + \bar{o}(n)}.$$

1. Нижняя оценка числа сумм и разностей в абелевой группе

При доказательстве нижней оценки нам понадобятся следующие понятия и вспомогательные утверждения.

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 Z_d .

Доказательство следующей леммы можно найти в [1].

Лемма 2. Пусть n — достаточно большое натуральное число, а $\mathcal{P}_1, \mathcal{P}_2$ — две арифметические прогрессии длины $\lfloor n/3 \rfloor$ в Z_n с разностями, равными d_1, d_2 соответственно. Предположим, что каждое из чисел d_1 и d_2 взаимно просто с n и при этом $d_1 \neq \pm d_2$. Тогда $|\mathcal{P}_1 \cap \mathcal{P}_2| \leq n/4 + 4$.

Пусть $\mathcal{P} = \{a + d, a + 2d, \dots, a + |P|d\}$ — арифметическая прогрессия группы Z_n . Будем говорить, что подмножество $\mathcal{X} \subseteq Z_n$ «точно» содержит \mathcal{P} , если $\mathcal{P} \subseteq \mathcal{X}$ и по крайней мере одно из чисел a и $a + (|P| + 1)d$ не принадлежит \mathcal{X} . Положим

$$SS_{k,l}(Z_n, A') = \{A \mid A \in SS_{k,l}(Z_n) \text{ и } A \text{ «точно» содержит } A'\}.$$

Лемма 3 [3, лемма 7; 2, лемма 5]. Пусть p — простое число, $p \geq 7$, а $\mathcal{P} \subseteq Z_p$ — арифметическая прогрессия длины $2(\lfloor p/3 \rfloor - 1)$. Тогда существует положительная константа c такая, что при всех простых $p \geq 7$

имеют место оценки

$$|SS_{2,0}(Z_p, \mathcal{P})| \geq c2^{p/3}, \quad |SS_{1,1}(Z_p, \mathcal{P})| \geq c2^{p/3}.$$

Практически без изменения доказательства получается

Лемма 4. Пусть n — натуральное число, $n \geq 6$, $\mathcal{P} \subseteq Z_n$ — произвольная арифметическая прогрессия длины $2(\lfloor n/3 \rfloor - 1)$, разность прогрессии взаимно проста с n , а k и l — неотрицательные целые числа, сумма которых равна 2. Тогда существует положительная константа $c = c(k, l)$ такая, что при всех $n \geq 6$ выполнена оценка

$$|SS_{k,l}(Z_n, \mathcal{P})| \geq c2^{n/3}.$$

Лемма 5. Пусть n — натуральное число, а k и l — неотрицательные целые числа, $k + l = 2$. Тогда при $n \rightarrow \infty$ справедлива оценка

$$n\varphi(n)2^{n/3} \ll |SS_{k,l}(Z_n)|. \quad (1)$$

Доказательство. Пусть $\mathcal{P}_1, \mathcal{P}_2 \subseteq Z_n$ — две различные арифметические прогрессии длины $2(\lfloor n/3 \rfloor - 1)$ с разностями, равными d_1 и d_2 соответственно, при этом числа d_1 и d_2 взаимно просты с n . Покажем, что количество множеств, которые «точно» содержат \mathcal{P}_1 и \mathcal{P}_2 , есть $\bar{o}(2^{n/3})$ при $n \rightarrow \infty$. Заметим, что при этом $d_1 \neq \pm d_2$. Через \bar{C} обозначим дополнение подмножества $C \subseteq Z_n$. В силу леммы 2 имеем $|\bar{\mathcal{P}}_1 \cap \bar{\mathcal{P}}_2| \leq n/4 + 10$, т. е. $|\mathcal{P}_1 \cup \mathcal{P}_2| \geq 3n/4 - 10$. Отсюда следует, что число множеств, которые «точно» содержат \mathcal{P}_1 и \mathcal{P}_2 , есть $\bar{o}(2^{n/3})$ при $n \rightarrow \infty$.

Таким образом, применяя лемму 4 для каждого из $n\varphi(n)/2$ возможных вариантов арифметических прогрессий длины $2(\lfloor n/3 \rfloor - 1)$, получим справедливость (1). Лемма 5 доказана.

Пусть G — абелева группа порядка n и экспоненты ν . В силу леммы 1 существует подгруппа H группы G такая, что фактор-группа G/H изоморфна циклической группе Z_ν . Тогда существует элемент g порядка ν такой, что

$$G = H \cup (g + H) \cup \dots \cup ((\nu - 1)g + H).$$

Для каждого подмножества B фактор-группы G/H

$$B = \{(b_i + H) \mid b_i \in \{0, g, \dots, (\nu - 1)g\}, i = 1, \dots, |B|\} \subseteq G/H$$

положим

$$B'(B) = \{b_i \mid b_i \in \{0, g, \dots, (\nu - 1)g\}, i = 1, \dots, |B|\} \subseteq G.$$

Заметим, что если $B_1, B_2 \subseteq G/H$ различны, то различны и подмножества $B'_1(B_1), B'_2(B_2) \subseteq G$. Нетрудно убедиться, что если $B = kA - lA$ для некоторого $A \subseteq G/H$, то $B'(B) = kA'(A) - lA'(A)$. Поскольку факторгруппа G/H изоморфна циклической группе Z_ν , в силу леммы 5 получим справедливость нижней оценки в теореме 3.

2. Гранулирование

Пусть G — абелева группа порядка n , $f_i: G \rightarrow \mathbb{R}$, $i = 1, \dots, m$. Определим

$$\begin{aligned} (f_1 * \dots * f_m)(x) \\ = \sum_{x_1 \in G} \dots \sum_{x_{m-1} \in G} f_1(x_1) \dots f_{m-1}(x_{m-1}) f_m(x - x_1 - \dots - x_{m-1}). \end{aligned}$$

Характером группы G называется отображение $\gamma: G \rightarrow \mathbb{C}$ 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 . Нетрудно убедиться, что Γ образует группу с операцией $\gamma_1 * \gamma_2(x) = \gamma_1(x)\gamma_2(x)$. *Преобразование Фурье* $f: G \rightarrow \mathbb{R}$ называется функцией $\widehat{f}: G \rightarrow \mathbb{C}$, определяемая равенством $\widehat{f}(\gamma) = \sum_{x \in G} f(x)\gamma(x)$. Заметим также, что справедлива

Лемма 6. Для любого $\gamma \in \Gamma$ выполняется равенство

$$\widehat{(f_1 * \dots * f_m)}(\gamma) = \widehat{f}_1(\gamma) \dots \widehat{f}_m(\gamma).$$

ДОКАЗАТЕЛЬСТВО. Действительно,

$$\begin{aligned} \widehat{(f_1 * \dots * f_m)}(\gamma) &= \sum_{x \in G} (f_1 * \dots * f_m)(x) \gamma(x) \\ &= \sum_{x \in G} \sum_{x_1 \in G} \dots \sum_{x_{m-1} \in G} f_1(x_1) \dots f_{m-1}(x_{m-1}) f_m(x - x_1 - \dots - x_{m-1}) \\ &\quad \times \gamma(x_1) \dots \gamma(x_{m-1}) \gamma(x - x_1 - \dots - x_{m-1}) \\ &= \sum_{x_1 \in G} f_1(x_1) \gamma(x_1) \dots \sum_{x_{m-1} \in G} f_{m-1}(x_{m-1}) \gamma(x_{m-1}) \\ &\quad \times \sum_{x \in G} f_m(x - x_1 - \dots - x_{m-1}) \gamma(x - x_1 - \dots - x_{m-1}) = \widehat{f}_1(\gamma) \dots \widehat{f}_m(\gamma). \end{aligned}$$

Лемма 6 доказана.

Пусть A_1, \dots, A_m — непустые подмножества группы G . Обозначим через $A_1(x), \dots, A_m(x)$ характеристические функции множеств A_1, \dots, A_m соответственно. Тогда $r(A_1, \dots, A_m, x) = (A_1 * \dots * A_m)(x)$ — количество наборов $(x_1, \dots, x_m) \in A_1 \times \dots \times A_m$ таких, что $x = x_1 + \dots + x_m$. Положим

$$S_h(A_1, \dots, A_m) = \{x \in G \mid (A_1 * \dots * A_m)(x) \geq h\}.$$

Следующее утверждение доказано в [4].

Лемма 7. Пусть G — абелева группа порядка n , A, B — непустые подмножества группы G и $h > 0$ такое, что $\sqrt{hn} \leq \min(|A|, |B|)$. Тогда справедлива оценка

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

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 $\text{ord}(d) \geq L$, где $\text{ord}(d)$ — порядок элемента d . Рассмотрим подгруппу G , порождённую элементом d , и разобьём каждый её смежный класс на $\lfloor \text{ord}(d)/L \rfloor$ прогрессий вида $\{x + id \mid 0 \leq i \leq L - 1\}$ и одно «остаточное» множество мощности менее L . Для каждого $d \in G$ фиксируем одно такое разбиение. Объединение полученных прогрессий называется L -гранулой типа прогрессии.

Доказательства следующих двух лемм можно найти в [4].

Лемма 8. Пусть n — достаточно большое натуральное число, а G — абелева группа порядка n . Тогда в группе G есть не более $2^{3n/L}$ L -гранул обоих типов (прогрессии и смежного класса).

Лемма 9. Пусть n достаточно велико, M — множество мощности n , ρ — вещественное число, меньшее некоторой абсолютной положительной константы. Тогда число подмножеств множества M мощности не более ρn не превосходит $2^{n\sqrt{\rho}}$.

Суть следующей леммы состоит в том, что для каждого $A \in \text{SS}_{k,l}(G)$ строится «подходящая» гранула.

Лемма 10 (гранулирование). Пусть n — достаточно большое натуральное число, G — абелева группа порядка n , $k > l \geq 0$, $k + l \geq 2$, A — произвольное подмножество группы G , $\varepsilon \in (0, \frac{1}{2})$, L и L' — положительные числа, удовлетворяющие неравенству

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

Тогда существует подмножество $A' \subseteq G$ такое, что

- (i) A' — либо L -гранула типа прогрессии, либо L' -гранула типа смежного класса;
- (ii) $|A \setminus A'| \leq \varepsilon n$;
- (iii) множество $kA - lA$ содержит все элементы $x \in G$ такие, что

$$\underbrace{(A' * \dots * A')}_k * \underbrace{(-A') * \dots * (-A')}_l(x) \geq \varepsilon n^{k+l-1},$$

за исключением не более εn элементов.

ДОКАЗАТЕЛЬСТВО. Положим $\delta = \varepsilon^{k+l+3/2}(k+l)^{-1}4^{-(k+l)}$. Сначала докажем, что существует подмножество $P \subseteq G$, удовлетворяющее условиям

- (A) P — либо прогрессия вида $\{id \mid L-1 \leq i \leq L-1\}$, причём $\text{ord}(d) \geq 2L/\varepsilon$, либо подгруппа группы G порядка не менее L' ;
- (B) для любых $B \subseteq G$ и $\gamma \in \Gamma$ имеет место неравенство

$$|\widehat{B}(\gamma)(1 - g(\gamma))| \leq \delta n,$$

где $g(\gamma) = |P|^{-1} \sum_{p \in P} \gamma(p)$, а $B(x)$ — характеристическая функция подмножества B .

Пусть R — множество характеров γ таких, что $|\widehat{B}(\gamma)| > \delta n/2$, а Γ_1 — подгруппа группы Γ , порождённая множеством R . Рассмотрим подгруппу G_1 группы G

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

Рассмотрим два случая.

СЛУЧАЙ 1. Пусть $|G_1| \geq L'$. Положим $P = G_1$. Так как $g(\gamma) \in [-1, 1]$, при $\gamma \in \Gamma \setminus \Gamma_1$ получим $|\widehat{B}(\gamma)(1 - g(\gamma))| \leq 2|\widehat{B}(\gamma)| < 2\delta n/2 = \delta n$, а при $\gamma \in \Gamma_1$ справедливо равенство $|\widehat{B}(\gamma)(1 - g(\gamma))| = 0$.

СЛУЧАЙ 2. Пусть $|G_1| < L'$. Будем выбирать такое d , что если в качестве P возьмём прогрессию $P = \{id \mid L-1 \leq i \leq L-1\}$, то требования (A) и (B) будут удовлетворены. Отметим, что (B) при $\gamma \in \Gamma \setminus \Gamma_1$ выполнено. Оценим величину $1 - g(\gamma)$. Фиксируем $\gamma \in \Gamma$ и через β обо-

значим $\arg \gamma(d) \in [-\pi, \pi)$. Таким образом, имеем

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

Если для всех $\gamma \in R$

$$|\arg \gamma(d)| \leq L^{-1} \sqrt{6\delta n / |\widehat{B}(\gamma)|},$$

то (В) выполнено. Отметим, что для выполнения условия $\text{ord}(d) \geq 2L/\varepsilon$ достаточно, чтобы при некотором $\gamma \in \Gamma$ было верно соотношение

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

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

$$|\arg \gamma(d)| \leq \frac{1}{L} \min(\pi\varepsilon, \sqrt{6\delta n / |\widehat{B}(\gamma)|}).$$

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 $|\arg(\gamma(d))| < \eta_\gamma$ достаточно, чтобы количество смежных классов по G_1 превосходило $\prod_{\gamma \in R} (1 + \lfloor 2\pi/\eta_\gamma \rfloor)$, т. е.

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

Справедливы неравенства

$$\begin{aligned} &\prod_{\gamma \in R} \left(1 + L \max \left(\frac{2}{\varepsilon}, \sqrt{\frac{2\pi|\widehat{B}(\gamma)|}{6\delta n}} \right) \right) \\ &\leq \prod_{\gamma \in R} \left(1 + 2L \max \left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}} \right) \right) \leq (4L)^{|R|} \prod_{\gamma \in R} \max \left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}} \right). \end{aligned}$$

В силу равенства Парсеваля имеем

$$\sum_{\gamma \in \Gamma} |\widehat{B}(\gamma)|^2 = n \sum_{x \in G} |B(x)|^2 = n|B| \leq n^2,$$

откуда $|R| \leq 4\delta^{-2}$. Также заметим, что $\max(x, y) \leq x^y$ при $x \geq 1$ и $y \geq e^{1/e}$. Таким образом, получаем

$$\begin{aligned} (4L)^{|R|} \prod_{\gamma \in R} \max\left(\frac{1}{\varepsilon}, \sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right) \\ \leq (4L)^{4\delta^{-2}} \left(\prod_{\gamma \in R} \max\left(\frac{1}{\varepsilon^4}, \left(\frac{|\widehat{B}(\gamma)|}{\delta n}\right)^2\right) \right)^{1/4} \\ \leq (4L)^{4\delta^{-2}} (\varepsilon^{-4})^{(4\delta^2 n^2)^{-1} \sum_{\gamma \in \Gamma} |\widehat{B}(\gamma)|^2} \leq (4L)^{4\delta^{-2}} \varepsilon^{-\delta^{-2}} \\ \leq (4L/\varepsilon)^{4\delta^{-2}} < \frac{n}{L'} \leq |G/G_1|. \end{aligned}$$

Тем самым существование подмножества $P \subseteq G$, удовлетворяющего требованиям (А) и (В), доказано. Так как по построению P — либо подгруппа, либо прогрессия, симметричная относительно нуля, $g(\gamma) = |P|^{-1} \sum_{p \in P} \gamma(p)$ — вещественное число из $[-1, 1]$.

Построим множество A' . Рассмотрим два случая.

СЛУЧАЙ 1. Если P — подгруппа, то в качестве A' возьмём объединение смежных классов G по P , содержащих не менее $\varepsilon|P|$ элементов множества A . Тогда

$$|A \setminus A'| \leq \varepsilon|P| \cdot \frac{n}{|P|} = \varepsilon n.$$

СЛУЧАЙ 2. Если P — прогрессия с разностью d , то рассмотрим структуру гранул типа прогрессии с разностью d и в качестве A' возьмём объединение прогрессий, содержащих не менее $\varepsilon L/2$ элементов множества A . Заметим, что не более чем $nL/\text{ord}(d)$ элементов из «остаточных» множеств не входят ни в одну из гранул. Тогда с учётом того, что $\text{ord}(d) \geq 2L/\varepsilon$, получим

$$|A \setminus A'| \leq \frac{\varepsilon L}{2} \cdot \frac{n}{L} + \frac{nL}{\text{ord}(d)} \leq \varepsilon n.$$

Требования (i) и (ii) леммы выполнены в обоих случаях. При таком определении множества A' имеем $(-A)' = -A'$.

Докажем (iii). Рассмотрим две функции $a_1(x) = |P|^{-1}|A \cap (P+x)|$ и $a_2(x) = |P|^{-1}|(-A) \cap (P+x)|$. Для преобразования Фурье функций $a_1(x)$ и $a_2(x)$ справедливы равенства $\hat{a}_1(\gamma) = g(\gamma)\hat{A}(\gamma)$ и $\hat{a}_2(\gamma) = g(\gamma)\widehat{(-A)}(\gamma)$. Действительно, с учётом того, что $P = -P$, имеем

$$\begin{aligned}\hat{a}_1(\gamma) &= \sum_{x \in G} a_1(x)\gamma(x) = \frac{1}{|P|} \sum_{x \in G} |A \cap (P+x)|\gamma(x) = \frac{1}{|P|} \sum_{a \in A} \sum_{p \in P} \gamma(a-p) \\ &= \frac{1}{|P|} \left(\sum_{a \in A} \gamma(a) \right) \left(\sum_{p \in P} \gamma(-p) \right) = \frac{1}{|P|} \left(\sum_{a \in A} \gamma(a) \right) \left(\sum_{p \in P} \gamma(p) \right) \\ &= g(\gamma)\hat{A}(\gamma).\end{aligned}$$

Аналогично доказывается, что $\hat{a}_2(\gamma) = g(\gamma)\widehat{(-A)}(\gamma)$. Таким образом, в силу равенства Парсеваля и леммы 6 получаем

$$\begin{aligned}\sum_{x \in G} & \left| \underbrace{(A * \dots * A)_k}_{k} * \underbrace{(-A * \dots * (-A))_l}_{l}(x) - \underbrace{(a_1 * \dots * a_1)_k}_{k} * \underbrace{(a_2 * \dots * a_2)_l}_{l}(x) \right|^2 \\ &= n^{-1} \sum_{\gamma \in \Gamma} \left| \underbrace{(A * \dots * A)_k}_{k} * \underbrace{\widehat{(-A)} * \dots * (-A)}_l(\gamma) - \underbrace{(a_1 * \dots * a_1)_k}_{k} * \underbrace{\widehat{a_2} * \dots * a_2}_l(\gamma) \right|^2 \\ &= n^{-1} \sum_{\gamma \in \Gamma} \left| (\hat{A}(\gamma))^k (\widehat{(-A)}(\gamma))^l - (\hat{a}_1(\gamma))^k (\hat{a}_2(\gamma))^l \right|^2 \\ &= n^{-1} \sum_{\gamma \in \Gamma} \left| \hat{A}(\gamma)^{2k} |\widehat{(-A)}(\gamma)|^{2l} |1 - (g(\gamma))^{k+l}|^2 \right| \\ &\leq \frac{1}{n} (k+l)^2 \max_{\gamma \in \Gamma} |\hat{A}(\gamma)|^{2(k+l-2)} \max_{\gamma \in \Gamma} (|\hat{A}(\gamma)| |1 - g(\gamma)|)^2 \sum_{\gamma \in \Gamma} |\hat{A}(\gamma)|^2 \\ &\leq \frac{1}{n} (k+l)^2 n^{2(k+l-2)} \max_{\gamma \in \Gamma} (|\hat{A}(\gamma)| |1 - g(\gamma)|)^2 n^2 \\ &\leq (k+l)^2 n^{2(k+l)-3} (\delta n)^2 = (k+l)^2 \delta^2 n^{2(k+l)-1}. \quad (2)\end{aligned}$$

Рассмотрим два случая: $x \in A'$ и $x \notin A'$.

СЛУЧАЙ 1. Пусть $x \in A'$. Если P — подгруппа, то $x + P$ содержит не менее $\varepsilon|P|$ элементов множества A , а если P — прогрессия, то $x + P$ содержит гранулу, включающую x , поэтому $|(x+P) \cap A| \geq \varepsilon|P|/4$. Таким образом, $a_1(x) \geq \varepsilon/4 = \varepsilon A'(x)/4$ для всех $x \in G$.

СЛУЧАЙ 2. Пусть $x \notin A'$, тогда $a_1(x) \geq 0 = \varepsilon A'(x)/4$.

Аналогично получается, что $a_2(x) \geq \varepsilon(-A)'(x)/4$ для всех $x \in G$. Из этих неравенств и леммы 6 вытекает, что для всех $x \in G$ имеет место соотношение

$$\begin{aligned} & (\underbrace{a_1 * \dots * a_1}_k * \underbrace{a_2 * \dots * a_2}_l)(x) \\ & \geq \varepsilon^{k+l} (\underbrace{A' * \dots * A'}_k * \underbrace{(-A)' * \dots * (-A)'}_l)(x) / 4^{k+l}. \end{aligned} \quad (3)$$

При $(\underbrace{A' * \dots * A'}_k * \underbrace{(-A)' * \dots * (-A)'}_l)(x) \geq \varepsilon n^{k+l-1}$ из (3) следует, что

$$(\underbrace{a_1 * \dots * a_1}_k * \underbrace{a_2 * \dots * a_2}_l g)(x) \geq \varepsilon^{k+l+1} n^{k+l-1} / 4^{k+l}.$$

Покажем, что число элементов $x \in G$, удовлетворяющих условиям

$$\begin{aligned} & (\underbrace{A * \dots * A}_k * \underbrace{(-A) * \dots * (-A)}_l)(x) = 0, \\ & (\underbrace{A' * \dots * A'}_k * \underbrace{(-A)' * \dots * (-A)'}_l)(x) \geq \varepsilon n^{k+l-1}, \end{aligned}$$

не превосходит εn . Семейство таких элементов обозначим через F . Заметим, что для всякого $x \in F$ верна оценка

$$\begin{aligned} & |(\underbrace{A * \dots * A}_k * \underbrace{(-A) * \dots * (-A)}_l)(x) - (\underbrace{a_1 * \dots * a_1}_k * \underbrace{a_2 * \dots * a_2}_l)(x)|^2 \\ & \geq \varepsilon^{2(k+l+1)} n^{2(k+l-1)} / 4^{2(k+l)}. \end{aligned} \quad (4)$$

Из (2) и (4) получаем

$$\begin{aligned} & (k+l)^2 \delta^2 n^{2(k+l)-1} \\ & \geq \sum_{x \in G} |(\underbrace{A * \dots * A}_k * \underbrace{(-A) * \dots * (-A)}_l)(x) - (\underbrace{a_1 * \dots * a_1}_k * \underbrace{a_2 * \dots * a_2}_l)(x)|^2 \\ & \geq \sum_{x \in F} |(\underbrace{A * \dots * A}_k * \underbrace{(-A) * \dots * (-A)}_l)(x) - (\underbrace{a_1 * \dots * a_1}_k * \underbrace{a_2 * \dots * a_2}_l)(x)|^2 \\ & \geq |F| \varepsilon^{2(k+l+1)} n^{2(k+l-1)} / 4^{2(k+l)}. \end{aligned}$$

Отсюда, полагая $\delta = \varepsilon^{k+l+3/2} (k+l)^{-1} 4^{-(k+l)}$, имеем $|F| \leq \varepsilon n$. Лемма 10 доказана.

3. Верхняя оценка числа сумм и разностей в абелевой группе

Пусть G — абелева группа порядка n , $k > l \geq 0$ и $k + l = 2$. Положим $L = L' = \lfloor \log n \rfloor$ и $\varepsilon = (\log n)^{-1/8}$. Заметим, что при достаточно большом n такой выбор параметров удовлетворяет условию леммы 10 для случая $k + l = 2$. Для каждого множества $A \subseteq G$, применяя лемму 10, построим множество $A'(A)$. Оценим величину $|\text{SS}_{k,l}(G)|$ путём подсчёта количества соответствующих пар $(A'(A), kA - lA)$.

Пусть A' — гранула типа прогрессии или смежного класса. Для каждого фиксированного A' рассмотрим два случая: $|A'| > n/3 + D(G)/3$ и $|A'| \leq n/3 + D(G)/3$.

СЛУЧАЙ 1. Пусть $|A'| > n/3 + D(G)/3$. В силу п. (iii) леммы 10 множество $\overline{kA - lA}$ является подмножеством объединения множества

$$\overline{S_{\varepsilon n}(\underbrace{A', \dots, A'}_k, \underbrace{(-A)', \dots, (-A)'}_l)}$$

с некоторым подмножеством группы G мощности, не превышающей εn . В силу леммы 7

$$|S_{\varepsilon n}(\underbrace{A', \dots, A'}_k, \underbrace{(-A)', \dots, (-A)'}_l)| \geq \min(n, 2|A'| - D(G)) - 3\sqrt{\varepsilon n^2}.$$

При $|A'| > n/3 + D(G)/3$ имеем

$$|\overline{S_{\varepsilon n}(\underbrace{A', \dots, A'}_k, \underbrace{(-A)', \dots, (-A)'}_l)}| \leq n/3 + D(G)/3 + 3n\sqrt{\varepsilon}.$$

Из леммы 9 и того, что множество $\overline{kA - lA}$ однозначно определяет множество $kA - lA$, получим, что число способов выбора $kA - lA$ при заданном множестве A' мощности, превышающей $n/3 + D(G)/3$, не превосходит $2^{n/3 + D(G)/3 + 4n\sqrt{\varepsilon}}$.

СЛУЧАЙ 2. Пусть $|A'| \leq n/3 + D(G)/3$. По п. (ii) леммы 10 A является подмножеством объединения множества A' с некоторым подмножеством группы G мощности, не превышающей εn . Из леммы 9 и того, что каждое множество $A \subseteq G$ порождает ровно одно множество вида $kA - lA$, следует, что число способов выбора $kA - lA$ при заданном множестве A' мощности, не превышающей $n/3 + D(G)/3$, не превосходит $2^{n/3 + D(G)/3 + n\sqrt{\varepsilon}}$.

Из вышеизложенного и леммы 8 с учётом того, что $3n/L \leq n\sqrt{\varepsilon}$ при достаточно большом n , получаем

$$|\text{SS}_{k,l}(G)| \leq 2^{n/3 + D(G)/3 + \bar{o}(n)}$$

при $n \rightarrow \infty$.

Верхняя оценка теоремы 3 доказана.

Автор выражает признательность профессору А. А. Сапоженко за постановку задачи и внимание к работе.

ЛИТЕРАТУРА

1. Сапоженко А. А. Решение проблемы Камерона — Эрдёша для групп простого порядка // Журн. вычисл. математики и мат. физики. 2009. Т. 49, № 8. С. 1–7.
2. Саргсян В. Г. Число разностей в группах простого порядка // Дискрет. математика. 2013. Т. 25, вып. 1. С. 152–158.
3. Green B., Ruzsa I. Z. Counting sumsets and sum-free sets modulo a prime // Stud. Sci. Math. Hung. 2004. Vol. 41. P. 285–293.
4. Green B., Ruzsa I. Z. Sum-free sets in abelian groups // Isr. J. Math. 2005. Vol. 147. P. 157–188.

Саргсян Ваге Гнелович

Статья поступила
20 марта 2014 г.

Исправленный вариант —
9 сентября 2014 г.

DISKRETNYYI ANALIZ I ISSLEDOVANIE OPERATSII
March–April 2015. Volume 22, No. 2. P. 73–85

UDC 519.1

DOI: 10.17377/daio.2015.22.449

COUNTING SUMSETS AND DIFFERENCES IN ABELIAN GROUP

V. G. Sargsyan¹

¹Lomonosov Moscow State University,
1 Leninskie gory, 119991 Moscow, Russia
e-mail: vahe_sargsyan@ymail.com

Abstract. A subset A of a group G is called (k, l) -sumset, if $A = kB - lB$ for some $B \subseteq G$, where $kB - lB = \{x_1 + \dots + x_k - x_{k+1} - \dots - x_{k+l} \mid x_1, \dots, x_{k+l} \in B\}$. Upper and lower bounds for the numbers of $(1, 1)$ -sumsets and $(2, 0)$ -sumsets in abelian groups are provided. Bibliogr. 4.

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

REFERENCES

1. **A. A. Sapozhenko**, Solution of the Cameron–Erdős problem for groups of prime order, *Zh. Vychisl. Mat. Mat. Fiz.*, **49**, No. 8, 1503–1509, 2009. Translated in *Comput. Math. Math. Phys.*, **49**, No. 8, 1435–1441, 2009.
2. **V. G. Sargsyan**, The number of differences in groups of prime order, *Diskretn. Mat.*, **25**, No. 1, 152–158, 2013. Translated in *Discrete Math. Appl.*, **23**, No. 2, 195–201, 2013.
3. **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.
4. **B. Green** and **I. Z. Ruzsa**, Sum-free sets in Abelian groups, *Isr. J. Math.*, **147**, 157–188, 2005.

Vahe G. Sargsyan

Received

20 March 2014

Revised

9 September 2014