

SQUARES IN SUMSETS

HOI H. NGUYEN AND VAN H. VU

ABSTRACT. A finite set A of integers is square-sum-free if there is no subset of A sums up to a square. In 1986, Erdős posed the problem of determining the largest cardinality of a square-sum-free subset of $\{1, \dots, n\}$. Answering this question, we show that this maximum cardinality is of order $n^{1/3+o(1)}$.

1. INTRODUCTION

Let A be a set of numbers. We denote by S_A the collection of finite partial sums of A ,

$$S_A := \left\{ \sum_{x \in B} x; B \subset A, 0 < |B| < \infty \right\}.$$

For a positive integer $l \leq |A|$ we denote by l^*A the collection of partial sums of l elements of A ,

$$l^*A := \left\{ \sum_{x \in B} x; B \subset A, |B| = l \right\}.$$

Let $[x]$ denote the set of positive integers at most x . In 1986, Erdős [5] raised the following question:

Question 1.1. *What is the maximal cardinality of a subset A of $[n]$ such that S_A contains no square?*

We denote by $SF(n)$ the maximal cardinality in question. Erdős observed that

$$SF(n) = \Omega(n^{1/3}). \tag{1}$$

To see this, consider the following example

The authors are partially supported by an NSF Career Grant.

Example 1.2. Let p be a prime and k be the largest integer such that $kp \leq n$. We choose p of order $n^{2/3}$ such that $k = \Omega(n^{1/3})$ and $1 + \dots + k < p$. Then the set $A := \{p, 2p, \dots, kp\}$ is square-sum-free.

Remark 1.3. The fact that p is a prime is not essential. The construction still works if we choose p to be a square-free number, namely, a number of the form $p = p_1 \dots p_l$ where p_i are different primes.

Erdős [5] conjectured that $SF(n)$ is close to the lower bound in (1). Shortly after Erdős' paper, Alon [1] proved the first non-trivial upper bound

$$SF(n) = O\left(\frac{n}{\log n}\right). \quad (2)$$

Next, Lipkin [9] improved to

$$SF(n) \leq n^{3/4+o(1)}. \quad (3)$$

In [2], Alon and Freiman improved the bound further to

$$SF(n) \leq n^{2/3+o(1)}. \quad (4)$$

The latest development was due to Sárközy [11], who showed

$$SF(n) = O(\sqrt{n \log n}). \quad (5)$$

In this paper, we obtain the asymptotically tight bound

$$SF(n) \leq n^{1/3+o(1)}. \quad (6)$$

Theorem 1.4. *There is a constant C such that for all $n \geq 2$*

$$SF(n) \leq n^{1/3}(\log n)^C \quad (7)$$

In fact, we are going to prove the following (seemingly) more general theorem

Theorem 1.5. *There is a constant C such that the following holds for all sufficiently large n . Let d be positive integer less than $n^{2/3}(\log n)^{-C}$ and A be a subset of cardinality $n^{1/3}(\log n)^C$ of $[n/d]$. Then there exists an integer z such that $dz^2 \in S_A$.*

Theorem 1.4 is the special case when $d = 1$. Furthermore, Theorem 1.4 implies many special cases of Theorem 1.5. To see this, choose A to have the form $A := \{db \mid b \in B\}$ where B is a subset of $[n/d]$ and d is a square-free-number. Then finding a square in S_A is the same as finding a number of the form dz^2 in S_B .

If one replaces squares by higher powers, then the problem becomes easier and asymptotic bounds have been obtained earlier (see next section).

Notations. We use Landau asymptotic notation such as O, Ω, Θ, o throughout the paper, under the assumption that $n \rightarrow \infty$. Notation such as $\Theta_c(\cdot)$ means that the hidden constant in Θ depends on a (previously defined) quantity c . We will also omit all unnecessary floors and ceilings. All logarithms have natural base. As usual, $e(x)$ means $\exp(2\pi ix) = \cos 2\pi x + i \sin 2\pi x$.

2. THE MAIN IDEAS

The general strategy for attacking Question 1.1 is as follows. One first tries to show that if $|A|$ is sufficiently large, then S_A should contain a large additive structure. Next, one would argue that a large additive structure should contain a square.

In previous works [1, 2, 9, 11], the additive structure was a (homogeneous) arithmetic progression. (An arithmetic progression is homogeneous if it is of the form $\{ld, (l+1)d, \dots, (l+k)d\}$.) It is easy to show that if P is a homogeneous AP of length $C_0 m^{2/3}$ in $[m]$, for some large constant C_0 , then P contains a square. Notice that the set S_A is a subset of $[m]$ where $m := |A|n$. Thus, if one can show that S_A contains a homogeneous AP of length $C_0 m^{2/3}$, then we are done. Sárközy could prove that this is indeed the case, given $|A| \geq C_1 \sqrt{n} \log n$ for a properly chosen constant C_1 . This also solves (asymptotically) the problem when squares are replaced by higher powers, since in these cases, the lower bound (which can be obtained by modifying Example 1.2) is $\Omega(\sqrt{n})$.

Unfortunately, \sqrt{n} is the limit of this argument, since there are examples of a subset A of $[n]$ of size $\Omega(\sqrt{n})$ where the longest AP in S_A is much shorter than $(|A|n)^{2/3}$. In order to present such an example, we will need the following definition (which will play a crucial role in the rest of the paper)

Definition 2.1 (Generalized arithmetic progression-GAP). A generalized arithmetic progression of rank r is a set of the form

$$Q = \{a_0 + x_1 a_1 + \dots + x_r a_r \mid 0 \leq x_i \leq L_i\}.$$

If all the sums $x_1 a_1 + \dots + x_r a_r$ are distinct, we say that Q is *proper*. If $a_0 = 0$, we say that Q is *homogeneous*. (Homogeneous arithmetic progression thus corresponds to the case $r = 1$.) We call L_1, \dots, L_r the sizes of Q and a_1, \dots, a_r its steps.

Example 2.2. Consider

$$A := \{q_1x_1 + q_2x_2 \mid 1 \leq x_i \leq N\}$$

where $q_1 \approx q_2 \approx n^{3/4}$ are different primes and $N = \frac{1}{100}n^{1/4}$. It is easy to show that A is a proper GAP of rank 2 and S_A is contained in the proper GAP

$$\{q_1x_1 + q_2x_2 \mid 1 \leq x_i \leq 1 + \dots + N\}.$$

Thus, the longest AP in S_A has length at most $1 + \dots + N = \Theta(n^{1/2})$, while A has cardinality $\Theta(n^{1/2})$.

The key fact that enables us to go below \sqrt{n} and reach the optimal bound $n^{1/3}$ is a recent theorem of Szemerédi and Vu [12] that showed that if $|A| \geq Cn^{1/3}$ for some sufficiently large constant C , then S_A does contain a large proper GAP of rank at most 2.

Lemma 2.3. [12] *There are positive constants C and c such that the following holds. If A is a subset of $[n]$ of cardinality at least $Cn^{1/3}$, then S_A contains either an AP Q of length $c|A|^2$ or a proper GAP Q of rank 2 and cardinality at least $c|A|^3$.*

Ideally, the next step would be showing that a large proper GAP Q (which is a subset of $[|A|n]$) contains a square. Thanks to strong tools from number theory, this is not too hard (though not entirely trivial) if Q is homogeneous. However, we do not know how to force this assumption.

The assumption of homogeneity is essential, as without this, one can easily run into local obstructions. For example, if Q is a GAP of the form

$$\{a_0 + a_1x_1 + a_2x_2 \mid 0 \leq x_i \leq L\}$$

where both a_1 and a_2 are divisible by 6, but $a_0 \equiv 2 \pmod{6}$, then clearly Q cannot contain a square, as 2 is not a square modulo 6.

In order to overcome this obstacle, we need to add several twists to the plan. First, we are going to use only a small subset A' of A to create a large GAP Q . Assume that Q has the form

$$\{a_0 + a_1x_1 + a_2x_2 \mid 0 \leq x_i \leq L\}.$$

(Q can also have rank one but that is the simpler case.) Let q be the g.c.d of a_1 and a_2 . If a_0 is a square modulo q , then there is no local obstruction and in principle we can treat Q as if it was homogeneous.

In the next move, we try to add the remaining elements of A (from $A'' := A \setminus A'$) to a_0 to make it a square modulo q . This, however, faces another local obstruction. For instance, if in the above example, all elements of A'' are divisible by 6, then a_0 will always be $2 \pmod{6}$ no matter how we add elements from A'' to it.

Now comes a key point. A careful analysis reveals that having all elements of A'' divisible by the same integer (larger than one, of course) is the *only* obstruction. Thus, we obtain a useful dichotomy: either S_A contains a square or there is an integer $d > 1$ which divides all elements of a large subset A'' of A .

Now we keep working with A'' . We can write this set as $\{db \mid b \in B\}$ where B is a subset of $[n/d]$. In order to show that $S_{A''}$ contains a square, it suffices to show that S_B contains a number of the form dz^2 . This explains the necessity of Theorem 1.5.

A nice feature of the above plan is that it also works for the more general problem considered in Theorem 1.5. We are going to iterate, setting new $A := A''$ of the previous step. Since the number of iterations (i.e., the number of p 's) is only $O(\log n)$, if we have $|A''| \geq (1 - \frac{1}{(\log n)^c})|A|$ in each step, for a sufficiently large constant c , then the set A'' will never be empty and this guarantees that the process should terminate at some point, yielding the desired result.

In the next lemma, which is the main lemma of the paper, we put these arguments into a quantitative form.

Lemma 2.4. *The followings holds for any sufficiently large constant C . Let p be positive integer less than $n^{2/3}(\log n)^{-C}$ and A be a subset of $[n/p]$ of cardinality $n^{1/3}(\log n)^C$. Then there exists $A' \subset A$ of cardinality $|A'| \leq n^{1/3}(\log n)^{C/3}$ such that one of the followings holds (with $A'' := A \setminus A'$)*

- $S_{A'}$ contains a GAP

$$Q = \{r + qx \mid 0 \leq x \leq L\}$$

where $L \geq n^{2/3}(\log n)^{C/4}$ and $q \leq \frac{n^{2/3}(\log n)^{C/12}}{p}$ and $r \equiv pz^2 \pmod{q}$ for some integer z .

- $S_{A'}$ contains a proper GAP

$$Q = \{r + q(q_1x_1 + q_2x_2) \mid 0 \leq x_1 \leq L_1, 0 \leq x_2 \leq L_2, (q_1, q_2) = 1\}$$

such that $\min(L_1, L_2) \geq n^{1/3}(\log n)^{C/4}$, $L_1L_2 \geq n(\log n)^{C/2}$, $q \leq \frac{n^{1/3}}{(\log n)^{C/6p}}$ and $r \equiv pz^2 \pmod{q}$ for some integer z .

- There exists an integer $d > 1$ such that $d \mid a$ for all $a \in A''$.

Given this lemma, we can argue as before and show that after some iterations, one of the first two cases must occur. We show that in these cases the GAP Q should contain a number of the form pz^2 , using classical tools from number theory (see Section 9 and Section 10).

The proof of Lemma 2.4 is technical and requires a preparation involving tools from both combinatorics and number theory. These tools will be the focus of the next two sections.

3. TOOLS FROM ADDITIVE COMBINATORICS

This section contains tools from additive combinatorics, which will be useful in the proof of Lemmas 3.7 and 2.4. Let X, Y be two sets of numbers. We define

$$X + Y := \{x + y \mid x \in X, y \in Y\}; X - Y := \{x - y \mid x \in X, y \in Y\}.$$

A translate of a set X is a set X' of the form $X' := \{a + x \mid x \in X\}$. For instance, every GAP is a translate of a homogeneous GAP.

The first tool is the so-called Covering lemma, due to Ruzsa (see [10] or [14, Lemma 2.14]).

Lemma 3.1 (Covering Lemma). *Assume that X, Y are finite sets of integers. Then X is covered by at most $|X + Y|/|Y|$ translates of $Y - Y$.*

The second tool is the powerful inverse theorem of Freiman [6], [14, Chapter 5]

Lemma 3.2 (Freiman's inverse theorem). *Let γ be a given positive number. Let X be a set in \mathbf{Z} such that $|X + X| \leq \gamma|X|$. Then there exists a proper GAP P of rank at most $d = d(\gamma)$ and cardinality $O_\gamma(|X|)$ that contains X .*

Assume that Q is a GAP, $Q = \{a_0 + x_1a_1 + \dots + x_ra_r : 0 \leq x_i \leq L_i, 1 \leq i \leq r\}$. For any $t > 0$, denote by tQ the set

$$\{ta_0 + x_1a_1 + \dots + x_ra_r : 0 \leq x_i \leq tL_i, 1 \leq i \leq r\}.$$

We say that Q is t -proper if tQ is proper. In general, a GAP is not necessarily t -proper. However, one can embed it into a t -proper one with some small loss (see [3, 4], [14, Theorem 3.40]).

Lemma 3.3 (Embedding into proper GAP). *Let Q be a GAP of rank r in a torsion-free group G , and let $t \geq 1$. Then there exists a t -proper GAP Q' with rank at most r and $|Q'| \leq (2t)^r r^{6r^2} |Q|$. Furthermore, if Q is not proper, we may choose Q' to have rank at most $r - 1$.*

Next, assume that A is a dense subset of a GAP Q , then the iterated sumsets kA contains a structure similar to Q (see [12, Lemma 4.4], [13, Lemma B3]).

Lemma 3.4 (Sárközy-type theorem in progressions). *Let Q be a proper GAP in a torsion-free group of rank r . Let $X \subset Q$ be a subset such that $|X| \geq \delta|Q|$ for some $0 < \delta < 1$. Then there exists a positive integer $1 \leq m \ll_{\delta, r} 1$ such that mX*

contains a GAP Q' of rank r and size $\Theta_{\delta,r}(|Q|)$. Furthermore, the generators of Q' are bounded multiples of the generators of Q . If Q and X are symmetric, then Q' can be chosen to be symmetric.

A more general result holds when we replace one set by many sets from the same GAP (see [12, Lemma 5.5]).

Lemma 3.5 (Sárközy-type theorem in progressions, generalized form). *Let Q be a proper GAP in a torsion-free group of rank r . Let $0 < \delta \leq 1$ be a given constant. Then there exists a positive integer $1 \leq m \ll_{\delta,r} 1$ such that the following holds. If $X_1, \dots, X_m \subset Q$ and $|X_i| \geq \delta|Q|$, then $X_1 + \dots + X_m$ contains a GAP Q' of rank r and size $\Theta_{\delta,r}(|Q|)$. Furthermore, the generators of Q' are bounded multiples of the generators of Q .*

We say that a GAP $Q = \{a_0 + x_1a_1 + \dots + x_da_d \mid 0 \leq x_i \leq L_i\}$ is *positive* if its steps a_i 's are positive. A useful observation is that if the elements of Q are positive, then Q itself can be brought into a positive form.

Lemma 3.6. *A GAP with positive elements can be brought into a positive form.*

Proof (Proof of Lemma 3.6.) Assume that

$$Q = \{a_0 + x_1a_1 + \dots + x_da_d \mid 0 \leq x_i \leq L_i\}.$$

By setting $x_i = 0$, we can conclude that $a_0 > 0$. Without loss of generality, assume that $a_1, \dots, a_j < 0$ and $a_{j+1}, \dots, a_d > 0$. By setting $x_i = 0$ for all $i > j$ and $x_i = L_i, i \leq j$, we have

$$a'_0 := a_0 + a_1L_1 + \dots + a_jL_j > 0.$$

Now we can rewrite Q as

$$Q := \{a'_0 + x_1(-a_1) + \dots + x_j(-a_j) + x_{j+1}a_{j+1} + \dots + x_da_d \mid 0 \leq x_i \leq L_i\},$$

completing the proof. ■

Since we only deal with positive integers, this lemma allows us to assume that all GAPs arising in the proof are in positive form.

Using the above tools and ideas from [12], we will prove Lemma 3.7 below, which asserts that if a set A of $[n/d]$ is sufficiently dense, then there exists a small set $A' \subset A$ whose subset sums contain a large GAP Q of small rank. Furthermore, the set $A'' = A \setminus A'$ is contained in only a few translates of Q . This lemma will serve

as a base from which we will attack Lemma 2.4, using number theoretical tools discussed in the next section.

Lemma 3.7. *The following holds for all sufficiently large constants C . Let p be positive integer less than $n^{2/3}(\log n)^{-C}$ and A be a subset of $[n/p]$ of cardinality $n^{1/3}(\log n)^C$. Then there exists a subset A' of A of cardinality $|A'| \leq n^{1/3}(\log n)^{C/3}$ such that one of the followings holds (with $A'' := A \setminus A'$):*

- $S_{A'}$ contains an AP

$$Q = \{r + qx \mid 0 \leq x \leq L\}$$

where $L \geq n^{2/3}(\log n)^{C/2}$ and there exist $m = O(1)$ different numbers s_1, \dots, s_m such that $A'' \subset \{s_1, \dots, s_m\} + Q$.

- $S_{A'}$ contains a proper GAP

$$Q = \{r + a_1x_1 + a_2x_2 \mid 0 \leq x_1 \leq L_1, 0 \leq x_2 \leq L_2\}$$

such that $L_1L_2 \geq n(\log n)^{C/2}$ and there exist $m = O(1)$ numbers s_1, \dots, s_m such that $A'' \subset \{s_1, \dots, s_m\} + Q$.

Remark. The proof actually gives a better lower bounds for L_1L_2 in the second case ($2C/3$ instead of $C/2$), but this is not important in applications.

4. TOOLS FROM NUMBER THEORY

Fourier Transform and Poisson summation. Let f be a function with support on \mathbf{Z} . The Fourier transform \widehat{f} is defined as

$$\widehat{f}(w) := \int_{\mathbf{R}} f(t)e(-wt) dt.$$

The classical Poisson summation formula asserts that

$$\sum_{n=-\infty}^{\infty} f(t + nT) = \frac{1}{T} \sum_{m=-\infty}^{\infty} \widehat{f}\left(\frac{2\pi m}{T}\right)e(mt/T). \quad (8)$$

For more details, we refer to [8, Section 4.3].

Smooth indicator functions. We will use the following well-known construction (see for instance [7, Theorem 18] for details).

Lemma 4.1. *Let $\delta < 1/16$ be a positive constant and let $[M, M+N]$ be an interval. Then there exists a real function f satisfying the following*

- $0 \leq f(x) \leq 1$ for any $x \in \mathbf{R}$.
- $f(x) = 0$ if $x \leq M$ or $x \geq M + N$.

- $f(x) = 1$ if $M + \delta N \leq x \leq M + N(1 - \delta)$.
- $|\widehat{f}(\lambda)| \leq 16\widehat{f}(0) \exp(-\delta|\lambda N|^{1/2})$ for every λ .

A *Weyl type estimate*. Next, we need a Weyl type estimate for exponential sums.

Lemma 4.2. *For any positive constant ε there exist positive constants $\alpha = \alpha(\varepsilon)$ and $c(\varepsilon)$ such that the following holds. Let a, q be co-prime integers, θ be a real number, and I be an interval of length N . Let M be a positive number such that $MN \geq q^{1+\varepsilon}$. Then,*

$$\sum_{\substack{|m| \leq M \\ m \neq 0}} \left| \sum_{z \in I} e\left(\frac{amz^2}{q} + \theta mz\right) \right| \leq c(M\sqrt{N} + \frac{MN}{\sqrt{q}})(\log MN)^\alpha.$$

Quadratic residues. Finally, and most relevant to our problem, we need the following lemma, which shows the existence of integer solutions with given constrains for a quadratic equation.

Lemma 4.3. *There is an absolute constants D such that the following holds. Let a_1, \dots, a_d, r, p, q be integers such that $p, q > 0$ and $(a_1, \dots, a_d, q) = 1$. Then the equation*

$$a_1x_1 + \dots + a_dx_d + r \equiv pz^2 \pmod{q} \tag{9}$$

has an integer solution (z, x_1, \dots, x_d) satisfying $0 \leq x_i \leq (pq)^{1/2}(\log q)^D$.

The rest of the paper is organized as follows. The proof of the combinatorial statement, Lemma 3.7, comes first in Section 5. We then start the number theoretical part by giving a proof for Lemma 4.2. The verification of Lemma 4.3 comes in Section 7. After all these preparations, we will be able to establish Lemma 2.4 in Section 8. The proof of the main result, Theorem 1.5, is presented in Sections 9 and 10.

5. PROOF OF LEMMA 3.7

We repeat some arguments from [12] with certain modifications. The extra information we want to get here (compared with what have already been done [12]) is the fact that the set A'' is covered by only few translates of Q .

5.1. An algorithm. Let A' be a subset of cardinality $|A'| = n^{1/3}(\log n)^{C/3}$ and let $A'' := A \setminus A'$. By a simple combinatorial argument (see [12, Lemma 7.9]), we can find in A' disjoint subsets A'_1, \dots, A'_{m_1} such that $|A'_i| \leq 20 \log_2 |A'|$ and $|l_1^* A'_i| \geq |A'|/2$ where

$$l_1 \leq 10 \log_2 |A'| \text{ and } m_1 = |A'| / (40 \log_2 |A'|). \quad (10)$$

(For the definition of l^*A see the beginning of the introduction.)

Without loss of generality, we can assume that m_1 is a power of 4. Let B_1, \dots, B_{m_1} be subsets of cardinality $b_1 = |A'|/2$ of the sets $l_1^*A'_1, \dots, l_1^*A'_{m_1}$ respectively. Following [12, Lemma 7.6]), we will run an algorithm with the B_i 's as input. The goal of this algorithm is to produce a GAP which has nice relations with A'' (while still not as good as the GAP we wanted in the lemma). In the next few paragraphs, we are going to describe this algorithm.

At the first step, set $B_1^1 := B_1, \dots, B_{m_1}^1 := B_{m_1}$ and let $\mathfrak{B}^1 = \{B_1^1, \dots, B_{m_1}^1\}$. Let h be a large constant to be determined later.

At the $(t+1)$ -th step, we choose indices i, j and elements $a_1, \dots, a_h \in A''$ that maximizes the cardinality of $\cup_{d=1}^h (B_i^t + B_j^t + a_d)$ (if there are many choices, choose one arbitrarily). Define $B_1^{t+1'}$ to be the union. Delete from A'' the used elements a_1, \dots, a_h , and remove from \mathfrak{B}^t the used sets B_i^t, B_j^t . Find the next maximum union $\cup_{k=1}^h B_i^t + B_j^t + a_k$ with respect to the updated sets \mathfrak{B}^t and A'' .

Assume that we have created $m_{t+1} := m_t/4$ sets $B_1^{t+1'}, \dots, B_{m_{t+1}}^{t+1}'$. By the algorithm, we have

$$|B_1^{t+1'}| \geq \dots \geq |B_{m_{t+1}}^{t+1}'| := b_{t+1}.$$

Now for each $1 \leq i \leq m_{t+1}$ we choose a subset B_i^{t+1} of cardinality exactly b_{t+1} in $B_i^{t+1'}$. These m_{t+1} sets (of the same cardinality) form a collection \mathfrak{B}^{t+1} , which is the output of the $(t+1)$ -th step.

Since $m_{t+1} = m_t/4$, there are still $m_t/2$ unused sets B_i^t left in \mathfrak{B}^t . Without loss of generality, assume that those are $B_1^t, \dots, B_{m_t/2}^t$. With a slight abuse of notation, we use A'' at every step, although this set loses a few elements each time. (The number of deleted elements is very small compared to the size of A'' .)

Let $l_{t+1} := 2l_t + 1$. Observe that

- $l_t \leq 2^t l_1$ (by definition);
- $b_t \leq l_t n/p$ (since $\cup_{d=1}^h (B_i^{t-1} + B_j^{t-1} + a_d) \subset [l_t n/p]$);
-

$$|\cup_{d=1}^h B_i^t + B_j^t + a_d| \leq b_{t+1} \quad (11)$$

for all $1 \leq i < j \leq m_t/2$ and $a_1, \dots, a_h \in A''$ (by the algorithm, as it always chooses a union with maximum size).

Now let c be a large constant and k be the largest index such that $b_i \geq cb_{i-1}$ for all $i \leq k$. Then we have

$$c^k b_1 \leq b_k \leq l_k n / p.$$

Since $b_1 = |A'|/2$ and $l_k \leq 2^k l_1$, we deduce an upper bound for k ,

$$k \leq \log_{c/2} \frac{l_1 n}{b_1 p}.$$

Next, by the definition of k , we have $b_{k+1} \leq cb_k$. By (11), the following holds for all unused sets B_i^k, B_j^k (with $1 \leq i \leq j \leq m_k/2$) and for all $a_1, \dots, a_h \in A''$:

$$|\cup_{d=1}^h (B_i^k + B_j^k + a_d)| \leq b_{k+1} \leq cb_k = c|B_i^k|.$$

In particular

$$|B_1^k + B_i^k| \leq c|B_1^k|$$

holds for all $2 \leq i \leq m_k/2$.

By Plunnecke-Ruzsa estimate (see [14, Corollary 6.28]), we have

$$|B_1^k + B_1^k| \leq c^2 |B_1^k|.$$

It then follows from Freiman's theorem, Theorem 3.2, that there exists a proper GAP R of rank $O_c(1)$, of size $O_c(1)|B_1^k|$ such that R contains B_1^k . Furthermore, by Lemma 3.1, B_i^k is contained in c translates of $B_1^k - B_1^k$, thus B_i^k is also contained in $O_c(1)$ translates of R .

Before continuing, we would like to point out that the parameter h has not yet played any role in the arguments. The freedom of choosing h will be important in what follows. We are going to obtain the desired GAP Q (claimed in the lemma) from R by a few additional operations.

5.2. Creation of many similar GAPs. One problem with R is that its cardinality can be significantly smaller than the bounds on Q in Lemma 3.7. We want to obtain larger GAPs by adding many translates of R . While we cannot do exactly this, we can do nearly as good by the following argument, which creates many GAPs which are translates of each other and have cardinalities comparable to that of R .

By the pigeon hole principle, for $i \leq m_k/2$, we can find a set $B'_i \subset B_i^k$ with cardinality $\Theta_c(1)b_k$ which is contained in one translate of R .

By Lemma 3.5, there exists $g = O_c(1)$ such that $B'_1 + \cdots + B'_g$ contains a proper GAP Q_1 of cardinality $\Theta_c(1)|R|$. Create Q_2 by summing B'_{g+1}, \dots, B'_{2g} , and so on. At the end we obtain $\frac{m_k}{2g} = \Theta_c(1)m_k$ such GAPs. We can require the Q_i 's to have the properties below

- $\text{rank}(Q_i) = \text{rank}(R) = O_c(1)$;
- $|Q_i| = \Theta_c(1)|R| = \Theta_c(1)b_k$;
- each Q_i is a subset of a translate of gR . Thus by Lemma 3.1, R is contained in $O_c(1)$ translates of $Q_i - Q_i$;
- the j -th size of Q_i is different from j -th size of R by a (multiplicative) factor of order $\Theta_c(1)$, for all j ;
- the j -th step of Q_i is a multiple of the j -th step of R for all j ;

Thus, by the pigeon hole principle and truncation (if necessary) we can obtain $m' = \Theta_c(m_k)$ GAPs, say, $Q_1, \dots, Q_{m'}$, which are translates of each other. An important remark here is that since the Q_i are obtained from summing different B 's, the sum $Q_1 + \cdots + Q_{m'}$ is a subset of $S_{A'}$. The desired GAP Q will be a subset of this sum.

5.3. Embedding A'' . In this step, we embed A'' in a union of few translates of a GAP Q_1 of constant rank.

We set the (so far untouched) parameter h to be sufficiently large so that

$$\Theta_c(1) = h > c|B_1^k|/|B'_1|.$$

Let d be the largest number such that there are d elements a_1, \dots, a_d of A'' for which the sets $B'_1 + B'_2 + a_i$ are disjoint. Assume for the moment that $d \geq h$, then we would have

$$|\cup_{i=1}^h (B'_1 + B'_2 + a_i)| = h|B'_1 + B'_2| \geq h|B'_1| > c|B_1^k|$$

However, this is impossible because $\cup_{i=1}^h (B'_1 + B'_2 + a_i) \subset \cup_{i=1}^h (B_1^k + B_2^k + a_i)$ and the latter has cardinality less than $c|B_1^k|$ by definition. Thus we have $d < h$. So $d = O_c(1)$.

Let us fix d elements a_1, \dots, a_d from A'' which attained the disjointness in the definition of d . By the maximality of d , for any $a \in A''$ there exists a_i so that $(B'_1 + B'_2 + a) \cap (B'_1 + B'_2 + a_i) \neq \emptyset$. Hence

$$a - a_i \in B_1^k + B_2^k - (B_1^k + B_2^k) = (B_1^k - B_1^k) + (B_2^k - B_2^k) \subset 2R - 2R.$$

Thus A'' is covered by at most $d = O_c(1)$ translates of $2R - 2R$. On the other hand, since R is contained in $O_c(1)$ translates of $Q_1 - Q_1$, $2R - 2R$ is contained in $O_c(1)$ translates of $4Q_1 - 4Q_1$. It follows that that A'' is covered by $O_c(1)$ translates of Q_1 .

The remaining problem here is that Q_1 does not yet have the required rank and cardinality. We will obtain these by adding the Q_i together (recall that these GAPs are translates of each other) and using a rank reduction argument, following [12] (see also [14, Chapter12]).

5.4. Rank reduction. Let P be the homogenous translate of Q_1 (and also of $Q_2, \dots, Q_{m'}$). Recall that

$$|P| = |Q_1| = \Theta_c(b_k) = \Omega_c(c^k b_1).$$

and also

$$m' = \Theta_c(m_k) = \Theta_c\left(\frac{b_1}{4^k}\right), \text{ and } l_{k+1} \leq 2^{k+1}l_1.$$

Set $l := \min\{m', |A'|/2l_{k+1}\}$. Recall that $|A'| = n^{1/3}(\log n)^{C/2}$, $l_1 \leq 10 \log_2 |A'|$ and $b_1 = |A'|/2$. By choosing c and C sufficiently large, we can guarantee that

$$l|P| \geq n^{2/3}(\log n)^{C/2} ; l^2|P| \geq n(\log n)^{2C/3}. \quad (12)$$

and also

$$l^3|P| \geq n^{4/3}(\log n)^C \quad (13)$$

Now we invoke Lemma 3.3 to find a large GAP in lP . Assume, without loss of generality, that $l = 2^s$ for some integer s . We start with $P_0 := P$ and $\ell_0 := l$. If $2^s P_0$ is proper, then we stop. If not, then there exists a smallest index i_1 such that $2^{i_1} P_0$ is proper but $2^{i_1+1} P_0$ is not.

By Lemma 3.3 (applying to $2^{i_1} P_0$) we can find a GAP S which contains $2^{i_1} P_0$ such that $\text{rank}(S) < r := \text{rank}(2^{i_1} P_0)$.

By Lemma 3.4, there is a constant $g = \Theta_c(1)$ such that the set $2^g(2^{i_1} P_0)$ contains a proper GAP P_1 of rank equals $\text{rank}(S)$ and cardinality $\Theta_c(1)|2^{i_1} P_0|$. Set $\ell_1 := \ell_0/2^{i_1+g}$ if $\ell_0/2^{i_1+g} \geq 1$ and proceed with P_1, ℓ_1 and so on. Otherwise we stop.

Observe that if $2^{i_j}P_j$ is proper, then $|2^{i_j}P_j| = (1 + o(1))2^{i_j r_j} |P_j|$, where r_j is the rank of P_j .

As the rank of P_0 is $O_c(1)$, and $r_{j+1} \leq r_j - 1$, we must stop after $\Theta_c(1)$ steps. Let Q' be the proper GAP Q' obtained when we stop. It has rank d' , for some integer $d' < r$ and cardinality at least $\Theta_c(1)l_0^{d'}|P_0| = \Theta_c(1)l^{d'}|P|$. On the other hand, since a translate of lP is contained in $S_{A'}$, $|Q'| \leq |A'|n/p \leq |A'|n$, that is $\Theta_c(1)l^{d'}|P| \leq |A'|n$. Because of (13), this holds only if $d' \leq 2$.

5.5. Properties of Q . By the Covering Lemma 3.1 and by the definition of P_j 's, P_i is contained in $O_c(1)$ translates of P_{i+1} for all $i \geq 0$. At the starting point, we know that A'' is contained in $O_c(1)$ translates of P_0 . Since there are only $O_c(1)$ different P_j 's, at the last step we conclude that A'' is covered by $O_c(1)$ translates of Q' .

Furthermore, Q' is a subset of lP . Thus a translate Q of Q' lies in $Q_1 + \dots + Q_{m'} \subset S_{A'}$. This Q has rank $1 \leq d' \leq 2$ and cardinality $|Q| = |Q'| \geq \Theta(1)l^{d'}|A'|$. (The right hand side satisfies the lower bounds claimed in Lemma 3.7, thanks to (12).) This is the GAP claimed in Lemma 3.7 and our proof is complete.

6. PROOF OF LEMMA 4.2

If q is a prime, the lemma is a corollary of the well known Weyl's estimate (see [8]). We need to add a few arguments to handle the general case. The following lemma will be useful.

Lemma 6.1. *Let $\tau(n)$ be the number of positive divisors of n . For any given $k \geq 3$ there exists a positive constant $\beta(k)$ such that the following holds for every n .*

$$\tau(n) = O_k\left(\sum_{\substack{d|n \\ d \leq n^{1/k}}} \tau(d)^{\beta(k)}\right).$$

Proof (Proof of Lemma 6.1). We can set $\beta(k) = k \log(k+1)$. We factorize n in the following specific way

$$n = \prod_{i=1}^u p_i^{a_i} \prod_{j=1}^v q_j^{b_j}$$

where $p_1 \leq \dots \leq p_u$, $q_1 \leq \dots \leq q_v$ are primes and $a_i \geq k > b_j \geq 1$. Set

$$d := \prod_{i=1}^u p_i^{\lfloor \frac{a_i}{k} \rfloor} \prod_{j \leq \lfloor \frac{v}{k} \rfloor} q_j.$$

Then $d \leq n^{1/k}$ by definition and

$$(k+1)^k \tau(d)^{\beta(k)} = (k+1)^k 2^{\lfloor \frac{v}{k} \rfloor k \log(k+1)} \prod_{i=1}^u (\lfloor \frac{a_i}{k} \rfloor + 1)^{k \log(k+1)} \geq (k+1)^v \prod_{i=1}^u (1+a_i) \geq \tau(n),$$

completing the proof. \blacksquare

Now we start the proof of Lemma 4.2. Let $S := \sum_{\substack{|m| \leq M \\ m \neq 0}} |\sum_{z \in I} e(\frac{amz^2}{q} + \theta mz)|$. Following Weyl's argument, we use Cauchy-Schwarz and the triangle inequality to obtain

$$S^2 \leq 2M \sum_{\substack{|m| \leq M \\ m \neq 0}} \sum_{z_1, z_2 \in I} e(\frac{am(z_1 - z_2)(z_1 + z_2)}{q} + \theta m(z_1 - z_2)).$$

For convenience, we change the variables, setting $u := z_1 - z_2, v := z_2$, then

$$\begin{aligned} S^2 &\leq 2M \sum_{\substack{|m| \leq M \\ m \neq 0}} \sum_{|u| \leq N} e(\frac{amu^2}{q} + \theta mu) \sum_{v \in I, v \in I-u} e(\frac{2amuv}{q}) \\ &\leq 2M \sum_{\substack{|m| \leq M \\ m \neq 0}} \sum_{|u| \leq N} | \sum_{v \in I, v \in I-u} e(\frac{2amuv}{q}) |. \end{aligned}$$

Next, using the basic estimate (see [8, Section 8.2], for instance)

$$| \sum_{K_0 < k \leq K_0 + K} e(\omega k) | \leq \min(K, \frac{1}{\|2\omega\|})$$

we obtain that

$$S^2 \leq 2M \sum_{\substack{|m| \leq M \\ m \neq 0}} \sum_{|u| \leq N} \min(N, \frac{1}{\|2amu/q\|}).$$

To estimate the right hand side, let N_r be the number of pairs (m, u) such that $2amu \equiv r \pmod{q}$. (In what follows, it is useful to keep in mind that a and q are co-primes.) We have

$$S(M, N, q)^2 \leq 2M \left(N_0 N + \sum_{1 \leq r \leq q/2} (N_r + N_{q-r}) \frac{q}{r} \right). \quad (14)$$

To finish the proof, we are going to derive a (uniform) bound for the N_r 's. For $0 \leq r \leq q-1$ let $0 \leq r_a \leq q-1$ be the only number such that $ar_a \equiv r \pmod{q}$. Thus $2amu \equiv r \pmod{q}$ is equivalent with $2mu \equiv r_a \pmod{q}$.

First we consider the case $r \neq 0$, thus $r_a \neq 0$. Write $2mu = r_a + sq$. It is clear that $r_a + sq \neq 0$ for all s . Since $2mu \leq 2MN$, we have $|s| \leq 2MN/q$. For each given s the number of such pairs (m, u) is bounded by $\tau(r_a + sq)$.

Choose $k = \max(\frac{1}{\varepsilon} + 2, 3)$, then $MN/q \geq (MN)^{2/k}$ by the assumption $MN \geq q^{1+\varepsilon}$. It follows from Lemma 6.1 that, for $r \neq 0$,

$$\begin{aligned} N_r &\leq \sum_{|s| \leq 2MN/q} \tau(r_a + sq) = O_\varepsilon \left(\sum_{d \leq (MN)^{1/k}} \tau(d)^{\beta(k)} \left(\sum_{\substack{|s| \leq 4MN/q \\ d|r_a + sq}} 1 \right) \right) \\ &= O_\varepsilon \left(\sum_{d \leq (MN)^{1/k}} \tau(d)^{\beta(k)} \left(\frac{4MN}{qd} + O(1) \right) \right) \\ &= O_\varepsilon \left(\frac{MN}{q} \sum_{d \leq (MN)^{1/k}} \frac{\tau(d)^{\beta(k)}}{d} + O((MN)^{1/k+o(1)}) \right) \\ &= O_\varepsilon \left(\frac{MN}{q} \sum_{d \leq (MN)^{1/k}} \frac{\tau(d)^{\beta(k)}}{d} \right). \end{aligned}$$

Notice that $\sum_{d \leq x} \tau(d)^{\beta(k)} \ll x \log^{\beta'(k)} x$ for some positive constant $\beta'(k)$ depending on $\beta(k)$ (see [8, Section 1.6], for instance). By summation by parts we deduce that

$$N_r = O_\varepsilon \left(\frac{MN}{q} \log^{\beta''(k)}(MN) \right)$$

for some positive constant $\beta''(k)$ depending on $\beta'(k)$.

Now we consider the case $r = 0$. The equation $2mu = sq$ has at most $\tau(sq)$ solution pairs (m, u) , except when $s = 0$, the case that has $2M$ solutions $\{(m, 0); |m| \leq 2M, m \neq 0\}$. Thus we have

$$N_0 \leq 2M + \sum_{|s| \leq 2MN/q, s \neq 0} \tau(sq),$$

and hence,

$$N_0 = O_\varepsilon\left(2M + \frac{MN}{q} \log^{\beta''(k)}(MN)\right).$$

Combining these estimates with (14), we can conclude that

$$S(M, N, q) \ll_\varepsilon (M\sqrt{N} + MN/\sqrt{q}) \log^\alpha(MN)$$

for some sufficiently large constant $\alpha = \alpha(\varepsilon)$.

7. PROOF OF LEMMA 4.3

We are going to need the following simple fact.

Fact 7.1. *Let a_1, \dots, a_m, q be integers such that $(a_1, \dots, a_m, q) = 1$. Then we can select a decomposition $q = q_1 \dots q_l$ of q and l different numbers a_{i_1}, \dots, a_{i_l} of $\{a_1, \dots, a_m\}$ (for some $l \geq 1$) such that*

$$(q_i, q_j) = 1 \text{ for every } i \neq j \text{ and } (a_{i_j}, q_j) = 1 \text{ for every } j.$$

Proof (of Fact 7.1) Let $q = q'_1 \dots q'_k$ be the decomposition of q into prime powers. For each q'_i we assign a number a'_i from $\{a_1, \dots, a_m\}$ such that $(q'_i, a'_i) = 1$ (the same a_i may be assigned to many q'_j). Let a_{i_j} 's be the collection of the a'_i 's without multiplicity. Set q_j to be the product of all q'_i assigned to a_{i_j} . ■

The core of the proof of Lemma 4.3 will be the following proposition, which is basically the case of one variable in a slightly more general setting.

Proposition 7.2. *There is a constants D such that the following holds. For given integers $g, h, p, t, z_1; g, h, p > 0$ there exist integers $x \in [0, (ph)^{1/2}(\log h)^D]$ and z_2 such that $gx + pz_1^2 + tk \equiv pz_2^2 \pmod{h}$, where $k = (g, h)$.*

Lemma 4.3 follows from Fact 7.1 and Proposition 7.2 by an inductive argument. Indeed, by the above fact we may assume that $q = q_1 \dots q_l$ where $(a_i, q_i) = 1$, and so

$$(a_l, q) | q_1 \dots q_{l-1}.$$

Now if Lemma 4.3 is true for $l - 1$ variables, i.e. there are appropriate x_1, \dots, x_{l-1} such that $a_1 x_1 + \dots a_{l-1} x_{l-1} + r = pz_1^2 + tq_1 \dots q_{l-1}$. Then we apply Proposition 7.2 for $q = h, g = a_l$ to find x_l . It thus remains to justify Proposition 7.2.

Proof (of Proposition 7.2) Without loss of generality we assume that $h \geq 3$. As $k = (g, h)$, we can write $g = ka, h = kq$ where $(a, q) = 1$. We shall find a solution

in the form $z_2 = z_1 + zk$. Plugging in z_2 in this form and simplifying by k , we end up with the equation

$$ax + t \equiv pkz^2 + 2pz_1z \pmod{q}.$$

or equivalently,

$$x \equiv \bar{a}pkz^2 + 2\bar{a}pz_1z - \bar{a}t \pmod{q} \tag{15}$$

where \bar{a} is the reciprocal of a modulo q , $a\bar{a} \equiv 1 \pmod{q}$.

Our task is to find $x \in [0, (ph)^{1/2}(\log h)^D]$ such that (15) holds for some integer z . Notice that if q is small and D is large then $(ph)^{1/2}(\log h)^D \geq (\log 3)^D$, therefore the interval $[0, (ph)^{1/2}]$ contains every residue class modulo q ; as a result, (15) holds trivially. From now on we can assume that q is large,

$$q \geq \exp(16(6(\alpha + 1)/e)^{\alpha+1}) \tag{16}$$

where c, α are constants arising from Lemma 4.2 with $\varepsilon = 1/3$.

Let $s = (pk, q)$; so we can write $pk = sp', q = sq'$ with $(p', q') = 1$.

Let D be a large constant (to be determined later) and set

$$L := (sq)^{1/2}(\log q)^D/2 \text{ and } I := [L, 2L].$$

Note that

$$ph = pkq = sp'q \geq sq.$$

Thus we have

$$I \subset [0, (ph)^{1/2}(\log h)^D].$$

Let f be a smooth function defined with respect to the interval I (as in Lemma 4.1). For fixed $z \in [1, q]$ the numbers of x in $[0, (sq)^{1/2} \log^D q]$ satisfying (15) is at least

$$N_z := \sum_{m \in \mathbf{Z}} f(\bar{a}pkz^2 + 2\bar{a}pz_1z - \bar{a}t + mq).$$

By Poisson summation formula (8)

$$N_z = \sum_{m \in \mathbf{Z}} \frac{1}{q} \widehat{f}\left(\frac{m}{q}\right) e\left(\frac{(\bar{a}pkz^2 + 2\bar{a}pz_1z - \bar{a}t)m}{q}\right).$$

By summing over $z \in [1, q]$ we obtain

$$N := \sum_{z=1}^q N_z = \frac{1}{q} \sum_{m \in \mathbf{Z}} \widehat{f}\left(\frac{m}{q}\right) \sum_{z=1}^q e\left(\frac{(\bar{a}pkz^2 + 2\bar{a}pz_1z - \bar{a}t)m}{q}\right).$$

To conclude the proof, it suffices to show that $N > 0$. We are going to show (as fairly standard in this area) that the sum is dominated by the contribution of the zero term.

By the triangle inequality, we have

$$|N - \widehat{f}(0)| \leq \frac{1}{q} \sum_{m \in \mathbf{Z}, m \neq 0} \left| \widehat{f}\left(\frac{m}{q}\right) \right| \left| \sum_{z=1}^q e\left(\frac{(\bar{a}pkz^2 + 2\bar{a}pz_1z)m}{q}\right) \right|.$$

Let γ_1, γ_2 be a sufficiently large constant and let

$$L' := \frac{\gamma_1 q (\log q)^{\gamma_2}}{L}.$$

Set

$$S_1 := \frac{1}{q} \sum_{|m| \geq L'} \left| \widehat{f}\left(\frac{m}{q}\right) \right| \left| \sum_{z=1}^q e\left(\frac{(\bar{a}pkz^2 + 2\bar{a}pz_1z)m}{q}\right) \right|$$

and

$$S_2 := \frac{1}{q} \sum_{\substack{|m| \leq L' \\ m \neq 0}} \left| \widehat{f}\left(\frac{m}{q}\right) \right| \left| \sum_{z=1}^q e\left(\frac{(\bar{a}pkz^2 + 2\bar{a}pz_1z)m}{q}\right) \right|.$$

We then have

$$|N - \widehat{f}(0)| \leq S_1 + S_2.$$

In what follows, we show that both S_1 and S_2 are less than $\widehat{f}(0)/4$.

Estimate for S_1 . It is not hard to show that

$$\sum_{k \in \mathbf{Z}} \exp(-\sqrt{x|k|}) < \frac{5}{x} \text{ for } 0 < x < 1.$$

To see this, observe that

$$\sum_{k \geq 1} \exp(-\sqrt{xk}) \leq \int_0^\infty \exp(-\sqrt{xt}) dt = \frac{2}{x},$$

where the integral is evaluated by changing variable and integration by parts.

Thus

$$\sum_{|k| \geq k_0} \exp(-\sqrt{x|k|}) < \sum_{k \in \mathbf{Z}} \exp(-\sqrt{x}(\frac{\sqrt{|k|} + \sqrt{k_0}}{2})) \leq \frac{20}{x} \exp(-\frac{\sqrt{xk_0}}{2}). \quad (17)$$

From the property of f (Lemma 4.1) we can deduce that

$$S_1 \leq 16\widehat{f}(0) \sum_{|m| \geq \frac{\gamma_1 q (\log q)^{\gamma_2}}{L}} \exp(-\delta \sqrt{|Lm/q|}),$$

which, via (17) and since $q \geq 3$, implies

$$S_1 \leq 16\widehat{f}(0) \frac{20}{Lq^{-1}} \exp(-\frac{\delta(\gamma_1(\log q)^{\gamma_2})^{1/2}}{2}) \leq \widehat{f}(0)/4,$$

given that we choose γ_1, γ_2 sufficiently large.

Estimate for S_2 . We have

$$S_2 = \frac{\widehat{f}(0)}{q} \sum_{\substack{|m| \leq L' \\ m \neq 0}} \left| \sum_{z=1}^q e(\frac{\bar{a}p'z^2}{q'} + \frac{2\bar{a}pz_1zm}{q}) \right|.$$

We shall choose $D > \gamma_2$.

Set

$$\gamma_1 := \left(\frac{6(D - \gamma_2)}{e} \right)^{D - \gamma_2}.$$

First, we observe that

$$L'q = \frac{2\gamma_1 q^2 (\log q)^{\gamma_2}}{(sq)^{1/2} (\log q)^D} = \frac{2\gamma_1 q^{3/2}}{s^{1/2} (\log q)^{D - \gamma_2}} = \frac{2\gamma_1 q^{1/2} q}{(\log q)^{D - \gamma_2}} \geq q^{4/3} \frac{\gamma_1 q^{1/6}}{(\log q)^{D - \gamma_2}}.$$

It is not hard to show that the function $q^{1/6}/(\log q)^{D - \gamma_2}$, where $q \geq 3$, attains its minimum at $q = \exp(6(D - \gamma_2))$. Therefore, by the choice of γ_1 , we have

$$L'q \geq q^{4/3}.$$

Next, Lemma 4.2 applied for $\varepsilon = 1/3$ (and with the mentioned c and α) yields

$$\begin{aligned} S_2 &= \frac{\widehat{f}(0)}{q} \sum_{\substack{|m| \leq L' \\ m \neq 0}} \left| \sum_{z=1}^q \epsilon \left(\frac{\bar{a}p'z^2}{q'} + \frac{2\bar{a}pz_1zm}{q} \right) \right| \\ &\leq c \frac{\widehat{f}(0)}{q} \left(\frac{L'q}{\sqrt{q'}} + L' \sqrt{q} \right) (\log q)^\alpha \\ &\leq 2c \frac{\widehat{f}(0)}{q} \frac{L'q}{\sqrt{q'}} (\log q)^\alpha = 2c \frac{\widehat{f}(0)L'}{\sqrt{q'}} (\log q)^\alpha. \end{aligned}$$

It follows that

$$S_2 \leq \frac{4c\gamma_1 q (\log q)^{\alpha + \gamma_2}}{(\sqrt{sq} \log^D q) \sqrt{q'}} \widehat{f}(0) = \frac{4c\gamma_1 (\log q)^{\alpha + \gamma_2}}{(\log q)^D} \widehat{f}(0).$$

Now we choose D, γ_2 so that $D - \gamma_2 - \alpha = 1$. Thus $\gamma_1 = (6(\alpha + 1)/e)^{\alpha + 1}$, and

$$S_2 \leq \frac{4c\gamma_1 (\log q)^{\alpha + \gamma_2}}{(\log q)^D} \widehat{f}(0) = \frac{4c(6(\alpha + 1)/e)^{\alpha + 1}}{\log q} \widehat{f}(0) \leq \widehat{f}(0)/4$$

where the last inequality comes from (16). ■

Remark 7.3. We can also use Burgess estimate to have an alternative proof with a slightly better bound. However, an improvement in this section does not improve the main theorem.

8. PROOF OF LEMMA 2.4

We first apply Lemma 3.7 to obtain a large proper GAP Q of rank 1 or 2. By this lemma, we have $A'' \subset \{s_1, \dots, s_m\} + Q$, where m is a constant.

Let $S_i = A'' \cap (s_i + Q)$ for $1 \leq i \leq m$. We would like to guarantee that all S_i are large by the following argument.

If S_i is smaller than $n^{1/3}(\log n)^{3C/10}$, then we delete it from A'' and add to A' . The new sets A' , A'' and Q still satisfy the claim of Lemma 3.7. On the other hand, that the total number of elements added to A' is only $O(n^{1/3}(\log n)^{3C/10}) = o(|A'|)$, thus the sizes of A' and A'' hardly changes.

From now on, we assume that $|S_i| \geq n^{1/3}(\log n)^{3C/10}$ for all i .

For convenience, we let

$$s'_i := s_i + r.$$

Thus every element of S_i is congruent with s'_i modulo q .

8.1. Q has rank one. In this subsection, we deal with the (easy) case when Q has rank one. We write $Q = \{r + qx \mid 0 \leq x \leq L\}$ where $L \geq n^{2/3}(\log n)^{C/2}$.

Since $Q \subset S_{A'} \subset [\frac{n}{p}|A'|]$, we have

$$q \leq \frac{|A'|n}{pL} \leq \frac{n^{2/3}}{(\log n)^{C/6}p}.$$

By setting C (of Lemma 3.7) sufficiently large compared to D (of Lemma 4.3), we can guarantee that

$$(pq)^{1/2}(\log q)^D \leq n^{1/3}. \tag{18}$$

Let $d := (s_1 + r, \dots, s_m + r, q) = (s'_1, \dots, s'_m, q)$. If $d > 1$ then all elements of A'' are divisible by d , since A'' are covered by $\{s_1, \dots, s_m\} + Q$. Thus we reach the third case of the lemma and are done.

Assume now that $d = 1$. By Lemma 4.3, we can find $0 \leq x_i \leq (pq)^{1/2}(\log q)^D$ such that

$$s'_1 x_1 + \cdots + s'_m x_m + r \equiv pz^2 \pmod{q}. \quad (19)$$

Pick from S_i 's exactly x_i elements and add them together to obtain a number s . The set $s + Q$ is a translate of Q which satisfies the first case of Lemma 2.4 and we are done.

8.2. Q has rank two. In this section, we consider the (harder) case when Q has rank two. The main idea is similar to the rank one case, but the technical details are somewhat more tedious. We write

$$Q = r + q(q_1 x + q_2 y) \mid 0 \leq x \leq L_1, 0 \leq y \leq L_2$$

where $L_1 L_2 = |Q| \geq n \log^{2C/3} n$.

As Q is proper, either $q_1 \geq L_2$ or $q_2 \geq L_1$ holds. Thus $qL_1 L_2 \leq |A'|n/p$, which yields (with room to spare)

$$q \leq \frac{n^{1/3}}{(\log n)^{C/6} p}. \quad (20)$$

We consider two cases. In the first (simple) case, both L_1 and L_2 are large. In the second, one of them can be small.

Case 1. $\min(L_1, L_2) \geq n^{1/3}(\log n)^{C/4}$. Define $d := (s'_1, \dots, s'_m, q)$ and argue as in the previous section. If $d > 1$, then we end up with the third case of Lemma 2.4. If $d = 1$ then apply Lemma 4.3. The fact that q is sufficiently small (see (20)) and that $|S_i|$ is sufficiently large guarantee that we can choose x_i elements from S_i . At the end, we will obtain a GAP of rank 2 which is a translate of Q and satisfies the second case of Lemma 2.4.

Case 2. $\min(L_1, L_2) \leq n^{1/3}(\log n)^{C/4}$. In this case the sides of GAP Q are unbalanced and one of them is much larger than the other. We are going to exploit this fact to create a GAP of rank one (i.e., an arithmetic progression) which satisfies the first case of Lemma 3.7, rather than trying to create a GAP of rank two as in the previous case.

Without loss of generality, we assume that $L_1 \leq n^{1/3}(\log n)^{C/4}$. By the lower bound on $L_1 L_2$, we have that $L_2 \geq n^{2/3}(\log n)^{C/4}$. This implies

$$qq_2 \leq \frac{|A'|n}{pL_2} \leq \frac{n^{2/3}}{(\log n)^{C/12} p}.$$

Again by setting C sufficiently large compared to D , we have

$$(pqq_2)^{1/2}(\log qq_2)^D \leq n^{1/3}(\log n)^{C/5}. \quad (21)$$

Creating a long arithmetic progression. In the rest of the proof we make use of A'' and Q to create an AP of type $\{r' + qq_2x_2 \mid 0 \leq x_2 \leq L_2, r' \equiv pz^2 \pmod{qq_2}\}$. This gives the first case in Lemma 3.7 and thus completes the proof of this lemma.

Let S be an element of $\{S_1, \dots, S_m\}$. Since S is contained in a translate of Q , there is a number s such that any $a \in S$ satisfies $a \equiv s + tqq_1 \pmod{qq_2}$ for some $0 \leq t \leq L_1$ (for instance, if $a \in S_i$ then $a \equiv s'_i + tqq_1 \pmod{qq_2}$). Let T denote the *multiset* of t 's obtained this way. Notice that T could contain one element of multiplicity $|S|$. Also recall that $|S| \geq n^{1/3}(\log n)^{3C/10}$.

For $0 \leq l \leq |S|/2$, let m_l and M_l (respectively) be the minimal and maximal values of the sum of l elements of T . Since $0 \leq t \leq L_1$ for every $t \in T$, by swapping summands of m_l with those of M_l , we can obtain a sequence $m_l = n_0 \leq \dots \leq n_l = M_l$ where each $n_i \in l^*T$ and $n_{i+1} - n_i \leq L_1$ for all relevant i .

By construction, we have

$$[m_l, M_l] \subset \{n_0, \dots, n_l\} + [0, L_1] \subset l^*T + [0, L_1]. \quad (22)$$

Next we observe that if l is large and $M_l - m_l$ is small, then T looks like a sequence of only one element with high multiplicity. We will call this element the *essential* element of T .

Proposition 8.3. *Assume that $\frac{1}{4}n^{1/3}(\log n)^{3C/10} \leq l \leq \frac{1}{2}n^{1/3}(\log n)^{3C/10}$ and $M_l - m_l < \frac{1}{4}n^{1/3}(\log n)^{3C/10}$. Then all but at most $\frac{1}{2}n^{1/3}(\log n)^{3C/10}$ elements of T are the same.*

Proof (Proof of Proposition 8.3) Let $t_1 \leq t_2 \leq \dots \leq t_l$ be the l smallest elements of T and $t'_1 \leq \dots \leq t'_l$ be the l largest. By the upper bound on l and lower bound on $|S| = |T|$, $t'_1 \geq t_l$. On the other hand, $M_l - m_l = (t'_1 - t_1) + \dots + (t'_l - t_l)$. Thus if $M_l - m_l < \frac{1}{4}n^{1/3}(\log n)^{3C/10} \leq l - 1$ then $t'_i = t_i$ for some i . The claim follows. ■

The above arguments work for any S among S_1, \dots, S_m . We now associate to each S_i a multiset T_i , for all $1 \leq i \leq m$.

Subcase 2.1 *The hypothesis in Proposition 8.3 holds for all T_i .* In this case we move to A' those elements of S_i whose corresponding parts in T_i is not the essential element. The number of elements moved is only $O(n^{1/3}(\log n)^{3C/10})$, which is negligible compared to both $|A'|$ and $|A''|$. Furthermore, the properties claimed in Lemma 3.7 remain unchanged and the size of new S_i are now at least $\frac{1}{2}n^{1/3}(\log n)^{3C/10}$.

Now consider the elements of A'' with respect to modulo qq_2 . Since each T_i has only the essential element, the elements of A'' produces at most m residues $u_i = s'_i + t_i qq_1$, each of multiplicity at least

$$|S_i| \geq \frac{1}{2} n^{1/3} (\log n)^{3C/10} \geq (pqq_2)^{1/2} (\log qq_2)^D$$

where the last inequality comes from (21). Define $d = (u_1, \dots, u_m, qq_2)$ and proceed as usual, applying Lemma 4.3.

Subcase 2.2 *The hypothesis in Proposition 8.3 does not hold for all T_i .* We can assume that, with respect to T_1 , $M_l - m_l \geq \frac{1}{4} n^{1/3} (\log n)^{3C/10}$ for all $\frac{1}{4} n^{1/3} (\log n)^{3C/10} \leq l \leq \frac{1}{2} n^{1/3} (\log n)^{3C/10}$. From now on, fix an l in this interval.

Next, for a technical reason, we extract from S_1 a very small part S'_1 of cardinality $n^{1/3} (\log n)^{C/5}$ and set $S''_1 = S_1 \setminus S'_1$. Let T be the multiset associated with S''_1 . We can assume that T satisfies the hypothesis of this subcase.

Define $d := (s'_1, \dots, s'_m, q)$. As usual, the case $d > 1$ leads to the third case of Lemma 2.4, so we can assume $d = 1$. By Lemma 4.3, there exist integers

$$0 \leq x_i \leq (pq)^{1/2} (\log n)^D \leq n^{1/3} (\log n)^{C/5} \leq |S_i|$$

and k, z_1 such that

$$s'_1 x_1 + \dots + s'_m x_m + (ls'_1 + r) = pz_1^2 + kq. \quad (23)$$

For $i \geq 2$ we pick from S_i exactly x_i elements $a_1^i, \dots, a_{x_i}^i$, and for $i = 1$ we pick x_1 elements $a_1^1, \dots, a_{x_1}^1$ from S'_1 and add them together. By (23) the following holds for some integer k' ,

$$\sum_{i=1}^m \sum_{j=1}^{x_i} a_j^i + (ls'_1 + r) = pz_1^2 + k'q. \quad (24)$$

Furthermore, by Proposition 7.2, as $q = (qq_1, qq_2)$, there exist $0 \leq x \leq (pqq_2)^{1/2} \log^D(qq_2)$ and k'', z_2 such that

$$qq_1 x + pz_1^2 + (k' + m_l q_1)q = pz_2^2 + k'' qq_2,$$

$$pz_1^2 + k'q + (x + m_l)qq_1 = pz_2^2 + k'' qq_2. \quad (25)$$

As $(pqq_2)^{1/2} \log^D(qq_2) \leq n^{1/3} \log^{C/5} n$ and $n^{1/3} \log^{C/5} n \leq M_l - m_l$, we have

$$m_l \leq x + m_l \leq M_l.$$

On the other hand, recall that $[m_l, M_l] \subset l^*T + [0, L_1]$ (see (22)), we have

$$\{ls'_1 + r + [m_l, M_l]qq_1\} \subset l^*S''_1 + r + [0, L_1]qq_1 \pmod{qq_2}.$$

Thus

$$ls'_1 + r + (x + m_l)qq_1 \in l^*S''_1 + r + [0, L_1]qq_1 \pmod{qq_2}. \quad (26)$$

Combining (24),(25) and (26) we infer that there exist l elements a_1, \dots, a_l of S''_1 , and there exist $0 \leq u \leq L_1$ and v such that

$$\sum_{i=1}^m \sum_{j=1}^{x_i} a_j^i + a_1 + \dots + a_l + r + uqq_1 = pz_2^2 + vqq_2.$$

Hence, $\sum_{i=1}^m \sum_{j=1}^{x_i} a_j^i + a_1 + \dots + a_l + Q$ contains the AP $\{(pz_2^2 + vqq_2) + qq_2x_2 \mid 0 \leq x_2 \leq L_2\}$, completing Subcase 2.2.

Finally, one checks easily that the number of elements of A'' involved in the creation of pz_2^2 in all cases is bounded by $O(n^{1/3} \log^{C/5} n) = o(|A'|)$, thus we may put all of them to A' without loss of generality.

9. PROOF OF THEOREM 1.5: THE RANK ONE CASE.

Here we consider the (easy) case when Q (in Lemma 2.4) has rank one. In this case, $S_{A'}$ contains an AP $Q = \{r + qx \mid 0 \leq x \leq L\}$, where $L \geq n^{2/3}(\log n)^{C/4}$ as in the first statement of Lemma 2.4. We are going to show that Q contains a number of the form pz^2 .

Write $r = pz_0^2 + tq$ for some $0 \leq z_0 \leq q$. Since r is a sum of some elements of A' , we have

$$0 \leq r \leq |A'|(n/p) \leq \frac{n^{4/3}(\log n)^{C/3}}{p}.$$

Thus

$$-pq \leq t \leq \frac{n^{4/3}(\log n)^{C/3}}{pq}. \quad (27)$$

The interval $[t/pq, (t+L)/pq]$ contains at least two squares because

$$\left(\frac{L}{pq}\right)^2 \geq \frac{n^{4/3}(\log n)^{C/2}}{(pq)^2} \geq 10\frac{t}{pq} + 20.$$

Thus, we can find an integer $x_0 \geq 0$ such that $\frac{t}{pq} < x_0^2 < (x_0 + 1)^2 \leq \frac{t+L}{pq}$. It is implied that (since $0 \leq z_0 \leq q$)

$$t \leq pqx_0^2 + 2pz_0x_0 \leq t + L. \quad (28)$$

Set $z := z_0 + qx_0$. We have

$$pz^2 = pz_0^2 + q(pqx_0^2 + 2pz_0x_0).$$

On the other hand, by (28), the right hand side belongs to

$$pz_0^2 + q[t, t+L] = pz_0^2 + tq + q[0, L] = r + q[0, L] = Q.$$

Thus, Q contains pz^2 , completing the proof for this case.

10. PROOF OF THEOREM 1.5: THE RANK TWO CASE

In this case, we assume that $S_{A'}$ contains a proper GAP as in the second statement of Lemma 2.4. We can write

$$Q = \{r + q(q_1x_1 + q_2x_2) \mid 0 \leq x_1 \leq L_1, 0 \leq x_2 \leq L_2, (q_1, q_2) = 1\}$$

where

- $\min(L_1, L_2) \geq n^{1/3}(\log n)^{C/4}$,
- $L_1L_2 \geq n(\log n)^{C/2}$,
- $q \leq \frac{n^{1/3}(\log n)^{-C/6}}{p}$,
- and $r = pz_0^2 + tq$ for some integers t and $0 \leq z_0 \leq q$.

Since r is a sum of some elements of A' , we have $0 \leq r \leq \frac{n^{4/3}(\log n)^{C/3}}{p}$, and so

$$-pq \leq t \leq \frac{n^{4/3}(\log n)^{C/3}}{pq}.$$

Without loss of generality, we assume that $q_2 L_2 \geq q_1 L_1$. Because Q is proper, either $q_2 \geq L_1$ or $q_1 \geq L_2$. On the other hand, if $q_2 < L_1$ then $L_2 \leq q_1$, which is impossible by the assumption. Hence,

$$q_2 \geq L_1.$$

Now we write $Q = \{pz_0^2 + q(q_1 x_1 + q_2 x_2 + t) \mid 0 \leq x_1 \leq L_1, 0 \leq x_2 \leq L_2, (q_1, q_2) = 1\}$ and notice that if we set $w := z_0 + zq$ then

$$pw^2 - pz_0^2 = p(z_0 + qz)^2 - pz_0^2 = q(pqz^2 + 2pz_0z).$$

Thus if there is an integer z satisfies

$$pqz^2 + 2pz_0z \in \{q_1x + q_2y + t \mid 0 \leq x \leq L_1, 0 \leq y \leq L_2\} \quad (29)$$

then $pw^2 \in Q$, and we are done with this case. The rest of the proof is the verification of the following proposition, which shows the existence of a desired z .

Proposition 10.1. *There exists an integer z which satisfies (29).*

Proof (Proof of Proposition 10.1) The method is similar to that of Lemma 4.3, relying on Poisson summation.

Set $a := pq$ and $b := 2pz_0$. Notice that since $0 \leq z_0 \leq q$, $0 \leq b \leq 2pq = 2a$. Our task is to find a z such that

$$az^2 + bz - q_1x - t = q_2y \text{ for some } 0 \leq x \leq L_1, 0 \leq y \leq L_2.$$

Define (with foresight; see (31)) $I_x := [L_1/8, L_1/4]$ and

$$I_z := \left[\left(\frac{q_1 L_1/4 + t}{a} \right)^{1/2} + 1, \left(\frac{q_2 L_2 + q_1 L_1/8 + t}{a} \right)^{1/2} - 1 \right].$$

(Notice the that the lower bounds on L_1, L_2 and the upper bound on pq guarantee that the expressions under the square roots are positive.)

Since $r + qq_1L_1 + qq_2L_2 = pz_0^2 + tq + q(q_1L_1 + q_2L_2) \in Q$, it follows that (with $\max(Q)$ denoting the value of the largest element of Q)

$$q_2L_2 + q_1L_1/8 + t \leq \max(Q)/q \leq \frac{p^{-1}n^{4/3}(\log n)^{C/3}}{q} = \frac{n^{4/3}(\log n)^{C/3}}{a}.$$

Thus

$$|I_z| \geq \frac{1}{4} \frac{(q_2L_2 - q_1L_1/4)a^{-1}}{\sqrt{\frac{q_2L_2 + q_1L_1/8 + t}{a}}}$$

$$|I_z| = \Omega\left(\frac{q_2L_2}{n^{2/3}(\log n)^{C/6}}\right). \quad (30)$$

By the definitions of I_x and I_z , we have, for any $x \in I_x$ and $z \in I_z$

$$0 \leq az^2 + bz - q_1x - t \leq a(z+1)^2 - q_1x - t \leq q_2L_2. \quad (31)$$

Thus, for any such pair of x and z , if $az^2 + bz - q_1x - t$ is divisible by q_2 , then $y := (az^2 + bz - q_1x - t)/q_2$ is an integer in $[1, L_2]$. We are now using the ideas from Section 7, with respect to modulo q_2 and the intervals I_x, I_z .

Let \bar{q}_1 be the reciprocal of q_1 modulo q_2 (recall that $(q_1, q_2) = 1$). Let f be a function given by Lemma 4.1 with respect to the interval I_x . For a given $z \in I_z$, the number of $x \in I_x$ satisfying (29) is at least N_z , where

$$N_z := \sum_{m \in \mathbf{Z}} f(\bar{q}_1az^2 + \bar{q}_1bz - \bar{q}_1t + mq_2).$$

By applying Poisson summation formula (8) and summing over z in I_z we obtain

$$N := \sum_{z \in I_z} N_z = \sum_{m \in \mathbf{Z}} \frac{1}{q_2} \hat{f}\left(\frac{m}{q_2}\right) \sum_{z \in I_z} e\left(\frac{(\bar{q}_1az^2 + \bar{q}_1bz - \bar{q}_1t)m}{q_2}\right).$$

It suffices to show that $N > 0$. Similar to the proof of Lemma 4.3, we will again show that the right hand side is dominated by the contribution at $m = 0$. By triangle inequality, we have

$$|N - \frac{1}{q_2} \widehat{f}(0)|_{I_z}| \leq \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{1}{q_2} |\widehat{f}(\frac{m}{q_2})| \left| \sum_{z \in I_z} e(\frac{(\bar{q}_1 a z^2 + \bar{q}_1 b z - \bar{q}_1 t)m}{q_2}) \right|.$$

Let γ be a sufficiently large constant and let

$$L' := \frac{8q_2(\log q_2)^\gamma}{L_1}.$$

We have

$$|N - \frac{1}{q_2} \widehat{f}(0)|_{I_z}| \leq S_1 + S_2$$

where

$$S_1 := \sum_{|m| \geq L'} \frac{1}{q_2} |\widehat{f}(\frac{m}{q_2})| \left| \sum_{z \in I_z} e(\frac{(\bar{q}_1 a z^2 + \bar{q}_1 b z - \bar{q}_1 t)m}{q_2}) \right|$$

and

$$S_2 := \sum_{\substack{|m| \leq L' \\ m \neq 0}} \frac{1}{q_2} |\widehat{f}(\frac{m}{q_2})| \left| \sum_{z \in I_z} e(\frac{(\bar{q}_1 a z^2 + \bar{q}_1 b z - \bar{q}_1 t)m}{q_2}) \right|.$$

To conclude the proof, we will show that both S_1 and S_2 are $o(\frac{\widehat{f}(0)|_{I_z}|}{q_2})$.

Estimate for S_1 . By the property of f ,

$$S_1 \leq \frac{\widehat{f}(0)|_{I_z}|}{q_2} \sum_{|m| \geq \frac{8q_2(\log q_2)^\gamma}{L_1}} \exp(-\delta \sqrt{|mL_1/(8q_2)|}).$$

By (17), and as q_2 is large ($q_2 \geq L_1 > n^{1/3}$), the inner sum is $o(1)$, so

$$S_1 = o\left(\frac{\widehat{f}(0)|_{I_z}|}{q_2}\right) \tag{32}$$

as desired.

Estimate for S_2 . Let $q' = (\bar{q}_1 a, q_2)$. We can write

$$\bar{q}_1 a = q' q'_1, q_2 = q' q'_2 \text{ with } (q'_1, q'_2) = 1. \quad (33)$$

Then

$$S_2 \leq \frac{\widehat{f}(0)}{q_2} \sum_{\substack{|m| \leq L' \\ m \neq 0}} \left| \sum_{z \in I_z} e\left(\frac{q'_1 m z^2}{q'_2} + \frac{(\bar{q}_1 b z - \bar{q}_1 t) m}{q_2}\right) \right|.$$

By Lemma 4.2 there are absolute constants c, α such that

$$S_2 \leq c \frac{\widehat{f}(0)}{q_2} \left(L' \sqrt{|I_z|} (\log n)^\alpha + \frac{L' |I_z| (\log n)^\alpha}{\sqrt{q'_2}} \right).$$

To show that $S_2 = o\left(\frac{\widehat{f}(0)|I_z|}{q_2}\right)$, it suffices to show that

$$L' (\log n)^\alpha = o(\sqrt{|I_z|}) \quad (34)$$

and

$$L' (\log n)^\alpha = o(q'_2) \quad (35)$$

To verify (34), notice that by (30), we have

$$|I_z| L_1^2 = \Omega\left(\frac{L_1^2 q_2 L_2}{n^{2/3} (\log n)^{C/6}}\right).$$

Thus

$$\frac{|I_z|}{L'^2 (\log n)^{2\alpha}} = \Omega\left(\frac{|I_z| L_1^2}{q_2^2 (\log n)^{2\alpha+2\gamma}}\right) = \Omega\left(\frac{L_1^2 L_2^2}{L_2 q_2 n^{2/3} (\log n)^{C/6+2\alpha+2\gamma}}\right).$$

Since $(L_1 L_2)^2 \geq (n (\log n)^{C/2})^2 = n^2 \log^C n$ and $L_2 q_2 = O(\max(Q)) = O(p^{-1} n^{4/3} (\log n)^{C/3})$, the last formula is $\omega(1)$ if we set C sufficiently large compared to α and γ . This proves (34).

As a result,

$$\frac{\widehat{f}(0)}{q_2} L' \sqrt{|I_z|} (\log n)^\alpha = o(\widehat{f}(0)|I_z|/q_2).$$

Now we turn to (35). Recall that $q_2 = q'q'_2$ and $q' = (\bar{q}_1 a, q_2) = (a, q_2)$ (as q_1 and q_2 are co-primes). Thus

$$q'_2 \geq \frac{q_2}{a} = \frac{q_2}{pq}.$$

To show (35), it suffices to show that

$$\frac{q_2}{pq} = \omega(L'^2 (\log n)^{2\alpha})$$

which (taking into account the definition of L') is equivalent to

$$q_2 L_1^2 = \omega(pqq_2^2 (\log n)^{2\alpha+2\gamma}).$$

Multiplying both sides with $L_2 q_2^{-1}$, it reduces to

$$L_1^2 L_2 = \omega(pqq_2 L_2 (\log n)^{2\alpha+2\gamma}).$$

Now we use the fact that $qq_2 L_2 = O(\max(Q)) = O(p^{-1} n^{4/3} (\log n)^{C/3})$ and the lower bounds $L_1 L_2 \geq n (\log n)^{C/2}$ and $L_1 \geq n^{1/3} (\log n)^{C/4}$. The claim follows by setting C sufficiently large compared to α and γ , as usual. Our proof is completed. ■

Acknowledgements. The authors would like to thank Henryk Iwaniec for helpful discussions.

REFERENCES

- [1] N. Alon, *Subset sums*, Journal of Number Theory, 27 (1987), 196-205.
- [2] N. Alon and G. Freiman, *On sums of subsets of a set of integers*, Combinatorica, 8 (1988), 297-306.
- [3] Y. Bilu, *Structure of sets with small sumset*, Structure theory of set addition. Asterisque 258 (1999), xi, 77-108.
- [4] M. C. Chang, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. 65 (1994), no. 4, 379-388.
- [5] P. Erdős, *Some problems and results on combinatorial number theory*, Proc. 1st. China Conference in Combinatorics (1986).
- [6] G. Freiman, *Foundations of a structural theory of set addition*, translated from the Russian, Translations of Mathematical Monographs, Vol 37. American Mathematical Society, Providence, R. I., 1973.

- [7] B. Green, *An exposition on triples in Arithmetic progression*, <http://www.dpmms.cam.ac.uk/~bjg23/papers/bourgain-roth.pdf>.
- [8] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Colloquium publications, Volume 53.
- [9] E. Lipkin *On representation of r -powers by subset sums*, Acta Arithmetica 52 (1989), 114-130.
- [10] I. Ruzsa, *An analogue of Freiman's theorem in group*, Structure theory of set addition. Asterisque 258 (1999), 323-326.
- [11] A. Sárközy, *Finite addition theorems, II*, Journal of Number Theory, 48 (1994), 197-218.
- [12] E. Szemerédi and V. H. Vu, *Long arithmetic progressions in sumsets: Thresholds and Bounds*, Journal of the A.M.S, 19 (2006), no 1, 119-169.
- [13] T. Tao, *Freiman's theorem in solvable groups*, <http://arxiv.org/abs/0906.3535>
- [14] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, 2006.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA

E-mail address: `hoi@math.rutgers.edu`

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, PISCATAWAY, NJ 08854, USA

E-mail address: `vanvu@math.rutgers.edu`