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

https://www.mathnet.ru/dm1471

Дискретная математика

том 30 выпуск 4 * 2018

УДК 519.112.7+512.542.52 DOI https://doi.org/10.4213/dm1471

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 $|A|, |B| \geqslant n(\log n)^{-1/8}$.

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 $|A|, |B| \to \infty$ при $n \to \infty$.

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@ymail.com

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

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

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

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

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

(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 $B \subseteq \{0, 1, \ldots, \lfloor (n-k)/2 \rfloor\}$ справедливо

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

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 $\{0, 1, 2, \ldots, \lfloor (n-k)/2 \rfloor\}$, 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 $|A|, |B| \geqslant n(\log n)^{-1/8}$ не меньше $2^{\lfloor (n-k)/2 \rfloor + 1} - 2^{\lfloor (n-k)/2 \rfloor \sqrt{(\log n)^{-1/8}}}$, т. е.

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

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

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

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

Пусть A' — подмножество факторгруппы G/H. Тогда

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

Положим

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

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 $f_1, f_2 \colon G \to \mathbb{R}$. 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 $\gamma : G \to \mathbb{C}$ 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 $\gamma_1 \star \gamma_2(x) = \gamma_1(x)\gamma_2(x)$. *Преобразованием Фурье* $f : G \to \mathbb{R}$ называется функция $\widehat{f} : \Gamma \to \mathbb{C}$, определяемая равенством $\widehat{f}(\gamma) = \sum\limits_{x \in G} f(x)\gamma(x)$. 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

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

$$= \sum_{x_1 \in G} f_1(x_1)\gamma(x_1) \sum_{x \in G} f_2(x - x_1)\gamma(x - x_1) = \widehat{f}_1(\gamma)\widehat{f}_2(\gamma).$$

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

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

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 $\sqrt{hn} \leqslant \min(|A|, |B|)$. 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 $d \in G$, причем $\operatorname{ord}(d) \geqslant L$, где $\operatorname{ord}(d)$ — порядок элемента d. Рассмотрим подгруппу G, порожденную элементом d, и разобьём каждый её смежный класс 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 («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 $L \leqslant \sqrt{n}$. 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 $\{id \mid -(L-1) \leqslant i \leqslant L-1\}$, причем $\operatorname{ord}(d) \geqslant 2L/\varepsilon$, либо подгруппа группы G порядка не менее L',*

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

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

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

Рассмотрим два случая:

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

$$\bigl|\widehat{A}(\gamma)\bigl(1-g(\gamma)\bigr)\bigr| \leqslant 2\bigl|\widehat{A}(\gamma)\bigr| \leqslant 2\delta n/2 = \delta n,$$
$$\bigl|\widehat{B}(\gamma)\bigl(1-g(\gamma)\bigr)\bigr| \leqslant 2\bigl|\widehat{B}(\gamma)\bigr| \leqslant 2\delta n/2 = \delta n,$$

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

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

2) Пусть $|G_1| < L'$. Выберем d так, что если в качестве P взять прогрессию $P = \{id \mid -(L-1) \leqslant i \leqslant L-1\}$, то условия пп. (i) и (ii) будут выполнены. Отметим, что при $\gamma \in \Gamma\backslash\Gamma_1$ 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

$$0 \leqslant 1 - g(\gamma) = 1 - \frac{1}{2L-1} \sum_{j=-L-1}^{L-1} \big(\cos j\beta + i \sin j\beta\big)$$

$$= 1 - \frac{1}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta = \frac{2L-2}{2L-1} - \frac{2}{2L-1} \sum_{j=1}^{L-1} \cos j\beta$$

$$= \frac{2}{2L-1} \sum_{j=1}^{L-1} \big(1 - \cos j\beta\big) \leqslant \frac{1}{2L-1} \sum_{j=1}^{L-1} (j\beta)^2 = \frac{L(L-1)}{6}\beta^2 \leqslant \frac{(L\beta)^2}{6}.$$

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

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

то п. (ii) выполнен. Также отметим, что для выполнения условия $\mathrm{ord}(d) \geqslant 2L/\varepsilon$ достаточно, чтобы при некотором $\gamma \in \Gamma$ имело место неравенство

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

Покажем, что можно выбрать $d \notin G_1$ так, чтобы при всех $\gamma \in R$ выполнялось условие

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

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

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

Заметим, что справедливы неравенства

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

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

$$\leqslant (4L)^{|R|}\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon},\sqrt{\frac{|\widehat{A}(\gamma)|}{\delta n}},\sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right).$$

В силу равенства Парсеваля имеем

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

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

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

$$\bigl(4L\bigr)^{|R|}\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon},\sqrt{\frac{|\widehat{A}(\gamma)|}{\delta n}},\sqrt{\frac{|\widehat{B}(\gamma)|}{\delta n}}\right)$$

$$\leqslant (4L)^{4\delta^{-2}}\left(\prod_{\gamma\in R}\max\left(\frac{1}{\varepsilon^4},\left(\frac{|\widehat{A}(\gamma)|}{\delta n}\right)^2,\left(\frac{|\widehat{B}(\gamma)|}{\delta n}\right)^2\right)\right)^{1/4}$$

$$\leqslant \bigl(4L\bigr)^{4\delta^{-2}}\bigl(\varepsilon^{-4}\bigr)^{(4\delta^2n^2)^{-1}\max\left(\sum\limits_{\gamma\in R}|\widehat{A}(\gamma)|^2,\sum\limits_{\gamma\in R}|\widehat{B}(\gamma)|^2\right)} \leqslant \bigl(4L\bigr)^{4\delta^{-2}}\varepsilon^{-\delta^{-2}}$$

$$\leqslant \bigl(4L/\varepsilon\bigr)^{4\delta^{-2}} < \frac{n}{L'} \leqslant \bigl|G/G_1\bigr|.$$

Таким образом, существование подмножества $P\subseteq G$, удовлетворяющего условиям пп. (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 $|A|,|B|\geqslant\varepsilon n$, 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) *$\bigl|A\setminus A'\bigr|\leqslant\varepsilon n$, $\bigl|B\setminus B'\bigr|\leqslant\varepsilon n$,*

(iii) *множество $A+B$ содержит все такие элементы $x\in G$, что $(A'*B')(x)\geqslant\varepsilon n$, 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 $g(\gamma) = |P|^{-1}\sum\limits_{p\in P}\gamma(p)$ 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 $|A|, |B| \geqslant \varepsilon n$, то эти объединения смежных классов непустые. Тогда имеем

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

2) Если P — прогрессия с разностью d, то расмотрим 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 $|A|, |B| \geqslant \varepsilon n$, то эти объединения прогрессий непустые. Заметим также, что не более чем $nL/\mathrm{ord}(d)$ элементов из «остаточных» множеств не входят ни в одну из гранул. Тогда, с учетом того, что $\mathrm{ord}(d) \geqslant 2L/\varepsilon$, получим

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

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

Докажем п. (iii). Рассмотрим две следующие функции $a(x) = \big|P\big|^{-1}\big|A \cap (P + x)\big|$ и $b(x) = \big|P\big|^{-1}\big|B \cap (P + x)\big|$. 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

$$\widehat{a}(\gamma) = \sum_{x\in G} a(x)\gamma(x) = \frac{1}{|P|}\sum_{x\in G}|A \cap (P + x)|\gamma(x) = \frac{1}{|P|}\sum_{c\in A}\sum_{p\in P}\gamma(c - p)$$

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

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

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

$$= n^{-1}\sum_{\gamma\in\Gamma}\big|\widehat{A}(\gamma)\widehat{B}(\gamma) - \widehat{a}(\gamma)\widehat{b}(\gamma)\big|^2 = n^{-1}\sum_{\gamma\in\Gamma}\big|\widehat{A}(\gamma)\big|^2\big|\widehat{B}(\gamma)\big|^2\big|1 - (g(\gamma))^2\big|^2$$

$$\leqslant \frac{1}{n}\cdot 4\cdot \max_{\gamma\in\Gamma}\big(\big|\widehat{A}(\gamma)\big|\big|1-g(\gamma)\big|\big)^2\cdot\sum_{\gamma\in\Gamma}\big|\widehat{B}(\gamma)\big|^2$$

$$\leqslant \frac{1}{n}\cdot 4\cdot \max_{\gamma\in\Gamma}\big(\big|\widehat{A}(\gamma)\big|\big|1-g(\gamma)\big|\big)^2\cdot n^2$$

$$\leqslant 4\cdot n\cdot\big(\delta n\big)^2 = 4\cdot\delta^2\cdot n^3. \tag{3}$$

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

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

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

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

При условии, что

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

из (4) получаем

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

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

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

и

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

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

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

Из (3) и (5) следует, что

$$4\cdot\delta^2\cdot n^3\geqslant\sum_{x\in G}\big|(A*B)(x)-(a*b)(x)\big|^2\geqslant$$

$$\geqslant\sum_{x\in F}\big|(A*B)(x)-(a*b)(x)\big|^2\geqslant|F|\varepsilon^6 n^2/4^4.$$

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

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 каждых подмножеств $A, B \subseteq G$, и $|A|, |B| \geqslant n(\log n)^{-1/8}$, 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 $|A'| + |B'| \leqslant n/2 + D(G)/2$.

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

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

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

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

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

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

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

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

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

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.