A NEW PROOF OF SÁRKÖZY’S THEOREM

NEIL LYALL

(Communicated by Michael T. Lacey)

Dedicated to Steve Wainger on the occasion of his retirement

Abstract. It is a striking and elegant fact (proved independently by Furstenberg and Sárközy) that in any subset of the natural numbers of positive upper density there necessarily exist two distinct elements whose difference is given by a perfect square. In this article we present a new and simple proof of this result by adapting an argument originally developed by Croot and Sisask to give a new proof of Roth’s theorem.

1. Introduction

Let $D(N)$ denote the maximum size of a subset of $\{1, \ldots, N\}$ that contains no perfect (non-zero) square differences. In other words, $D(N)$ is the threshold such that if $A \subseteq \{1, \ldots, N\}$ with $|A| > D(N)$, then the set $A$ will necessarily contain two distinct elements whose difference is a perfect square.

In this note we shall be concerned with the behavior of this quantity for large values of $N$ and at the outset we encourage readers to convince themselves of the essentially trivial upper and lower bounds for $D(N)$ of approximate quality $N/4$ and $\sqrt{N}$ respectively, and furthermore that any improvements on these bounds would be less than trivial to achieve. In Appendix B we give full justification for the following specific bounds:

$$\sqrt{N} - 1 \leq D(N) \leq (N + 543443)/4.$$  

It was conjectured by Lovász that $D(N) \leq \delta N$ for any $\delta > 0$, provided that $N$ is sufficiently large, or equivalently that in any subset of the natural numbers of positive upper density there necessarily exist two distinct elements (and hence infinitely many pairs of distinct elements) whose difference is given by a perfect square. This conjecture was subsequently proven to be correct, independently, by Sárközy and Furstenberg.

Theorem 1 (Sárközy [17]/Furstenberg [3]).

$$\lim_{N \to \infty} D(N)/N = 0.$$  

The purpose of this note is to give a new and simple proof of this result by adapting an argument that was originally developed by Croot and Sisask [2] to give...
a new proof of Roth’s theorem on three-term arithmetic progressions. In particular
we will establish the following result, which clearly implies Theorem 1.

**Theorem 2.** Let $M, N \in \mathbb{N}$. Then

$$\frac{D(N)}{N} \leq \frac{3}{4} \frac{D(M)}{M},$$

provided $N \geq e^{CM^7}$, for some absolute constant $C > 0$, and $M$ is sufficiently large.

**Remark on quantitative bounds.** Although its proof is simple, Theorem 2 patently
leads to quantitative upper bounds of the quantity $N/\log^* N$ for $D(N)$ that are
extremely weak in comparison to the current best known upper bound, namely

$$D(N) \leq CN/(\log N)^{\frac{1}{4}\log \log \log \log N}$$

for some absolute constant $C > 0$, which was established by Pintz, Steiger and
Szemerédi in [15] using an ingenious and intricate Fourier analytic argument. For
extremely readable accounts of easier arguments leading to intermediate bounds
of the quantities $N/(\log \log N)^{1/11}$ and $N\log \log N/\log N$, see Green [4] and Lyall
and Magyar [13], respectively.

We further note that it is conjectured that $D(N) \geq N^{1-\varepsilon}$ for any $\varepsilon > 0$, provided
$N$ is sufficiently large (with respect to $\varepsilon$), and that Ruzsa [16] has demonstrated
this conjecture to be true for all $\varepsilon \geq 0.267$.

**Remark on other polynomial differences.** At this point the reader is presumably
curious to know what is so special about square differences. The following theorem
gives a complete answer to this question.

**Theorem 3** (Kamae and Mendès France [8]). Let $f \in \mathbb{Z}[n]$ and let $D_f(N)$ denote
the maximum size of a subset of $\{1, \ldots, N\}$ that contains no two distinct elements
whose difference is given by $f(n)$ for some $n \in \mathbb{Z}$. Then,

$$\lim_{N \to \infty} \frac{D_f(N)}{N} = 0$$

if and only if $f$ is an intersective polynomial, namely if $f$ has a root modulo $q$ for
every $q \geq 2$.

The approach of Kamae and Mendès France in [8] was indirect and gave no
quantitative bounds for $D_f(N)$, and while the methods of Pintz, Steiger and Sze-
merédi were later extended by Balog, Pelikán, Pintz and Szemerédi [1] to establish
the quantitative bounds

$$D_{nk}(N) \leq C_k N/(\log N)^{v \log \log \log \log N}$$

for any integer $k \geq 2$, the current best known upper bounds for general intersective
polynomials $f \in \mathbb{Z}[n]$ are due to Lucier [10], who showed that

$$D_f(N) \leq C_f N \left( \frac{(\log \log N)^{\mu}}{\log N} \right)^{1/(k-1)},$$

where $k = \deg(f)$ and $\mu = 3$ if $k = 2$ and $\mu = 2$ if $k \geq 3$. However, bounds of the
same quality as [11] have recently been obtained for general intersective quadratic
polynomials by Hamel, Lyall and Rice in [7].

2 Recall that $\log^* N$ is the height required for a tower of 2’s to exceed $N$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The methods used to prove Theorem 2 can in fact be extended using some (rather technical) additional results of Lucier to also establish Theorem 3; these arguments will appear elsewhere.

A result almost as general as Theorem 3, namely that (3) holds whenever $f$ is a polynomial in $\mathbb{Z}[n]$ with at least one integer root, follows in a more straightforward manner using the same methods as those used in the proof of Theorem 2; see [10] (a preliminary online version of this current paper) for a brief outline of how to extend the proof of Theorem 2 in this direction. For the current best known upper bounds for this class of polynomials, see [11] and [12].

In this note we shall focus exclusively on the case of square differences and proving Theorem 2.

2. Proof of Theorem 2

Let $A \subseteq \{1, \ldots, N\}$ with no square differences and $|A| = D(N)$. Key to the argument we present is to construct, from this extremal set $A$, a new set $B \subseteq \{1, \ldots, N\}$ with the following properties:

(i) $|B| \geq \frac{5}{3}|A|$.

(ii) # of square differences in $B \leq \frac{C_0}{\sqrt{\log N}} N^{3/2}$, for some absolute constant $C_0 > 0$.

This construction, which will amount to defining $B$ to be $A \cup (A + t^2)$ for some appropriate (large) value of $t$, will be carried out in Section 2.2 below. Having constructed a set with such properties we will then establish Theorem 2 by combining this with the following lower bound on the number of square differences contained in any given set $B \subseteq \{1, \ldots, N\}$.

Lemma 1. Given any $B \subseteq \{1, \ldots, N\}$ and $1 \leq M \leq N$,

$$\text{# of square differences in } B \geq \left(\frac{|B|/N - (D(M) + 2)/M}{M^{5/2}}\right) N^{3/2}.$$ 

The proof of this result is a straightforward exercise using ideas that were first exploited by Varnavides [18] in the context of counting three-term arithmetic progressions. While, in our context of counting square differences, this quantitative result can easily be deduced by adapting the proof of Theorem 3.1 in [6] (for example) we will, for the sake of completeness, include a proof of Lemma 1 in Section 3.1 below.

We should also note at this point that the standard application Varnavides’ argument is to show that Theorem 1 is equivalent to the statement that for any $\delta > 0$ and $B \subseteq \{1, \ldots, N\}$ with $|B| \geq \delta N$,

$$\text{# of square differences in } B \geq c(\delta) N^{3/2},$$

for some $c(\delta) > 0$. In other words, provided $N$ is sufficiently large, $B$ will contain not only one square difference, but a positive proportion of all the square differences in $\{1, \ldots, N\}$. This result clearly follows easily from Lemma 1.

---

While it is clear that any polynomial $f$ in $\mathbb{Z}[n]$ with an integer root is plainly intersective, there do in fact exist polynomials with no rational roots that also have this property, for example $(n^3 - 19)(n^2 + n + 1)$. 


2.1. Proof of Theorem 2. It follows immediately from the upper bound on the number of square differences in $B$ given by property (ii) and the lower bound given by Lemma 1 that

$$|B| \leq \frac{D(M)}{M} + \frac{2}{M} + \frac{C_0 M^{5/2}}{\sqrt{\log N}}.$$  

Assuming that $N$ satisfies $C_0 M^{7/2} \leq \sqrt{\log N}$, it follows that

$$\frac{|B|}{N} \leq \frac{D(M)}{M} + \frac{3}{M},$$

and hence, using the trivial lower bound $D(M) \geq \sqrt{M} - 1$ (see Section B.2), that

$$\frac{|B|}{N} \leq \frac{5}{4} \frac{D(M)}{M},$$

provided that $M$ is sufficiently large (in fact $M \geq 169$ is sufficient). Combining this observation with the inequality

$$\frac{|B|}{N} \geq \frac{5}{3} \frac{|A|}{N} = \frac{5}{3} \frac{D(N)}{N},$$

which follows immediately from property (i) of our constructed set $B$, gives the desired inequality. □

2.2. Construction of the set $B$. Given any set $B \subseteq \{1, \ldots, N\}$, it is easy to see that

$$\# \text{ of square differences in } B = \sum_{n=1}^{\sqrt{N}} \sum_{x \in \mathbb{Z}} B(x)B(x-n^2),$$

where $B(x) = 1_{B}(x)$ denotes the indicator function of the set $B$. Using the familiar orthogonality relation

$$\int_0^1 e^{2\pi i x \alpha} d\alpha = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \in \mathbb{Z} \setminus \{0\} \end{cases},$$

we can, as is standard, express our count (6) on the “transform side” as

$$\# \text{ of square differences in } B = \int_0^1 |\hat{B}(\alpha)|^2 \hat{S}(\alpha) \, d\alpha,$$

where

$$\hat{B}(\alpha) = \sum_{x \in \mathbb{Z}} B(x)e^{-2\pi i x \alpha}$$

denotes the Fourier transform (on $\mathbb{Z}$) of the set $B$ and

$$\hat{S}(\alpha) = \sum_{n=1}^{\sqrt{N}} e^{-2\pi i n^2 \alpha}$$

is the Fourier transform of the set of perfect squares contained in $\{1, \ldots, N\}$.

Key to our proof (and essentially the only true “machinery” used in the proof) is the following well-known estimate for the Weyl sum $\hat{S}(\alpha)$, which states that the only possible obstruction to cancellation in this exponential sum arises if $\alpha$ is “close” to a rational with “small” denominator.
Proposition 1. Let $\varepsilon > 0$ and
\[
\mathbf{M}_{a/q}(\varepsilon) = \left\{ \alpha \in [0,1] : \left| \alpha - \frac{a}{q} \right| \leq \frac{1}{\varepsilon^2 N} \right\}.
\]
If $\alpha \notin \mathbf{M}_{a/q}(\varepsilon)$ for any $(a,q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, then
\[
|\widehat{S}(\alpha)| \leq 5\varepsilon N^{1/2},
\]
provided $N$ is sufficiently large with respect to $\varepsilon$; in particular, $N \geq C\varepsilon^{-50}$ would be sufficient.

We are now ready to define our set $B$. Recalling that $A \subseteq \{1,\ldots,N\}$ is an extremal set with no square differences, we define (for a value of $\varepsilon > 0$ to be determined)
\[
(9) \quad B := A' \cup (A' + q_\varepsilon^2),
\]
where $q_\varepsilon = \operatorname{lcm}\{1 \leq q \leq \varepsilon^{-2}\}$ and $A' = A \cap \{1,\ldots,N - q_\varepsilon^2\}$.

Using the fact that $|A| = D(N) \geq \sqrt{N} - 1$, it follows that $|A'| \geq 5|A|/6$ and consequently also that property (i) for our set $B$ will hold, provided $\varepsilon > 0$ is chosen large enough for
\[
(10) \quad q_\varepsilon^2 \ll \sqrt{N}.
\]
In order to see what actual restriction this places on our choice of $\varepsilon > 0$, we recall, as one can verify using only elementary properties of the prime numbers, that
\[
\exp(\varepsilon^{-2}/2) \leq q_\varepsilon \leq \exp(\varepsilon^{-2})
\]
and hence that inequality $\text{(10)}$ will hold whenever
\[
\varepsilon^{-2} \ll \log N.
\]

Remark (on “$\ll$ notation”). Whenever we write $E \ll F$ for any two quantities $E$ and $F$ we shall mean that $E \leq cF$, for some sufficiently small constant $c > 0$.

We therefore now fix
\[
(11) \quad \varepsilon := C_1 (\log N)^{-1/2}
\]
with $C_1 > 0$ a sufficiently large (but absolute) constant. In order to establish that our set $B$ also satisfies property (ii) it will suffice to show, for this choice of $\varepsilon > 0$, that
\[
(12) \quad \# \text{ of square differences in } B \leq 20 \varepsilon N^{3/2}
\]
for all sufficiently large $N$.

To establish $\text{(12)}$ we first note that since $A' \subseteq A$ contains no square differences, it follows that
\[
B(x) = A'(x) + A'(x - q_\varepsilon^2)
\]
since $A'$ and $A' + q_\varepsilon^2$ are disjoint and hence, using the familiar and easily verified property that Fourier transformation takes translations to modulations, that
\[
\hat{B}(\alpha) = \hat{A}'(\alpha) (1 + e^{-2\pi i q_\varepsilon^2 \alpha}).
\]
Multiplying this expression for $\hat{B}(\alpha)$ by its complex conjugate, we see that
\[
\int_0^1 |\hat{B}(\alpha)|^2 \hat{S}(\alpha) \, d\alpha = 2 \int_0^1 |\hat{A}'(\alpha)|^2 (\cos(2\pi q_\varepsilon^2 \alpha) + 1) \hat{S}(\alpha) \, d\alpha.
\]
In light of (7) and the fact that $A'$ contains no square differences, it follows that
\[
\int_0^1 |\hat{A'}(\alpha)|^2 \hat{S}(\alpha) \, d\alpha = 0
\]
and hence that
\[
\# \text{ of square differences in } B = 2 \int_0^1 |\hat{A'}(\alpha)|^2 (\cos(2\pi q_\varepsilon^2 \alpha) - 1) \hat{S}(\alpha) \, d\alpha
\]
\[
\leq 2 \int_0^1 |\hat{A'}(\alpha)|^2 \left| \cos(2\pi q_\varepsilon^2 \alpha) - 1 \right| |\hat{S}(\alpha)| \, d\alpha.
\]

A crucial observation at this point, which completes the proof of inequality (12), is the fact that
\[
\# \text{ of square differences in } B \leq 10 \varepsilon \sqrt{N}
\]
uniformly in $\alpha$. It then follows that
\[
\# \text{ of square differences in } B \leq 20 \varepsilon \sqrt{N} \int_0^1 |\hat{A'}(\alpha)|^2 \, d\alpha \leq 20 \varepsilon N^{3/2},
\]
where to establish the final inequality we have invoked the Plancherel identity, namely
\[
\int_0^1 |\hat{A'}(\alpha)|^2 \, d\alpha = \sum_{x \in \mathbb{Z}} |A'(x)|^2,
\]
whose validity in this setting can be easily verified (using orthogonality), together with the simple observation that
\[
\sum_{x \in \mathbb{Z}} |A'(x)|^2 = |A'| \leq N.
\]

It remains to verify the uniform estimate (13). Since $|\cos(2\pi q_\varepsilon^2 \alpha) - 1| \leq 2$ for all $\alpha \in [0, 1]$, it follows from Proposition 1 that (13) will hold whenever $\alpha \notin M_{a/q}(\varepsilon)$ for any $(a, q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, since $N = \exp(C_1^2 \varepsilon^{-2}) \gg \varepsilon^{-50}$. While if $\alpha \in M_{a/q}(\varepsilon)$ for some $(a, q) = 1$ with $1 \leq q \leq \varepsilon^{-2}$, then by definition we know that $|\alpha - a/q| \leq \varepsilon^{-2} N^{-1}$. Moreover, since $q|q_\varepsilon^2$ (by the definition of $q_\varepsilon$) it follows that
\[
\cos \left(2\pi q_\varepsilon^2 \alpha\right) = \cos \left(2\pi q_\varepsilon^2 (\alpha - a/q)\right),
\]
and hence, by the Mean Value Theorem, we see that
\[
|\cos(2\pi q_\varepsilon^2 \alpha) - 1| = |\cos(2\pi q_\varepsilon^2 (\alpha - a/q)) - 1|
\leq 2\pi q_\varepsilon^2 |\alpha - a/q|
\leq 2\pi q_\varepsilon^2 \varepsilon^{-2} N^{-1}.
\]
The result then follows, provided that the constant $C_1$ in our choice of fixed $\varepsilon > 0$ is chosen sufficiently large, since
\[
2\pi q_\varepsilon^2 \varepsilon^{-2} N^{-1} \leq \varepsilon
\]
whenever $\varepsilon^{-2} \ll \log N$ (again) and we trivially know that $|\hat{S}(\alpha)| \leq \sqrt{N}$ for all $\alpha \in [0, 1]$.

This completes the proof of Theorem 2 modulo Lemma 1 and Proposition 1. The proofs of these two results are given in Section 3 below.
3. PROOFS OF LEMMA 1 AND PROPOSITION 1

3.1. Proof of Lemma 1. Let $B \subseteq \{1, \ldots, N\}$ and $1 \leq M \leq N$. We proceed by covering $\{1, \ldots, N\}$ by the collection of all square-difference progressions of length $M$ of the form

$$P_{a,r} = \{a + r^2, \ldots, a + Mr^2\}$$

with $1 \leq r \leq R := \sqrt{N}/M$ and $1 \leq a \leq N - MR^2$. We will say that such a progression $P_{a,r}$ is good if

$$|B \cap P_{a,r}| \geq D(M) + 1$$

since, by virtue of the fact that square differences are preserved under translations and dilations by a perfect square, each such progression clearly contributes at least one square difference in $B$.

A simple counting argument, which we give below, shows that

$$\# \text{ of good progressions } P_{a,r} \geq \left(\frac{|B|}{N} - \frac{D(M) + 2}{M}\right) RN. \tag{14}$$

Now while, as noted above, each of these good progressions contributes at least one square difference in $B$, it is of course also the case that some of these square differences could be getting over counted. However, as we shall also see below, each square difference in $B$ is being over counted at most $M^{3/2}$ times, from which it follows that

$$\# \text{ of square differences in } B \geq \left(\frac{|B|/N - (D(M) + 2)/M}{M^{5/2}}\right) N^{3/2},$$

as required. We are thus left with the straightforward tasks of verifying (14) and the claim that each square difference in $B$ is being over counted in this argument at most $M^{5/2}$ times.

We will address the over counting argument first. Suppose we are given a pair $\{b, b + n^2\}$ in $B$. If this pair is contained in $P_{a,r}$, then $r$ must be a divisor of $n$ and moreover $n^2 \leq Mr^2$. It therefore follows that there are at most $\sqrt{M}$ choices for $r$, and it is easy to see that each choice of $r$ fixes $a$ in at most $M$ ways; thus each square difference is indeed over counted at most $M^{3/2}$ times.

Finally, we verify (14). By combining the upper bound

$$\sum_{r=1}^{R} \sum_{a=1}^{N-MR^2} |B \cap P_{a,r}| \leq \sum_{a,r \text{ good } P_{a,r}} M + \sum_{a,r \text{ not good } P_{a,r}} D(M)$$

$$\leq (\# \text{ of good progressions } P_{a,r}) M + D(M)RN$$

with the lower bound

$$\sum_{r=1}^{R} \sum_{a=1}^{N-MR^2} |B \cap P_{a,r}| \geq M \sum_{r=1}^{R} |B \cap \{Mr^2, \ldots, N - Mr^2\}| \geq MR (|B| - 2MR^2)$$

it follows that

$$\# \text{ of good progressions } P_{a,r} \geq \left(\frac{|B|}{N} - \frac{2MR^2}{N} - \frac{D(M)}{M}\right) RN$$

from which (14) follows. □
3.2. Proof of Proposition 1: We first recall Dirichlet’s (pigeonhole) principle:

Given any $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$, there exist $(a, q) = 1$ with $1 \leq q \leq Q$ such that

$$|\alpha - \frac{a}{q}| \leq \frac{1}{qQ} \leq \min\left\{\frac{1}{q^2}, \frac{1}{Q}\right\}.$$ 

The proof of the following key result is completely standard; see for example [14] or [5].

**Proposition 2** (The Weyl inequality). If $|\alpha - a/q| \leq q^{-2}$ and $(a, q) = 1$, then

$$|\hat{S}(\alpha)| \leq 40\sqrt{N}\log N(1/q + 1/\sqrt{N} + q/N)^{1/2}.$$ 

We note (by Dirichlet’s principle) that for any given $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$, there always exist $(a, q) = 1$ with $1 \leq q \leq Q$ that satisfy the hypothesis of the Weyl inequality. Moreover, it is easy to see that this inequality gives a non-trivial conclusion whenever $N^\mu \leq q \leq N^{1-\mu}$ for some $0 < \mu < 1/2$. For the purposes of this exposition we shall take $Q = N^{1-\mu}$ with $\mu = 1/20$ and define

$$M'_{a/q} = \left\{ \alpha \in [0, 1] : \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{N^{19/20}} \right\}.$$ 

It is customary to say that $\alpha$ is in a major arc if $\alpha \in M'_{a/q}$ for some $(a, q) = 1$ with $1 \leq q \leq N^{1/20}$, and we call the complement of these major arcs the minor arcs. If $\alpha$ is in one of these minor arcs, then it follows from Dirichlet’s principle that there must exist a reduced fraction $a/q$ with $N^{1/20} \leq q \leq N^{19/20}$ such that $|\alpha - a/q| \leq q^{-2}$ and hence, by the Weyl inequality, that

$$|\hat{S}(\alpha)| \leq 80N^{19/40}\log N \leq \varepsilon\sqrt{N}$$

for any $\varepsilon > 0$ that satisfies $N \gg \varepsilon^{-50}$.

In order to obtain the full conclusion of Proposition 1 which is valid on a subset of $[0, 1]$ which is strictly larger than the collection of classical minor arcs defined above, we must perform a careful analysis of the behavior of our exponential sum $\hat{S}(\alpha)$ on the major arcs. In particular, we will invoke the following.

**Lemma 2** (Major arc estimate). If $\alpha \in M'_{a/q}$ for some $(a, q) = 1$ with $1 \leq q \leq N^{1/20}$, then

$$|\hat{S}(\alpha)| \leq 5\sqrt{N}q^{-1/2}(1 + N|\alpha - a/q|)^{-1/2}.$$ 

It now follows immediately from this lemma that for any given $\varepsilon > 0$ and $\alpha \in M'_{a/q}$, our exponential sum will satisfy

$$|\hat{S}(\alpha)| \leq 5\varepsilon\sqrt{N}$$

provided $(a, q) = 1$ and either $\varepsilon^{-2} \leq q \leq N^{1/20}$ or $\varepsilon^{-2}N^{-1} \leq |\alpha - a/q| \leq N^{-19/20}$, as required.

The proof of Lemma 2 is standard, but for the sake of completeness we have chosen to included a proof in Appendix A below.

**Appendix A. Proof of Lemma 2 (Major arc estimate)**

The proof of Lemma 2 hinges on the key observation that for each $\alpha$ in a major arc corresponding to a rational $a/q$, our exponential sum $\hat{S}(\alpha)$ breaks naturally into an arithmetic part $S(a, q)$ and a continuous part $I_N(\alpha - a/q)$, up to a manageable error term. In particular we have
Lemma 3. If $\alpha \in \mathbb{M}_{a/q}'$ with $1 \leq q \leq N^{1/20}$, then
\begin{equation}
\hat{S}(\alpha) = \sqrt{N} q^{-1} S(a, q) I_N(\alpha - a/q) + O(N^{1/10}),
\end{equation}
where
\begin{align*}
S(a, q) &= \sum_{r=0}^{q-1} e^{-2\pi i ar^2/q} \quad \text{and} \quad I_N(\beta) = \int_0^1 e^{-2\pi i N^2 \beta x^2} \, dx.
\end{align*}

Remark (on “big O notation”). Whenever we write $E = O(F)$ for any two quantities $E$ and $F$ we shall mean that $|E| \leq CF$, for some constant $C > 0$.

Proof. We can write $\alpha = a/q + \beta$, where $|\beta| \leq 1/N^{19/20}$ and $1 \leq q \leq N^{1/20}$. We can also write each $1 \leq d \leq \sqrt{N}$ uniquely as $d = mq + r$ with $1 \leq r \leq q$ and $0 \leq m \leq \sqrt{N}/q$. It then follows that
\begin{align*}
\hat{S}(\alpha) &= \sum_{r=1}^{q} \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i (a/q + \beta)(mq+r)^2} + O(q) \\
&= \sum_{r=1}^{q} e^{-2\pi i r^2/q} \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i \beta (mq+r)^2} + O(q).
\end{align*}

Since
\begin{align*}
|e^{-2\pi i (mq+r)^2\beta} - e^{-2\pi i m^2 q^2 \beta}| &\leq |e^{-2\pi i (2mq+r)^2\beta} - 1| \leq Cdr|\beta| \leq CqN^{-9/20}
\end{align*}
and
\begin{align*}
\left| \sum_{m=0}^{\sqrt{N}/q} e^{-2\pi i m^2 q^2 \beta} - \int_0^{\sqrt{N}/q} e^{-2\pi ix^2 q^2 \beta} \, dx \right| &\leq \sum_{m=0}^{\sqrt{N}/q} \int_m^{m+1} \left| e^{-2\pi i m^2 q^2 \beta} - e^{-2\pi i x^2 q^2 \beta} \right| \, dx \\
&\leq \sum_{m=0}^{\sqrt{N}/q} 2\pi (2m+1)q^2|\beta| \\
&\leq CN^{1/20}
\end{align*}
it follows that
\begin{align*}
|\hat{S}(\alpha) - \sqrt{N} q^{-1} S(a, q) I_N(\beta)| &\leq CN^{1/10}. \quad \square
\end{align*}

Lemma 2 follows almost immediately from this and the two basic lemmas below.

Lemma 4 (Gauss sum estimate). If $(a, q) = 1$, then $|S(a, q)| \leq \sqrt{2q}$. More precisely,
\begin{align*}
|S(a, q)| &= \begin{cases}
\sqrt{q} & \text{if } q \text{ odd}, \\
\sqrt{2q} & \text{if } q \equiv 0 \mod 4, \\
0 & \text{if } q \equiv 2 \mod 4.
\end{cases}
\end{align*}

Lemma 5 (Oscillatory integral estimate). For any $\lambda \geq 0$,
\begin{align*}
\left| \int_0^1 e^{2\pi i \lambda x^2} \, dx \right| &\leq \min\{1, 2\lambda^{-1/2}\} \leq 2\sqrt{2}(1 + \lambda)^{-1/2}.
\end{align*}
Proof of Lemma 2 Lemmas 4 and 5 imply that
\[ \sqrt{N} q^{-1} S(a,q) I_N(\alpha - a/q) \leq 4 \sqrt{N} q^{-1/2} (1 + N |\alpha - a/q|)^{-1/2}, \]
and since \( q^{-1/2} \geq N^{-1/40} \) and \( N |\alpha - a/q| \leq N^{1/20} \), it follows that
\[ N^{-1/10} \ll \sqrt{N} q^{-1/2} (1 + N |\alpha - a/q|)^{-1/2}. \]
\[ \square \]

Proof of Lemma 4 Squaring-out \( S(a,q) \) we obtain
\[ |S(a,q)|^2 = \sum_{s=0}^{q-1} \sum_{r=0}^{q-1} e^{2\pi i a(r^2 - s^2)/q}. \]
Letting \( r = s + t \) and using the fact that \( (a,q) = 1 \) and
\[ \sum_{s=0}^{q-1} e^{2\pi i a(2st)/q} = \begin{cases} q & \text{if } 2at \equiv 0 \mod q, \\ 0 & \text{otherwise}, \end{cases} \]
it follows that
\[ |S(a,q)|^2 = \sum_{t=0}^{q-1} e^{2\pi i a t^2/q} \sum_{s=0}^{q-1} e^{2\pi i a(2st)/q} = \begin{cases} q & \text{if } q \text{ odd}, \\ q (e^{2\pi i a(q/4) + 1}) & \text{if } q \text{ even}. \end{cases} \]
\[ \square \]

Proof of Lemma 5 We need only consider the case when \( \lambda \geq 1 \). We write
\[ \int_0^1 e^{2\pi i \lambda x^2} dx = \int_0^{\lambda^{-1/2}} e^{2\pi i \lambda x^2} dx + \int_{\lambda^{-1/2}}^1 e^{2\pi i \lambda x^2} dx = : I_1 + I_2. \]
It is easy to then see that \( |I_1| \leq \lambda^{-1/2} \), while integration by parts gives that
\[ |I_2| = \left| \int_{\lambda^{-1/2}}^1 \frac{1}{\lambda} \frac{d}{dx} e^{2\pi i \lambda x^2} dx \right| \leq \frac{1}{4\pi} \left| \frac{1}{x} e^{2\pi i \lambda x^2} \right|_{\lambda^{-1/2}}^1 + \int_{\lambda^{-1/2}}^1 \frac{1}{x^2} e^{2\pi i \lambda x^2} dx \leq \lambda^{-1/2}. \]
\[ \square \]

APPENDIX B. JUSTIFICATION OF INEQUALITY (11): THE PURPORTED TRIVIAL BOUNDS FOR \( D(N) \)

B.1. Upper bounds. Let \( A \subseteq \{1, \ldots, N\} \) with no square differences.
It clearly follows that \( A \cap (A + t^2) = \emptyset \) for all \( t \in \mathbb{N} \) and in particular that
\[ |A| \leq (N + 1)/2 \]
since \( |(A + 1) \cap \{1, \ldots, N\}| \geq |A| - 1 \) and hence
\[ 2|A| - 1 \leq |(A \cup (A + 1)) \cap \{1, \ldots, N\}| \leq N. \]
In order to obtain the superior bound (at least when \( N \geq 65 \)) of
\[ |A| \leq (N + 34)/3, \]
one can use the further observation that if \( (r, s, t) \) form a Pythagorean triple with \( r^2 + s^2 = t^2 \), then
\[ A \cap (A + s^2) = A \cap (A + t^2) = (A + s^2) \cap (A + t^2) = \emptyset. \]
In particular, taking \( s = 3 \) and \( t = 5 \), it follows that
\[ 3|A| - 34 \leq |(A \cup (A + 9) \cup (A + 25)) \cap \{1, \ldots, N\}| \leq N, \]
as required, since clearly \(|(A+9)\cap\{1,\ldots,N\}| \geq |A|-9\) and \(|(A+25)\cap\{1,\ldots,N\}| \geq |A|-25\).

The superior bound (at least when \(N \geq 1630193\)) of
\[|A| \leq \frac{(N+543443)}{4},\]
claimed in the introduction, follows (as above) once one observes that
\[153^2, 185^2, 697^2, 185^2 - 153^2, 697^2 - 185^2, 697^2 - 153^2\]
are all perfect squares.

**B.2. Lower bound.** We now show that given any subset \(H\) of the natural numbers and any \(N \in \mathbb{N}\), there always exists a set \(A \subseteq \{1,\ldots,N\}\) such that \((A-A)\cap H = \emptyset\) and
\[
|A| \geq \frac{N-1}{|H\cap\{1,\ldots,N\}|+1}.
\]
Taking \(H\) to be the set of square numbers, this corresponds to the desired lower bound \(D(N) \geq \sqrt{N} - 1\).

We construct the set \(A\) recursively as follows: Select \(a_1 = 1\) to be the first element in \(A\). Having selected \(a_1,\ldots,a_k\), with \(k \geq 1\), we define \(X_k = \{a_1,\ldots,a_k\} + H \cap \{1,\ldots,N\}\) and select \(a_{k+1}\) to be the smallest element in \(\{1,\ldots,N\}\setminus\{a_1,\ldots,a_k,X_k\}\). In order to guarantee the existence of such an element \(a_{k+1}\), we clearly must have \(|\{a_1,\ldots,a_k,X_k\}| \leq N - 1\), and since it is possible that \(|\{a_1,\ldots,a_k,X_k\}| = k\) \(|H\cap\{1,\ldots,N\}| + 1\), this corresponds to the restriction that
\[
k \leq \left\lfloor \frac{N-1}{|H\cap\{1,\ldots,N\}|+1} \right\rfloor,
\]
from which (16) immediately follows.

**References**


Department of Mathematics, The University of Georgia, Athens, Georgia 30602
E-mail address: lyall@math.uga.edu