

# THE WEYL INEQUALITY AND SÁRKÖZY'S THEOREM

NEIL LYALL

## 1. THE WEYL INEQUALITY

A *Weyl sum* is an exponential sum of the form

$$(1) \quad S = \sum_{n=1}^N e^{2\pi i P(n)}$$

where  $P(x)$  is a polynomial with real coefficients. The purpose of this section is to derive Weyl's estimates for these sums in the special case when  $P(x) = \alpha x^2$ .

**Theorem 1.1** (The Weyl inequality for quadratic monomials). *Let  $a \in \mathbf{Z}$  and  $q \in \mathbf{N}$  with  $(a, q) = 1$  and  $N \in \mathbf{N}$  with  $N \geq 2$ . If  $\alpha \in \mathbf{R}$  with  $|\alpha - a/q| \leq q^{-2}$ , then*

$$\left| \sum_{n=1}^N e^{2\pi i \alpha n^2} \right| \leq 10N \log N (N + q + N^2/q)^{-1/2}.$$

We remark that this gives a non-trivial estimate whenever  $N^\eta \leq q \leq N^{2-\varepsilon}$  for some  $0 < \eta, \varepsilon < 1$ . We begin with the following elementary lemma.

**Lemma 1.2.** *Let  $\alpha \in \mathbf{R}$ . Then for all  $N \in \mathbf{N}$ ,*

$$\left| \sum_{n=1}^N e^{2\pi i \alpha n} \right| \leq \min \left\{ N, \frac{1}{2\|\alpha\|} \right\}$$

where  $\|\alpha\|$  is the distance from  $\alpha$  to the nearest integer.

*Proof.* If  $\alpha = 0$ , then the sum is  $N$ . If  $\alpha \neq 0$ , then

$$\left| \sum_{n=1}^N e^{2\pi i \alpha n} \right| \leq \frac{|1 - e^{2\pi i \alpha N}|}{|1 - e^{2\pi i \alpha}|} \leq \frac{|\sin \pi \alpha N|}{|\sin \pi \alpha|} \leq \frac{1}{2\|\alpha\|}. \quad \square$$

The method of *Weyl differencing* allows us to treat higher degree polynomials, the idea is simply to *square-out* the Weyl sum (1);

$$\begin{aligned} |S|^2 &= \sum_{n=1}^N \sum_{m=1}^N e^{2\pi i [P(m) - P(n)]} \\ &= \sum_{n=1}^N \sum_{h=1-n}^{N-n} e^{2\pi i [P(n+h) - P(n)]} \\ &= N + \sum_{h=1}^{N-1} \sum_{n=1}^{N-h} e^{2\pi i [P(n+h) - P(n)]} + \sum_{h=1-N}^{-1} \sum_{n=1-h}^N e^{2\pi i [P(n+h) - P(n)]} \\ &= N + 2 \operatorname{Re} \sum_{h=1}^{N-1} \sum_{n=1}^{N-h} e^{2\pi i [P(n+h) - P(n)]} \\ &\leq N + 2 \sum_{h=1}^{N-1} \left| \sum_{n=1}^{N-h} e^{2\pi i [P(n+h) - P(n)]} \right|. \end{aligned}$$

Since  $P(x+h) - P(x)$  is a polynomial of degree one less than that of  $P(x)$ , the possibility of inducting on the degree of  $P$  arises.

In Theorem 1.1 we are considering Weyl sums with  $P(x) = \alpha x^2$  so in this case the difference  $P(x+h) - P(x) = 2\alpha h + \alpha h^2$ , and it follows from *Weyl differencing* and Lemma 1.2 that

$$\begin{aligned} |S|^2 &\leq N + 2 \sum_{h=1}^{N-1} \left| \sum_{n=1}^{N-h} e^{2\pi i(2\alpha h)n} \right| \\ &\leq N + 2 \sum_{h=1}^{N-1} \min \left\{ N-h, \frac{1}{\|2\alpha h\|} \right\} \\ &\leq N + 2 \sum_{h=1}^{2N} \min \left\{ N, \frac{1}{\|\alpha h\|} \right\}. \end{aligned}$$

Theorem 1.1 therefore follows immediately from the following proposition (with  $H = 2N$ ).

**Proposition 1.3.** *Let  $a \in \mathbf{Z}$  and  $q \in \mathbf{N}$  with  $(a, q) = 1$ ,  $N \in \mathbf{N}$  with  $N \geq 2$ , and  $H \in \mathbf{N}$ . If  $\alpha \in \mathbf{R}$  with  $|\alpha - a/q| \leq q^{-2}$ , then*

$$\sum_{h=1}^H \min \left\{ N, \frac{1}{\|\alpha h\|} \right\} \leq 24 \log N (N + q + H + HN/q).$$

The proof of this proposition follows from the lemma below together with the key observation that if  $0 < |h_2 - h_1| \leq q/2$ , then  $\|\alpha h_2 - \alpha h_1\| \geq 1/2q$ .

**Lemma 1.4.** *Let  $L, M, N \in \mathbf{N}$  with  $N \geq 2$  and  $L \leq M$ . If  $\alpha_1, \dots, \alpha_L \in \mathbf{R}$  with  $\|\alpha_\ell - \alpha_{\ell'}\| \geq M^{-1}$  whenever  $\ell \neq \ell'$ , then*

$$\sum_{\ell=1}^L \min \left\{ N, \frac{1}{\|\alpha_\ell\|} \right\} \leq 6(N + M) \log N.$$

*Proof of Proposition 1.3.* Write  $\alpha = a/q + \beta$ . We first note that if  $0 < |h_2 - h_1| \leq q/2$ , then

$$\|\alpha h_2 - \alpha h_1\| \geq \|(h_2 - h_1)a/q\| - \|(h_2 - h_1)\beta\| \geq 1/q - 1/2q = 1/2q$$

since  $(h_2 - h_1)a \not\equiv 0 \pmod{q}$ . It then follows from Lemma 1.4 that

$$\sum_{h=1}^H \min \left\{ N, \frac{1}{\|\alpha h\|} \right\} \leq \sum_{k=0}^{\lfloor 2H/q \rfloor} \sum_{h=k\lfloor q/2 \rfloor+1}^{(k+1)\lfloor q/2 \rfloor} \min \left\{ N, \frac{1}{\|\alpha h\|} \right\} \leq 6(1 + 2H/q)(N + 2q) \log N. \quad \square$$

*Proof of Lemma 1.4.* Without loss of generality we may assume that each  $\alpha_\ell \in [-1/2, 1/2]$  and that

$$S^+ = \sum_{\substack{1 \leq \ell \leq L \\ \alpha_\ell \geq 0}} \min \left\{ N, \frac{1}{\|\alpha_\ell\|} \right\} \geq \frac{1}{2} \sum_{\ell=1}^L \min \left\{ N, \frac{1}{\|\alpha_\ell\|} \right\}.$$

Relabeling the non-negative  $\alpha_\ell$  as  $0 \leq \alpha_1 < \alpha_2 < \dots < \alpha_K$  and noting that  $\alpha_k \geq (k-1)/M$  for  $k = 1, \dots, K$ , we see that

$$S^+ = \sum_{k=0}^{K-1} \min \left\{ N, \frac{M}{k} \right\} = \sum_{k=0}^{\lfloor M/N \rfloor} N + \sum_{M/N < k < K} \frac{M}{k} \leq (N + M) + 2M \log N. \quad \square$$

In the next two sections we shall prove two standard facts about squares, these results will then be used in the proceeding section to give a proof (due to Ben Green) of a result of Sárközy and Furstenberg on the existence of a *square difference* in any subset of  $\mathbf{Z}$  of positive upper density.

## 2. HEILBRONN PROPERTY

As a first application of Weyl's inequality we now prove a quantitative version of the fact that the squares form a Heilbronn set.

**Definition 2.1** (Heilbronn set). We say that  $H$  is a Heilbronn set if given any  $\alpha \in \mathbf{R}$  and  $\varepsilon > 0$  there exists  $h \in H$  such that  $\|\alpha h\| \leq \varepsilon$ .

**Theorem 2.2.** *For all sufficiently large  $M \in \mathbf{N}$  and  $\alpha \in \mathbf{R}$  there exists  $1 \leq q \leq M$  such that  $\|\alpha q^2\| \leq M^{-1/10}$ .*

We begin with the following elementary lemma.

**Lemma 2.3** (Dirichlet). *Let  $\alpha \in \mathbf{R}$  and  $M \in \mathbf{N}$ . Then there exists  $1 \leq q \leq M$  such that  $\|\alpha q\| \leq M^{-1}$ .*

*Proof.* Of the reals  $\alpha, 2\alpha, \dots, (M+1)\alpha$ , two clearly lie within  $M^{-1}$  of each other (mod 1). Thus there exists  $j, k \in \mathbf{N}$  with  $j \neq k$  such that  $\|(k-j)\alpha\| \leq M^{-1}$ . Set  $q = |k-j|$ .  $\square$

**Lemma 2.4.** *Let  $A \subseteq \mathbf{Z}_N$  with  $|A| = M$ . If  $L$  is even and  $A \cap (-L, L] = \emptyset$ , then there exists  $r \in \mathbf{Z}_N$  with  $0 < |r| \leq N^2/L^2$  such that  $|\widehat{1}_A(r)| \geq LM/2N$ , where  $|r|$  denotes the distance from  $r$  to the nearest integer multiple of  $N$ .*

*Proof of Theorem 2.2.* It suffices to establish the result for  $\alpha \in \mathbf{Q}$ . Our proof will be by contradiction. We therefore assume that  $\alpha = a/N$  and that the conclusion of the theorem is false.

If we set  $A = \{a, 2^2a, \dots, M^2a\}$  and  $L = 2\lfloor NM^{-1/10}/2 \rfloor$ , then  $A \cap (-L, L] = \emptyset$  and it follows from Lemma 2.4 that there exists  $r$  with  $0 < |r| \leq 2M^{1/5}$  such that  $|\widehat{1}_A(r)| \geq M^{9/10}/4$ . However,

$$\widehat{1}_A(r) = \sum_{m=1}^M e^{2\pi i(-\alpha r)m^2}$$

is a Weyl sum, and by Dirichlet (Lemma 2.3) there exists  $1 \leq q \leq M$  such that  $|(-\alpha r) - a/q| \leq 1/qM$ . Therefore if  $M^{1/4} \leq q \leq M$  it follows from Weyl's inequality that  $|\widehat{1}_A(r)| \leq CM^{7/8} \log M$ . Hence we must have  $1 \leq q \leq M^{1/4}$ , but in this case it follows immediately that

$$\|\alpha(rq)^2\| \leq |r|q/M \leq 2M^{-11/20},$$

a contradiction.  $\square$

*Proof of Lemma 2.4.* Let  $I = (-L/2, L/2]$ . It then follows that  $A \cap (I - I) = \emptyset$  and

$$\frac{1}{N} \sum_{r=0}^{N-1} |\widehat{1}_I(r)|^2 \widehat{1}_A(r) = \sum_{n=0}^{N-1} 1_I * 1_I(n) 1_A(n) = 0,$$

from which we can conclude that

$$\frac{1}{N} \sum_{r \neq 0} |\widehat{1}_I(r)|^2 |\widehat{1}_A(r)| \geq \frac{1}{N} |\widehat{1}_I(0)|^2 |\widehat{1}_A(0)| = \frac{L^2 M}{N}.$$

But it follows from Lemma 1.2 that

$$|\widehat{1}_I(r)| \leq \min \left\{ L, \frac{1}{2\|r/N\|} \right\} = \min \left\{ L, \frac{N}{2|r|} \right\}.$$

Hence

$$\begin{aligned} \frac{1}{N} \sum_{r \neq 0} |\widehat{1}_I(r)|^2 |\widehat{1}_A(r)| &\leq \max_{0 < |r| \leq N^2/L^2} |\widehat{1}_A(r)| \frac{1}{N} \sum_{r=0}^{N-1} |\widehat{1}_I(r)|^2 + \frac{M}{N} \sum_{|r| \geq N^2/L^2} \frac{N^2}{4|r|^2} \\ &\leq L \max_{0 < |r| \leq N^2/L^2} |\widehat{1}_A(r)| + \frac{ML^2}{2N} \end{aligned}$$

and we must conclude that

$$\max_{0 < |r| \leq N^2/L^2} |\widehat{1}_A(r)| \geq \frac{ML}{2N}. \quad \square$$

## 3. SUMS OF SQUARES

For  $k, M \in \mathbf{N}$  we define

$$r_{2k}(M) = \#\{(m_1, \dots, m_k, n_1, \dots, n_k) \in [1, M]^{2k} : m_1^2 + \dots + m_k^2 = n_1^2 + \dots + n_k^2\}.$$

The main objective of this section is to establish the following result.

**Theorem 3.1.** *If  $k \geq 3$  then there exists a constant  $c_0 > 0$  such that  $r_{2k}(M) \leq c_0 M^{2k-2}$ .*

In actual fact  $r_{2k}(M) \sim M^{2k-2}$  when  $k \geq 3$ , but we content ourselves with establishing upper bounds only. We begin with the observation that the following estimate holds for  $r_4(M)$ .

**Lemma 3.2.** *For any  $\eta > 0$  there exists a constant  $c_\eta > 0$  such that  $r_4(M) \leq c_\eta M^{2+\eta}$ .*

*Proof.* We note that

$$r_4(M) = \sum_{\ell=-M^2}^{M^2} \#\{(m, n) \in [1, M] \mid m^2 - n^2 = \ell\}^2 \leq 2M^2 + 4 \sum_{\ell=1}^{M^2} d(\ell)^2,$$

where  $d(\ell)$  denotes the number of divisors of  $\ell$ . The result then follows once we recall the basic fact that for every fixed  $\eta > 0$ ,

$$\lim_{\ell \rightarrow \infty} \frac{d(\ell)}{\ell^\eta} = 0 \quad \left( \iff r_2(M) \leq c_\eta M^\eta \right).$$

This is easy to verify; since  $f(\ell) = d(\ell)/\ell^\eta$  is multiplicative it suffice to prove that  $\lim_{p^k \rightarrow \infty} f(p^k) = 0$  as  $p^k$  runs through the sequence of all prime powers. We leave the details the reader.  $\square$

It is easy to see that the argument above can also be applied to establish that  $r_{2k}(M) \leq c_\eta M^{2k-2+\eta}$  for every  $\eta > 0$  when  $k \geq 3$ . In order to obtain the desired stronger result (Theorem 3.1) we will make use of estimates, on specific major and minor arcs, for the Weyl sum

$$S_M(\alpha) = \sum_{m=1}^M e^{2\pi i m^2 \alpha}.$$

To see how the behavior of these sums relates to the size of  $r_{2k}(M)$  we use the fact that

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

from which it is then easy to see that

$$r_{2k}(M) = \sum_{1 \leq m_j, n_j \leq M} \int_0^1 e^{2\pi i (m_1^2 + \dots + m_k^2 - n_1^2 - \dots - n_k^2) \alpha} d\alpha = \int_0^1 |S_M(\alpha)|^{2k} d\alpha.$$

**3.1. The major and minor arcs.** Informally one refers to the points in  $[0, 1]$  that are close to rationals  $a/q$  with small denominators as the major arcs and denotes them by  $\mathbf{M}_{a/q}$ . The remaining points are referred to as the minor arcs and are denoted by  $\mathbf{m}$ .

We recall that it follows from the Dirichlet principle (Lemma 2.3) that for every  $\alpha \in [0, 1]$  there exists  $1 \leq q \leq M^{2-1/10}$  and  $1 \leq a < q$  with  $(a, q) = 1$  such that  $|\alpha - a/q| \leq 1/qM^{2-1/10}$ .

We now make our informal definition more precise.

**Definition 3.3** (Major arcs). The major arcs are defined to be

$$\mathfrak{M} = \bigcup_{1 \leq q \leq M^{1/10}} \bigcup_{\substack{1 \leq a < q \\ (a, q) = 1}} \mathbf{M}_{a/q} \cup \mathbf{M}_{0/1}$$

where for  $1 \leq a < q$  with  $(a, q) = 1$  (and  $a = 0, q = 1$ ) we define

$$\mathbf{M}_{a/q} = \left\{ \alpha : \left| \alpha - \frac{a}{q} \right| \leq \frac{1}{qM^{2-1/10}} \right\}.$$

It is easy to see that  $|\mathfrak{M}| \leq M^{-2+1/5}$ . We further make the observation that the major arcs are in fact a union of (necessarily short) pairwise disjoint intervals.

**Lemma 3.4.** *If  $a/q \neq a'/q'$  with  $1 \leq q, q' \leq M^{1/10}$ , then  $\mathbf{M}_{a/q} \cap \mathbf{M}_{a'/q'} = \emptyset$ .*

*Proof.* Suppose that  $\mathbf{M}_{a/q} \cap \mathbf{M}_{a'/q'} \neq \emptyset$ . Using the fact that  $aq' - a'q \neq 0$ , we see that

$$\frac{2}{M^{2-1/10}} \geq \left| \frac{a}{q} - \frac{a'}{q'} \right| = \left| \frac{aq' - a'q}{qq'} \right| \geq \frac{1}{qq'} \geq \frac{1}{M^{1/5}},$$

a contradiction. □

**Definition 3.5** (Minor arcs). The minor arcs  $\mathfrak{m}$  are simply defined to be  $[0, 1] \setminus \mathfrak{M}$ .

**Proposition 3.6** (Minor arc estimate). *Let  $M \in \mathbf{N}$ . If  $\alpha \in \mathfrak{m}$ , then  $|S_M(\alpha)| \leq CM^{1-1/40}$ .*

**Corollary 3.7.** *Let  $k, M \in \mathbf{N}$ . If  $k \geq 3$ , then*

$$\int_{\mathfrak{m}} |S_M(\alpha)|^{2k} d\alpha \leq CM^{2k-2} M^{-1/40}.$$

*Proof.* It then follows Proposition 3.6 and Lemma 3.2, with  $\eta = 1/40$ , that

$$\begin{aligned} \int_{\mathfrak{m}} |S_M(\alpha)|^{2k} d\alpha &\leq \sup_{\alpha \in \mathfrak{m}} |S_M(\alpha)|^{2k-4} \int_0^1 |S_M(\alpha)|^4 d\alpha \\ &\leq CM^{2k-4} M^{-(k-2)/20} M^2 M^{1/40} \\ &\leq CM^{2k-2} M^{-1/40}. \end{aligned} \quad \square$$

*Proof of Proposition 3.6.* It follows from the Dirichlet principle and the fact that  $\alpha \in \mathfrak{m}$  that there exists a reduced fraction  $a/q$  with

$$M^{1/10} \leq q \leq M^{2-1/10}$$

such that  $|\alpha - a/q| \leq q^{-2}$ . It therefore follows from the Weyl inequality that

$$|S_M(\alpha)| \leq 30M^{1-1/20} \log M \leq CM^{1-1/40}. \quad \square$$

In order to prove Theorem 3.1 it therefore suffice to establish the following estimate.

**Proposition 3.8** (Major arc estimate). *If  $\alpha \in \mathbf{M}_{a/q}$  with  $1 \leq q \leq M^{1/10}$ , then*

$$|S_M(\alpha)| \leq CMq^{-1/2} (1 + M^2 |\alpha - a/q|)^{-1/2}.$$

**Corollary 3.9.** *If  $\alpha \in \mathfrak{M}$ , then*

$$\int_{\mathfrak{M}} |S_M(\alpha)|^{2k} d\alpha \leq CM^{2k-2}.$$

*Proof.* It follows from Proposition 3.8 that on a fixed major arc

$$\begin{aligned} \int_{\mathbf{M}_{a/q}} |S_M(\alpha)|^{2k} d\alpha &\leq CM^{2k} q^{-k} \int_{|\beta| \leq 1/qM^{2-1/10}} (1 + M^2 |\beta|)^{-k} d\beta \\ &\leq CM^{2k-2} q^{-k} \int_{-\infty}^{\infty} (1 + |\beta|)^{-k} d\beta \\ &\leq CM^{2k-2} q^{-k}. \end{aligned}$$

Therefore

$$\int_{\mathfrak{M}} |S_M(\alpha)|^{2k} d\alpha \leq CM^{2k-2} \sum_{q=1}^{M^{1/10}} \sum_{a=0}^{q-1} q^{-k} \leq CM^{2k-2} \sum_{q=1}^{\infty} q^{-k+1} \leq CM^{2k-2}. \quad \square$$

Theorem 3.1 now follows immediately from Corollaries 3.7 and 3.9. We are thus left with the task of proving Proposition 3.8, key to this is the following approximation.

**Proposition 3.10.** *If  $\alpha \in \mathbf{M}_{a/q}$  with  $1 \leq q \leq M^{1/10}$ , then*

$$(2) \quad S_M(\alpha) = q^{-1} S(a, q) I_M(\alpha - a/q) + O(M^{1/5}),$$

where

$$S(a, q) := \sum_{r=0}^{q-1} e^{2\pi i ar^2/q} \quad \text{and} \quad I_M(\beta) := \int_0^M e^{2\pi i \beta x^2} dx.$$

*Proof.* We can write  $\alpha = a/q + \beta$  where  $|\beta| \leq 1/qM^{2-1/10}$  and  $1 \leq q \leq M^{1/10}$ . We can also write each  $1 \leq m \leq M$  uniquely as  $m = nq + r$  with  $0 \leq r < q$  and  $0 \leq n \leq M/q$ . It then follows that

$$\begin{aligned} S_M(\alpha) &= \sum_{r=0}^{q-1} \sum_{n=0}^{M/q} e^{2\pi i(a/q+\beta)(nq+r)^2} + O(q) \\ &= \sum_{r=0}^{q-1} e^{2\pi iar^2/q} \sum_{n=0}^{M/q} e^{2\pi i\beta(nq+r)^2} + O(q). \end{aligned}$$

Since

$$\left| e^{2\pi i(nq+r)^2\beta} - e^{2\pi in^2q^2\beta} \right| \leq \left| e^{2\pi i(2nqr+r^2)\beta} - 1 \right| \leq C \frac{M}{q} q^2 \frac{1}{qM^{2-1/10}} \leq CM^{-1+1/10},$$

and

$$\begin{aligned} \left| \sum_{n=0}^{M/q} e^{2\pi in^2q^2\beta} - \int_0^{M/q} e^{2\pi ix^2q^2\beta} dx \right| &\leq \sum_{n=0}^{M/q} \int_n^{n+1} \left| e^{2\pi in^2q^2\beta} - e^{2\pi ix^2q^2\beta} \right| dx \\ &\leq \sum_{n=0}^{M/q} 2\pi(2n+1)q^2|\beta| \\ &\leq 20M^{1/10}, \end{aligned}$$

it follows that

$$\left| S_M(\alpha) - \frac{1}{q} S(a, q) I_M(\beta) \right| \leq CM^{1/5}. \quad \square$$

Proposition 3.8 then follows almost immediately from the two basic lemmas below.

**Lemma 3.11** (Gauss sum estimate). *If  $(a, q) = 1$ , then  $|S(a, q)| \leq \sqrt{2q}$ . More precisely,*

$$|S(a, q)| = \begin{cases} \sqrt{q} & \text{if } q \text{ odd} \\ \sqrt{2q} & \text{if } q \equiv 0 \pmod{4} \\ 0 & \text{if } q \equiv 2 \pmod{4} \end{cases}.$$

**Lemma 3.12** (Oscillatory integral estimate). *For any  $\lambda \geq 0$*

$$\left| \int_0^1 e^{2\pi i\lambda x^2} dx \right| \leq C(1 + \lambda)^{-1/2}.$$

*Proof of Proposition 3.8.* Lemmas 3.11 and 3.12 imply that the main term in (2)

$$q^{-1} S(a, q) I_M(\alpha - a/q) \leq Mq^{-1/2} (1 + M^2|\alpha - a/q|)^{-1/2},$$

and since  $q^{-1/2} \geq M^{-1/20}$  and  $M^2|\alpha - a/q| \leq M^{1/10}$ , it follows that

$$Mq^{-1/2} (1 + M^2|\alpha - a/q|)^{-1/2} \geq M^{9/10} \gg M^{1/5}. \quad \square$$

*Proof of Lemma 3.11.* Squaring-out  $S(a, q)$  we obtain

$$|S(a, q)|^2 = \sum_{s=0}^{q-1} \sum_{r=0}^{q-1} e^{2\pi ia(r^2-s^2)/q}.$$

Letting  $r = s + t$  the we see that

$$|S(a, q)|^2 = \sum_{t=0}^{q-1} e^{2\pi iat^2/q} \sum_{s=0}^{q-1} e^{2\pi ia(2st)/q} \leq \sum_{t=0}^{q-1} \left| \sum_{s=0}^{q-1} e^{2\pi ia(2st)/q} \right|.$$

The result then follows since  $(a, q) = 1$  and

$$\sum_{s=0}^{q-1} e^{2\pi ia(2st)/q} = \begin{cases} q & \text{if } 2at \equiv 0 \pmod{q} \\ 0 & \text{otherwise} \end{cases}. \quad \square$$

*Proof of Lemma 3.12.* 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 then easy to see that  $|I_1| \leq \lambda^{-1/2}$ , while integration by parts gives that

$$\begin{aligned} |I_2| &= \left| \int_{\lambda^{-1/2}}^1 \frac{1}{4\pi i \lambda x} \left( \frac{d}{dx} e^{2\pi i \lambda x^2} \right) dx \right| \\ &\leq \frac{1}{4\pi \lambda} \left| \left[ \frac{1}{x} e^{2\pi i \lambda x^2} \right]_{\lambda^{-1/2}}^1 + \int_{\lambda^{-1/2}}^1 \frac{1}{x^2} e^{2\pi i \lambda x^2} dx \right| \\ &\leq C \lambda^{-1/2}. \end{aligned}$$

□

#### 4. THE SÁRKÖZY-FURSTENBERG THEOREM

**Theorem 4.1** (Sárközy and Furstenberg). *Let  $\delta > 0$ . There exists an absolute constant  $C > 0$  such that if  $N \geq \exp \exp(C\delta^{-5/2})$  and  $A \subseteq [1, N]$  with  $|A| = \delta N$ , then  $A$  necessarily contains two distinct elements  $a$  and  $a'$  whose difference  $a - a'$  is a perfect square.*

Let  $B = A \cap [0, N/2]$ , we may assume without loss in generality that  $|B| \geq \delta N/2$ . If we let

$$S = \{d^2 : 1 \leq d \leq (N/2)^{1/2}\}$$

then we see that in order to prove Theorem 4.1 it suffices to show that

$$\#\{m \in A, \ell \in B : m - \ell \in S\} \geq 1.$$

To do so we consider the following bilinear expression

$$\Lambda(g, h) = \sum_{m, \ell \in \mathbf{Z}_N} g(\ell) h(m) 1_S(m - \ell) = \frac{1}{N} \sum_{r \in \mathbf{Z}_N} \widehat{g}(r) \widehat{h}(-r) \widehat{1}_S(r).$$

The significance of this expression is that

$$\Lambda(1_B, 1_A) = \#\{m \in A, \ell \in B : m - \ell \in S\}.$$

In the proof of Theorem 4.1 it shall be convenient to consider functions of mean value zero.

**Definition 4.2** (Balanced function). We define the *balanced* function of  $A$  to be  $f_A = 1_A - \delta$ .

It is clear from the definition of  $f_A$  that  $\widehat{f}_A(r) = \widehat{1}_A(r)$  for all  $r \in \mathbf{Z}_N \setminus \{0\}$ , while (in contrast to the fact that  $\widehat{1}_A(0) = |A|$ ) the fact that  $f_A$  has mean value zero implies that  $\widehat{f}_A(0) = 0$ .

Decomposing  $1_A = \delta + f_A$  we obtain that

$$\Lambda(1_B, 1_A) = \frac{\delta^2 N^{3/2}}{2^{3/2}} + \Lambda(1_B, f_A),$$

which is instructive since  $\delta^2 N^{3/2}/2^{3/2}$  is the number of square differences (not exceeding  $N/2$  with at least one point in  $B$ ) that we would expect  $A$  to contain if it were random, obtained by selecting each natural number from 1 to  $N$  independently with probability  $\delta$ .

**Definition 4.3** ( $\varepsilon$ -uniformity). We say that  $A$  is  $\varepsilon$ -uniform if  $|\widehat{f}_A(r)| \leq \varepsilon N$  for all  $r \in \mathbf{Z}_N$ .

**Lemma 4.4** (Quasirandomness). *If  $A$  is  $\varepsilon$ -uniform with  $\varepsilon = \delta^{7/2}/32c_0^{1/2}$ , then  $\Lambda(1_B, 1_A) \geq \delta^2 N^{3/2}/2^{5/2}$ .*

*Proof.* We will show that under this regularity assumption on  $A$  the term  $\Lambda(1_B, f_A)$  is in fact an *error* term and satisfies the estimate

$$|\Lambda(1_B, f_A)| \leq \delta^2 N^{3/2}/2^{5/2}.$$

To this end we first note that from Hölder's inequality it follows that

$$\begin{aligned} |\Lambda(1_B, f_A)| &\leq \frac{1}{N} \sum_{r \in \mathbf{Z}_N} |\widehat{1_B}(r)| |\widehat{f_A}(r)| |\widehat{1_S}(r)| \\ &\leq \|\widehat{f_A}\|_3 \|\widehat{1_B}\|_2 \|\widehat{1_S}\|_6 \\ &\leq \max_{r \in \mathbf{Z}_N} |\widehat{f_A}(r)|^{1/3} \|\widehat{f_A}\|_2^{2/3} \|\widehat{1_B}\|_2 r_6 ((N/2)^{1/2})^{1/6}, \end{aligned}$$

where  $\|g\|_p^p = \frac{1}{N} \sum_{r \in \mathbf{Z}_N} |g(r)|^p$ . Plancherel's identity implies that  $\|\widehat{f_A}\|_2 \leq |A|^{1/2}$  and  $\|\widehat{1_B}\|_2 = |B|^{1/2}$  while Theorem 3.1 gives the estimate  $r_6((N/2)^{1/2}) \leq c_0 N^2/4$ , we can therefore conclude that

$$|\Lambda(1_B, f_A)| \leq c_0^{1/6} \varepsilon^{1/3} (\delta/2)^{5/6} N^{3/2}. \quad \square$$

**Lemma 4.5** (Additive structure). *If  $A$  is not  $\varepsilon$ -uniform with  $\varepsilon = \delta^{7/2}/32c_0^{1/2}$ , then there exists a square-difference arithmetic progression  $P$  with  $|P| \geq N^{1/30}/4\pi$  such that  $|A \cap P| \geq (\delta + \varepsilon/8)|P|$ .*

*Proof.* Since  $A$  is not  $\varepsilon$ -uniform we know there exists  $r \neq 0$  such that  $|\widehat{1_A}(r)| \geq \varepsilon N$ . It follows from Theorem 2.2, with  $\alpha = r/N$ , that there exists  $1 \leq d \leq N^{1/3}$  such that  $\|d^2 r/N\| \leq N^{-1/30}$ , therefore if we let  $P_0$  be the square-difference arithmetic progression  $d^2, 2d^2, \dots, Ld^2$  in  $\mathbf{Z}_N$  with  $L = \lfloor N^{1/30}/4\pi \rfloor$ , it is easy to see that

$$|\widehat{1_{P_0}}(r)| \geq L - \sum_{\ell=1}^L \left| e^{2\pi i \ell d^2 r/N} - 1 \right| \geq L \left( 1 - 2\pi L \left\| \frac{d^2 r}{N} \right\| \right) \geq L/2.$$

Since  $f_A$  has mean value zero it then follows that

$$\sum_{m \in \mathbf{Z}_N} (f_A * 1_{P_0}(m))_+ = \frac{1}{2} \sum_{m \in \mathbf{Z}_N} |f_A * 1_{P_0}(m)| \geq \frac{1}{2} |\widehat{f_A}(r)| |\widehat{1_{P_0}}(r)| \geq \frac{\varepsilon |P_0| N}{4}$$

and hence that there exists  $m \in \mathbf{Z}_N$  such that

$$f_A * 1_{P_0}(m) = |A \cap (m - P_0)| - \delta |P_0| \geq \varepsilon |P_0|/4.$$

To complete the proof we note that since  $Ld^2 \leq LN^{2/3} \leq N^{7/10}$ , for all but at most  $N^{7/10}$  values  $m$  the  $\mathbf{Z}_N$ -progression  $P := m - P_0$  is in fact a genuine square-difference arithmetic progression in  $[1, N]$ . Since the sum over these ‘‘bad’’ values of  $m$ ,

$$\sum_{\text{‘‘bad’’ } m \in \mathbf{Z}_N} |f_A * 1_{P_0}(m)| \leq LN^{7/10} \leq \frac{\varepsilon |P_0| N}{8}$$

whenever  $\varepsilon \geq 8/N^{3/10}$  (as it surely will be) the existence of a ‘‘good’’  $m \in \mathbf{Z}_N$  such that

$$f_A * 1_{P_0}(m) = |A \cap (m - P_0)| - \delta |P_0| \geq \varepsilon |P_0|/8$$

is guaranteed and the result follows.  $\square$

*Proof of Theorem 4.1.* We assume that  $A$  does not contain a non-trivial square difference. It then follows from Lemmas 4.4 and 4.5 that there exists a constant  $c > 0$  and a square-difference arithmetic progression  $P_1$  with  $|P_1| \geq cN^{1/30}$  such that  $|A \cap P_1| \geq (\delta + c\delta^{7/2})|P_1|$ . If we pass to this subprogression and rescale it to have common difference 1, we obtain a set  $A_1 \subseteq [1, N_1]$  with  $|A_1| = \delta_1 N_1$  where  $N_1 \geq cN^{1/30}$  and  $\delta_1 \geq \delta + c\delta^2$  that still does not contain a square difference. After iterating this argument  $k = 2/c\delta^{5/2}$  times the density increases beyond 1, that is  $\delta_k > 1$ , an absurdity if  $N_k$  also remains large. Since  $\log N_k \geq 30^{-k} \log N - c'$ , for some  $c' > 0$ , this will be achieved if  $\log N \geq e^{C\delta^{-5/2}}$  for some suitably large constant  $C > 0$ .  $\square$

## REFERENCES

- [1] H. FURSTENBERG, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. d'Analyse Math, 71 (1977), pp. 204–256.
- [2] W. T. GOWERS, *Additive and Combinatorial Number Theory*, www.dpmms.cam.ac.uk/~wtg10/addnoth.notes.dvi.
- [3] B. GREEN, *On arithmetic structures in dense sets of integers*, Duke Math. Jour., 114, (2002) (2), 215–238.
- [4] H. L. MONTGOMERY, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics, 84.
- [5] A. SÁRZÖZY, *On difference sets of sequences of integers III*, Acta Math. Acad. Sci. Hungar. 31 (1978), pp. 355–386.