



Math-Net.Ru

Общероссийский математический портал

А. А. Сапоженко, В. Г. Саргсян, Число сумм в Абелевой группе, *Дискрет. матем.*, 2018, том 30, выпуск 4, 96–105

DOI: 10.4213/dm1471

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: 18.97.9.168

27 марта 2025 г., 05:53:48



Число сумм в Абелевой группе

© 2018 г. А. А. Сапоженко*, В. Г. Саргсян**

Получены нижняя и верхняя асимптотические оценки числа различных подмножеств $A + B$ в абелевой группе порядка n при $|A|, |B| \geq n(\log n)^{-1/8}$.

Работа выполнена при финансовой поддержке РФФИ, проект № 16-01-00593А

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

1. Введение

Пусть G — абелева группа порядка n . Для любых подмножеств $A, B \subseteq G$ определим подмножество $A + B$:

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

и назовем его их *суммой*. Заметим, что число подмножеств в абелевой группе G порядка n равно 2^n , и любое из них является *суммой*, так как $A = A + \{0\}$ для любого $A \subseteq G$. Однако если ввести ограничение на мощность слагаемых, то число *сумм* становится существенно меньше.

В 2004 г. Б. Грин и И. Ружа (B. Green, I. Ruzsa) [1] доказали, что в группе простого порядка p имеется $2^{p/3+\bar{o}(p)}$ различных подмножеств $A + A$ (здесь и далее запись $\bar{o}(p)$ означает «о-малое от p »). Аналогичная оценка получена в [2] для числа различных подмножеств $A - A$ в группе простого порядка p . Для конечной абелевой группы G определим $D(G)$ как наибольшую мощность собственной подгруппы группы G (если группа G не содержит собственных подгрупп, то $D(G) = 0$), а $\varphi(n)$ — функция Эйлера. В [3] было 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 $A - A$. Число таких подмножеств не превышает $2^{n/3+D(G)/3+\bar{o}(n)}$. В 2010 г. Н. Алон, А. Гранвиль и А. Убис (N. Alon, A. Granville, A. Ubis) [4] доказали, что в группе простого порядка p имеется $2^{p/2+\bar{o}(p)}$ различных подмножеств $A + B$ при условии, что $|A|, |B| \rightarrow \infty$ при $n \rightarrow \infty$.

В настоящей работе доказана следующая теорема.

*Место работы: МГУ имени М.В. Ломоносова, e-mail: sapozhenko@mail.ru

**Место работы: МГУ имени М.В. Ломоносова, e-mail: vahe_sargsyan@yandex.com

Теорема 1. Пусть G — абелева группа порядка n и экспоненты $\nu, \nu \leq n$. Семейство различных подмножеств $A + B$, где $|A|, |B| \geq n(\log n)^{-1/8}$, обозначим через $S(G)$. Тогда справедливы неравенства

$$2^{\nu/2+\varepsilon_1(\nu)} \leq |S(G)| \leq 2^{n/2+D(G)/2+\varepsilon_2(n)}, \quad (1)$$

где $\varepsilon_1(\nu)/\nu \rightarrow 0$ при $\nu \rightarrow \infty$, и $\varepsilon_2(n)/n \rightarrow 0$ при $n \rightarrow \infty$.

2. Нижняя оценка числа сумм в абелевой группе

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

- (i) экспонента группы G делится на d ,
- (ii) существует такая подгруппа H группы G , что факторгруппа G/H изоморфна циклической группе порядка d .

Лемма 2 ([5, стр. 166, Лемма 3.4]). 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 $2^{n\sqrt{\rho}}$.

Пусть Z_n — циклическая группа порядка n . Для каждого данного $k < n$ положим

$$A = \{0, \lfloor (n-k)/2 \rfloor + 1, \lfloor (n-k)/2 \rfloor + 2, \dots, \lfloor (n-k)/2 \rfloor + k - 1\} \subseteq Z_n,$$

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

Заметим, что для каждого подмножества $B \subseteq \{0, 1, \dots, \lfloor (n-k)/2 \rfloor\}$ справедливо

$$B = (A + B) \cap \{0, 1, 2, \dots, \lfloor (n-k)/2 \rfloor\}.$$

Отсюда следует, что все множества $A + B$ попарно различны. Следовательно, в группе Z_n существует по меньшей мере $2^{\lfloor (n-k)/2 \rfloor + 1}$ различных подмножеств $A + B$. Положим $k = \lceil n(\log n)^{-1/8} \rceil$. Из леммы 2 следует, что число подмножеств множества $\{0, 1, 2, \dots, \lfloor (n-k)/2 \rfloor\}$, мощность которых не превышает $n(\log n)^{-1/8}$, не больше $2^{\lfloor (n-k)/2 \rfloor \sqrt{(\log n)^{-1/8}}}$. Следовательно, число различных подмножеств $A + B$ с $|A|, |B| \geq n(\log n)^{-1/8}$ не меньше $2^{\lfloor (n-k)/2 \rfloor + 1} - 2^{\lfloor (n-k)/2 \rfloor \sqrt{(\log n)^{-1/8}}}$, т. е.

$$|S(Z_n)| \geq 2^{n/2+\varepsilon_1(n)}, \quad (2)$$

где $\varepsilon_1(n)/n \rightarrow 0$ при $n \rightarrow \infty$.

Пусть G — абелева группа порядка n и экспоненты ν . В силу леммы 1 существует такая подгруппа H группы G , что факторгруппа G/H изоморфна циклической группе порядка ν . Тогда существует такой элемент g порядка ν , что G можно представить в виде

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

Пусть A' — подмножество факторгруппы G/H . Тогда

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

Положим

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

Другими словами $A(A')$ — множество представителей смежных классов A' .

Заметим, 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 A'_1 и A'_2 соответственно.

Пусть C' — подмножество факторгруппы G/H , и $C' = A' + B'$ для некоторых $A', B' \subseteq G/H$. Пусть $C(C')$ — множество представителей смежных классов $A' + B'$. Нетрудно убедиться в том, что $C(C') = A(A') + B(B')$, т. е. $C(C')$ равно сумме множеств представителей смежных классов A' и B' . Так как факторгруппа G/H изоморфна циклической группе порядка ν , то из неравенства (2) вытекает справедливость нижней оценки в (1).

3. Гранулирование

Обозначим множества вещественных и комплексных чисел через \mathbb{R} и \mathbb{C} соответственно. Пусть G — абелева группа порядка n , а $f_1, f_2 : G \rightarrow \mathbb{R}$. Определим свертку функций f_1 и f_2 следующим образом

$$(f_1 * f_2)(x) = \sum_{x_1 \in G} f_1(x_1) f_2(x - x_1).$$

Характером группы G называется такое отображение $\gamma : G \rightarrow \mathbb{C}$ такое, что для любых $x, y \in G$ имеют место равенства $|\gamma(x)| = 1$ и $\gamma(x + y) = \gamma(x)\gamma(y)$. Обозначим через Γ множество всех характеров группы G . Нетрудно убедиться, что Γ образует группу с операцией $\gamma_1 * \gamma_2(x) = \gamma_1(x)\gamma_2(x)$. *Преобразованием Фурье* $f : G \rightarrow \mathbb{R}$ называется функция $\widehat{f} : \Gamma \rightarrow \mathbb{C}$, определяемая равенством $\widehat{f}(\gamma) = \sum_{x \in G} f(x)\gamma(x)$.

Заметим также, что справедливо следующее утверждение.

Лемма 3. Для любого $\gamma \in \Gamma$ выполняется равенство

$$(\widehat{f_1 * f_2})(\gamma) = \widehat{f_1}(\gamma)\widehat{f_2}(\gamma).$$

Доказательство. Действительно, по определению преобразования Фурье

$$\begin{aligned} (\widehat{f_1 * f_2})(\gamma) &= \sum_{x \in G} (f_1 * f_2)(x)\gamma(x) = \sum_{x \in G} \sum_{x_1 \in G} f_1(x_1)f_2(x - x_1)\gamma(x_1)\gamma(x - x_1) \\ &= \sum_{x_1 \in G} f_1(x_1)\gamma(x_1) \sum_{x \in G} f_2(x - x_1)\gamma(x - x_1) = \widehat{f_1}(\gamma)\widehat{f_2}(\gamma). \end{aligned}$$

Пусть A, B — непустые подмножества группы G . Обозначим через $A(x), B(x)$ характеристические функции соответственно множеств A и B . Тогда $(A * B)(x)$ есть число таких пар $(a, b) \in A \times B$, что $x = a + b$. Положим

$$S_h(A, B) = \{x \in G \mid (A * B)(x) \geq h\}.$$

Лемма 4 ([5, стр. 174, Следствие 6.2]). Пусть G – абелева группа порядка n , а A, B – непустые подмножества группы G , и $h > 0$ – такое число, 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 $d \in G$, причем $\text{ord}(d) \geq L$, где $\text{ord}(d)$ – порядок элемента d . Рассмотрим подгруппу G , порожденную элементом d , и разобьем 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 («остаточное» множество может быть пустым, если порядок элемента d является кратным L). Для каждого $d \in G$ фиксируем одно такое разбиение. Объединение полученных прогрессий называется L -гранулой типа прогрессии.

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

Лемма 5 ([5, стр. 166, Лемма 3.3]). Пусть n – достаточно большое натуральное число, G – абелева группа порядка n , а $L \leq \sqrt{n}$. Тогда в группе G имеется не более $2^{3n/L}$ L -гранул обоих типов (прогрессии и смежного класса).

Лемма 6. Пусть n – достаточно большое натуральное число, G – абелева группа порядка n , A, B – произвольные подмножества группы G , а $0 < \varepsilon < 1/2$, $0 < \delta < 1$, L и L' – положительные числа, удовлетворяющие неравенству

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

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

- (i) P – либо прогрессия вида $\{id \mid -(L-1) \leq i \leq L-1\}$, причем $\text{ord}(d) \geq 2L/\varepsilon$, либо подгруппа группы G порядка не менее L' ,
- (ii) для любого $\gamma \in \Gamma$ имеют место неравенства $|\hat{A}(\gamma)(1-g(\gamma))| \leq \delta n$ и $|\hat{B}(\gamma)(1-g(\gamma))| \leq \delta n$, где $g(\gamma) = |P|^{-1} \sum_{p \in P} \gamma(p)$, а $A(x), B(x)$ – характеристические функции множеств A и B соответственно.

Доказательство. Пусть R – множество таких характеров γ , что $|\hat{A}(\gamma)| > \delta n/2$ и $|\hat{B}(\gamma)| > \delta n/2$, а Γ_1 – подгруппа группы Γ , порожденная множеством R . Введем подгруппу G_1 группы G

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

Рассмотрим два случая:

- 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, что

$$\begin{aligned} |\hat{A}(\gamma)(1-g(\gamma))| &\leq 2|\hat{A}(\gamma)| \leq 2\delta n/2 = \delta n, \\ |\hat{B}(\gamma)(1-g(\gamma))| &\leq 2|\hat{B}(\gamma)| \leq 2\delta n/2 = \delta n, \end{aligned}$$

а при $\gamma \in \Gamma_1$ справедливо равенство

$$|\hat{A}(\gamma)(1-g(\gamma))| = |\hat{B}(\gamma)(1-g(\gamma))| = 0.$$

2) Пусть $|G_1| < L'$. Выберем d так, что если в качестве P взять прогрессию $P = \{id \mid -(L-1) \leq i \leq L-1\}$, то условия пп. (i) и (ii) будут выполнены. Отметим, что при $\gamma \in \Gamma \setminus \Gamma_1$ пункт (ii) выполнен. Оценим величину $1 - g(\gamma)$. Фиксируем $\gamma \in \Gamma$ и через β обозначим $\arg \gamma(d) \in [-\pi, \pi)$. Таким образом, имеем

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

Заметим, что если для всех $\gamma \in R$

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

то п. (ii) выполнен. Также отметим, что для выполнения условия $\text{ord}(d) \geq 2L/\varepsilon$ достаточно, 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 $d \notin G_1$ так, чтобы при всех $\gamma \in R$ выполнялось условие

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

Заметим, 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 такой характер $\gamma \in R$, что $\gamma(d_1) \neq \gamma(d_2)$. Положим $\eta_\gamma = L^{-1} \min \left(\pi\varepsilon, \sqrt{6\delta n / |\widehat{A}(\gamma)|}, \sqrt{6\delta n / |\widehat{B}(\gamma)|} \right)$. Таким образом, для существования $d = d_1 - d_2$ с ограничением $|\arg(\gamma(d))| < \eta_\gamma$ достаточно, чтобы количество смежных классов по G_1 ($|G/G_1|$) превосходило $\prod_{\gamma \in R} (1 + \lfloor 2\pi/\eta_\gamma \rfloor)$. Подставив соответствующее значение η_γ в ранее написанное неравенство для $|G/G_1|$, получим

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

Заметим, что справедливы неравенства

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

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

В силу равенства Парсеваля имеем

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

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

Отсюда и из того, что $R \subseteq \Gamma$ и $|\widehat{B}(\gamma)| > \delta n/2$ для любого $\gamma \in R$, следует, что $|R| \leq 4\delta^{-2}$. Также заметим, что справедливо неравенство $\max(x, y) \leq x^y$ при $x \geq 1$ и $y \geq e^{1/e}$. Поэтому

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

Таким образом, существование подмножества $P \subseteq G$, удовлетворяющего условиям ш. (i) и (ii), доказано.

Лемма 7 (Гранулирование).

Пусть n — достаточно большое натуральное число, G — абелева группа порядка n , $0 < \varepsilon < 1/2$, A, B — произвольные подмножества группы G и $|A|, |B| \geq \varepsilon n$, а L и L' — положительные числа, удовлетворяющие неравенству

$$n > L' (4L/\varepsilon)^{2^{12}\varepsilon^{-7}}.$$

Тогда существуют такие подмножества $A', B' \subseteq G$, что

- (i) A', B' — либо L -гранулы типа прогрессии, либо L' -гранулы типа смежного класса,
- (ii) $|A \setminus A'| \leq \varepsilon n$, $|B \setminus B'| \leq \varepsilon n$,
- (iii) множество $A + B$ содержит все такие элементы $x \in G$, что $(A' * B')(x) \geq \varepsilon n$, за исключением не более εn элементов.

Доказательство. Построим множество P по лемме 6 при $\delta = \varepsilon^{7/2}2^{-5}$. Так как P — подгруппа или прогрессия, симметричная относительно 0, то $g(\gamma) = |P|^{-1} \sum_{p \in P} \gamma(p)$ есть вещественное число из отрезка $[-1, 1]$.

Построим множества A', B' . Рассмотрим два случая:

- 1) Если P — подгруппа, то в качестве A' возьмем объединение смежных классов G по P , содержащих не менее $\varepsilon|P|$ элементов множества A . Аналогично определяем B' : в качестве B' возьмем объединение смежных классов G по P , содержащих не менее $\varepsilon|P|$ элементов множества B . Так как $|A|, |B| \geq \varepsilon n$, то эти объединения смежных классов непустые. Тогда имеем

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

- 2) Если P — прогрессия с разностью d , то рассмотрим структуру гранул типа прогрессии с разностью d , и в качестве A' возьмем объединение прогрессий, содержащих не менее $\varepsilon L/2$ элементов множества A . Аналогично определяем B' : в качестве B' возьмем объединение прогрессий, содержащих не менее $\varepsilon L/2$ элементов множества B . Так как $|A|, |B| \geq \varepsilon n$, то эти объединения прогрессий непустые. Заметим также, что не более чем $nL/\text{ord}(d)$ элементов из «остаточных» множеств не входят ни в одну из гранул. Тогда, с учетом того, что $\text{ord}(d) \geq 2L/\varepsilon$, получим

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

Условия (i) и (ii) леммы выполнены в обоих случаях.

Докажем п. (iii). Рассмотрим две следующие функции $a(x) = |P|^{-1}|A \cap (P+x)|$ и $b(x) = |P|^{-1}|B \cap (P+x)|$. Заметим, что для преобразований Фурье функций $a(x)$ и $b(x)$ справедливы равенства $\widehat{a}(\gamma) = g(\gamma)\widehat{A}(\gamma)$ и $\widehat{b}(\gamma) = g(\gamma)\widehat{B}(\gamma)$. Действительно, с учетом того, что $P = -P$, имеем

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

Аналогично доказывается, что $\widehat{b}(\gamma) = g(\gamma)\widehat{B}(\gamma)$. Нетрудно убедиться в том, что для любого $\gamma \in \Gamma$ имеет место неравенство $1 - (g(\gamma))^2 \leq 2(1 - g(\gamma))$. Отсюда и из равенства Парсеваля и лемм 3 и 6 следует, что

$$\begin{aligned} \sum_{x \in G} |(A * B)(x) - (a * b)(x)|^2 &= n^{-1} \sum_{\gamma \in \Gamma} |(\widehat{A * B})(\gamma) - (\widehat{a * b})(\gamma)|^2 \\ &= n^{-1} \sum_{\gamma \in \Gamma} |\widehat{A}(\gamma)\widehat{B}(\gamma) - \widehat{a}(\gamma)\widehat{b}(\gamma)|^2 = n^{-1} \sum_{\gamma \in \Gamma} |\widehat{A}(\gamma)|^2 |\widehat{B}(\gamma)|^2 |1 - (g(\gamma))^2|^2 \end{aligned}$$

$$\begin{aligned} &\leq \frac{1}{n} \cdot 4 \cdot \max_{\gamma \in \Gamma} (|\widehat{A}(\gamma)| |1 - g(\gamma)|)^2 \cdot \sum_{\gamma \in \Gamma} |\widehat{B}(\gamma)|^2 \\ &\leq \frac{1}{n} \cdot 4 \cdot \max_{\gamma \in \Gamma} (|\widehat{A}(\gamma)| |1 - g(\gamma)|)^2 \cdot n^2 \\ &\leq 4 \cdot n \cdot (\delta n)^2 = 4 \cdot \delta^2 \cdot n^3. \end{aligned} \tag{3}$$

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

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 , и поэтому $|(x + P) \cap A| \geq \varepsilon|P|/4$. Таким образом, $a(x) \geq \varepsilon/4 = \varepsilon A'(x)/4$ для всех $x \in G$. Если $x \notin A'$, то $a(x) \geq 0 = \varepsilon A'(x)/4$.

Аналогично получается, что для всех $x \in G$ справедливо неравенство $b(x) \geq \varepsilon B'(x)/4$.

Из этих неравенств и леммы 3 вытекает, что для всех $x \in G$ имеет место неравенство

$$(a * b)(x) \geq \varepsilon^2 (A' * B')(x)/4^2. \tag{4}$$

При условии, что

$$(A' * B')(x) \geq \varepsilon n,$$

из (4) получаем

$$(a * b)(x) \geq \varepsilon^3 n/4^2.$$

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

$$(A * B)(x) = 0$$

и

$$(A' * B')(x) \geq \varepsilon n,$$

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

$$|(A * B)(x) - (a * b)(x)|^2 \geq \varepsilon^6 n^2/4^4. \tag{5}$$

Из (3) и (5) следует, что

$$\begin{aligned} 4 \cdot \delta^2 \cdot n^3 &\geq \sum_{x \in G} |(A * B)(x) - (a * b)(x)|^2 \geq \\ &\geq \sum_{x \in F} |(A * B)(x) - (a * b)(x)|^2 \geq |F| \varepsilon^6 n^2/4^4. \end{aligned}$$

Остюда, полагая $\delta = \varepsilon^{7/2} 2^{-5}$, получим, что $|F| \leq \varepsilon n$.

Лемма 7 доказана.

4. Верхняя оценка числа сумм в абелевой группе

Пусть G — абелева группа порядка n . 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 7. Для каждого подмножеств $A, B \subseteq G$, и $|A|, |B| \geq n(\log n)^{-1/8}$, применяя лемму 7, построим множества A' и B' соответственно. Оценим величину $|S(G)|$ путем подсчета количества соответствующих пар $((A', B'), A + B)$.

Пусть A' и B' — либо L -гранулы типа прогрессии, либо L' -гранулы типа смежного класса. Для каждой фиксированной пары (A', B') рассмотрим два случая: $|A'| + |B'| > n/2 + D(G)/2$ и $|A'| + |B'| \leq n/2 + D(G)/2$.

Пусть $|A'| + |B'| > n/2 + D(G)/2$. В силу п. (iii) леммы 7 получим, что множество $\overline{A+B}$ (запись \overline{C} означает дополнение множества C) является подмножеством объединения множества $\overline{S_{\varepsilon n}(A', B')}$ с некоторым подмножеством группы G мощности, не превышающей εn . В силу леммы 4 имеем

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

При условии $|A'| + |B'| > n/2 + D(G)/2$ получаем, что

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

Из леммы 2 и того, что множество $\overline{A+B}$ однозначно определяет множество $A+B$, получим, что число способов выбора $A+B$ при заданной паре множеств (A', B') , для которых имеет место $|A'| + |B'| > n/2 + D(G)/2$, не превосходит

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

Пусть $|A'| + |B'| \leq n/2 + D(G)/2$. По п. (ii) леммы 7 множество A является подмножеством объединения множества A' с некоторым подмножеством группы G мощности, не превышающей εn . Аналогично получается, что B является подмножеством объединения множества B' с некоторым подмножеством группы G мощности, не превышающей εn . Из леммы 2 и того, что каждая пара множеств (A, B) порождает ровно одно множество вида $A+B$, следует, что число способов выбора $A+B$ при заданной паре множеств (A', B') , для которых имеет место $|A'| + |B'| \leq n/2 + D(G)/2$, не превосходит

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

Из вышеизложенного и леммы 5, с учетом того, что $6n/L \leq n\sqrt{\varepsilon}$ при достаточно большом n , получаем

$$|S(G)| \leq 2^{n/2 + D(G)/2 + \varepsilon_2(n)}$$

где $\varepsilon_2(n)/n \rightarrow 0$ при $n \rightarrow \infty$.

Верхняя оценка в 1 доказана.

Список литературы

1. Green B., Ruzsa I., “Counting sumsets and sum-free sets modulo a prime”, *Studia Sci. Math. Hungarica.*, **41** (2004), 285–293.

2. Саргсян В. Г., “Число разностей в группах простого порядка”, *Дискретная математика*, **25**:1 (2013), 152–158; англ. пер.: Sargsyan V. G., “The number of differences in groups of prime order”, *Discrete Math. Appl.*, **23**:2 (2013), 195–201.
3. Саргсян В. Г., “Число сумм и разностей в абелевой группе”, *Дискретный анализ и исследование операций*, **22**:2 (2015), 73–85; англ. пер.: Sargsyan V. G., “Counting sumsets and differences in an abelian group”, *J. Applied and Industrial Mathematics*, **9**:2, 275–282.
4. Alon N., Granville A., Ubis A., “The number of sumsets in a finite field”, *Bulletin of the London mathematical society*, **42**:5 (2010), 784–794.
5. Green B., Ruzsa I., “Sum-free sets in abelian groups”, *Israel J. Math.*, **147** (2005), 157–188.

Статья поступила 11.09.2017.

Переработанный вариант поступил 24.10.2018.