A Fourier-positive proof of Erdős Problem 42

Draft note

April 30, 2026

Abstract

We prove the following form of Erdős Problem 42 [1]. For every fixed $M \geq 1$ and all sufficiently large N, every non-empty Sidon set $A \subset [N]$ admits a Sidon set $B \subset [N]$ of size M such that

$$(A-A) \cap (B-B) = \{0\}.$$

The proof follows the Fourier-positive route suggested in the forum comments on the problem [2]. Embed $[N]$ in a prime cyclic group of order $p \asymp N$. If $F = A - A$, then Sidonicity gives

$$\widehat{\mathbf{1}_F}(r) = |\widehat{\mathbf{1}_A}(r)|^2 - (|A|-1) \geq -O(\sqrt{p}),$$

so $\mathbf{1}_F$ is asymptotically positive definite. A one-sided complexity-one counting lemma then shows that a positive proportion of M-tuples in $[N]^M$ have all pairwise differences outside F. Discarding the $O_M(N^{M-1})$ non-Sidon tuples leaves the desired set B.

1 Notation and the main statement

Write $[N] = \{1, \dots, N\}$. A finite set $S \subset \mathbb{Z}$ is called *Sidon* if its non-zero ordered differences are all distinct; in other words, if

$$s_1 - s_2 = s_3 - s_4 \neq 0, \qquad s_i \in S,$$

then $(s_1, s_2) = (s_3, s_4)$. Equivalently, the positive differences $s - s'$ with $s > s'$ are all distinct.

Theorem 1.1 (Erdős Problem 42 [1])**.** *For every integer $M \geq 1$ there is $N_0(M)$ such that, whenever $N \geq N_0(M)$ and $A \subset [N]$ is a non-empty Sidon set, there is a Sidon set $B \subset [N]$ with $|B| = M$ and*

$$(A-A) \cap (B-B) = \{0\}.$$

The empty set is excluded only because then $0 \notin A-A$, so the literal conclusion with equality to $\{0\}$ cannot hold. If the problem is phrased with $(A-A) \cap (B-B) \subseteq \{0\}$, the empty case is of course vacuous.

For a function $f : \mathbb{F}_p \to \mathbb{C}$ we use the unnormalised Fourier transform

$$\widehat{f}(r) = \sum_{x \in \mathbb{F}_p} f(x)\, e^{2\pi i - rx/p}, \qquad r \in \mathbb{F}_p.$$

If $F \subset \mathbb{F}_p$ is symmetric, then $\widehat{\mathbf{1}_F}(r)$ is real for all r.

2 A one-sided positive-definite avoidance lemma

The main input is the following compactness form of the "key lemma" discussed in the forum thread [2]; it is also closely related to the Delsarte/positive-exponential-sum viewpoint of Matolcsi–Ruzsa [4]. It is a one-sided version of the usual complexity-one counting lemma: only lower bounds on the Fourier coefficients of the forbidden set are assumed.

Lemma 2.1 (One-sided avoidance lemma)**.** *Fix $M \geq 1$ and constants $0 < \alpha_0 \leq \alpha_1 < 1/2$. Let $p_n \to \infty$ be primes, let L_n be integers with $\alpha_0 p_n \leq L_n \leq \alpha_1 p_n$, and put $I_n = \{1, \dots, L_n\} \subset \mathbb{F}_{p_n}$. Let $F_n \subset \mathbb{F}_{p_n}$ be symmetric sets with $0 \in F_n$ such that*

$$|F_n| \leq p_n/2 \tag{1}$$

and

$$\widehat{\mathbf{1}_{F_n}}(r) \geq -o(p_n) \qquad \text{uniformly for } r \in \mathbb{F}_{p_n}. \tag{2}$$

Then

$$\liminf_{n\to\infty} \mathbb{P}_{x_1,\dots,x_M \in I_n}\big(x_i - x_j \notin F_n \text{ for every } 1 \leq i < j \leq M\big) > 0,$$

where the x_i are sampled independently and uniformly from I_n, and differences are taken in $\mathbb{F}_{p_n}$.

We first record the standard compactness/counting principle from which Lemma 2.1 follows. It is the U^2 case of arithmetic regularity together with the complexity-one counting lemma for the linear forms $x_i - x_j$.

Proposition 2.2 (Compact U^2 counting principle)**.** *Let p_n, L_n, I_n be as in Lemma 2.1, and let $f_n : \mathbb{F}_{p_n} \to [0,1]$ be symmetric functions. After passing to a subsequence, there are a compact connected abelian group G, a Borel probability measure ν on G, and a measurable function $f : G \to [0,1]$ such that the following hold.*

(i) *For every fixed graph H on vertex set $\{1, \dots, h\}$,*

$$\lim_{n\to\infty} \mathbb{E}_{x_1,\dots,x_h \in I_n} \prod_{ij \in E(H)} f_n(x_i - x_j) = \int_{G^h} \prod_{ij \in E(H)} f(y_i - y_j)\, d\nu(y_1) \cdots d\nu(y_h). \tag{3}$$

(ii) *If $\mathbb{E}_{x \in \mathbb{F}_{p_n}} f_n(x) \leq 1/2 + o(1)$, then*

$$\int_G f \, d\mu_G \leq 1/2,$$

where μ_G denotes Haar probability measure on G.

(iii) *If $\widehat{f_n}(r) \geq -o(p_n)$ uniformly in $r \in \mathbb{F}_{p_n}$, then f is positive definite: after changing f on a null set, it has a Fourier expansion*

$$f(x) = \sum_{\gamma \in \widehat{G}} a_\gamma \gamma(x), \qquad a_\gamma \geq 0, \qquad \sum_\gamma a_\gamma < \infty.$$

(iv) *If $H_0 < G$ is a proper closed subgroup, then*

$$(\nu \times \nu)\{(y,z) : y - z \in H_0\} = 0. \tag{4}$$

Proof of Proposition 2.2. This is a routine compactness packaging of the $s = 1$ arithmetic regularity and counting lemma of Green–Tao [3]. Apply the U^2 arithmetic regularity lemma to f_n with an error parameter tending to zero. The structured factors are generated by boundedly many characters of $\mathbb{F}_{p_n}$, together with the archimedean coordinate x/p_n needed to keep track of the interval I_n. Since $p_n \to \infty$ through primes, every non-trivial character appearing in the limit has unbounded order; after diagonalising over the error parameter and the bounded lists of characters, the resulting inverse-limit group G is compact and connected.

The forms $x_i - x_j$ have Cauchy–Schwarz complexity one. The complexity-one counting lemma therefore transfers every fixed graph count from f_n to the limiting model, giving (3). The global averages pass to Haar averages, which gives (ii). The Fourier lower bound passes to every character of the limiting compact group and gives non-negative Fourier coefficients, which is (iii).

It remains only to justify the spread-out property (iv). Let $H_0 < G$ be proper and closed. By Pontryagin duality there is a non-trivial character $\gamma \in \widehat{G}$ with $\gamma|_{H_0} = 1$. Pulling γ back to the finite models gives a non-trivial additive character of $\mathbb{F}_{p_n}$ for all sufficiently large n. Such a character has kernel $\{0\}$. Hence, for two independent uniformly sampled points $x, z \in I_n$,

$$\mathbb{P}(\gamma_n(x - z) = 1) \le \mathbb{P}(x = z) = 1/L_n \to 0.$$

Passing to the limit gives (4). □

Proof of Lemma 2.1. Suppose the conclusion fails. Passing to a subsequence, we may assume that the displayed probability in Lemma 2.1 tends to zero. Apply Proposition 2.2 to $f_n = \mathbf{1}_{F_n}$.

By (1), the limiting function f has Haar mean at most $1/2$. By (2), it is positive definite. Replacing f by its continuous positive-definite representative, write

$$f(x) = \sum_{\gamma \in \widehat{G}} a_\gamma \gamma(x), \qquad a_\gamma \ge 0.$$

Since $0 \le f \le 1$, we have $f(0) \le 1$. If $f(0) < 1$, then $|f(x)| \le f(0) < 1$ for all x, and so $f(x) < 1$ everywhere. Otherwise $f(0) = 1$ and $\sum_\gamma a_\gamma = 1$. In that case equality $f(x) = 1$ can occur only when every character in $\mathrm{supp}(a)$ takes the value 1 at x. Thus

$$K := \{x \in G : f(x) = 1\} = \{x \in G : \gamma(x) = 1 \text{ for every } \gamma \in \mathrm{supp}(a)\}$$

is a closed subgroup of G. It is proper, since otherwise $f \equiv 1$, contradicting $\int f \, d\mu_G \le 1/2$.

By the spread-out property (4), for every pair $i < j$ the set of $(y_1, \dots, y_M) \in G^M$ with $y_i - y_j \in K$ has ν^M-measure zero. Outside the union of these finitely many null sets, one has $f(y_i - y_j) < 1$ for all $i < j$. Hence

$$\prod_{1 \le i < j \le M} \big(1 - f(y_i - y_j)\big) > 0$$

for ν^M-almost every $(y_1, \dots, y_M)$, and the integral of this non-negative product is strictly positive.

Expanding the product $\prod_{i<j}(1 - \mathbf{1}_{F_n}(x_i - x_j))$ and applying (3) to each subgraph of K_M gives

$$\begin{aligned} &\lim_{n \to \infty} \mathbb{E}_{x_1, \dots, x_M \in I_n} \prod_{1 \le i < j \le M} \big(1 - \mathbf{1}_{F_n}(x_i - x_j)\big) \\ &\quad = \int_{G^M} \prod_{1 \le i < j \le M} \big(1 - f(y_i - y_j)\big) \, d\nu(y_1) \cdots d\nu(y_M) > 0, \end{aligned}$$

contradicting the assumption that the avoidance probability tends to zero. □

3 The reduction from arbitrary Sidon sets

We now prove Theorem 1.1. The point of this section is that no maximality or extremality assumption on A is needed.

Lemma 3.1 (Fourier positivity of $A-A$)**.** *Let $A \subset [N]$ be Sidon and non-empty. Let $p > 2N$ be prime, and view A as a subset of $\mathbb{F}_p$. Put $F = A - A \subset \mathbb{F}_p$. Then*

$$\mathbf{1}_F = \mathbf{1}_A * \mathbf{1}_{-A} - (|A|-1)\delta_0$$

and consequently

$$\widehat{\mathbf{1}_F}(r) = |\widehat{\mathbf{1}_A}(r)|^2 - (|A|-1) \geq -(|A|-1) \qquad (r \in \mathbb{F}_p). \tag{5}$$

Moreover

$$|F| = 1 + |A|(|A|-1) \leq 2N-1. \tag{6}$$

Proof. Since $p > 2N$, all differences between elements of $[N]$ are represented without wrap-around in $\mathbb{F}_p$. Sidonicity says that every non-zero difference has at most one ordered representation $a - a'$ with $a, a' \in A$. Thus $\mathbf{1}_A * \mathbf{1}_{-A}$ is equal to $\mathbf{1}_F$ away from 0, while at 0 it is $|A|$ and must be reduced to 1. This gives the convolution identity and hence (5).

The positive differences of A are distinct and lie in $\{1, \dots, N-1\}$. Hence $\binom{|A|}{2} \leq N-1$. Since the non-zero elements of F are the positive and negative differences,

$$|F| = 1 + 2\binom{|A|}{2} \leq 2N-1.$$

□

Proof of Theorem 1.1. The case $M = 1$ is immediate, so assume $M \geq 2$. It is enough to rule out a sequence of counterexamples with $N \to \infty$.

Let $A_n \subset [N_n]$ be non-empty Sidon sets with $N_n \to \infty$. Choose, by Bertrand's postulate, a prime p_n satisfying

$$4N_n < p_n < 8N_n.$$

Set $F_n = A_n - A_n \subset \mathbb{F}_{p_n}$ and $I_n = [N_n] \subset \mathbb{F}_{p_n}$. Then $N_n/p_n \in (1/8, 1/4)$, and Lemma 3.1 gives

$$|F_n| \leq 2N_n - 1 < p_n/2$$

and

$$\widehat{\mathbf{1}_{F_n}}(r) \geq -(|A_n|-1) \geq -O(\sqrt{N_n}) = -o(p_n),$$

uniformly in $r \in \mathbb{F}_{p_n}$. Lemma 2.1, with $\alpha_0 = 1/8$ and $\alpha_1 = 1/4$, therefore implies that a positive proportion of ordered M-tuples

$$(b_1, \dots, b_M) \in [N_n]^M$$

satisfy

$$b_i - b_j \notin A_n - A_n \qquad (1 \leq i < j \leq M). \tag{7}$$

Here there is no ambiguity between integer and modular differences, because all differences lie in $(-N_n, N_n)$ and $p_n > 2N_n$. Since $0 \in A_n - A_n$, every tuple satisfying (7) has pairwise distinct entries.

It remains to impose the Sidon condition on the tuple. The number of ordered M-tuples in $[N_n]^M$ which are not Sidon is $O_M(N_n^{M-1})$. Indeed, failure of the Sidon property gives a non-trivial linear equation

$$b_i - b_j = b_k - b_l$$

among four indexed variables, and there are only $O_M(1)$ choices of i, j, k, l; each non-trivial equation has $O(N_n^{M-1})$ solutions. The good tuples supplied by Lemma 2.1 number $\gg_M N_n^M$ along the sequence, so for all sufficiently large n at least one of them is Sidon. Its set of entries is a Sidon set $B \subset [N_n]$ of size M, and (7) gives

$$(A_n - A_n) \cap (B - B) = \{0\}.$$

This contradicts the existence of counterexamples and proves the theorem. □

4 Relation with the extremal Fourier-counting argument

The proof above uses only the one-sided Fourier positivity which every Sidon set has. It is useful to record how this compares with the more concrete extremal argument for largest Sidon sets.

Suppose $A \subset [N]$ is a Sidon set satisfying

$$|A| = N^{1/2}(1 + o(1))$$

and

$$\left\| \widehat{\mathbf{1}_A} - \frac{|A|}{N} \widehat{\mathbf{1}_{[N]}} \right\|_{L^\infty(\mathbb{T})} = o(N^{1/2}), \tag{8}$$

where the Fourier transform is now taken on $\mathbb{Z}$ and restricted to $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Largest Sidon subsets of $[N]$ satisfy (8) by the theorem of Ortega–Prendiville [5].

Let $D = A - A$ and

$$R_N = \mathbf{1}_{[N]} * \mathbf{1}_{-[N]}, \qquad R_N(d) = (N - |d|)_+, \qquad \lambda = \left(\frac{|A|}{N}\right)^2.$$

Since A is Sidon,

$$\mathbf{1}_D = \mathbf{1}_A * \mathbf{1}_{-A} - (|A| - 1)\delta_0.$$

The Fourier-uniformity assumption gives

$$\left\| \widehat{\mathbf{1}_D - \lambda R_N} \right\|_{L^\infty(\mathbb{T})} = o(N).$$

Consequently, for every $X, Y \subset [N]$,

$$\left| \sum_{x \in X} \sum_{y \in Y} \big(\mathbf{1}_D(x - y) - \lambda R_N(x - y) \big) \right| = o(N^2),$$

by Fourier inversion and Cauchy–Schwarz. Thus the kernels

$$W_A(x, y) = 1 - \mathbf{1}_D(x - y), \qquad W_0(x, y) = 1 - \lambda R_N(x - y)$$

have cut distance $o(N^2)$. The dense graph counting lemma transfers K_M counts from W_A to W_0. Since

$$W_0(x,y) = \frac{|x-y|}{N} + o(1)$$

uniformly in $x, y \in [N]$, a Riemann-sum calculation gives

$$N^{-M} \sum_{b_1,\dots,b_M \in [N]} \prod_{1 \le i < j \le M} \left(1 - \mathbf{1}_D(b_i - b_j)\right) \to \int_{[0,1]^M} \prod_{1 \le i < j \le M} |x_i - x_j| \, dx_1 \cdots dx_M > 0.$$

After discarding $O_M(N^{M-1})$ non-Sidon tuples, this gives the desired B for extremal Sidon sets. The previous sections supply the missing unconditional reduction: arbitrary Sidon sets need not be extremal, but their difference sets are nevertheless asymptotically positive definite, and Lemma 2.1 is exactly the one-sided counting input needed to exploit that fact.

References

[1] T. F. Bloom, *Erdős Problem #42*, https://www.erdosproblems.com/42, accessed 30 April 2026.

[2] T. Tao, forum comments on Erdős Problem #42, April 2026, https://www.erdosproblems.com/forum/thread/42#post-6092.

[3] B. Green and T. Tao, *An arithmetic regularity lemma, associated counting lemma, and applications*, arXiv:1002.2028.

[4] M. Matolcsi and I. Z. Ruzsa, *Difference sets and positive exponential sums I. General properties*, arXiv:1207.1781.

[5] M. Ortega and S. Prendiville, *Extremal Sidon sets are Fourier uniform, with applications to partition regularity*, arXiv:2110.13447.