

Об оценке мощности разностного подмножества многомерного дискретного тора $\mathbb{Z}_3^{n*}$

Е. П. ДАВЛЕТЯРОВА, А. А. ЖУКОВА, А. А. ЮДИН

Владимирский государственный гуманитарный университет

УДК 511.29

Ключевые слова: разностные множества, векторные пространства над конечным полем.

Аннотация

Найдена оценка сверху мощности подмножества дискретного тора над полем из трёх элементов, никакие четыре различные точки которого не образуют невырожденного параллелограмма.

Abstract

E. P. Davletyarova, A. A. Zhukova, A. A. Yudin, Estimating the cardinality of a difference subset of the discrete multi-torus $\mathbb{Z}_3^n$, Fundamentalnaya i prikladnaya matematika, vol. 16 (2010), no. 6, pp. 23–32.

In this paper, we obtain an upper estimate for the cardinality of a subset of the discrete torus over a field of three elements of which any four points do not form a nonsingular parallelogram.

1. Основные определения

Пусть G — группа, операцию которой будем описывать аддитивно. Подмножество $A \subset G$ назовём разностным, если для любых $x, y, u, v \in A$ равенство $x - y = u - v$ возможно, если и только если $x = u, y = v$ или $y = u$.

Пусть $\mathbb{Z}_3$ — поле $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}_3^n = \mathbb{Z}_3^{n-1} \oplus \mathbb{Z}_3$, A — разностное подмножество $\mathbb{Z}_3^n$. Число элементов множества A будем обозначать $\text{card}(A)$; $A(n) = \max_A \text{card}(A)$, где максимум берётся по всем разностным множествам A пространства $\mathbb{Z}_3^n$.

Изучение разностных множеств имеет долгую историю (см. [3–6]). Настоящая работа посвящена исследованию мощности и структуры разностного множества A . Известно, что разностное подмножество $\mathbb{Z}_p^n$ (см. [2, 6]) имеет мощность порядка $p^{n/2}$, если p достаточно велико по сравнению с n . Нами найдена следующая оценка:

$$\sqrt[3]{2} \cdot 3^{n/3} \leq A(n) \leq \sqrt[3]{3} \cdot 3^{n/3},$$

* Работа выполнена при финансовой поддержке гранта РФФИ № 07-01-00118-а.

она даёт точный порядок роста $A(n)$ и показывает, насколько сильно могут отличаться мощности разностных множеств дискретных торов.

Пусть a_1, a_2, a_3, a_4 — произвольные элементы пространства $\mathbb{Z}_3^n$. Будем говорить, что $\{a_1, a_2, a_3, a_4\}$ образуют параллелограмм, если при подходящей перестановке σ на множестве из четырёх элементов $\{1, 2, 3, 4\}$ выполнено равенство

$$a_{\sigma 1} - a_{\sigma 2} = a_{\sigma 3} - a_{\sigma 4}.$$

Параллелограмм будем называть невырожденным, если a_1, a_2, a_3, a_4 различны.

Пусть a_1, a_2, a_3 — произвольные элементы пространства $\mathbb{Z}_3^n$. Будем говорить, что они образуют прямую, заданную уравнением $x_i = a_1 + (a_3 - a_2)t$, где $i = 1, 2, 3$, $t = 0, 1, 2$, если $a_1 + a_2 + a_3 \equiv 0 \pmod{3}$.

Две прямые l_1, l_2 пространства $\mathbb{Z}_3^n$ назовём параллельными, если для образующих их точек $a_1, a_2, a_3 \in l_1, b_1, b_2, b_3 \in l_2$ при подходящем выборе $\alpha_1, \alpha_2 \in \{1, 2, 3\}, \beta_1, \beta_2 \in \{1, 2, 3\}$ выполнено соотношение

$$a_{\alpha_1} - a_{\alpha_2} \equiv b_{\beta_1} - b_{\beta_2} \pmod{3}.$$

Пусть a_1, a_2 — произвольные элементы пространства $\mathbb{Z}_3^n$. Разность $a_1 - a_2$ будем называть направлением. Заметим, что две разности $a_1 - a_2$ и $a_3 - a_4$ задают одно и то же направление, если $a_1 - a_2 \equiv a_3 - a_4 \pmod{3}$, где $a_1, a_2, a_3, a_4 \in \mathbb{Z}_3^n$. Направление $a_2 - a_1$ будем считать противоположным для направления $a_1 - a_2$.

Лемма 1. Любые четыре различные точки пространства $\mathbb{Z}_3^n$, лежащие на двух параллельных прямых, образуют невырожденный параллелограмм.

Доказательство. Пусть прямые l_1 и l_2 , $l_1 \parallel l_2$, заданы уравнениями

$$l_1: x_i = a_i + p_i t, \quad l_2: y_i = b_i + p_i t,$$

где $i = 1, 2, \dots, n$, $t = 0, 1, 2$. На прямой l_1 лежат две точки, координаты которых могут быть записаны следующим образом:

$$\begin{aligned} A_1(x_1^1, x_2^1, \dots, x_n^1), \quad \text{где } x_i^1 &= a_i + p_i t, \\ A_2(x_1^2, x_2^2, \dots, x_n^2), \quad \text{где } x_i^2 &= a_i + p_i(t+1). \end{aligned}$$

Две точки на прямой l_2 можно выбрать тремя способами.

I способ:

$$\begin{aligned} B_1(y_1^1, y_2^1, \dots, y_n^1), \quad \text{где } y_i^1 &= b_i + p_i t, \\ B_2(y_1^2, y_2^2, \dots, y_n^2), \quad \text{где } y_i^2 &= b_i + p_i(t+1). \end{aligned}$$

В этом случае мы получим четыре вектора

$$\begin{aligned} \overrightarrow{A_1 A_2}(p_1, p_2, \dots, p_n), \quad \overrightarrow{B_1 B_2}(p_1, p_2, \dots, p_n), \\ \overrightarrow{A_1 B_1}(b_1 - a_1, b_2 - a_2, \dots, b_n - a_n), \quad \overrightarrow{A_2 B_2}(b_1 - a_1, b_2 - a_2, \dots, b_n - a_n), \end{aligned}$$

т. е. точки A_1, A_2, B_1, B_2 образуют невырожденный параллелограмм.

II способ:

$$\begin{aligned} B_1(y_1^1, y_2^1, \dots, y_n^1), \quad \text{где } y_i^1 &= b_i + p_i(t+1), \\ B_2(y_1^2, y_2^2, \dots, y_n^2), \quad \text{где } y_i^2 &= b_i + p_i(t+2). \end{aligned}$$

В этом случае мы получим четыре вектора

$$\begin{aligned} \overrightarrow{A_1 A_2}(p_1, p_2, \dots, p_n), \\ \overrightarrow{B_1 B_2}(p_1, p_2, \dots, p_n), \\ \overrightarrow{A_1 B_1}(b_1 - a_1 + p_1, b_2 - a_2 + p_2, \dots, b_n - a_n + p_n), \\ \overrightarrow{A_2 B_2}(b_1 - a_1 + p_1, b_2 - a_2 + p_2, \dots, b_n - a_n + p_n), \end{aligned}$$

т. е. точки A_1, A_2, B_1, B_2 образуют невырожденный параллелограмм.

III способ:

$$\begin{aligned} B_1(y_1^1, y_2^1, \dots, y_n^1), \quad \text{где } y_i^1 &= b_i + p_i t, \\ B_2(y_1^2, y_2^2, \dots, y_n^2), \quad \text{где } y_i^2 &= b_i + p_i(t+2). \end{aligned}$$

В этом случае мы получим четыре вектора

$$\begin{aligned} \overrightarrow{A_1 A_2}(p_1, p_2, \dots, p_n), \\ \overrightarrow{B_2 B_1}(-2p_1, -2p_2, \dots, -2p_n) \quad \text{или} \quad \overrightarrow{B_2 B_1}(p_1, p_2, \dots, p_n), \\ \overrightarrow{A_1 B_2}(b_1 - a_1 + 2p_1, b_2 - a_2 + 2p_2, \dots, b_n - a_n + 2p_n), \\ \overrightarrow{A_2 B_1}(b_1 - a_1 - p_1, b_2 - a_2 - p_2, \dots, b_n - a_n - p_n) \\ \text{или} \quad \overrightarrow{A_2 B_1}(b_1 - a_1 + 2p_1, b_2 - a_2 + 2p_2, \dots, b_n - a_n + 2p_n), \end{aligned}$$

т. е. точки A_1, A_2, B_2, B_1 образуют невырожденный параллелограмм.

Лемма доказана. $\square$

Лемма 2. Любые четыре различные точки, лежащие на двух пересекающихся прямых пространства $\mathbb{Z}_3^n$, образуют невырожденный параллелограмм.

Доказательство. Пусть прямые l_1 и l_2 , $l_1 \cap l_2$, заданы уравнениями

$$l_1: x_i = a_i + p_i t, \quad l_2: y_i = a_i + q_i t,$$

где $i = 1, 2, \dots, n$, $t = 0, 1, 2$.

Прямая l_1 состоит из точек

$$\begin{aligned} A(a_1, a_2, \dots, a_n), \quad B(a_1 + p_1, a_2 + p_2, \dots, a_n + p_n), \\ C(a_1 + 2p_1, a_2 + 2p_2, \dots, a_n + 2p_n). \end{aligned}$$

Прямая l_2 состоит из точек

$$\begin{aligned} D(a_1, a_2, \dots, a_n), \quad E(a_1 + q_1, a_2 + q_2, \dots, a_n + q_n), \\ F(a_1 + 2q_1, a_2 + 2q_2, \dots, a_n + 2q_n). \end{aligned}$$

В этом случае мы получим четыре вектора:

$$\begin{aligned} &\overrightarrow{BD}(q_1 - p_1, q_2 - p_2, \dots, q_n - p_n), \\ &\overrightarrow{EC}(2p_1 - 2q_1, 2p_2 - 2q_2, \dots, 2p_n - 2q_n) \text{ или } \overrightarrow{EC}(q_1 - p_1, q_2 - p_2, \dots, q_n - p_n), \\ &\overrightarrow{BE}(2q_1 - p_1, 2q_2 - p_2, \dots, 2q_n - p_n), \\ &\overrightarrow{DC}(2p_1 - q_1, 2p_2 - q_2, \dots, 2p_n - q_n) \text{ или } \overrightarrow{DC}(2q_1 - p_1, 2q_2 - p_2, \dots, 2q_n - p_n), \end{aligned}$$

т. е. точки B, D, E, C образуют невырожденный параллелограмм.

Лемма доказана. $\square$

2. Точное решение задачи для торов малой размерности

Пусть $\mathbb{Z}_3$ — поле вычетов по модулю 3, $\mathbb{Z}_3^n$ — n -мерное пространство над этим полем, A — подмножество $\mathbb{Z}_3^n$, состоящее из различных точек a_j с координатами $(a_{j1}; a_{j2}; \dots; a_{jn})$, таких что если $a_1, a_2, a_3, a_4 \in A$, то $a_{1t} + a_{2t} \equiv a_{3t} + a_{4t} \pmod{3}$ тогда и только тогда, когда $a_{1t} = a_{3t}$, $a_{2t} = a_{4t}$ или $a_{3t} = a_{4t}$, где $t = 1, 2, \dots, n$, $A(n) = |A|$ — мощность множества A . Найдём оценку сверху для $A(n)$.

Для $n = 1, 2, 3, 4, 5$ приведём точные значения мощности разностного множества.

Очевидно, что $A(1) = 3$.

Покажем, что $A(2) < 6$. Предположим, что $|A| = 6$. Тогда найдутся образующие параллелограмм четыре точки, лежащие на двух параллельных прямых. Значит, по лемме 1 в множестве A есть невырожденный параллелограмм. Мы получили противоречие с определением разностного множества A .

Предположим, что $|A| = 5$. Возможны два случая:

- 1) найдутся четыре точки, лежащие по две на двух параллельных прямых;
- 2) найдутся четыре точки, лежащие на двух пересекающихся прямых.

Первый случай невозможен, так как по лемме 1 четыре точки, лежащие по две на двух параллельных прямых, образуют невырожденный параллелограмм, который не может содержаться в разностном множестве A . Второй случай невозможен, так как по лемме 2 четыре различные точки, лежащие на двух пересекающихся прямых, образуют невырожденный параллелограмм, что противоречит определению разностного множества. Таким образом, $|A| < 5$.

Покажем, что $|A| = 4$. Три точки, лежащие на одной прямой, и одна точка, ей не принадлежащая, образуют множество A , так как у невырожденного параллелограмма любые три точки линейно независимы и не могут лежать на одной прямой. Приведём пример разностного множества A пространства $\mathbb{Z}_3^2$ мощности 4:

$$A = \{(0; 0), (0; 1), (0; 2), (1; 0)\}.$$

Покажем, что в $\mathbb{Z}_3^3$ мощность экстремального разностного множества A равна 6. $\mathbb{Z}_3^3$ можно интерпретировать как трёхмерный куб, состоящий из трёх параллельных плоскостей π_1, π_2, π_3 , где π_i изоморфны $\mathbb{Z}_3^2$, $i = 1, 2, 3$. Максимальное количество точек множества A в π_1 равно 4, причём три из этих точек лежат на одной прямой. Эти четыре точки задают четыре различных направления. Заметим, что в пространстве $\mathbb{Z}_3^n$ имеется $(3^{2n} - 3^n)/6$ различных прямых (см. [1]), т. е. в пространстве $\mathbb{Z}_3^3$ — 12 различных прямых, образующих четыре тройки параллельных прямых. Таким образом, если в плоскости π_2 взять прямую l , то в плоскости π_1 найдётся прямая $l', l' \parallel l$, и на прямой l' уже лежат две точки, т. е. по лемме 1 на прямой l может быть только одна точка, принадлежащая множеству A . Те же рассуждения, очевидно, справедливы и для плоскости π_3 . Значит, $|A| \leq 6$.

Приведём схему построения множества A в $\mathbb{Z}_3^3$. Возьмём в плоскости π_1 точки T_1, T_2, T_3, T_4 , причём $\{T_1, T_2, T_3\} = l$, $T_4 \notin l$. Тогда в плоскости π_2 в качестве $T_5 \in A$ можно взять любую точку, так как не существует параллелограмма, у которого три вершины лежат в плоскости, которой не принадлежит четвёртая вершина. Точка T_5 и прямая l задают плоскость α , которая пересекает плоскость π_3 по прямой l_1 , $l_1 \parallel l$. Так как $T_1, T_2, T_3, T_5 \in A$ и $T_1, T_2, T_3, T_5 \in \alpha$, то в плоскости α не может быть ещё одной точки, принадлежащей множеству A , и следовательно, на прямой l_1 нет точек, принадлежащих A . Через точку T_4 проведём плоскость β , $\beta \parallel \alpha$, $\beta \cap \pi_3 = l_2$. Так как в плоскости α уже есть четыре точки, принадлежащие множеству A , то по доказанному ранее в плоскости $\beta \parallel \alpha$ может быть только одна точка, принадлежащая множеству A — это точка T_4 . Следовательно, на прямой l_2 нет точек, принадлежащих множеству A . В качестве шестой точки $T_6 \in A$ можно взять любую точку прямой l_3 , $l_3 \in \pi_3$, $l_3 \parallel l_1$, $l_3 \parallel l_2$. Примером такого множества является

$$A = \{(0; 0; 0), (0; 0; 1), (0; 0; 2), (0; 1; 0), (1; 0; 0), (2; 2; 0)\}.$$

Вычисления на компьютере дали возможность получить примеры разностных множеств A для торов размерностей 4 и 5. Так, в пространстве $\mathbb{Z}_3^4$ $A(4) \geq 9$; например,

$$A = \{(0; 0; 0; 0), (0; 0; 0; 1), (0; 0; 0; 2), (0; 0; 1; 0), \\ (0; 1; 0; 0), (0; 2; 2; 0), (1; 0; 0; 0), (1; 1; 2; 1), (1; 2; 1; 2)\}.$$

Для $\mathbb{Z}_3^5$ $A(5) \geq 14$; например,

$$A = \{(0; 0; 0; 0; 0), (0; 0; 0; 0; 2), (0; 0; 0; 1; 1), (0; 0; 0; 2; 0), (0; 0; 1; 0; 0), \\ (0; 0; 2; 0; 0), (0; 1; 0; 0; 0), (0; 1; 1; 1; 2), (0; 1; 2; 2; 1), (1; 0; 0; 0; 0), \\ (1; 0; 1; 2; 1), (1; 0; 2; 1; 2), (1; 1; 0; 0; 2), (1; 2; 0; 2; 2)\}.$$

3. Доказательство основного результата

Теорема. Для любого $n \geq n_0$ справедливо неравенство*

$$\sqrt[3]{2} \cdot 3^{n/3} \leq A(n) \leq \sqrt[3]{3} \cdot 3^{n/3}.$$

Доказательство. Пусть $A(n) = k$, $a_j = (a_{j1}; a_{j2}; \dots; a_{jn})$, $a_j \in \mathbb{Z}_3^n$ и $(a_j, a_m) = a_{j1}a_{m1} + \dots + a_{jn}a_{mn}$. Определим комплекснозначную функцию

$$S_A(x) = \sum_{j=1}^k e^{2\pi i \frac{(a_j, x)}{3}},$$

где $x = (x_1; x_2; \dots; x_n)$, $x \in \mathbb{Z}_3^n$, $a_j \in A$.

Представим $\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4$ в виде суммы:

$$\begin{aligned} \sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4 &= \sum_{x \in \mathbb{Z}_3^n} \sum_{\substack{j, l, m, p=1, \\ a_j + a_l - a_m - a_p \equiv 0 \pmod{3}}}^k e^{2\pi i \frac{(a_j + a_l - a_m - a_p, x)}{3}} + \\ &+ \sum_{x \in \mathbb{Z}_3^n} \sum_{\substack{j, l, m, p=1, \\ a_j + a_l - a_m - a_p \not\equiv 0 \pmod{3}}}^k e^{2\pi i \frac{(a_j + a_l - a_m - a_p, x)}{3}} = \sum_1 + \sum_2. \end{aligned}$$

Вычислим второе слагаемое, изменив в нём порядок суммирования:

$$\sum_2 = \sum_{\substack{j, l, m, p=1, \\ a_j + a_l - a_m - a_p \not\equiv 0 \pmod{3}}}^k \sum_{x \in \mathbb{Z}_3^n} e^{2\pi i \frac{(a_j + a_l - a_m - a_p, x)}{3}}.$$

Рассмотрим внутреннюю сумму в $\sum_2$:

$$\begin{aligned} \sum_{x \in \mathbb{Z}_3^n} e^{2\pi i \frac{(a_j + a_l - a_m - a_p, x)}{3}} &= \\ &= \sum_{x_1, \dots, x_{n-1} \in \mathbb{Z}_3^n} e^{2\pi i \sum_{d=1}^{n-1} \frac{(a_{jd} + a_{ld} - a_{md} - a_{pd})x_d}{3}} \sum_{x_n=0}^2 e^{2\pi i \frac{(a_{jn} + a_{ln} - a_{mn} - a_{pn})x_n}{3}} = 0, \end{aligned}$$

так как

$$\sum_{x_n=0}^2 e^{2\pi i \frac{ax_n}{3}} = 1 + e^{2\pi i \frac{a}{3}} + e^{2\pi i \frac{2a}{3}} = 0$$

при $a \not\equiv 0 \pmod{3}$.

Итак, $\sum_2 = 0$.

*Результаты, полученные для торов малой размерности, позволяют сделать вывод, что указанная оценка верна при $n_0 = 20$.

Разобьём $\sum_1$ на четыре части:

$$\sum_1 = \sum_3 + \sum_4 + \sum_5 + \sum_6.$$

К $\sum_3$ отнесём слагаемые, соответствующие тем точкам пространства $\mathbb{Z}_3^n$, которые образуют невырожденные параллелограммы, в оставшиеся части войдут слагаемые, определяемые точками, образующими вырожденные параллелограммы: в $\sum_4$ — параллелограммы, состоящие из одной точки, в $\sum_5$ — параллелограммы, состоящие из двух точек, в $\sum_6$ — параллелограммы, состоящие из трёх точек.

По определению множества A имеем $\sum_3 = 0$, $\sum_4 = 3^n k$, $\sum_5 = 3^n k(k-1)$.

Очевидно, что

$$\sum_6 = 6N3^n,$$

где N — количество прямых в множестве A . Найдём оценку сверху для N . Для этого заметим, что по лемме 2 в множестве A нет пересекающихся прямых и $N \leq \frac{k}{3}$. Таким образом,

$$\sum_6 \leq 2k \cdot 3^n$$

и

$$\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4 \leq 3^n(k^2 + 2k). \quad (1)$$

Представим $\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4$ в виде суммы двух слагаемых:

$$\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4 = |S_A(0)|^4 + \sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4 = k^4 + \sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4. \quad (2)$$

Подставив (2) в (1), получим, что

$$\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4 \leq 3^n(k^2 + 2k) - k^4. \quad (3)$$

Найдём оценку снизу для суммы $\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^4$. Для этого представим её в виде суммы двух слагаемых:

$$\sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^2 = |S_A(0)|^2 + \sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^2 = k^2 + \sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^2. \quad (4)$$

С другой стороны,

$$\begin{aligned} \sum_{x \in \mathbb{Z}_3^n} |S_A(x)|^2 &= \sum_{x \in \mathbb{Z}_3^n} \sum_{j,m=1}^k e^{2\pi i \frac{(a_j - a_m, x)}{3}} = \sum_{x \in \mathbb{Z}_3^n} \sum_{\substack{j,m=1 \\ j=m}}^k e^{2\pi i \frac{(a_j - a_m, x)}{3}} + \\ &+ \sum_{x \in \mathbb{Z}_3^n} \sum_{\substack{j,m=1 \\ j \neq m}}^k e^{2\pi i \frac{(a_j - a_m, x)}{3}} = 3^n k + 0 = 3^n k. \end{aligned} \quad (5)$$

Объединяя равенства (4) и (5), получаем

$$\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^2 = 3^n k - k^2. \quad (6)$$

Согласно неравенству Коши

$$\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^2 \leq \left(\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} 1 \right)^{1/2} \left(\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4 \right)^{1/2}. \quad (7)$$

Из (6), (7) следует, что

$$3^n k - k^2 \leq \sqrt{3^n - 1} \left(\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4 \right)^{1/2}. \quad (8)$$

Обе части неравенства неотрицательны, так как если бы выполнялось неравенство $3^n k - k^2 < 0$, то мы бы имели $k > 3^n$, чего быть не может. Поэтому, возведя обе части неравенства (8) в квадрат, имеем

$$(3^n k - k^2)^2 \leq (3^n - 1) \sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4,$$

откуда получаем, что

$$\sum_{\substack{x \neq 0, \\ x \in \mathbb{Z}_3^n}} |S_A(x)|^4 \geq \frac{3^{2n} k^2 - 2 \cdot 3^n k^3 + k^4}{3^n - 1}. \quad (9)$$

Объединяя неравенства (9) и (3), получаем, что

$$\frac{3^{2n} k^2 - 2 \cdot 3^n k^3 + k^4}{3^n - 1} \leq 3^n (k^2 + 2k) - k^4,$$

или

$$k^3 - 2k^2 + k - 2 \cdot 3^n + 2 \leq 0.$$

Исследуем на отрезке $[0; 3^n]$ поведение непрерывной функции

$$f(t) = t^3 - 2t^2 + t - 2 \cdot 3^n + 2.$$

На данном отрезке функция $f(t)$ обращается в ноль в одной, двух или трёх точках, так как

$$f(0) = 2(1 - 3^n) < 0, \quad f(3^n) = 3^{3n} - 2 \cdot 3^{2n} + 3^n + 2(1 - 3^n) > 0.$$

Экстремумами функции $f(t)$ на этом отрезке являются точки $t_1 = 1$, $t_2 = 1/3$, и $f(1/3) < 0$, $f(1) < 0$. Следовательно, уравнение $f(t) = 0$ имеет единственный корень на отрезке $[1; 3^n]$. Вычисляя значения функции $f(t)$ в различных точках данного отрезка, приходим к выводу, что корень уравнения $f(t) = 0$ находится на отрезке $[3^{n/3}; \sqrt[3]{3} \cdot 3^{n/3}]$, т. е. $k < \sqrt[3]{3} \cdot 3^{n/3}$.

Итак, получена оценка сверху для мощности множества A , являющегося подмножеством n -мерного пространства над полем $\mathbb{Z}_3$. Отметим, что множество A таково, что если $a_1, a_2, a_3, a_4 \in A$ и a_1, a_2, a_3, a_4 попарно различны, то

$$a_1 + a_2 - a_3 - a_4 \not\equiv 0 \pmod{3}.$$

Теперь найдём оценку снизу для мощности разностного множества A , $A \subset \mathbb{Z}_3^n$.

Пусть разностное множество A мощности k экстремально. Тогда оно неполняемо, т. е. в него нельзя добавить ни одной новой точки из пространства $\mathbb{Z}_3^n$ так, чтобы в множестве A не появился невырожденный параллелограмм.

Выясним, когда мы сможем пополнить разностное множество A . Множество A будет пополняемым, если в пространстве $\mathbb{Z}_3^n$ найдётся такая точка x , что для любых $a_1, a_2, a_3 \in A$, где a_1, a_2, a_3 различны, $a_1 - a_2 \not\equiv a_3 - x \pmod{3}$, или $x \not\equiv a_3 + (a_2 - a_1) \pmod{3}$. Количество различных (без учёта противоположных) направлений в множестве A мощности k равно $k(k-1)/2$, следовательно, количество точек, которыми нельзя дополнить множество A , равно $k^2(k-1)/2$. Значит, множество A можно пополнить, если $k^2(k-1)/2 < 3^n$. Но мы в качестве множества A взяли экстремальное разностное множество, следовательно, его нельзя пополнить. Итак, $k^2(k-1)/2 \geq 3^n$. Найдём, при каких k выполняется данное неравенство.

Как было доказано выше, $k < \sqrt[3]{3} \cdot 3^{n/3}$. Рассмотрим поведение непрерывной функции

$$f(t) = t^3 - t^2 - 2 \cdot 3^n$$

на отрезке $[0; \sqrt[3]{3} \cdot 3^{n/3}]$. На данном отрезке функция $f(t)$ обращается в ноль в одной, двух или трёх точках, так как

$$f(0) < 0, \quad f(\sqrt[3]{3} \cdot 3^{n/3}) > 0$$

при $n > 2$. Экстремумами функции $f(t)$ на этом отрезке являются точки $t_1 = 0$, $t_2 = 2/3$, и $f(2/3) < 0$, $f(0) < 0$. Значит, уравнение $f(t) = 0$ имеет единственный корень на отрезке $[1; \sqrt[3]{3} \cdot 3^{n/3}]$. Находя значения функции $f(t)$ в различных точках этого отрезка, заключаем, что корень уравнения $f(t) = 0$ принадлежит отрезку $[\sqrt[3]{2} \cdot 3^{n/3}; \sqrt[3]{3} \cdot 3^{n/3}]$, т. е. $k > \sqrt[3]{2} \cdot 3^{n/3}$.

Нами получена оценка снизу для мощности множества A , $A \subset \mathbb{Z}_3^n$. Отметим, что множество A таково, что если $a_1, a_2, a_3, a_4 \in A$ и a_1, a_2, a_3, a_4 попарно

различны, то

$$a_1 + a_2 - a_3 - a_4 \not\equiv 0 \pmod{3}.$$

□

Литература

- [1] Артин Э. Геометрическая алгебра. — М.: Наука, 1969.
- [2] Babai L., Sós V. Sidon sets in groups and induced subgraphs of Cayley graphs // Eur. J. Combin. — 1985. — Vol. 6. — P. 101—114.
- [3] Chaimovich M. Subset sum problem with different summands: Computations // Discrete Appl. Math. — 1990. — Vol. 27. — P. 277—282.
- [4] Folkman J. On the representation of integers as sums of distinct terms from a fixed sequence // Can. J. Math. — 1966. — Vol. 18. — P. 643—655.
- [5] Freiman G. A. Subset-sum problem with different summands // Congr. Numer. — 1990. — Vol. 70. — P. 207—215.
- [6] Hamidoune Y. O. Subsets with small sums in Abelian groups. I // Eur. J. Combin. — 1997. — Vol. 18, no. 5. — P. 541—556.