hexagon:2611.01316v1

Additive energy and the exceptional set in Goldbach's problem

Wren Aquila

29 November 2026

Abstract

Assume the generalized Riemann hypothesis for Dirichlet L-functions, including $\zeta(s)$. For every fixed $\beta < 1/4$, the number of even integers up to X that fail to be sums of two primes is $O_\beta(\sqrt{X}\exp\{-(\log X)^\beta\})$. A mean-square estimate for primes in short arithmetic progressions bounds the additive energy of each subset of the exceptions from below. We apply it first at stride one and then on a progression obtained from a containment theorem of Konyagin. Assuming also Theorem 1.4 of Raghavan's 2026 preprint, the exponential factor becomes $\exp\{-c\sqrt{\log X}/\log\log X\}$. At stride two it also gives the following conclusion for every large even N. Almost every prime $\ell \le M$ admits a representation $N = p_1 + p_2 + 2\ell^2$, where one may take $M = (\log N)^5(\log\log N)^2\log\log\log N$.

1 Results

Let $E(X)$ count the even integers v in $[4, X]$ for which $v = p + p'$ has no solution in primes, and let $\pi(x)$ count the primes up to x. In this paper GRH means the generalized Riemann hypothesis for every Dirichlet L-function, including $\zeta(s)$.

Theorem 1. *Assume the generalized Riemann hypothesis for all Dirichlet L-functions, including the Riemann zeta function. For every fixed real $\beta < 1/4$ and every $X \ge 4$,*

$$E(X) \ll_\beta \sqrt{X}\,\exp\{-(\log X)^\beta\}. \tag{1}$$

In particular, $E(X) \ll_B \sqrt{X}/(\log X)^B$ for every fixed $B > 0$.

Under GRH, Hardy and Littlewood [10, Theorem B, p. 55] obtained $E(X) \ll_\varepsilon X^{1/2+\varepsilon}$. In 1992 Goldston obtained $E(X) \ll \sqrt{X}(\log X)^4$ [7, p. 122, following Corollary 3.1, and (8.5) on p. 152]. The third logarithmic power follows from the 1993 short-interval result of Kaczorowski, Perelli and Pintz [11, Corollary]. Under GRH they bound the number of exceptions in $(x, x+H]$ by $O(\sqrt{H}(\log x)^3)$ for $H \le x$ with $H/(\log x)^6 \to \infty$. Taking $H = x$ and summing dyadically gives $E(X) \ll \sqrt{X}(\log X)^3$. Their corrigendum [12] credits Goldston with the correction to their (18). Languasco and Perelli [13, §5, (26), pp. 359–360] treat the endpoints in Lemma 1 of [11] and recover the corollary under GRH. Bhowmik and Halupczok state $E(x) \ll x^{1/2}\log x$ under the Riemann hypothesis for $\zeta(s)$ [2, §3.3 of the preprint].

Languasco and Perelli's hypothesis GMC(θ) adds a pair-correlation bound for zeros across Dirichlet characters to GRH. For fixed $0 < \theta \le 1/2$ they obtain $O_\varepsilon(X^\varepsilon)$ exceptions in $[X, X+X^{2\theta}]$ and $O_\varepsilon(X^{1-2\theta+\varepsilon})$ in $[X, 2X]$ [13, (4) and Corollary 1, pp. 350–351]. Summing the latter bound gives $E(X) \ll_\varepsilon X^{1-2\theta+\varepsilon}$. Under GRH and their Dirichlet ratios conjecture $\mathrm{RC}_D(\omega_D)$ for all primitive conductors, with fixed $\omega_D > 0$, Gou, Wang and Xu obtain a Goldbach asymptotic for every even total, giving $E(X) \ll 1$ [9, Theorem 1.1, (1.3)].

Corollary 2. *Assume the generalized Riemann hypothesis for all Dirichlet L-functions, including the Riemann zeta function. Let N tend to infinity through even integers, put $L = \log N$, and let $M = M(N)$ be a positive integer with*

$$M \le \frac{\sqrt{N}}{8L^4}, \qquad \frac{M}{L^5(\log(2M))^2} \longrightarrow \infty.$$

For all but $o(\pi(M))$ primes $\ell \le M$, there exist primes $p_1 \in [N/10, N/6]$ and $p_2 > p_1$ such that $N = p_1 + p_2 + 2\ell^2$. In particular, one may take

$$M = \left\lceil L^5 (\log L)^2 \log\log L \right\rceil,$$

or replace the last factor by any more slowly diverging positive function.

For the displayed choice of M, the exceptional proportion is $O((\log\log\log N)^{-1/4})$. Perelli [16, Corollary 1] studied Goldbach exceptions among the values of a fixed polynomial. Brüdern, Kawada and Wooley [3, Theorem 1] bounded the number of exceptional indices using mean values of their exponential sum. Althöfer, Chen, Perelli and Pintz give further bounds for polynomial values [1, Theorem 1]. Corollary 2 fixes N and varies the prime-square shift with $\ell \le M$.

For a finite set $D \subset \mathbb{Z}$ write $\mathcal{E}(D) = \#\{(u,v,w,t) \in D^4 : u + v = w + t\}$. It is always at most $|D|^3$, since three entries determine the fourth. The next estimate supplies the reverse constraint at a missing total. Its uniformity in the initial point and stride will allow both to depend on the exceptional set.

Proposition 3. *Assume the generalized Riemann hypothesis for all Dirichlet L-functions, including the Riemann zeta function. Let X be sufficiently large, $L = \log X$, and $R = \lfloor \sqrt{X}/L^4 \rfloor$. Let $a \in \mathbb{Z}$ and $q, H \ge 1$ be integers with $qH \le X/1000$. Suppose $D \subset [-H, H] \cap \mathbb{Z}$ and every $a + qk$, $k \in D$, is even, belongs to $[X/2, X]$, and has no representation $p + p'$ with $p \in [X/10, X/6]$ and p' prime. Then*

$$|D|^4 \ll L^{12} \sqrt{H}\, \mathcal{E}(D). \tag{2}$$

If $2q\sqrt{H} \le R$, the factor L^{12} can be replaced by L^5. The constants are absolute.

At stride one, (2) gives an energy refinement of the short-interval count in [11]. It bounds each exceptional subset in terms of its own energy and gives $|D| \ll L^{12}\sqrt{H}$ on using $\mathcal{E}(D) \le |D|^3$. Li and Liu assume that all nontrivial zeros of primitive Dirichlet L-functions, including $\zeta(s)$, satisfy $\Re\rho \le \Theta$, for a fixed $1/2 \le \Theta < 11/12$. Their minor-arc fourth moment gives $E(X) \ll_\Theta \sqrt{X}(\log X)^{100}$ [15, Theorems 1 and 2]. Earlier, under a common fixed zero-free half-plane $\Re s > \Theta$ with $\Theta < 1$, Pintz and Althöfer obtained $E(X) \ll_{\Theta,\varepsilon} X^{7/12+\varepsilon}$ [18, Theorem 1].

The fourth moment of the exceptional set itself occurs in Althöfer, Chen, Perelli and Pintz [1, (4.3)–(4.6)]. For an arbitrary set A of even Goldbach exceptions in $(X/2, X]$, take their exponent to be four and put $K_A(\alpha) = \sum_{v \in A} e^{-2\pi i v\alpha}$. Let $I_j(\mathfrak{a}) = \int_{\mathfrak{a}} |S_w(\alpha)|^j \, d\alpha$ for their smoothed prime sum. With $\mathfrak{m}$ their minor arcs and $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ of measure one, their Hölder step gives

$$(X|A|)^4 \ll I_4(\mathfrak{m}) I_2(\mathbb{T})^2 \int_{\mathbb{T}} |K_A(\alpha)|^4 \, d\alpha, \qquad \int_{\mathbb{T}} |K_A(\alpha)|^4 \, d\alpha = \mathcal{E}(A).$$

Li and Liu's bound $I_4(\mathfrak{m}) \ll_\Theta X^{5/2}(\log X)^{100}$ and Parseval's estimate $I_2(\mathbb{T}) \ll X \log X$ thus give $|A|^4 \ll_\Theta \sqrt{X}(\log X)^{102}\mathcal{E}(A)$ under their zero hypothesis with $\Theta < 11/12$ [15, Theorem 1 and Proposition 4.1]. Proposition 3 proves a bound at each admissible stride q and length H, including for totals missing a representation with one prime in the prescribed interval.

For subsets of the squares, Chang [4], following Bourgain, combined Balog–Szemerédi–Gowers and Freiman's theorem with bounds for squares on progressions to estimate the fourth moment. Sanders [22, Theorem 11.7] sharpened this argument using his Bogolyubov–Ruzsa lemma. Here the inverse argument applies to the Goldbach exceptions. At stride one, (2) forces any set of nearly $\sqrt{X}$ exceptions in a dyadic interval to have large additive energy. Balog–Szemerédi–Gowers then gives a large subset with a small difference set. Konyagin's iteration, in the containment form recorded by Sanders, gives a pair of sets of small relative growth in a finite model. Their large Fourier coefficients yield a long ordinary progression which lifts into an iterated sum and difference set of the exceptions. Averaging translates puts many of the original exceptions on a segment of this progression. Applying (2) at the stride of that segment gives the contradiction. For Corollary 2 the indices are negative prime squares, whose energy has a direct upper bound.

Changes in version 2. In version 1 the torsion-free theorem of Sanders gave exponent 1/5 [22, Theorem 11.3]. Its general abelian-group form gives 1/7 [22, Theorem 1.1]. Konyagin's containment estimate [23, Proposition 8.5] gives every fixed $\beta < 1/4$ in Theorem 1. Under GRH and Theorem 1.4 of Raghavan's preprint, Section 5 gives a stronger bound. A digit construction there bounds the saving obtainable from the energy estimate alone. The exponent 5 in Corollary 2 comes directly from Proposition 3 at stride two.

2 A prime model at a missing total

Write $\mathrm{e}(t) = \exp(2\pi i t)$, $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, and use probability Haar measure on $\mathbb{T}$. Let $\vartheta(n) = \log n$ if n is prime and zero otherwise. The von Mangoldt function is denoted by Λ, the Möbius function by μ, and Euler's totient by φ. As usual (a, b) is the greatest common divisor. For $I = [X/10, X/6]$, take $g = \vartheta \mathbf{1}_I$. Fix a real smooth $0 \le W \le 1$ supported on $[1/4, 1]$, equal to one on $[1/3, 9/10]$. With a star denoting reduced residue classes, put

$$c_d(n) = \sideset{}{^*}\sum_{u \bmod d} \mathrm{e}(un/d), \qquad F(n) = \sum_{d \le R} \frac{\mu(d)}{\varphi(d)} c_d(n), \qquad f(n) = W(n/X)(\vartheta(n) - F(n)).$$

The term at $d = 1$ is one. All these weights are real, since the unit residues are closed under negation. We use $(f * g)(v) = \sum_n f(v - n) g(n)$.

For $y \ge 2$ we will use the estimates

$$\sum_{d \le y} \frac{1}{\varphi(d)} \ll \log(2y), \qquad \sum_{d \le y} \frac{\mu^2(d) d}{\varphi(d)^2} \ll \log(2y). \tag{3}$$

Indeed, for $j = 1, 2$ one has $(d/\varphi(d))^j = \sum_{s \mid d} b_j(s)$, where b_j is multiplicative, supported on squarefree integers, with $b_j(p) = (1 - 1/p)^{-j} - 1 = O(1/p)$. Summing after division by d and using $\sum_s b_j(s)/s = \prod_p (1 + b_j(p)/p) < \infty$ gives both bounds. Also $d/\varphi(d) = \sum_{s \mid d} \mu^2(s)/\varphi(s) \ll \log(2d)$.

Under GRH the prime number theorem in a reduced class $b \bmod d$ gives, uniformly for $t \asymp X$, $d \le R$,

$$\sum_{\substack{p \le t \\ p \equiv b \bmod d}} \log p = t/\varphi(d) + O(\sqrt{X} L^2).$$

For $d \ge 3$ this follows from Ernvall-Hytönen and Palojärvi [6, Theorem 3]. For every $U \ge 2$ the number of higher prime powers up to U is at most $U^{1/2} + O(U^{1/3} \log(2U)) \ll \sqrt{U}$, by counting

the squares and then the exponents $3 \le j \le \log U/\log 2$. At $U = 2X$ their total weight is $O(\sqrt{X}L)$. The two reduced classes modulo 3 and the prime 3 together give the estimate for $d = 1$. Removing the prime 2 gives it for $d = 2$. In particular $\sum_{p\le x} \log p \sim x$ and $\pi(x) \sim x/\log x$ by partial summation.

For $X/2 \le v \le X$ and $p \in I$, the cutoff equals one at $(v-p)/X$. Every such prime is prime to $d \le R$ for large X. Summing the defining exponential sum over reduced b gives $\sum_b^* c_d(v-b) = \mu(d)c_d(v)$, since $c_d(u) = \mu(d)$ when $(u,d) = 1$. To control the errors, Möbius inversion in the coprimality condition gives $c_d(t) = \sum_{s|(d,t)} s\mu(d/s)$. A reduced residue modulo $s \mid d$ has $\varphi(d)/\varphi(s)$ reduced lifts modulo d, as follows prime by prime. Consequently

$$\frac{1}{\varphi(d)} \sideset{}{^*}\sum_{b \bmod d} |c_d(v-b)| \le \sum_{s|d} \frac{s}{\varphi(s)}, \qquad \sum_{d\le R} \sum_{s|d} \frac{s}{\varphi(s)} \le R \sum_{s\le R} \frac{1}{\varphi(s)} \ll R\log(2R).$$

Applying the progression estimate at both endpoints of I (a possible endpoint prime costs $O(L)$) therefore gives

$$(F * g)(v) = |I| \sum_{d\le R} \frac{\mu^2(d)c_d(v)}{\varphi(d)^2} + O(\sqrt{X}L^2 R\log(2R)), \tag{4}$$

where $|I| = X/15$. The error is $O(X/L)$.

For squarefree d, the Chinese remainder theorem gives $c_d(v) = \prod_{p|d} c_p(v)$, with $c_p(v) = p-1$ if $p \mid v$ and $c_p(v) = -1$ otherwise. In particular $|c_d(v)| \le (d,v)$. For any fixed $0 < \delta < 1/4$, the pointwise bound $d/\varphi(d) \ll \log(2d)$ proved above gives $\varphi(d)^{-2} \ll d^{-2}\log^2(2d) \ll_\delta d^{-2+\delta}$. The absolute tail of the series in (4) is bounded by

$$\ll_\delta \sum_{s|v} s \sum_{\substack{d>R \\ s|d}} d^{-2+\delta} \ll_\delta R^{-1+\delta}\tau(v).$$

The inner sum is $O_\delta(s^{-1}R^{-1+\delta})$, also for $s > R$. To see that the divisor count satisfies $\tau(v) \ll_\delta v^\delta$, write $\tau(v) = \prod_{p^\nu \| v}(\nu+1)$ and use $\nu + 1 \le p^{\delta\nu}$ for $p^\delta \ge 2$, absorbing the supremum of $(\nu+1)p^{-\delta\nu}$ at each of the finitely many smaller primes. Taking, for example, $\delta = 1/10$ makes the tail $o(1)$ uniformly. For even v, the completed product is

$$2\prod_{p>2}\Big(1 - \frac{1}{(p-1)^2}\Big) \prod_{\substack{p|v \\ p>2}} \frac{p-1}{p-2}.$$

The first product converges to a positive constant. Thus for every missing total specified in Proposition 3, there is an absolute $c_0 > 0$ such that

$$(f * g)(v) = -(F * g)(v) \le -c_0 X. \tag{5}$$

3 Mean squares on progressions

For an interval $J_0 \subset [X/5, 2X]$ of starting points write $\|u\|_{J_0}^2 = X^{-1}\sum_{x\in J_0\cap\mathbb{Z}} |u(x)|^2$. All the following estimates are uniform in J_0. For integers $m, J \ge 1$ with $mJ \le X/20$, set

$$U_m(x) = \frac{m}{\varphi(m)}\mathbf{1}_{(x,m)=1}, \qquad \Delta_m = \mathbf{1}_{m>R}\frac{mL}{R^2} + \frac{L^2}{\sqrt{X}}.$$

We shall prove the prefix estimate

$$\Big\| \sum_{j=1}^{J} (\vartheta - F)(x + mj) \Big\|_{J_0}^2 \ll JL^2 + J^2\Delta_m. \tag{6}$$

The prime contribution

For $(b,m)=1$ put $\psi(y;m,b)=\sum_{n\le y,\ n\equiv b \bmod m}\Lambda(n)$. Prachar's original GRH estimate is a weighted mean square for primes in multiplicative intervals $(y,y+y/U]$, for sufficiently large U [19, §2, (6), p. 273]. We use the fixed-length formulation recorded by Goldston and Yıldırım [8, (1.1)–(1.4), p. 563]. Their (1.4) gives, for each modulus throughout the full range of their (1.3), namely $Y\ge 2$, $1\le m\le Y$ and $1\le s\le Y$,

$$\sideset{}{^*}\sum_{b \bmod m}\int_{Y}^{2Y}\left|\psi(y+s;m,b)-\psi(y;m,b)-\frac{s}{\varphi(m)}\right|^2 dy \ll sY\log^2(mY). \tag{7}$$

Use $s=mJ$. If $x\equiv b \bmod m$, the class members in $(y,y+s]$ for $x\le y<x+m$ are exactly $x+m,\dots,x+mJ$. The intervals $[x,x+m)$ have disjoint interiors for successive starts within a class. Their union for $x\in J_0$ lies in $[X/5,\,2X+X/20]$, covered by four intervals $[Y,2Y]$ with $Y=2^iX/5$, $0\le i\le 3$. Thus $m,s\le X/20<Y$ even for a one-term prefix. Integrating and dividing by mX bounds the squared norm of $\sum_{j\le J}\Lambda(x+mj)-JU_m(x)$ over unit starts by $O(JL^2)$. For ϑ both terms vanish at nonunit starts, since any prime $x+mj$ is larger than m. On unit starts, Cauchy's inequality bounds the squared cost of removing higher prime powers by

$$\frac{J}{X}\sum_{j\le J}\sum_{x\in J_0\cap\mathbb{Z}}|(\Lambda-\vartheta)(x+mj)|^2\ll J^2X^{-1/2}L^2,$$

using the higher-prime-power bound of Section 2 at $U=3X$. This proves

$$\left\|\sum_{j\le J}\vartheta(x+mj)-JU_m(x)\right\|_{J_0}^2\ll JL^2+J^2X^{-1/2}L^2. \tag{8}$$

One can also see why Prachar's original weight suffices for the prefixes in Section 4, where $J\le\sqrt{T}+2$, $T=4H\le X/250$, and $Y\ge X/5$. Thus $\log(Y/J)\ge L/2$ for large X. For $U\asymp Y/s$ one has $\log(mU)=\log(Y/J)+O(1)$, so Prachar's $\sigma_0=1/2+O(1/\log(mU))$ gives $y^{-1-2\sigma_0}\asymp Y^{-2}$ for $y\asymp Y$ [19, §2, (1), (5)–(6)]. To pass to length s, let $D_b(y,u)$ denote the sum of prime weights in class b in $(y,y+u]$ minus $u/\varphi(m)$. Square $D_b(y,s)=D_b(y,u)-D_b(y+s,u-s)$, bound by twice the sum of the two squares, and average over $2s\le u\le 3s$. In the two resulting bounds set $\delta=u/y$ and $\delta=(u-s)/(y+s)$, respectively. In each case $\delta\asymp s/Y$, $du\ll Y\,d\delta$, and (6) of [19] with $U=1/\delta$ bounds the sum of the integrals in y by $O(Y^2\delta L^2)$. The fixed-length variance is consequently $\ll(Y/s)\int_{\delta\asymp s/Y}Y^2\delta L^2\,d\delta\ll sYL^2$. If necessary, first split the interval into a fixed number of equal pieces to ensure that U exceeds Prachar's absolute lower threshold.

The model contribution

We use the following elementary form of the large sieve. For distinct reduced fractions $\beta\in\mathbb{T}$ with denominators at most R, and complex coefficients a_β, one has

$$\sum_{x\in J_1\cap\mathbb{Z}}\left|\sum_{\beta}a_\beta\mathrm{e}(x\beta)\right|^2\ll X\sum_{\beta}|a_\beta|^2 \tag{9}$$

on every interval J_1 of length at most $3X$. To see this, majorize its indicator by a translate and dilation by X of a fixed nonnegative smooth compactly supported function. The trivial $O(X)$

bound for the exponential sum of this weight and two applications of summation by parts give $O(X(1+X\|t\|_{\mathbb{T}})^{-2})$, since the sum of the absolute second differences is $O(X^{-1})$. Here $\|t\|_{\mathbb{T}}$ is distance to the nearest integer. Distinct fractions have circular spacing at least $R^{-2} \geq X^{-1}$, so the sum of these bounds over β' at $t = \beta - \beta'$ is $O(X)$ for each β. Expanding the square and using $2|a_\beta a_{\beta'}| \leq |a_\beta|^2 + |a_{\beta'}|^2$ proves (9).

The fractions with $d \mid m$ have constant phase as j varies. Completing the divisor sum gives the progression mean

$$\sum_{d \mid m} \frac{\mu(d)}{\varphi(d)} c_d(x) = \prod_{p \mid m} \left(1 - \frac{c_p(x)}{p-1}\right) = U_m(x).$$

By orthogonality of the distinct reduced fractions on one period modulo m, the omitted terms with $d > R$ have mean square $\sum_{d \mid m,\ d>R} \mu^2(d)/\varphi(d)$. Covering J_0 by complete periods costs an absolute factor because $m \leq X/20$. There are at most m/R such divisors, by the injection $d \mapsto m/d$, and $1/\varphi(d) \ll L/R$. Hence their contribution to the squared norm of the sum of J terms is $O(J^2 \mathbf{1}_{m>R} mL/R^2)$.

For $d \nmid m$, apply (9) in x to the average over j. Write a squarefree $d = ev$, $e = (d, m)$, $v > 1$. Then $(v, m) = 1 = (e, v)$, and cancelling e maps the unit numerators of um/d mod 1 onto the unit numerators modulo v, each with multiplicity $\varphi(e)$. For $A_J(t) = J^{-1} \sum_{j=1}^{J} \mathrm{e}(jt)$, we have

$$\sum_{w \bmod v}^{*} |A_J(w/v)|^2 \ll v/J.$$

If $v \geq J$, summing over all residues gives v/J by orthogonality. If $1 < v < J$, the geometric sum bound gives $O(v^2/J^2)$ after summing the inverse squares of $\min(w, v-w)$ for $1 \leq w < v$. Thus the sum of squared coefficients in (9) is at most

$$\ll \frac{1}{J} \sum_{e \mid m} \frac{\mu^2(e)}{\varphi(e)} \sum_{v \leq R} \frac{\mu^2(v) v}{\varphi(v)^2} \ll \frac{L^2}{J}$$

by (3) and $\sum_{e \mid m} \mu^2(e)/\varphi(e) = m/\varphi(m)$. Multiplying by J^2 and combining the two parts of the model with (8) proves (6). We shall also use the global masses

$$\frac{1}{X} \sum_{n \in \mathbb{Z}} |f(n)|^2 \ll L, \qquad \frac{1}{X} \sum_{n \in \mathbb{Z}} |g(n)|^2 \ll L. \tag{10}$$

For the primes this follows from $\sum_{p \leq X} \log p \ll X$. For F on the support of W, use (9) and the squared coefficient sum $\sum_{d \leq R} \mu^2(d)/\varphi(d) \ll L$.

4 From progressions to additive energy

Let a, q, H satisfy the hypotheses of Proposition 3. Put $T = 4H$, and for $\alpha \in \mathbb{T}$ define

$$F_x(\alpha) = \frac{1}{T} \sum_{i=1}^{T} f(x + qi) \mathrm{e}(i\alpha), \qquad K_f(\alpha) = \frac{1}{X} \sum_{x \in \mathbb{Z}} |F_x(\alpha)|^2.$$

We first prove the uniform bounds

$$\sup_{\alpha \in \mathbb{T}} K_f(\alpha) \ll \begin{cases} L^9/\sqrt{H} & \text{for every admissible } q, H, \\ L^2/\sqrt{H} & \text{if } q\sqrt{T} \leq R. \end{cases} \tag{11}$$

Only $x \in J_* = [X/4 - qT, X]$ can contribute. As $qT \le X/250$, all translates of J_* by integers between $-q\sqrt{T}$ and qT lie in $[X/5, 2X]$. Put $Q = \lfloor \sqrt{T} \rfloor$. The $Q+1$ points $0, \alpha, \dots, Q\alpha$, counted with multiplicity, have a circular gap of length at most $1/(Q+1) < 1/\sqrt{T}$. Subtracting the indices at its ends gives $\alpha = c/r + \eta \bmod 1$ with $1 \le r \le Q$ and $|\eta| < 1/(r\sqrt{T})$. Divide $[1, T] \cap \mathbb{Z}$ into $\lceil T/(r\sqrt{T}) \rceil$ consecutive blocks as equally as possible. Each block length $h \asymp r\sqrt{T}$.

In any prefix of a block, split the indices i into residue classes modulo r. On each class $\mathrm{e}(ci/r)$ is constant. For a nonempty class write the arguments as $x + q(i_0 - r) + mj$, $1 \le j \le J$, with i_0 its first index and $m = qr$. Here $J \le h/r + 1 \le \sqrt{T} + 2$ by the balanced block lengths, $mJ \le q(h + r) \le 2qT < X/20$, and the translated starts are in the range of (6). The triangle inequality for $\| \cdot \|_{J_*}$, followed by (6) on the translated intervals, shows that each rationally phased block prefix of $\vartheta - F$ has norm at most

$$Ch \left(L\sqrt{r/h} + \sqrt{\Delta_m} \right).$$

Indeed $\sum_{\text{classes}} \sqrt{J} \le \sqrt{rh}$ and $\sum_{\text{classes}} J \le h$, including partial blocks. Restore the weight $w_i(x) = W((x + qi)/X)\mathrm{e}(i\eta)$ by summation by parts within the block. Its supremum is at most one and $\sum_i \sup_x |w_{i+1}(x) - w_i(x)| \ll h(q/X + |\eta|) \ll 1$. The norm bound thus also holds for the weighted block. Summing in norm over the blocks and dividing by T gives

$$K_f(\alpha) \ll L^2/\sqrt{T} + \Delta_{qr}.$$

Since $qr \le q\sqrt{T} \le X/(250\sqrt{T})$ and $R \asymp \sqrt{X}/L^4$, the discarded divisors cost at most $O(L^9/\sqrt{T})$. They contribute zero when $q\sqrt{T} \le R$. Also $X^{-1/2} \le T^{-1/2}$. This proves (11).

To recover the missing totals, reflect the other prime weight about a and form

$$G_x(\alpha) = \frac{1}{T} \sum_{j=1}^{T} g(a - x - qj)\mathrm{e}(j\alpha), \qquad V(\alpha) = \frac{T}{X} \sum_{x \in \mathbb{Z}} F_x(\alpha)\overline{G_x(\alpha)}.$$

All sums are finite. With $t_+ = \max(t, 0)$, using $\widehat{V}(k) = \int_{\mathbb{T}} V(\alpha)\mathrm{e}(-k\alpha)\, d\alpha$ gives

$$\widehat{V}(k) = (1 - |k|/T)_+ \, (f * g)(a + qk)/X. \tag{12}$$

Indeed $i - j = k$, and upon setting $n = x + qi$ the second factor becomes $g(a + qk - n)$. There are $(T - |k|)_+$ such pairs.

Write $K_g = X^{-1} \sum_x |G_x|^2$. By orthogonality in α, translation in x and (10),

$$\int_{\mathbb{T}} K_f = \frac{1}{XT} \sum_n |f(n)|^2 \ll \frac{L}{T}, \qquad \int_{\mathbb{T}} K_g = \frac{1}{XT} \sum_n |g(n)|^2 \ll \frac{L}{T}.$$

Pointwise Cauchy gives $|V| \le T\sqrt{K_f K_g}$. Integrating once and then squaring before integration yields

$$\|V\|_1 \ll L, \qquad \|V\|_2^2 \ll TL \sup_\alpha K_f(\alpha).$$

Hölder interpolation therefore gives

$$\|V\|_{4/3}^4 \le \|V\|_1^2 \|V\|_2^2 \ll TL^3 \sup_\alpha K_f(\alpha). \tag{13}$$

For $k \in D$ the taper in (12) is at least $3/4$. By (5) all the corresponding coefficients are real and at most $-3c_0/4$. Put $S_D(\alpha) = \sum_{k \in D} \mathrm{e}(k\alpha)$. Then

$$\tfrac{3}{4} c_0 |D| \le \left| \int_{\mathbb{T}} V\overline{S_D} \right| \le \|V\|_{4/3} \|S_D\|_4, \qquad \|S_D\|_4^4 = \mathcal{E}(D),$$

the last identity following by expansion and orthogonality. Equations (11) and (13) give the factor L^{12} in (2) and L^5 when $q\sqrt{T} \le R$. This proves Proposition 3.

5 A progression through the exceptional set

Assume the generalized Riemann hypothesis for all Dirichlet L-functions, including the Riemann zeta function. Put $L = \log X$ and let z count the exceptions in $[X/2, X]$. We use the following reduction for two choices of $u = u(X)$. Suppose that

$$z \geq \sqrt{X} e^{-u}, \qquad 1 \leq u = o(L). \tag{14}$$

Put $H_0 = \lfloor X/2000 \rfloor$. Partition the integers in the interval into $O(1)$ consecutive blocks of at most H_0 integers. Some block contains a set A_0 of $z_0 \gg z$ exceptions. Apply Proposition 3 with $q = 1,\ H = H_0$ to their offsets from the start of the block. Translation preserves energy, so

$$\mathcal{E}(A_0) \geq z_0^3/K, \qquad K = \max\{2, C_0 L^{12} \sqrt{X}/z_0\}$$

for an absolute C_0. The quantitative Balog–Szemerédi–Gowers theorem of Reiher and Schoen [21, Theorem 1.2, with $\varepsilon = 1/4$] gives $B \subset A_0$ with $b = |B| \gg z_0 K^{-1/2}$ and $|B - B| \leq K' b$, where $K' = C_1 K^4 \geq 2$ for an absolute C_1. Put $k = \log(2K') + \log(2L)$. Then (14) gives

$$k \ll u + \log(2L), \qquad \log b \geq \tfrac{1}{2} L - O(u + \log(2L)). \tag{15}$$

Write jB for a j-fold sumset, with $0B = \{0\}$. The Plünnecke–Ruzsa inequality [17, Theorem 1.2], with base set $-B$ and summand B, gives $|jB - \ell B| \leq (K')^{j+\ell} b$ for $j, \ell \geq 0,\ j + \ell \geq 2$.

For any nonempty $V \subseteq B$ and any integer arithmetic progression P of T_0 distinct terms, we have

$$\sqrt{T_0} \ll L^{12} \frac{|V - P|}{|V|}.$$

Indeed, orient P to have positive stride q when $T_0 > 1$. If $q > H_0$, a translate meets the block containing B at most once. Otherwise its intersection with the block consists, when nonempty, of $H \leq T_0$ consecutive terms with $qH \leq H_0 + q \leq X/1000$. Use the first such term as origin and take the indices D of the members of V on this segment. Every indexed total is an even exception in $[X/2, X]$. By (2) and $\mathcal{E}(D) \leq |D|^3$, each translate contains $O(L^{12}\sqrt{T_0})$ members of V. This also holds for $T_0 = 1$. Sum over $t \in V - P$ using $\sum_t |V \cap (t + P)| = |V| T_0$ to obtain the claim.

Proof of Theorem 1. Fix $0 < \gamma < 1/4$ and take $u = L^\gamma$ in (14). Put $s = \lceil k \rceil$. By Bertrand's postulate there is a prime p between $2|sB - sB|$ and $4|sB - sB|$. Ruzsa's modelling lemma in Croot, Łaba and Sisask [5, Proposition 5.1], applied to $B, \{0\}$ at order s, gives a subset $B_0 \subset B$ of size at least $b/(2s)$ and a Freiman s-isomorphism from B_0 onto $A \subset G = \mathbb{Z}/p\mathbb{Z}$. This bijection preserves equalities of s-term sums in both directions. Padding by a fixed element gives the same property at every lower order. In particular,

$$\log p \gg L, \qquad \log(p/|A|) \ll sk, \qquad |A + A|/|A| \leq 2s(K')^2.$$

Here $p \geq 2b$, $p/|A| \leq 8s(K')^{2s}$, and $|A + A| = |B_0 + B_0| \leq (K')^2 b$.

Apply Konyagin's iteration in Sanders' survey [23, Proposition 8.5, from Proposition 8.3 and Corollary 8.4] to A in G. Since $\log(2s(K')^2) \ll k$, it gives symmetric sets S, T containing zero and an integer $r \geq 1$ such that

$$A - A \subset S \subset r(A - A), \qquad |S + T| \leq C|S|,$$
$$r \ll (\log(2k))^a, \qquad \log(|S|/|T|) \ll k^3 (\log(2k))^a$$

with absolute $C \geq 1$ and $a > 0$. Some $y \in S + T$ has at least $|T|/C$ representations as a sum. Then $U = (T \cap (y - S)) - y$ lies in S, has size at least $|T|/C$, and satisfies $|S + U| \leq C|S|$. Since $|S| \geq |A|$ and $s = \lceil k \rceil$, $\log(2p/|U|) \ll k^3(\log(2k))^a$.

We use the large spectrum as in [5, proof of Theorem 6.2]. Give G probability measure, write $*$ for its convolution and $\widehat{g}(\xi) = p^{-1}\sum_x g(x)\mathrm{e}(-\xi x/p)$. For nonempty W put $\mu_W = p\mathbf{1}_W/|W|$. Define

$$g = \mathbf{1}_{S+U} * \mu_{-S}, \qquad F = g * \mu_{-U}.$$

Then $g = 1$ on U, $F(0) = 1$, and $\operatorname{supp} F \subset S+U-S-U \subset 4S$. Cauchy–Schwarz and Parseval give $\sum_\xi |\widehat{g}(\xi)| \leq \sqrt{|S+U|/|S|} \leq \sqrt{C}$. Take $\rho = 1/(8\sqrt{C})$. By Chang's lemma [24, Lemma 4.36], the frequencies with $|\widehat{\mu}_U(\xi)| \geq \rho$ lie among the sums $\sum_{i=1}^d \epsilon_i\lambda_i$, $\epsilon_i \in \{-1, 0, 1\}$, for $d \ll \log(2p/|U|)$. We may take $d \geq 1$. If $t \in G$ satisfies $\|\lambda_i t/p\|_{\mathbb{T}} \leq c_0/(d+1)$ for all i, where $\|\cdot\|_{\mathbb{T}}$ is distance to the nearest integer, then

$$|F(t) - 1| \leq (2\pi c_0 + 2\rho)\sqrt{C} \leq \tfrac{1}{2}$$

for a sufficiently small absolute $c_0 > 0$. Indeed, in Fourier inversion $|\mathrm{e}(\xi t/p) - 1| \leq 2\pi c_0$ on those sums, and $|\widehat{\mu}_{-U}(\xi)| < \rho$ off the large spectrum. Thus every such t belongs to $4S$.

Put $m = \lfloor (p-1)^{1/d} \rfloor$. Among the p points $(\lambda_i x/p)_{i=1}^d$ of $\mathbb{T}^d$, two indices lie in the same one of $m^d < p$ equal boxes. Their difference $v \neq 0$ satisfies $\|\lambda_i v/p\|_{\mathbb{T}} \leq 1/m$ for all i. The multiples jv, $0 \leq j \leq \lfloor c_0 m/(d+1) \rfloor$, all belong to $4S$ and are distinct since p is prime and $c_0 < 1$. Their number T_0 satisfies

$$\log T_0 \geq \frac{\log p}{d} - O(\log(2d)), \qquad d \ll k^3(\log(2k))^a. \tag{16}$$

In particular $T_0 \to \infty$, since (15) gives $d\log(2d) = o(L)$.

Put $h = 4r$, so that $4S \subset hA - hA$. For large X one has $4h = 16r \leq s$, since $k \geq \log(2L)$. To lift $hA - hA$, replace each summand in a representation by its inverse image in B_0. Equality of two differences is an equality of $2h$-term sums, so the lift is well-defined and injective. The relation between three consecutive terms, $jv+(j+2)v = 2(j+1)v$, becomes an equality of $4h$-term sums on moving negative summands across. It therefore lifts too. This gives an ordinary integer progression $P \subset hB_0 - hB_0$ of T_0 distinct terms. As in Sanders' proof of Proposition 2.5 in [23], the containment in Proposition 8.5 gives

$$|B - P| \leq |(h+1)B - hB| \leq (K')^{8r+1}b.$$

The translate estimate above with $V = B$ gives $\log T_0 \ll rk + \log L$. Together with (16) this yields, for an absolute $a_1 > 0$,

$$L \ll d\big(rk + \log L + \log(2d)\big) \ll k^4(\log(2k))^{a_1}.$$

By (15), $k \ll L^\gamma$, so $4\gamma < 1$ gives a contradiction. The powers of $\log(2k)$ in the containment estimate account for the strict inequality in the exponent.

For a fixed $\beta < 1/4$ choose $\max\{0, \beta\} < \gamma < 1/4$. Sum the dyadic bounds with upper endpoints $Y = X/2^j \geq X^{1/3}$. Here $(\log Y)^\gamma \geq (L/3)^\gamma \geq L^\beta$ for large X and $\sum_j \sqrt{X/2^j} \ll \sqrt{X}$. The remaining integers contribute $O(X^{1/3})$. This proves (1), with the implied constant covering bounded X. Any fixed positive $\beta < 1/4$ gives the logarithmic consequence. $\square$

Conditional remark on Raghavan's covering theorem. Assume the generalized Riemann hypothesis for all Dirichlet L-functions, including the Riemann zeta function. Assume also Theorem 1.4 of Rushil Raghavan's unrefereed preprint *Improved bounds for the Freiman–Ruzsa theorem* [20, version 2]. Then there are absolute $c, C > 0$ such that for $X \geq 16$,

$$E(X) \leq C\sqrt{X} \exp\left\{ -c \frac{\sqrt{\log X}}{\log\log X} \right\}.$$

To see this, take $u = \eta\sqrt{L}/\log L$ in (14), with $0 < \eta \leq 1$ fixed for now. Since $|B + B| \leq (K')^2 b$, the assumed theorem covers B by at most e^f translates of a convex coset progression M of dimension $D \leq f$ and size $|M| \leq e^f b$, where $f = C_2 k \log(2k)$. Here we have used the covering function $O(\log(3K)\log\log(3K))$ of [20, Question 1.2 and Theorem 1.4] at $K = (K')^2$. By [20, Definition 2.6], $M = \phi(Q \cap \Lambda)$, where $Q = -Q$ is a convex body, $\Lambda = \mathbb{Z}^D$, and $\phi : \Lambda \to \mathbb{Z}$ is a homomorphism. Finiteness of M makes its subgroup trivial in $\mathbb{Z}$. One translate $x + M$ meets B in a set V of size at least $e^{-f} b$, so $|M| \geq e^{-f} b$.

For clarity, restrict the body and lattice to the real span of $Q \cap \Lambda$, using its dimension for D. The body then has interior in this span, since it contains a spanning set and its negatives. For $a, t > 0$ choose a maximal family of points $y \in aQ \cap \Lambda$ with the interiors of $y + (t/2)Q$ disjoint. These translates lie in $(a + t/2)Q$, so volume bounds their number by $(1 + 2a/t)^D$. Maximality and symmetry cover $aQ \cap \Lambda$ by the same number of translates of $tQ \cap \Lambda$. Taking $a = 2, t = 1$ and applying ϕ gives $|M + M| \leq 5^D |M|$. Taking $a = 1, t = 1/n$ shows that if $(2n+1)^D < |M|$, then $\phi((Q/n) \cap \Lambda)$ contains some $q \neq 0$, since otherwise those translates would cover M by at most $(2n+1)^D$ points. By convexity and symmetry $P = \{jq : |j| \leq n\} \subset M$.

By (15), $f \ll \eta\sqrt{L}$ for sufficiently large X depending on η, with an absolute implied constant. Also $\log|M| \geq \log b - f \geq L/2 - o(L)$, so $D \geq 1$ and $|M|^{1/D} \to \infty$. Set $n = \lfloor |M|^{1/D}/4 \rfloor$. The progression above has $T_0 = 2n + 1$ distinct terms and $\log T_0 \geq D^{-1} \log|M| - O(1)$. Since $V \subset x + M$ and $P \subset M = -M$, we have $|V - P|/|V| \leq 5^D e^{2f}$. Our translate estimate now gives $\log T_0 \ll f + \log L$. It follows that $\log b \ll f^2 + f \log L$, with absolute constants. For sufficiently small fixed $\eta > 0$ this contradicts $\log b \geq L/2 - o(L)$. Summing dyadically as above gives the asserted bound, since $\sqrt{\log Y}/\log\log Y \geq \sqrt{L/3}/\log L$ for $X^{1/3} \leq Y \leq X$ and X large.

Limits of the progression energy estimate. Let X be large and $L = \log X$. Fix $\nu \in \{10, 24\}$ and $\delta > 0$, and take a prime $s \in [\delta L^\nu, 2\delta L^\nu]$. Put $n = \lfloor \log(X/4)/\log s \rfloor$, $d = \lfloor (\sqrt{s} + 1)/2 \rfloor$, and form the integers with n base-s digits in $\{0, \dots, d-1\}$, allowing leading zeros. Keep the more numerous parity class (either in a tie) and translate by the integer of matching parity among $\lceil X/2 \rceil, \lceil X/2 \rceil + 1$. This gives a set of even integers in $[X/2, X]$, of size between $d^n/2$ and d^n. Since $n \log s = L + O(\log s)$ and $\log d = \frac{1}{2}\log s - \log 2 + O(s^{-1/2})$, its size is

$$\sqrt{X} \exp\left\{ -\left(\frac{\log 2}{\nu} + o(1) \right) \frac{L}{\log L} \right\}.$$

Suppose $a + qj$ lies in this set for every $j \in D \subset [-H, H] \cap \mathbb{Z}$, where $a \in \mathbb{Z}$ and $q, H \geq 1$ are integers. Write $q = s^v q'$ with $s \nmid q'$, and take the least m with $s^m > 4H$. Each $q(j - j')$ has signed base-s digits in $[-(d-1), d-1]$ obtained by termwise subtraction, padded with zeros. Its first v digits vanish successively on reduction modulo s. Its next m digits determine $q'(j - j') \bmod s^m$, hence $j - j'$ itself by invertibility and $|j - j'| \leq 2H$. Consequently

$$|D - D| \leq (2d-1)^m \leq s^{m/2} \leq 2\sqrt{sH}, \qquad |D|^4 \leq |D - D|\mathcal{E}(D) \leq 2\sqrt{2\delta}\, L^{\nu/2}\sqrt{H}\, \mathcal{E}(D),$$

by Cauchy–Schwarz on the difference counts. The choice $\nu = 24$ gives the factor L^{12} in (2). With $\nu = 10$ the example satisfies even the L^5 bound at every stride. The union of these examples at $X = 8^j$ has the same bounds, since each dyadic interval meets at most one example and its upper endpoint is then comparable to X. Thus an exponent growing faster than $L/\log L$ in the exponential saving requires information beyond these energy bounds.

6 Prime-square shifts of a prescribed total

Proof of Corollary 2. In Proposition 3 take $X = a = N$, $q = 2$, $H = M^2$. The upper bound on M ensures $2M^2 \le N/1000$ and $4M = 2q\sqrt{H} \le R$ for large N. Thus every $N - 2\ell^2$ under consideration lies in $[N/2, N]$. Let D consist of $-\ell^2$ for the primes $\sqrt{M} < \ell \le M$ for which this even total has no representation with $p_1 \in [N/10, N/6]$. The second bound of Proposition 3 gives

$$|D|^4 \ll L^5 M\, \mathcal{E}(D). \tag{17}$$

We use the fourth moment of prime squares in Languasco and Zaccagnini [14, Lemma 5]. In their normalization, for integers $Y \ge 2$,

$$\int_{\mathbb{T}} \left| \sum_{n \ge 1} \Lambda(n) \exp(-n^2/Y) \mathrm{e}(n^2\alpha) \right|^4 d\alpha \ll Y(\log(2Y))^2.$$

By orthogonality this counts equal sums of two squares with nonnegative weights. At $Y = M^2$, every occurrence of a prime $\sqrt{M} < \ell \le M$ has weight at least $e^{-1}(\log M)/2$. Each quadruple in $\mathcal{E}(D)$ is therefore counted with weight $\gg (\log M)^4$, since changing all four signs preserves the equation. Consequently

$$\mathcal{E}(D) \ll \frac{M^2}{(\log(2M))^2}, \qquad |D|^4 \ll \frac{L^5 M^3}{(\log(2M))^2}.$$

There are at most $\sqrt{M}$ additional primes to consider. Dividing by $\pi(M) \asymp M/\log(2M)$, the proportion of exceptions to the claimed representation is at most

$$\ll \frac{\log(2M)}{\sqrt{M}} + \left(\frac{L^5 (\log(2M))^2}{M} \right)^{1/4}.$$

This tends to zero under the stated condition. For the displayed choice of M, one has $\log M \sim 5 \log L$, so the bound is $O((\log\log L)^{-1/4}) = O((\log\log\log N)^{-1/4})$. The partner prime satisfies $p_2 = N - 2\ell^2 - p_1 \ge N/2 - N/6 = N/3 > p_1$. □

The quadruples (u, v, u, v) give $\mathcal{E}(D) \ge |D|^2$. At $M \asymp L^5 (\log M)^2$, inequality (17) is therefore compatible with $|D|$ a fixed positive fraction of $\pi(M)$. The diverging factor in Corollary 2 gives the vanishing proportion.

Remark. L. Alpöge has announced a proof of GRH, formalised in Lean. If the announced proof is correct, the theorems of this paper would then hold unconditionally.

References

[1] I. Althöfer, D. Chen, A. Perelli and J. Pintz, The exceptional set of Goldbach numbers among polynomial values, arXiv:2611.09386 (2026).

[2] G. Bhowmik and K. Halupczok, Asymptotics of Goldbach representations, *Adv. Stud. Pure Math.* **84** (2020), 1–21. Preprint arXiv:1809.06920.

[3] J. Brüdern, K. Kawada and T. D. Wooley, Additive representation in thin sequences, II: The binary Goldbach problem, *Mathematika* **47** (2000), 117–125.

[4] M.-C. Chang, On problems of Erdős and Rudin, *J. Funct. Anal.* **207** (2004), 444–460.

[5] E. Croot, I. Łaba and O. Sisask, Arithmetic progressions in sumsets and L^p-almost-periodicity, *Combin. Probab. Comput.* **22** (2013), 351–365.

[6] A.-M. Ernvall-Hytönen and N. Palojärvi, Explicit bound for the number of primes in arithmetic progressions assuming the generalized Riemann hypothesis, *Math. Comp.* **91** (2022), 1317–1365.

[7] D. A. Goldston, On Hardy and Littlewood's contribution to the Goldbach conjecture, in *Proceedings of the Amalfi Conference on Analytic Number Theory* (Maiori, 1989), Università di Salerno, Salerno, 1992, 115–155.

[8] D. A. Goldston and C. Y. Yıldırım, Primes in short segments of arithmetic progressions, *Canad. J. Math.* **50** (1998), 563–580.

[9] H. Gou, V. Y. Wang and M. W. Xu, Landau's problems through ratios of L-functions, arXiv:2611.18825 (2026).

[10] G. H. Hardy and J. E. Littlewood, Some problems of "Partitio numerorum" (V): A further contribution to the study of Goldbach's problem, *Proc. London Math. Soc.* (2) **22** (1924), 46–56.

[11] J. Kaczorowski, A. Perelli and J. Pintz, A note on the exceptional set for Goldbach's problem in short intervals, *Monatsh. Math.* **116** (1993), 275–282.

[12] J. Kaczorowski, A. Perelli and J. Pintz, Corrigendum of A note on the exceptional set for Goldbach's problem in short intervals, *Monatsh. Math.* **119** (1995), 215–216.

[13] A. Languasco and A. Perelli, A pair correlation hypothesis and the exceptional set in Goldbach's problem, *Mathematika* **43** (1996), 349–361.

[14] A. Languasco and A. Zaccagnini, Sum of one prime and two squares of primes in short intervals, *J. Number Theory* **159** (2016), 45–58.

[15] H. Li and Z. Liu, Fourth moments of prime exponential sums and exceptional sets for sums and differences of primes, arXiv:2610.26756 (2026).

[16] A. Perelli, Goldbach numbers represented by polynomials, *Rev. Mat. Iberoam.* **12** (1996), 477–490.

[17] G. Petridis, New proofs of Plünnecke-type estimates for product sets in groups, *Combinatorica* **32** (2012), 721–733.

[18] J. Pintz and I. Althöfer, The Goldbach exceptional set: an exponent 7/12 and conditional refinement, arXiv:2610.15559 (2026).

[19] K. Prachar, Generalisation of a theorem of A. Selberg on primes in short intervals, in *Topics in Number Theory* (Debrecen, 1974), Colloq. Math. Soc. János Bolyai **13**, North-Holland, Amsterdam, 1976, 267–280.

[20] R. Raghavan, Improved bounds for the Freiman–Ruzsa theorem, arXiv:2512.11217v2 (26 February 2026).

[21] C. Reiher and T. Schoen, Note on the theorem of Balog, Szemerédi, and Gowers, *Combinatorica* **44** (2024), 691–698.

[22] T. Sanders, On the Bogolyubov–Ruzsa lemma, *Anal. PDE* **5** (2012), 627–655.

[23] T. Sanders, The structure theory of set addition revisited, *Bull. Amer. Math. Soc.* (N.S.) **50** (2013), 93–127.

[24] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge University Press, Cambridge, 2006.