ON SUMSETS CONTAINING A PERFECT SQUARE

ZACHARY CHASE

Abstract. We show $A+B$ contains a perfect square if $A, B \subseteq \{1, \ldots, N\}$ have $|A|, |B| \geq (\frac{3}{8}+\epsilon)N$. The constant $\frac{3}{8}$ is optimal.

1. Introduction

Let A, B be subsets of the first N positive integers. What are the maximum possible sizes of A and B if $A+B$ does not contain a perfect square?

Let us first discuss the history of the related question of the largest size of a subset $A \subseteq \{1, \ldots, N\}$ with $A+A$ not containing a perfect square, originally raised by Erdős and Silverman [2, p. 87, 107]. Erdős initially conjectured that the answer is roughly $\frac{1}{3}N$, coming from

$$A := \{n \leq N : n \equiv 1 \bmod 3\}.$$

However, Massias [9] noted that

$$A := \{n \leq N : n \bmod 32 \in \{1, 5, 9, 13, 14, 17, 21, 25, 26, 29, 30\}\}$$

gives the larger size of roughly $\frac{11}{32}N$. The two mentioned sets A indeed have the property that $A+A$ does not contain a perfect square, since the sumset of $\{1\} \subseteq \mathbb{Z}/3\mathbb{Z}$ with itself does not contain a quadratic residue (in $\mathbb{Z}/3\mathbb{Z}$), and the sumset of $\{1, 5, 9, 13, 14, 17, 21, 25, 26, 29, 30\} \subseteq \mathbb{Z}/32\mathbb{Z}$ with itself avoids quadratic residues.

Given that these two examples come from "lifting up" a set $A \subseteq \mathbb{Z}/q\mathbb{Z}$ for some $q \in \mathbb{N}$, and that any perfect square must be a quadratic residue mod q, it is natural to first solve the "modular" version of the problem: for given $q \in \mathbb{N}$, what is the largest size of a set $A \subseteq \mathbb{Z}/q\mathbb{Z}$ such that $A+A$ does not contain a quadratic residue?

In 1982, Lagarias, Odlyzko, and Shearer [6] showed the answer is $\frac{11}{32}q$ (which is tight if $32 \mid q$). In 1983, they released a companion paper [7] proving that if $A \subseteq [N]$ has $|A| \geq 0.475N$ then $A+A$ contains a perfect square. Finally, in 2001, Khalfalah, Lodha, and Szemerédi [5] resolved the Erdős-Silverman problem, by showing that for all $\epsilon > 0$, if N is sufficiently large, then any $A \subseteq [N]$ with $A+A$ avoiding perfect squares must have $|A| \leq (\frac{11}{32}+\epsilon)N$.

Date: January 11, 2022.

The author is partially supported by Ben Green's Simons Investigator Grant 376201 and gratefully acknowledges the support of the Simons Foundation.

In this paper, we solve the aformentioned "bipartite" version of the Erdős-Silverman question. Our result is asymptotically optimal.

Theorem 1. *For any $\epsilon > 0$, if N is sufficiently large and $A, B \subseteq [N]$ have $|A|, |B| \geq (\frac{3}{8} + \epsilon)N$, then $A + B$ contains a perfect square.*

An example achieving roughly $\frac{3}{8}N$ is

$$A := \{n \leq N : n \bmod 8 \in \{0, 1, 5\}\}$$
$$B := \{n \leq N : n \bmod 8 \in \{2, 5, 6\}\},$$

which works since the $\mathbb{Z}/8\mathbb{Z}$-sumset $\{0, 1, 5\} + \{2, 5, 6\}$ avoids quadratic residues.

We prove Theorem 1 by first resolving the associated "modular" version of the problem. While the methods of [6], solving the modular problem for $A+A$, are highly graph-theoretic, our methods use Fourier analysis to reduce (in one direction) to solving some optimization problem in 48 variables. Interestingly, the paper [6] also involved solving some optimization problems, specifically various integer programs. It is plausible our methods could solve the modular $A + A$ problem, though the number of variables in the obtained optimization problem would be significantly too large.

We then obtain the result in the integers by basic Fourier-analytic arguments. While [5], solving the $A + A$ problem in the integers, introduced a novel "shifting method" and a low-level strong arithmetic regularity lemma with tower-type bounds, our Fourier arguments amount to a rather basic arithmetic regularity lemma with only singly exponential bounds. In rough terms, we approximate the characteristic function of $A \subseteq [N]$ (and of B) by its best modulo Q weight function approximation on η^{-1} intervals each of length ηN, where η^{-1} and $\log Q$ are polynomials of ϵ^{-1}. Counting the number of perfect squares "in" the convolution of these weight functions essentially reduces to the modular problem. For details, see Section 4.

2. Notation

We use the standard $[N] := \{1, \ldots, N\}$ and $e(\theta) := e^{2\pi i\theta}$. Let $\frac{1}{\mathbb{N}} := \{\frac{1}{n} : n \geq 1\}$. Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. For $f : [N] \to \mathbb{C}$, define $\widehat{f} : \mathbb{T} \to \mathbb{C}$ by

$$\widehat{f}(\theta) := \sum_{n \leq N} f(n)e(-n\theta).$$

For $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, define $\widehat{f} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ by

$$\widehat{f}(r) := \frac{1}{q} \sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x)e\left(-\frac{rx}{q}\right).$$

Define the weighted indicator function of the quadratic residues $f_q : \mathbb{Z}/q\mathbb{Z} \to \mathbb{R}$ by

$$f_q(t) := |\{x \in \mathbb{Z}/q\mathbb{Z} : x^2 = t\}|.$$

For functions $f, g : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, define the convolution of f, g as

$$(f * g)(x) := \frac{1}{q} \sum_{a \in \mathbb{Z}/q\mathbb{Z}} f(a)g(x-a),$$

while for finitely supported functions $f, g : \mathbb{Z} \to \mathbb{C}$, we define the convolution as

$$(f * g)(x) := \sum_{n \in \mathbb{Z}} f(n)g(x-n).$$

3. The Modular Problem

In this section, we prove the following, a (doubly) weighted, quantitative version of the statement that $A + B$ contains a quadratic residue if $A, B \subseteq \mathbb{Z}/q\mathbb{Z}$ have $|A|, |B| > \frac{3}{8}q$.

Theorem 2. *For any $\epsilon > 0$ there is some $c(\epsilon) > 0$ so that for any $q \geq 1$, if $w_A, w_B : \mathbb{Z}/q\mathbb{Z} \to [0,1]$ have $\sum_{t \in \mathbb{Z}/q\mathbb{Z}} w_A(t), \sum_{t \in \mathbb{Z}/q\mathbb{Z}} w_B(t) \geq (\frac{3}{8} + \epsilon)q$, then*

$$\sum_{t \in \mathbb{Z}/q\mathbb{Z}} (w_A * w_B)(t) f_q(t) \geq c(\epsilon) q.$$

In fact, one can take $c(\epsilon) = \frac{1}{\sqrt{5}}\epsilon$.

Our approach is Fourier-analytic. We start by noting the Fourier representation of this weighted count of quadratic residues "in" the convolution of w_A and w_B.

Lemma 3.1. *For any $w_A, w_B : \mathbb{Z}/q\mathbb{Z} \to \mathbb{R}$, we have*

$$\frac{1}{q} \sum_{t \in \mathbb{Z}/q\mathbb{Z}} (w_A * w_B)(t) f_q(t) = \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \widehat{w_A}(m) \widehat{w_B}(m) \widehat{f_q}(-m).$$

Proof. The right hand side is, by definition, equal to

$$\sum_{m \in \mathbb{Z}/q\mathbb{Z}} \frac{1}{q^3} \sum_{x,y,z \in \mathbb{Z}/q\mathbb{Z}} w_A(x) w_B(y) f_q(z) e\left(\frac{m(z-x-y)}{q}\right).$$

Interchanging summations and using the orthogonality condition

$$\sum_{m \in \mathbb{Z}/q\mathbb{Z}} e\left(\frac{mr}{q}\right) = \begin{cases} q & \text{if } r \equiv 0 \bmod q \\ 0 & \text{if } r \not\equiv 0 \bmod q \end{cases}$$

finishes the proof. □

Remark 3.2. Let us take a moment to motivate the arguments to come. Suppose for now q is divisible by 8. We (a posteriori) expect $\sum_{t \in \mathbb{Z}/q\mathbb{Z}} (w_A * w_B)(t) f_q(t)$ to be minimized by weights w_A, w_B that are "lift-ups" of weights $\overline{w}_A, \overline{w}_B : \mathbb{Z}/8\mathbb{Z} \to [0,1]$ in the sense[1] $w_A(t) = \overline{w}_A(t \bmod 8)$ and $w_B(t) = \overline{w}_B(t \bmod 8)$. If w_A and w_B were

[1] Note "mod 8" makes sense since $8 \mid q$.

indeed of this form, then, as one may easily check, we would have $\widehat{w}_A(m), \widehat{w}_B(m) = 0$ for each $m \in \mathbb{Z}/q\mathbb{Z}$ with $\frac{q}{\gcd(q,m)} \nmid 8$. Therefore, in our setting (in which w_A, w_B might not be exactly of that form), it's natural to separate[2],

$$\sum_{m\in\mathbb{Z}/q\mathbb{Z}} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f}_q(-m) = \sum_{q|8m} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f}_q(-m) + \sum_{q\nmid 8m} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f}_q(-m).$$

The latter term we shall upper-bound in magnitude, using that $\widehat{f}_q(-m)$ is small for all m with $q \nmid 8m$ (this follows from quadratic Gauss sum bounds). And the first term actually turns out to be just the weighted count of mod 8 quadratic residues in the weighted sumset of the mod 8 projections of the weight functions w_A, w_B.

For technical reasons, we work mod 24 instead of mod 8.

Lemma 3.3. *Let $q \in \mathbb{N}$ be a multiple of 24. Let $w_A, w_B : \mathbb{Z}/q\mathbb{Z} \to [0,1]$ be two (weight) functions, and let $a, b : \mathbb{Z}/24\mathbb{Z} \to [0,1]$ be the mod 24-projections of w_A, w_B:*

$$a(k) := \frac{1}{q/24} \sum_{\substack{x\in\mathbb{Z}/q\mathbb{Z} \\ x\equiv k \bmod 24}} w_A(x)$$

$$b(k) := \frac{1}{q/24} \sum_{\substack{x\in\mathbb{Z}/q\mathbb{Z} \\ x\equiv k \bmod 24}} w_B(x).$$

Then one has

$$\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z} \\ q|24m}} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f}_q(-m) = \frac{1}{24} \sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a * b)(t) f_{24}(t).$$

Proof. Noting $q \mid 24m$ if and only if $m = \frac{rq}{24}$, we may write the LHS as

$$\sum_{r=0}^{23} \frac{1}{q^3} \sum_{x,y,z\in\mathbb{Z}/q\mathbb{Z}} w_A(x)w_B(y)f_q(z)e\left(\frac{rq}{24}\,\frac{z-x-y}{q}\right),$$

which by orthogonality (mod 24) is equal to

$$\frac{24}{q^3} \sum_{\substack{x,y,z\in\mathbb{Z}/q\mathbb{Z} \\ x+y\equiv z \bmod 24}} w_A(x)w_B(y)f_q(z).$$

Splitting into cases mod 24, we may write the above as

$$(1) \qquad \frac{24}{q^3} \sum_{i,j\in\mathbb{Z}/24\mathbb{Z}} \left(\sum_{\substack{x\in\mathbb{Z}/q\mathbb{Z} \\ x\equiv i \bmod 24}} w_A(x)\right)\left(\sum_{\substack{y\in\mathbb{Z}/q\mathbb{Z} \\ y\equiv j \bmod 24}} w_B(y)\right)\left(\sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z} \\ z\equiv i+j \bmod 24}} f_q(z)\right).$$

[2] Note that $\frac{q}{\gcd(q,m)} \nmid 8$ is equivalent to $q \nmid 8m$.

Noting

$$\sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z}\\ z\equiv i+j \bmod 24}} f_q(z) = \sum_{\substack{z\in\mathbb{Z}/q\mathbb{Z}\\ z\equiv i+j \bmod 24}} \sum_{v\in\mathbb{Z}/q\mathbb{Z}} 1_{v^2\equiv z \bmod q} = \sum_{v\in\mathbb{Z}/q\mathbb{Z}} 1_{v^2\equiv i+j \bmod 24} = \frac{q}{24} f_{24}(i+j),$$

and using the definitions of a, b, we may write (1) as

$$\frac{1}{24^2} \sum_{i,j\in\mathbb{Z}/24\mathbb{Z}} a(i)b(j)f_{24}(i+j) = \frac{1}{24} \sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a*b)(t)f_{24}(t),$$

as desired. □

We now go on to handle the other Fourier term, $\sum_{q\nmid 24m} \widehat{w}_A(m)\widehat{w}_B(m)\widehat{f_q}(-m)$.

Lemma 3.4. *Let $q\in\mathbb{N}$ be a multiple of 24. Then for any $m\in\mathbb{Z}$ with $q\nmid 24m$, one has*

$$\left|\widehat{f_q}(-m)\right| \le \frac{1}{\sqrt{5}}.$$

Proof. By definition,

$$\widehat{f_q}(-m) = \frac{1}{q}\sum_{t\in\mathbb{Z}/q\mathbb{Z}} \left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} 1_{x^2\equiv t}\right) e(\frac{mt}{q}) = \frac{1}{q}\sum_{x\in\mathbb{Z}/q\mathbb{Z}} e\left(\frac{mx^2}{q}\right) = \frac{1}{q/g}\sum_{x\in\mathbb{Z}/\frac{q}{g}\mathbb{Z}} e\left(\frac{\frac{m}{g}x^2}{q/g}\right),$$

where $g := \gcd(m,q)$. Thus, by standard quadratic Gauss sum estimates (e.g., [4]),

$$\left|\widehat{f_q}(-m)\right| \le \begin{cases} \sqrt{\frac{1}{q/g}} & \text{if } q/g \in \{1,3\} \bmod 4 \\ \sqrt{\frac{2}{q/g}} & \text{if } q/g \equiv 0 \bmod 4 \\ 0 & \text{if } q/g \equiv 2 \bmod 4. \end{cases}$$

Now, $q\nmid 24m$ implies $\frac{q}{g}\nmid 24$. This implies, firstly, that $\frac{q}{g}\ge 5$, giving $\sqrt{\frac{1}{q/g}} \le \frac{1}{\sqrt{5}}$, and, secondly, that if $\frac{q}{g}\equiv 0 \bmod 4$, then $\frac{q}{g}\ge 16$, giving $\sqrt{\frac{2}{q/g}} \le \frac{1}{\sqrt{8}} \le \frac{1}{\sqrt{5}}$. □

Lemma 3.5. *Let $q\in\mathbb{N}$ be a multiple of 24. Let $w_A, w_B : \mathbb{Z}/q\mathbb{Z}\to[0,1]$ be two (weight) functions, and let $a, b : \mathbb{Z}/24\mathbb{Z}\to[0,1]$ be the projections of w_A, w_B mod 24 as in Lemma 3.3. Then,*

$$\left|\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f_q}(-m)\right| \le \frac{1}{24\sqrt{5}}\sqrt{\sum_{k\in\mathbb{Z}/24\mathbb{Z}}(a(k)-a(k)^2)}\sqrt{\sum_{k\in\mathbb{Z}/24\mathbb{Z}}(b(k)-b(k)^2)}.$$

Proof. By Lemma 3.4 and Cauchy-Schwarz, we have

$$\begin{aligned}\left|\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} \widehat{w_A}(m)\widehat{w_B}(m)\widehat{f}_q(-m)\right| &\le \left(\sup_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} |\widehat{f}_q(-m)|\right)\left(\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} |\widehat{w_A}(m)|\,|\widehat{w_B}(m)|\right)\\ &\le \frac{1}{\sqrt{5}}\sqrt{\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} |\widehat{w_A}(m)|^2}\sqrt{\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\nmid 24m}} |\widehat{w_B}(m)|^2}.\end{aligned}$$

The following two (in)equalities (and their analogues for B) finish the proof:

$$\begin{aligned}\sum_{\substack{m\in\mathbb{Z}/q\mathbb{Z}\\ q\mid 24m}} |\widehat{w_A}(m)|^2 &= \sum_{r=0}^{23}\frac{1}{q^2}\sum_{x,y\in\mathbb{Z}/q\mathbb{Z}} w_A(x)w_A(y)e\left(\frac{r(x-y)}{24}\right)\\ &= \frac{24}{q^2}\sum_{i\in\mathbb{Z}/24\mathbb{Z}}\left(\sum_{\substack{x\in\mathbb{Z}/q\mathbb{Z}\\ x\equiv i \bmod 24}} w_A(x)\right)^2 = \frac{1}{24}\sum_{k\in\mathbb{Z}/24\mathbb{Z}} a(k)^2.\end{aligned}$$

$$\begin{aligned}\sum_{m\in\mathbb{Z}/q\mathbb{Z}} |\widehat{w_A}(m)|^2 &= \sum_{m\in\mathbb{Z}/q\mathbb{Z}}\frac{1}{q^2}\sum_{x,y\in\mathbb{Z}/q\mathbb{Z}} w_A(x)w_A(y)e\left(\frac{m(x-y)}{q}\right)\\ &= \frac{1}{q}\sum_{x\in\mathbb{Z}/q\mathbb{Z}} w_A(x)^2 \le \frac{1}{q}\sum_{x\in\mathbb{Z}/q\mathbb{Z}} w_A(x) = \frac{1}{24}\sum_{k\in\mathbb{Z}/24\mathbb{Z}} a(k).\end{aligned}$$

□

Combining Lemmas 3.1, 3.3, and 3.5 (and multiplying through by 24) yields

$$\begin{aligned}\frac{24}{q}\sum_{t\in\mathbb{Z}/q\mathbb{Z}}(w_A * w_B)(t)f_q(t) \ge &\sum_{t\in\mathbb{Z}/24\mathbb{Z}}(a*b)(t)f_{24}(t)\\ &-\frac{1}{\sqrt{5}}\sqrt{\sum_{k\in\mathbb{Z}/24\mathbb{Z}}(a(k)-a(k)^2)}\sqrt{\sum_{k\in\mathbb{Z}/24\mathbb{Z}}(b(k)-b(k)^2)}.\end{aligned}\tag{2}$$

Note that $a(k)\in[0,1]$ for each k and that

$$\sum_{k\in\mathbb{Z}/24\mathbb{Z}} a(k) = 24\cdot\frac{1}{q}\sum_{x\in\mathbb{Z}/q\mathbb{Z}} w_A(x),$$

implying $\sum_{k\in\mathbb{Z}/24\mathbb{Z}} a(k) \ge 9+24\epsilon$ if $\sum_{x\in\mathbb{Z}/q\mathbb{Z}} w_A(x) \ge (\frac{3}{8}+\epsilon)q$. We prove the following proposition in Section 5. We assume it to be true for the rest of this section. In it, we use the notation $a(i) := a_i, b(i) := b_i$. We emphasize that it is "merely" a (quadratic) optimization problem in 48 variables.

Proposition 3.6. *For any $\epsilon > 0$, there is some $c'(\epsilon) > 0$ so that the following holds. For all $a_0, \dots, a_{23}, b_0, \dots, b_{23} \in [0,1]$ with $\sum_{i=0}^{23} a_i \geq 9 + \epsilon, \sum_{i=0}^{23} b_i \geq 9 + \epsilon$, one has*

$$\sum_{t \in \mathbb{Z}/24\mathbb{Z}} (a * b)(t) f_{24}(t) \geq c'(\epsilon) + \frac{1}{\sqrt{5}} \sqrt{\sum_i a_i - \sum_i a_i^2} \sqrt{\sum_i b_i - \sum_i b_i^2}.$$

In fact, one can take $c'(\epsilon) = \frac{1}{\sqrt{5}}\epsilon$.

Proof of Theorem 2. If $24 \mid q$, then Theorem 2 follows immediately from (2) and Proposition 3.6 (with $c(\epsilon) = c'(24\epsilon)/24$). Otherwise, we use a simple "lift-up" argument to reduce to the case $q \mid 24$. Define $\widetilde{w}_A, \widetilde{w}_B : \mathbb{Z}/24q\mathbb{Z} \to [0,1]$ by $\widetilde{w}_A(x) := \frac{1}{24} \sum_{\substack{y \in \mathbb{Z}/24\mathbb{Z} \\ y \equiv x \bmod q}} w_A(y), \widetilde{w}_B(x) := \frac{1}{24} \sum_{\substack{y \in \mathbb{Z}/24\mathbb{Z} \\ y \equiv x \bmod q}} w_B(y)$. Then

$$\frac{1}{q} \sum_{t \in \mathbb{Z}/q\mathbb{Z}} (w_A * w_B)(t) f_q(t) = \frac{1}{24q} \sum_{t \in \mathbb{Z}/24q\mathbb{Z}} (\widetilde{w}_A * \widetilde{w}_B)(t) f_{24q}(t)$$

and

$$\frac{1}{24q} \sum_{x \in \mathbb{Z}/24q\mathbb{Z}} \widetilde{w}_A(x) = \frac{1}{q} \sum_{x \in \mathbb{Z}/q\mathbb{Z}} w_A(x)$$

$$\frac{1}{24q} \sum_{x \in \mathbb{Z}/24q\mathbb{Z}} \widetilde{w}_B(x) = \frac{1}{q} \sum_{x \in \mathbb{Z}/q\mathbb{Z}} w_B(x).$$

□

4. Converting to Integers

In this section, we "boost" the solution to the modular problem (Theorem 2) to the integers to establish our main theorem (Theorem 1). For subsets $A, B \subseteq [N]$ with $|A|, |B| \geq (\frac{3}{8} + \epsilon)N$ we shall, as in the modular problem, look at the number of squares in the weighted sumset of A and B:

$$\sum_{n \geq 1} (1_A * 1_B)(n) 1_S(n),$$

where $S \subseteq \mathbb{N}$ is the set of perfect squares, $S := \{m^2 : m \in \mathbb{N}\}$. Our approach is inspired by the arithmetic regularity lemma (see, e.g., [1, 3]), though a much lower-tech version suffices for our purposes; the dependence on the relevant parameters will be singly-exponential rather than tower-type.

Definition 4.1. *Fix (parameters) $Q \in \mathbb{N}$ and $\eta \in \frac{1}{\mathbb{N}}$. For $k \in \{0, 1, \dots, \eta^{-1} - 1\}$, let*

$$I_{\eta,k} = \Big(k\eta N, (k+1)\eta N\Big] \cap \mathbb{N}.$$

For $N \in \mathbb{N}$ (large) and $A \subseteq [N]$, define[3] *the function $w^A_{Q;\eta,k} : I_{\eta,k} \to [0,1]$ by*

$$w^A_{Q;\eta,k}(n) := \frac{\#\{m \in I_{\eta,k} : m \in A \text{ and } m \equiv n \bmod Q\}}{\#\{m \in I_{\eta,k} : m \equiv n \bmod Q\}}.$$

Finally, define the function $w^A_{Q;\eta} : \mathbb{N} \to [0,1]$ by

$$w^A_{Q;\eta} := \sum_{k=0}^{\eta^{-1}-1} w^A_{Q;\eta,k} 1_{I_{\eta,k}}.$$

Remark 4.2. One should think of the function $w^A_{Q;\eta,k}$ as the best mod Q approximation to A, or as a "smoothed out" version of A modulo Q, on $I_{\eta,k}$. Indeed, for $n \in I_{\eta,k}$, the function $w^A_{Q;\eta,k}(n)$ just depends on the residue of n modulo Q, and, immediately from the definition, for any $r \in \{0, \dots, Q-1\}$, one has

$$\sum_{\substack{n \in I_{\eta,k} \\ n \equiv r \bmod Q}} w^A_{Q;\eta,k}(n) = \sum_{\substack{n \in I_{\eta,k} \\ n \equiv r \bmod Q}} 1_A(n). \tag{3}$$

The use of $w^A_{Q;\eta}$ comes from the fact that its Fourier transform models that of A nearly perfectly on rationals with denominator dividing Q. As long as Q is sufficiently composite (which we will choose it to be), we don't need to care much about other rationals, since the Fourier transform of the indicator function of the squares will be sufficiently small there.

For the following lemma, fix $Q, N \in \mathbb{N}, \eta \in \frac{1}{\mathbb{N}}$, and $A \subseteq [N]$.

Definition 4.3. *Define the balanced function $f^A_{Q;\eta} : \mathbb{N} \to \mathbb{R}$ by $f^A_{Q;\eta} := 1_A - w^A_{Q;\eta}$.*

Lemma 4.4. *Take some $a, q \in \mathbb{N}$ with $q \mid Q$. Then, for any $\beta \in \mathbb{R}$, it holds that*

$$\left| \widehat{f^A_{Q;\eta}} \left(\frac{a}{q} + \beta \right) \right| \le 2|\beta|\eta N^2.$$

Proof. For $k \in \{0, \dots, \eta^{-1} - 1\}$, define $f^A_{Q;\eta,k} := f^A_{Q;\eta} 1_{I_{\eta,k}} = 1_{I_{\eta,k}} 1_A - w^A_{Q;\eta,k}$ so that

$$f^A_{Q;\eta} = \sum_{k=0}^{\eta^{-1}-1} f^A_{Q;\eta,k}. \tag{4}$$

Fix $a, q \in \mathbb{N}$ with $q \mid Q$, and fix $\beta \in \mathbb{R}$. By (4), linearity of the fourier transform, and the triangle inequality, to prove Lemma 4.4 it suffices to show

$$\left| \widehat{f^A_{Q;\eta,k}} (\frac{a}{q} + \beta) \right| \le 2|\beta|\eta N |I_{\eta,k}|$$

[3] Extend (the domain of) $w^A_{Q;\eta,k}$ to $\mathbb{N}$ by setting $w^A_{Q;\eta,k} = 0$ outside $I_{\eta,k}$.

for each $k \in \{0, \ldots, \eta^{-1} - 1\}$. So fix some such k. By definition,

$$\widehat{f^A_{Q;\eta,k}}(\frac{a}{q} + \beta) = \sum_{n \in I_{\eta,k}} 1_A(n) e\left((\frac{a}{q} + \beta)n\right) - \sum_{n \in I_{\eta,k}} w^A_{Q;k}(n) e\left((\frac{a}{q} + \beta)n\right). \tag{5}$$

Letting $L = \lfloor k\eta N \rfloor + 1$ denote the left endpoint of $I_{\eta,k}$, we trivially from (5) have

$$\left|\widehat{f^A_{Q;\eta,k}}(\frac{a}{q} + \beta)\right| = \left|\sum_{n \in I_{\eta,k}} 1_A(n) e\left((\frac{a}{q} + \beta)(n - L)\right) - \sum_{n \in I_{\eta,k}} w^A_{Q;\eta,k}(n) e\left((\frac{a}{q} + \beta)(n - L)\right)\right|.$$

The reason for shifting the phase by L is that if we now use

$$\sum_{n \in I_{\eta,k}} 1_A(n) e\left(\frac{a(n-L)}{q}\right) - \sum_{n \in I_{\eta,k}} w^A_{Q;\eta,k}(n) e\left(\frac{a(n-L)}{q}\right) = 0$$

(which follows from (3) and that $q \mid Q$) to write

$$\begin{aligned}\left|\widehat{f^A_{Q;\eta,k}}(\frac{a}{q} + \beta)\right| = \Bigg| &\sum_{n \in I_{\eta,k}} 1_A(n) \left[e\left((\frac{a}{q} + \beta)(n - L)\right) - e\left(\frac{a(n-L)}{q}\right)\right] \\ &- \sum_{n \in I_{\eta,k}} w^A_{Q;\eta,k}(n) \left[e\left((\frac{a}{q} + \beta)(n - L)\right) - e\left(\frac{a(n-L)}{q}\right)\right]\Bigg|,\end{aligned}$$

then the trivial $|e(x) - e(y)| \leq |x - y|$ is strong enough to give the sufficient bound

$$\begin{aligned}\left|\widehat{f^A_{Q;\eta,k}}(\frac{a}{q} + \beta)\right| &\leq \sum_{n \in I_{\eta,k}} 1_A(n)|\beta|(n - L) + \sum_{n \in I_{\eta,k}} |w^A_{Q;\eta,k}(n)|\,|\beta|\,(n - L) \\ &\leq 2|\beta|\eta N|I_{\eta,k}|,\end{aligned}$$

the last inequality using that $n - L \leq \eta N$ for each $n \in I_{\eta,k}$. □

Remark 4.5. The plan to prove Theorem 1 is to decompose

$$1_A * 1_B = w^A_{Q;\eta} * w^B_{Q;\eta} + f^A_{Q;\eta} * w^B_{Q;\eta} + w^A_{Q;\eta} * f^B_{Q;\eta} + f^A_{Q;\eta} * f^B_{Q;\eta}$$

and use Lemma 4.4 to argue that the "number" of squares "in" $1_A * 1_B$ is approximately the same as that in $w^A_{Q;\eta} * w^B_{Q;\eta}$. The latter, involving the convolution of two functions constant on residues modulo Q, is more easily calculable and comes down to the weighted number of mod Q quadratic residues in the convolution of the natural mod Q projections of $w^A_{Q;\eta}, w^B_{Q;\eta}$. The following (with Lemma 4.4) will be used to prove the validity of the approximation.

Proposition 4.6. *Let $f, g : [N] \to [-1,1]$ be (1-bounded) functions. Suppose $\delta > 0$ is such that $\left|\widehat{f}(\frac{a}{q} + \beta)\right| \leq \delta|\beta|N^2$ for each $a, q \leq \lambda^{-2}$ and*[4] *$\beta \in \mathbb{R}$. Then we have*

$$\left|\sum_{n\geq 1}(f * g)(n)1_S(n)\right| \leq 10(\delta\lambda^{-8} + \lambda)N^{3/2}.$$

Proof. We may replace S by $S_{2N} := \{m^2 : m \in \mathbb{N}, m^2 \leq 2N\}$ and write

$$\sum_{n\geq 1}(f * g)(n)1_{S_{2N}}(n) = \int_{\mathbb{T}} \widehat{f}(\theta)\widehat{g}(\theta)\widehat{1_{S_{2N}}}(-\theta)d\theta. \tag{6}$$

We import the needed "minor arc" estimate from [8]:

Lemma 4.7 ([8], Proposition 1)**.** *For any $\lambda > 0$, if $N \in \mathbb{N}$ is sufficiently large and $\theta \in \mathbb{T}$ is such that $|\theta - \frac{a}{q}| > \frac{\lambda^{-2}}{N}$ for each $a, q \leq \lambda^{-2}$, then $|\widehat{1_{S_N}}(\theta)| \leq 5\lambda N^{1/2}$.*

This lemma together with Cauchy-Schwarz and Plancherel immediately gives

$$\begin{aligned}
\left|\int_{\mathfrak{m}} \widehat{f}(\theta)\widehat{g}(\theta)\widehat{1_{S_{2N}}}(-\theta)d\theta\right| &\leq 5\lambda\sqrt{2N}\int_{\mathfrak{m}} |\widehat{f}(\theta)||\widehat{g}(\theta)|d\theta \\
&\leq 10\lambda N^{1/2}\left(\int_{\mathbb{T}} |\widehat{f}(\theta)|^2 d\theta\right)^{1/2}\left(\int_{\mathbb{T}} |\widehat{g}(\theta)|^2 d\theta\right)^{1/2} \\
&= 10\lambda N^{1/2}\left(\sum_{n\leq N} f(n)^2\right)^{1/2}\left(\sum_{n\leq N} g(n)^2\right)^{1/2} \\
&\leq 10\lambda N^{3/2},
\end{aligned}$$

where $\mathfrak{m}$ is defined so that

$$\mathbb{T} \setminus \mathfrak{m} := \bigcup_{q=1}^{\lambda^{-2}} \bigcup_{\substack{1\leq a\leq q \\ (a,q)=1}} \left\{\theta \in \mathbb{T} : \left|\theta - \frac{a}{q}\right| \leq \frac{\lambda^{-2}}{2N}\right\}.$$

Letting $\beta_* = \frac{\lambda^{-2}}{2N}$ for notational ease, we handle the "major arc" as follows:

$$\begin{aligned}
\left|\int_{\mathbb{T}\setminus\mathfrak{m}} \widehat{f}(\theta)\widehat{g}(\theta)\widehat{1_{S_{2N}}}(-\theta)d\theta\right| &\leq \sum_{q=1}^{\lambda^{-2}}\sum_{1\leq a\leq q}\left|\int_{\frac{a}{q}-\beta_*}^{\frac{a}{q}+\beta_*} \widehat{f}(\theta)\widehat{g}(\theta)\widehat{1_{S_{2N}}}(-\theta)d\theta\right| \\
&\leq \sum_{q=1}^{\lambda^{-2}}\sum_{1\leq a\leq q}\int_{-\beta_*}^{\beta_*} \delta|\beta|N^2 N\sqrt{2N}d\beta \\
&\leq \sqrt{2}\delta N^{7/2}\sum_{q=1}^{\lambda^{-2}}\sum_{1\leq a\leq q} 2\beta_*^2 \\
&\leq 10\delta\lambda^{-8}N^{3/2}.
\end{aligned}$$

[4] We will only need the condition for $|\beta| \leq \frac{\lambda^{-2}}{2N}$.

(The bound “10” here is loose and used for simplicity.) We're done by (6). □

To complete the plan outlined in Remark 4.5, we need to argue that $w^A_{Q;\eta} * w^B_{Q;\eta}$ “contains” many squares. We start by focusing on particular intervals. We abstract out from our exact the situation the relevant property of $w^A_{Q;\eta,k}$ and $w^B_{Q;\eta,k}$.

Proposition 4.8. *Fix $\epsilon > 0$ and $Q \geq 1$. Let functions $\overline{w}_1, \overline{w}_2 : \mathbb{Z}/Q\mathbb{Z} \to [0,1]$ satisfy*

$$\sum_{t\in\mathbb{Z}/Q\mathbb{Z}} \overline{w}_i(t) \geq \left(\frac{3}{8}+\epsilon\right) Q$$

for $i = 1,2$. For large $M \in \mathbb{N}$ and intervals $I_i = [k_iM, (k_i+1)M]$, $i = 1,2$, define

$$w_i(n) := 1_{I_i}(n)\overline{w}_i(n \bmod Q)$$

for $i = 1,2$. Then we have the lower bound

$$\sum_{n\geq 1}(w_1 * w_2)(n)1_S(n) \geq \frac{1}{200}c(\epsilon)\frac{M^{3/2}}{\sqrt{k_1+k_2}},$$

where $c(\epsilon) > 0$ is the constant guaranteed by Theorem 2.

Proof. Let

$$J = \left[(k_1+k_2+1)M - \frac{1}{10}M, (k_1+k_2+1)M + \frac{1}{10}M\right]$$

so that for any $n \in J$ and $a \in \{0,\ldots,Q-1\}$, it holds that

$$\#\left\{m \in I_1 : m \equiv a \bmod Q \text{ and } n-m \in I_2\right\} \geq \frac{1}{10}\frac{M}{Q}$$

(provided M is large enough). Therefore,

$$\begin{aligned}\sum_{n\geq 1}(w_1 * w_2)(n)1_S(n) &\geq \sum_{n\in J}\sum_{\substack{m\in I_1\\ n-m\in I_2}} w_1(m)w_2(n-m)1_S(n)\\ &= \sum_{\substack{n\in J\\ n\in S}}\sum_{a=0}^{Q-1}\overline{w}_1(a)\overline{w}_2(n-a \bmod Q)\sum_{\substack{m\equiv a \bmod Q\\ m\in I_1\\ n-m\in I_2}} 1\\ &\geq \frac{M}{10Q}Q\sum_{\substack{n\in J\\ n\in S}}(\overline{w}_1 * \overline{w}_2)(n \bmod Q)\\ &= \frac{M}{10}\sum_{t=0}^{Q-1}(\overline{w}_1 * \overline{w}_2)(t)\cdot\#\{m \in \mathbb{N} : m^2 \in J,\, m^2 \equiv t \bmod Q\}.\end{aligned}$$

Note that, for $\overline{J} := \{m \in \mathbb{N} : m^2 \in J\}$, we have as $M \to \infty$ that

$$\#\{m \in \mathbb{N} : m^2 \in J,\, m^2 \equiv t \bmod Q\} = (1 + o(1))\, f_Q(t) \frac{|\overline{J}|}{Q}.$$

We lower-bound

$$\begin{aligned}
|\overline{J}| &\geq \frac{1}{2}\left(\sqrt{(k_1 + k_2 + 1)M + \frac{1}{10}M} - \sqrt{(k_1 + k_2 + 1)M - \frac{1}{10}M}\right) \\
&= \frac{1}{2}\frac{\frac{2}{10}M}{\sqrt{(k_1 + k_2 + 1)M + \frac{1}{10}M} + \sqrt{(k_1 + k_2 + 1)M - \frac{1}{10}M}} \\
&\geq \frac{1}{2}\frac{\frac{1}{10}M}{\sqrt{(k_1 + k_2)M}}.
\end{aligned}$$

Combining everything, we obtain

$$\sum_{n \geq 1} (w_1 * w_2)(n) 1_S(n) \geq \frac{M}{10Q}\frac{\sqrt{M}}{20\sqrt{k_1 + k_2}} \sum_{t=0}^{Q-1} (\overline{w}_1 * \overline{w}_2)(t) f_Q(t).$$

By the assumptions of the current theorem, Theorem 2 finishes the proof. □

Back to our specific setting, we can now handle $w^A_{Q;\eta} * w^B_{Q;\eta}$.

Proposition 4.9. *Fix $\epsilon > 0, Q \in \mathbb{N}$, and $\eta \in \frac{1}{\mathbb{N}}$. Then for all large $N \in \mathbb{N}$ and any $A, B \subseteq [N]$ with $|A|, |B| \geq (\frac{3}{8} + \epsilon)N$, we have*

$$\sum_{n \geq 1} (w^A_{Q;\eta} * w^B_{Q;\eta})(n) 1_S(n) \geq \frac{\epsilon^2}{5000} c\left(\frac{\epsilon}{2}\right) N^{3/2},$$

where $c(\epsilon) > 0$ is the constant guaranteed by Theorem 2.

Proof. It is easy to see that $|A| \geq (\frac{3}{8} + \epsilon)N$ implies there are at least $\frac{\epsilon}{3}\eta^{-1}$ values of $k \in \{0, \ldots, \eta^{-1} - 1\}$ with $|A \cap I_{\eta,k}| \geq (\frac{3}{8} + \frac{3\epsilon}{4})|I_{\eta,k}|$. Therefore, by taking N large enough, if we let[5]

$$J^A := \left\{ k \in \{0, \ldots, \eta^{-1} - 1\} : \sum_{n = \lfloor k\eta N \rfloor + 1}^{\lfloor k\eta N \rfloor + Q} w^A_{Q;\eta,k}(n) \geq \left(\frac{3}{8} + \frac{\epsilon}{2}\right) Q \right\},$$

[5] The choice of summing n over $[\lfloor k\eta N \rfloor + 1, \lfloor k\eta N \rfloor + Q]$ is arbitrary; any Q numbers in $I_{\eta,k}$, all distinct modulo Q, would of course be equivalent.

then we have $|J^A| \geq \frac{\epsilon}{4}\eta^{-1}$. Defining J^B in the analogous way, we by symmetry have $|J^B| \geq \frac{\epsilon}{4}\eta^{-1}$. The point is that Proposition 4.8 (with $M = \eta N$) then lets us bound

$$\begin{aligned}
\sum_{n\geq 1}(w^A_{Q;\eta} * w^B_{Q;\eta})(n)1_S(n) &= \sum_{k_1,k_2=0}^{\eta^{-1}-1}\sum_{n\geq 1}(w^A_{Q;\eta,k_1} * w^B_{Q;\eta,k_2})(n)1_S(n)\\
&\geq \sum_{\substack{k_1\in J^A\\ k_2\in J^B}}\sum_{n\geq 1}(w^A_{Q;\eta,k_1} * w^B_{Q;\eta,k_2})(n)1_S(n)\\
&\geq \sum_{\substack{k_1\in J^A\\ k_2\in J^B}}\frac{1}{200}c\left(\frac{\epsilon}{2}\right)\frac{(\eta N)^{3/2}}{\sqrt{k_1+k_2}}\\
&\geq \frac{1}{200}c\left(\frac{\epsilon}{2}\right)\frac{(\eta N)^{3/2}}{\sqrt{2\eta^{-1}}}|J^A||J^B|.
\end{aligned}$$

The proof is complete by inserting the lower bounds $|J^A|, |J^B| \geq \frac{\epsilon}{4}\eta^{-1}$. □

We now put everything together to obtain (a more quantitative version of) our main theorem.

Theorem 1. *For any $\epsilon > 0$, if N is sufficiently large and $A, B \subseteq [N]$ have $|A|, |B| \geq (\frac{3}{8}+\epsilon)N$, then $A + B$ contains a perfect square. In fact, we have the quantitative*

$$\#\{(a,b) \in A \times B : a + b \in S\} \geq 10^{-6}\epsilon^3 N^{3/2}.$$

Proof. Let $\eta \in \frac{1}{\mathbb{N}}, \overline{Q} \in \mathbb{N}$ be parameters (based on ϵ) to be determined, and set $Q := \mathrm{lcm}(1, \dots, \overline{Q})$. Take N sufficiently large and $A, B \subseteq [N]$ with $|A|, |B| \geq (\frac{3}{8}+\epsilon)N$. As remarked earlier, we decompose

$$1_A * 1_B = w^A_{Q;\eta} * w^B_{Q;\eta} + f^A_{Q;\eta} * w^B_{Q;\eta} + w^A_{Q;\eta} * f^B_{Q;\eta} + f^A_{Q;\eta} * f^B_{Q;\eta}.$$

Proposition 4.9 gives

$$\sum_{n\geq 1}(w^A_{Q;\eta} * w^B_{Q;\eta})(n)1_S(n) \geq \frac{\epsilon^2}{5000}c\left(\frac{\epsilon}{2}\right)N^{3/2},$$

and Proposition 4.6 together with Lemma 4.4 gives

$$\left|\sum_{n\geq 1}(f^A_{Q;\eta} * w^B_{Q;\eta})(n)1_S(n)\right| \leq 10\left(2\eta\overline{Q}^4 + \overline{Q}^{-1/2}\right)N^{3/2},$$

and the same bound for the analogous inequalities involving $w^A_{Q;\eta} * f^B_{Q;\eta}$ and $f^A_{Q;\eta} * f^B_{Q;\eta}$. Therefore,

$$\sum_{n\geq 1}(1_A * 1_B)(n)1_S(n) \geq \frac{\epsilon^2}{5000}c\left(\frac{\epsilon}{2}\right)N^{3/2} - 30\left(2\eta\overline{Q}^4 + \overline{Q}^{-1/2}\right)N^{3/2}.$$

Setting $\eta = \overline{Q}^{-9/2}$ and using $c(\epsilon) \geq \epsilon/3$, we obtain

$$\sum_{n\geq 1}(1_A * 1_B)(n)1_S(n) \geq \left(\frac{\epsilon^3}{30000} - 90\overline{Q}^{-1/2}\right) N^{3/2}.$$

Choosing $\overline{Q}$ a perfect square (merely so that $\eta \in \frac{1}{\mathbb{N}}$) with $\overline{Q}^{-1/2} \leq 10^{-7}\epsilon^3$, say, finishes the proof. □

5. Solving the Optimization Problem

We finish the paper by proving the inequality that Theorem 2 relied upon. It could be verified directly by a computer but would take quite a bit of time.

For $a_0, \ldots, a_{23} \in [0,1]$, we let $a : \mathbb{Z}/24\mathbb{Z} \to [0,1]$ be given by $a(i) = a_i$. Recall, for $a, b \in \mathbb{Z}/24\mathbb{Z}$ and $t \in \mathbb{Z}/24\mathbb{Z}$, we define

$$(a * b)(t) := \frac{1}{24}\sum_{i\in\mathbb{Z}/24\mathbb{Z}} a(i)b(t-i)$$

$$f_{24}(t) := \#\{j \in \mathbb{Z}/24\mathbb{Z} : j^2 \equiv t \bmod 24\}.$$

In this section, we prove the following, stated previously in Section 3.

Proposition 3.6. For any $\epsilon > 0$, there is some $c'(\epsilon) > 0$ so that the following holds. For all $a_0, \ldots, a_{23}, b_0, \ldots, b_{23} \in [0,1]$ with $\sum_{i=0}^{23} a_i \geq 9 + \epsilon, \sum_{i=0}^{23} b_i \geq 9 + \epsilon$, we have

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a * b)(t) f_{24}(t) \geq c'(\epsilon) + \frac{1}{\sqrt{5}}\sqrt{\sum_i a_i - \sum_i a_i^2}\sqrt{\sum_i b_i - \sum_i b_i^2}.$$

In fact, one can take $c'(\epsilon) = \frac{1}{\sqrt{5}}\epsilon$.

The proof, with $c'(\epsilon) = \frac{1}{\sqrt{5}}\epsilon$, will follow from the proof of the "$\epsilon = 0$" case, in which we also identify the extremizers. We say a is a *lift-up* of a subset A of $\mathbb{Z}/8\mathbb{Z}$ if: $a_i = 1$ if and only if $i \bmod 8 \in A$, and $a_i = 0$ otherwise.

Proposition 5.1. *For all $a_0, \ldots, a_{23}, b_0, \ldots, b_{23} \in [0,1]$ with $\sum_{i=0}^{23} a_i \geq 9, \sum_{i=0}^{23} b_i \geq 9$, we have*

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a * b)(t) f_{24}(t) \geq \frac{1}{\sqrt{5}}\sqrt{\sum_i a_i - \sum_i a_i^2}\sqrt{\sum_i b_i - \sum_i b_i^2}$$

with equality if and only if there is some $x \in \mathbb{Z}/8\mathbb{Z}$ so that a, b are lift-ups of $\{0,1,5\} + x, \{2,5,6\} - x \subseteq \mathbb{Z}/8\mathbb{Z}$.

We prove Proposition 5.1 by first massaging the desired inequality into a homogeneous quadratic form. It is of course easy to check the "if" implication of the equality part of Proposition 5.1; the "only if" direction will follow from equality needing to hold at each step of the proof and equality holding only for the claimed extremizers at the end of the proof.

By the arithmetic-geometric inequality, it suffices to show

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a*b)(t)f_{24}(t) \geq \frac{1}{2\sqrt{5}}\left(\sum_i a_i - \sum_i a_i^2 + \sum_i b_i - \sum_i b_i^2\right)$$

for all $a_i, b_i \in [0,1]$ with $\sum_i a_i, \sum_i b_i \geq 9$. Since[6] $\frac{2}{9}xy \geq x+y$ if $x, y \geq 9$, it suffices to show

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a*b)(t)f_{24}(t) \geq \frac{1}{2\sqrt{5}}\left(\frac{2}{9}(\sum_i a_i)(\sum_i b_i) - \sum_i a_i^2 - \sum_i b_i^2\right)$$

for all $a_i, b_i \in [0,1]$ with $\sum_i a_i, \sum_i b_i \geq 9$. Of course it then suffices to prove the inequality for any non-negative reals a_i, b_i.

Proposition 5.2. *For any $a_0, b_0, \ldots, a_{23}, b_{23} \in [0,\infty)$ one has*

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a*b)(t)f_{24}(t) \geq \frac{1}{2\sqrt{5}}\left(\frac{2}{9}(\sum_i a_i)(\sum_i b_i) - \sum_i a_i^2 - \sum_i b_i^2\right).$$

We will present a proof of Proposition 5.2 due to Fedor Nazarov. The (quite ingenious) proof significantly reduces the computational power needed.

Proof.

Step 1: Reduction to a norm inequality in a single (non-negative) variable.

Using that

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (a*b)(t)f_{24}(t) = \sum_{t\in\mathbb{Z}/24\mathbb{Z}} (\widetilde{a}*f_{24})(t)b(t),$$

where $\widetilde{a}(i) := a(-i)$ and

$$\left(\sum_i a_i\right)\left(\sum_i b_i\right) = 24\sum_{t\in\mathbb{Z}/24\mathbb{Z}} (\widetilde{a}*\mathbb{1})(t)b(t),$$

where $\mathbb{1} : \mathbb{Z}/24\mathbb{Z} \to [0,1]$ is the constant function $\equiv 1$, we wish to prove

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} \left(\widetilde{a}*(\frac{16}{3}\mathbb{1} - 2\sqrt{5}f_{24})\right)(t)\, b(t) \leq \sum_{t\in\mathbb{Z}/24\mathbb{Z}} \left[a(t)^2 + b(t)^2\right].$$

[6] If $x, y \geq 9+\epsilon$, then $\frac{2}{9}xy \geq x+y+2\epsilon$, which is why $c'(\epsilon) := \frac{1}{\sqrt{5}}\epsilon$ suffices.

We may, of course, ignore the distinction between a and $\widetilde{a}$, so we drop the $\widetilde{\ }$ from here on[7]. Since $2xy \le x^2 + y^2$ for all $x, y \in \mathbb{R}$, it suffices to show

$$\sum_{t\in\mathbb{Z}/24\mathbb{Z}} \left(a * (\frac{16}{3}\mathbb{1} - 2\sqrt{5}f_{24})\right)(t)\; b(t) \le 2\left(\sum_{t\in\mathbb{Z}/24\mathbb{Z}} a(t)^2\right)^{1/2}\left(\sum_{t\in\mathbb{Z}/24\mathbb{Z}} b(t)^2\right)^{1/2},$$

which we write more compactly as

$$\langle a * \varphi, b\rangle \le 2\|a\|_2\|b\|_2,$$

with $\varphi := \frac{16}{3}\mathbb{1} - 2\sqrt{5}f_{24}$. Since $b(t) \ge 0$ for each t, it suffices to prove

$$\Big\langle (a*\varphi)_+, b\Big\rangle \le 2\|a\|_2\|b\|_2.$$

By Cauchy-Schwarz, it then suffices to prove

$$\|(a*\varphi)_+\|_2 \le 2\|a\|_2$$

for each $a : \mathbb{Z}/24\mathbb{Z} \to [0,\infty)$.

Step 2: Showing the maximizer is an eigenvector of a related operator.

By compactness, let $a = \widehat{a}$ be a maximizer of $\|(a*\varphi)_+\|_2$ subject to $\|a\|_2 = 1$ and $a \ge 0$ (pointwise). Let $\widehat{\sigma} : \mathbb{Z}/24\mathbb{Z} \to \mathbb{R}$ satisfy $|\widehat{\sigma}(t)| < \widehat{a}(t)$ whenever $\widehat{a}(t) > 0$ (think $\widehat{\sigma} \to 0$). Then

$$\begin{aligned}\left\|((\widehat{a}+\widehat{\sigma})*\varphi)_+\right\|_2^2 - \|(\widehat{a}*\varphi)_+\|_2^2 &= \sum_{t\in\mathbb{Z}/24\mathbb{Z}}\left[\Big((\widehat{a}*\varphi)(t) + (\widehat{\sigma}*\varphi)(t)\Big)_+^2 - \Big((\widehat{a}*\varphi)(t)\Big)_+^2\right]\\ &= 2\sum_{t\in\mathbb{Z}/24\mathbb{Z}}\Big((\widehat{a}*\varphi)(t)\Big)_+(\widehat{\sigma}*\varphi)(t) + O\left(\|\widehat{\sigma}\|^2\right)\\ &= 2\Big\langle(\widehat{a}*\varphi)_+\,,\,\widehat{\sigma}*\varphi\Big\rangle + O\left(\|\widehat{\sigma}\|^2\right)\\ &= 2\Big\langle(\widehat{a}*\varphi)_+ * \widetilde{\varphi}\,,\,\widehat{\sigma}\Big\rangle + O\left(\|\widehat{\sigma}\|^2\right),\end{aligned}$$

where the second equality used the fact that $(x+y)_+^2 - x_+^2 = 2yx_+ + O(y^2)$ for any reals x, y with $|y| < |x|$, and in the last equality, we again use the notation $\widetilde{\varphi}(\cdot) := \varphi(-\cdot)$. Let $\widehat{v} : \mathbb{Z}/24\mathbb{Z} \to \mathbb{R}$ be $\widehat{v} := (\widehat{a}*\varphi)_+ * \widetilde{\varphi}$ so that

$$\left\|((\widehat{a}+\widehat{\sigma})*\varphi)_+\right\|_2^2 - \|(\widehat{a}*\varphi)_+\|_2^2 = 2\langle\widehat{v},\widehat{\sigma}\rangle + O\left(\|\widehat{\sigma}\|^2\right).$$

We see that no $t \in \mathbb{Z}/24\mathbb{Z}$ can satisfy $\widehat{a}(t) = 0$ and $\widehat{v}(t) > 0$, for otherwise we could let $\widehat{\sigma}(t) = +\alpha$ for some (very) small $\alpha > 0$, $\widehat{\sigma}(t') = -\delta$ for some t' with $\widehat{a}(t') > 0$ and appropriate $\delta > 0$ (which will be $O(\alpha^2)$), and $\widehat{\sigma} = 0$ elsewhere, to have

$$||\widehat{a}+\widehat{\sigma}||_2 = 1 \quad\text{and}\quad \left\|((\widehat{a}+\widehat{\sigma})*\varphi)_+\right\| > \left\|(\widehat{a}*\varphi)_+\right\|,$$

[7] However, the reader should keep in mind that we are "mirroring" the extremizers.

contradicting the maximality of $\widehat{a}$. And similarly no $t \in \mathbb{Z}/24\mathbb{Z}$ can satisfy $\widehat{a}(t) > 0$ and $\widehat{v}(t) \le 0$. Therefore, $\widehat{v}_+$ is positive exactly when $\widehat{a}$ is, and each are 0 otherwise. This implies

$$\widehat{v}_+ \equiv \lambda \widehat{a}$$

for some $\lambda > 0$, for otherwise one could make $2\langle \widehat{v}, \widehat{\sigma} \rangle + O(\|\widehat{\sigma}\|^2)$ negative for suitable small $\widehat{\sigma}$, contradicting the maximality of $\widehat{a}$. To end this step, quickly note

$$\begin{aligned} \|(\widehat{a} * \varphi)_+\|_2^2 &= \Big\langle (\widehat{a} * \varphi)_+, (\widehat{a} * \varphi)_+ \Big\rangle \\ &= \Big\langle (\widehat{a} * \varphi)_+, \widehat{a} * \varphi \Big\rangle \\ &= \langle \widehat{v}, \widehat{a} \rangle \\ &= \langle \widehat{v}_+, \widehat{a} \rangle \\ &= \lambda. \end{aligned} \tag{7}$$

Step 3: Choosing a convenient norm.

We are given $\widehat{a} : \mathbb{Z}/24\mathbb{Z} \to [0, \infty)$ satisfying

$$((\widehat{a} * \varphi)_+ * \widetilde{\varphi})_+ \equiv \lambda \widehat{a}$$

and, by (7), we wish to show $\lambda \le 4$. It suffices to find a function ("norm") $N : [0, \infty)^{\mathbb{Z}/24\mathbb{Z}} \to [0, \infty)$ satisfying the multiplicativity condition

$$N(\gamma a) = \gamma N(a) \tag{8}$$

for all $\gamma \in [0, \infty)$ and $a : \mathbb{Z}/24\mathbb{Z} \to [0, \infty)$, and the two (dual) norm bounds

$$N\left((a * \varphi)_+\right) \le 2N(a) \tag{9}$$

$$N\left((a * \widetilde{\varphi})_+\right) \le 2N(a) \tag{10}$$

for all $a : \mathbb{Z}/24\mathbb{Z} \to [0, \infty)$. Indeed, with such a norm N, we have

$$\lambda N(\widehat{a}) = N(\lambda \widehat{a}) = N\Big(((\widehat{a} * \varphi)_+ * \widetilde{\varphi})_+ \Big) \le 2N\Big((\widehat{a} * \varphi)_+ \Big) \le 4N(\widehat{a}).$$

Motivated by the (conjectured) extremizers, we use the norm

$$N(a) := \max\left(9\|a\|_\infty, \|a\|_1\right).$$

Step 4: Showing the desired norm bounds.

It is clear that N satisfies condition (8). To prove (9), we may normalize to $N(a) = 9$ so that it suffices to show

$$\left\{ \begin{array}{c} \|a\|_\infty \le 1 \\ \|a\|_1 \le 9 \end{array} \right\} \implies \left\{ \begin{array}{c} \|(a * \varphi)_+\|_\infty \le 2 \\ \|(a * \varphi)_+\|_1 \le 18 \end{array} \right\},$$

where, to recall,

$$\varphi = \frac{16}{3}\mathbb{1} - 2\sqrt{5} f_{24}.$$

So take $a : \mathbb{Z}/24\mathbb{Z} \to [0, \infty)$ with $\|a\|_\infty \leq 1$ and $\|a\|_1 \leq 9$. Then we easily have

$$\|(a * \varphi)_+\|_\infty \leq \max_{t \in \mathbb{Z}/24\mathbb{Z}} \frac{1}{24} \sum_{j \in \mathbb{Z}/24\mathbb{Z}} a(j)\varphi(t-j) \leq \frac{1}{24} \cdot \frac{16}{3} \cdot 9 = 2.$$

As $a \mapsto \|(a * \varphi)_+\|_1$ is convex, it simply suffices to check that $\|(a * \varphi)_+\|_1 \leq 18$ for all $a \in \{0,1\}^{24} \subseteq [0,1]^{\mathbb{Z}/24\mathbb{Z}}$. We may assume WLOG that $a_0 = 1$, so that there are only $\sum_{k=0}^{8} \binom{23}{k} < 10^6$ cases to check, which is easily handled by a computer.

We do everything analogous to establish (10) as well.

Below is the python code, presented in two columns to save space.

```
import math
import itertools

f = []
for t in range(0,24):
    sum1 = 0
    for j in range(0,24):
        if ((j*j)%24 == t):
            sum1 = sum1+1
    f.append(sum1)
phi = []
for t in range(0,24):
    phi.append(16/3-2*math.sqrt(5)*f[t])
phit = []
for t in range(0,24):
    phit.append(phi[23-t])

def h(a,psi):
    sum1 = 0
    for t in range(0,24):
        sum2 = 0
        for j in range(0,24):
            sum2=sum2+a[j]*psi[(t-j)%24]
        sum2 = sum2/24
        sum2 = max(sum2,0)
        sum1 = sum1+sum2
    return sum1
```

```
c = []
for j in range(1,24):
    c.append(j)
max1 = 0
max2 = 0
for k in range(0,9):
    for A in itertools.combinations(c,k):
        A = list(A)
        A.insert(0,0)
        a = []
        for j in range(0,24):
            if (j in A):
                a.append(1)
            else:
                a.append(0)
        v1 = h(a,phi)
        v2 = h(a,phit)
        max1 = max(max1,v1)
        max2 = max(max2,v2)
        if (v1 >= 17.99):
            print ("extremizer - "+str(a))
        if (v2 >= 17.99):
            print ("extremizer for dual - "+str(a))
print (max1)
print (max2)
```

The output of the python code is as follows.

```
extremizer - [1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0]
extremizer for dual - [1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0]
extremizer for dual - [1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0]
extremizer - [1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1]
extremizer - [1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0]
extremizer for dual - [1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1]
18.000000000000004
18.000000000000004
```

Since we printed all a for which $\|(a * \varphi)_+\|_1, \|(a * \widetilde{\varphi})_+|_1 \geq 17.99$ and the ones printed have $\|(a * \varphi)_+\|_1, \|(a * \widetilde{\varphi})_+\|_1 = 18$, the $+4 \cdot 10^{-15}$ (added to 18) is merely a computer-induced rounding error.

We finish by analyzing the extremizers. We obtained only 3 of the 8 conjectured extremizers; however, we assumed WLOG that $a_0 = 1$. Translating the outputted extremizers indeed recovers all 8 conjectured extremizers for a. Since such a have $\sum_i a_i - \sum_i a_i^2 = 0$, the only extremizing b, for a given a, must satisfy $\sum_t (a * b)(t) f_{24}(t) = 0$, i.e., $a+b$ "contains" no squares. Since all extremizers a are translates of one another, we may focus on a particular extremizer a. Then, as is easily checked, b is uniquely determined merely by "process of elimination". □

6. Acknowledgments

I would like to thank my advisor Ben Green for suggesting this problem to me and Fedor Nazarov for nearly solving the optimization problem by hand.

References

[1] S. Eberhard. The abelian arithmetic regularity lemma. Expository note, available on arXiv:1606.09303.

[2] P. Erdős, R.L. Graham. Old and new problems and results in combinatorial number theory. In *Monographs Enseign. Math., No. 28, University of Geneva, 1980.*

[3] B. Green, T. Tao. An arithmetic regularity lemma, an associated counting lemma, and applications. In *An irregular mind, volume 21 of Bolyai Soc. Math. Stud., pages 261–334. János Bolyai Math. Soc., Budapest, 2010.*

[4] K. Ireland, M. Rosen. A Classical Introduction to Modern Number Theory. In *Springer-Verlag. ISBN 0-387-97329-X, 1990.*

[5] A.Khalfalah, S. Lodha, and E. Szemerédi. Tight bound for the density of sequence of integers the sum of no two of which is a perfect square. In *Discrete mathematics 256.1, 243-255, 2002.*

[6] J.P.Lagarias, A.M. Odlyzko, and J.B. Shearer. On the density of sequences of integers the sum of no two of which is a square. I. Arithmetic progressions. In *Journal of Combinatorial Theory, Series A, 33, 167-185, 1982.*

[7] J.P.Lagarias, A.M. Odlyzko, and J.B. Shearer. On the density of sequences of integers the sum of no two of which is a square. II. General sequences. In *Journal of Combinatorial Theory, Series A, 34, 123-139, 1983.*

[8] N. Lyall. A new proof of Sárközy's theorem. In *Proc. Amer. Math. Soc. 141, 2253-2264, 2013.*

[9] J.P. Massias. Sur les suites dont les sommes des terms deux a deux ne sont pas des carrés. In *Publications du Département de Mathématiques de Limoges, 1982.*

Mathematical Institute, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK
E-mail address: zachary.chase@maths.ox.ac.uk