hexagon:2611.00750v1

INFINITELY MANY EXCEPTIONS TO A PRIME-SQUARE REPRESENTATION PROBLEM OF ERDŐS

WILL HOWE, GRANT HUFFMAN, JENSEN KOHLMEYER, AND LIAM KRUER

Abstract. We prove that infinitely many positive integers have no representation $n = ap^2 + b$ with p prime, $a \geq 1$, and $0 \leq b < p$. More precisely, the number of such integers in $(X, 2X]$ is of order $X/\log X$. The lower bound combines a positive-proportion avoidance estimate for large primes with first- and second-moment estimates for a short average of the small-prime sieve. A separated-frequency argument permits the large primes to be added in finitely many blocks. The small-prime moments have quadratic loss in the cutoff exponent, and a boundary estimate makes the large-prime avoidance stable under the averaging shifts.

1. The representation problem

Erdős asked whether every sufficiently large integer can be written as

$$n = ap^2 + b, \qquad p \text{ prime}, \quad a \geq 1, \quad 0 \leq b < p; \tag{1.1}$$

see [1, p. 68, problem 3]. Call an integer *exceptional* if it has no representation (1.1), and put

$$E(X) = \#\{n \in \mathbb{Z} : X < n \leq 2X,\ n \text{ is exceptional}\}.$$

Theorem 1.1. *There are constants $c, C > 0$ and X_0 such that*

$$c\frac{X}{\log X} \leq E(X) \leq C\frac{X}{\log X} \qquad (X \geq X_0). \tag{1.2}$$

In particular, infinitely many positive integers have no representation (1.1).

Erdős recorded $g(x) \ll x/(\log x)^c$ for some $c > 0$, with $g(x)$ counting exceptions up to x, in [1, p. 68]. We determine the order of the exceptional count and prove the upper bound from the same sieve estimate.

We first work with positive integer X and write $I = (X, 2X] \cap \mathbb{Z}$. For a prime p, let

$$A_p(n) = \mathbf{1}_{\{n \bmod p^2 < p\}}, \qquad V(z) = \prod_{p \leq z}\left(1 - \frac{1}{p}\right), \qquad S_z(n) = \prod_{p \leq z}(1 - A_p(n)).$$

The remainder $n \bmod p^2$ is taken in $\{0, \dots, p^2 - 1\}$. Euclidean division shows that a prime p gives a representation (1.1) precisely when $p^2 \leq n$ and $A_p(n) = 1$. The associated intervals are $[ap^2, ap^2 + p - 1] \cap \mathbb{Z}$ for $a \geq 1$.

All sums and products indexed by p run over primes. We use $\mathrm{e}(t) = \exp(2\pi i t)$ and write $\|t\|_{\mathbb{R}/\mathbb{Z}}$ for distance to the nearest integer. The notation $o_\alpha(1)$ means that α and all other exponent parameters have been fixed before X tends to infinity.

Date: November 11, 2026.

2020 *Mathematics Subject Classification.* Primary 11N35; Secondary 11N36, 11A07.

Key words and phrases. Erdős problems, prime-square residues, sieve methods, exceptional sets.

E-mail addresses: howew@purdue.edu (W. Howe), huffma97@purdue.edu (G. Huffman), jenwin@purdue.edu (J. Kohlmeyer), kruerl@purdue.edu (L. Kruer).

The classical prime estimates needed below are

$$\sum_{p\le t}\frac{1}{p}=\log\log t+B+o(1),\qquad V(t)\sim\frac{e^{-\gamma}}{\log t},\tag{1.3}$$

$$\pi(t)\ll\frac{t}{\log t},\qquad \vartheta(t):=\sum_{p\le t}\log p\ll t.\tag{1.4}$$

Here γ is Euler's constant. These are Mertens' estimates and Chebyshev's bounds [2, 3]. Partial summation also gives

$$\sum_{p\le t}\frac{\log p}{p}\ll\log t,\qquad \sum_{p\le t}\frac{(\log p)^2}{p}\ll(\log t)^2.\tag{1.5}$$

The proof uses a fixed dyadic cutoff $z=X^\alpha$. Section 2 gives a positive proportion of points avoiding the larger primes. Section 3 estimates a short average of S_z with relative error $O(\alpha^2)$ in both moments. Section 4 combines the estimates and proves the theorem.

2. Avoiding the large primes

We begin with the averaging estimate that permits separated blocks of primes to be added successively.

Lemma 2.1 (Separated prime blocks)**.** *Fix $0<a\le b\le 1/4$ and $b<c\le 1/2$. Let $\mathcal{P}$ be any set of primes in $[X^a,X^b]$, and set*

$$G(n)=\sum_{p\in\mathcal{P}}A_p(n),\qquad \lambda=\sum_{p\in\mathcal{P}}\frac{1}{p}.$$

Let $\mathcal{Q}$ be any set of primes in $[X^c,2\sqrt{X}]$, and let

$$U(n)=\mathbf{1}_I(n)\prod_{q\in\mathcal{Q}}(1-A_q(n)).$$

There is $\delta>0$, depending only on the fixed exponents, such that

$$\sum_{n\in\mathbb{Z}}G(n)U(n)=\lambda\sum_{n\in\mathbb{Z}}U(n)+O(X^{1-\delta}).\tag{2.1}$$

The error is uniform in $\mathcal{P}$ and $\mathcal{Q}$.

Proof. Choose $b<\eta<c$, put $H=\lfloor X^\eta\rfloor$, and fix $0<\epsilon<\eta-b$. Take an even, nonnegative, smooth function ϕ, supported in $[-1,1]$ and positive near zero. For large H,

$$\nu_H(h)=\frac{\phi(h/H)}{\sum_{r\in\mathbb{Z}}\phi(r/H)}\quad(h\in\mathbb{Z})$$

is a probability measure supported on $[-H,H]$. For each fixed positive integer J, finite differencing gives

$$\left|\sum_h\nu_H(h)\mathrm{e}(h\theta)\right|\ll_J(1+H\|\theta\|_{\mathbb{R}/\mathbb{Z}})^{-J}.\tag{2.2}$$

Indeed, the normalizing denominator is $\asymp H$, and the sum of the absolute Jth differences of $\phi(h/H)$ is $O_J(H^{1-J})$. Multiplication by $(1-\mathrm{e}(\theta))^J$ gives (2.2), together with the trivial bound 1.

The Fourier expansion modulo p^2 is

$$A_p(n)=\sum_{k\bmod p^2}\widehat{A}_p(k)\mathrm{e}\big(kn/p^2\big),\qquad \widehat{A}_p(k)=\frac{1}{p^2}\sum_{r=0}^{p-1}\mathrm{e}\big(-kr/p^2\big).$$

In particular, $\widehat{A}_p(0) = 1/p$ and $|\widehat{A}_p(k)| \le 1/p$. Define $G_H(n) = \sum_h \nu_H(h)G(n+h)$ and put $D = X^\epsilon/H$. Discard from $G_H - \lambda$ the frequencies with distance greater than D from an integer. Their total absolute contribution is

$$\ll_J X^{-J\epsilon} \sum_{p \le X^b} p \ll_J X^{2b-J\epsilon},$$

which is as small a power of X as required after fixing J.

Every remaining nonzero frequency has a representative k/p^2 with

$$0 < |k| \le p^2 D < p$$

for sufficiently large X. It is therefore in lowest terms. Different labels give different points of $\mathbb{R}/\mathbb{Z}$, and their circular separation is at least $X^{-4b} \ge X^{-1}$. There are at most $2p^2D$ retained labels for each prime, so the sum of squared coefficients is

$$\ll \sum_{p \in \mathcal{P}} \frac{p^2 D}{p^2} \ll X^b D \ll X^{b+\epsilon-\eta}. \tag{2.3}$$

For completeness, a separated family of frequencies $\{\theta_r\}$ with spacing at least X^{-1} satisfies

$$\sum_{n \in J_X} \left| \sum_r u_r \mathrm{e}(n\theta_r) \right|^2 \ll X \sum_r |u_r|^2 \tag{2.4}$$

on any interval J_X of length $O(X)$. To prove this, choose a nonnegative smooth majorant $w(n/X)$ for the interval after translation. Twice summing by parts gives

$$\left| \sum_n w(n/X)\mathrm{e}(n\theta) \right| \ll X(1 + X\|\theta\|_{\mathbb{R}/\mathbb{Z}})^{-2}.$$

Spacing implies that each row sum of these bounds is $O(X)$. Expanding the square and using $2|u_r u_s| \le |u_r|^2 + |u_s|^2$ proves (2.4). Combining (2.3) and (2.4), and including the discarded frequencies, yields some $\delta_1 > 0$ for which

$$\sum_{X-H \le n \le 2X+H} |G_H(n) - \lambda|^2 \ll X^{1-\delta_1}. \tag{2.5}$$

Enlarge and contract both the ambient interval and every forbidden residue interval by H at its endpoints. This gives indicators U_- and U_+ such that, for $|h| \le H$,

$$U_-(n-h) \le U(n) \le U_+(n-h).$$

The enlarged ambient interval lies in $[X - H, 2X + H]$. For a prime q, the boundary change meets at most $O(H(X/q^2 + 1))$ integers in that interval. Thus

$$\begin{aligned} \sum_n (U_+(n) - U_-(n)) &\ll H + H \sum_{X^c \le q \le 2\sqrt{X}} (X/q^2 + 1) \\ &\ll HX^{1-c}, \end{aligned}$$

where the reciprocal-square tail can be bounded by the sum over all integers and $c \le 1/2$. Also $\lambda = O_{a,b}(1)$ by (1.3).

Since $G \ge 0$, averaging the pointwise comparisons and changing variables gives

$$\sum_n U_-(n)G_H(n) \le \sum_n U(n)G(n) \le \sum_n U_+(n)G_H(n).$$

Cauchy–Schwarz and (2.5) bound either centered sum by $O(X^{1-\delta_1/2})$. The boundary error is $O(HX^{1-c})$, which also saves a positive power because $\eta < c$. This proves (2.1). □

Put $d = 1 - \log 2$. We have $1/4 < d < 1$, since $\exp(3/4) > 1 + 3/4 + (3/4)^2/2 > 2$.

Proposition 2.2. *There is an absolute constant $c_0 > 0$ such that, for every fixed integer $L \geq 2$, with $\alpha = 2^{-L}$,*

$$\#\{n \in I : A_p(n) = 0 \text{ for every } X^\alpha < p \leq 2\sqrt{X}\} \geq c_0 d^L X \tag{2.6}$$

for all sufficiently large X, depending on L.

Proof. Each prime contributes $X/p + O(p)$ points of I to its forbidden residues. Consequently the number of points surviving all primes $X^{1/4} < p \leq 2\sqrt{X}$ is at least

$$X - X \sum_{X^{1/4} < p \leq 2\sqrt{X}} \frac{1}{p} - O\left(\sum_{p \leq 2\sqrt{X}} p\right) = (d - o(1))X.$$

Here (1.3) gives the reciprocal sum $\log 2 + o(1)$, and (1.4) gives $\sum_{p \leq 2\sqrt{X}} p \ll X/\log X$.

Set $K = L - 2$ and $c_j = 2^{-j}/4$ for $0 \leq j \leq K$. Fix $0 < \tau < 1/2$ and add, in the order $j = 0, \ldots, K-1$, the blocks

$$X^{c_{j+1}} < p \leq X^{(1-\tau)c_j}.$$

At stage j, the previously imposed primes are all greater than X^{c_j}, so Lemma 2.1 applies. The reciprocal mass of the new block tends to $\log(2(1-\tau)) < \log 2$. If N_j points survive before the block is added, the union bound and (2.1) give

$$N_{j+1} \geq dN_j - o(X).$$

There are only K stages, all fixed before $X \to \infty$. The final selected-prime count is therefore at least $(d^{K+1} - o(1))X$.

The omitted gaps are $X^{(1-\tau)c_j} < p \leq X^{c_j}$. Their total reciprocal mass tends to $K[-\log(1-\tau)]$. Removing all their forbidden points costs at most

$$\big(K[-\log(1-\tau)] + o(1)\big)X;$$

their combined $O(p)$ errors are $o(X)$ by (1.4). Choose τ, still at fixed K, so that $K[-\log(1-\tau)] < d^{K+1}/4$. For large X at least $d^{K+1}X/2$ points remain. This gives (2.6) with $c_0 = 1/(2d)$. The case $K = 0$ follows directly from the initial estimate. □

3. The averaged small-prime sieve

Fix a small positive α and define

$$z = X^\alpha, \qquad \eta = \alpha(1 - \alpha^2), \qquad H = \lfloor X^\eta \rfloor, \qquad B(n) = \frac{1}{H} \sum_{j=0}^{H-1} S_z(n + j). \tag{3.1}$$

The following proposition supplies the two estimates used in the final argument.

Proposition 3.1. *There are absolute constants $C_1, C_2 > 0$ such that, for all sufficiently small fixed $\alpha > 0$,*

$$\sum_{n \in I} B(n) \geq (1 - C_1\alpha^2 - o_\alpha(1))XV(z), \tag{3.2}$$

$$\sum_{n \in I} B(n)^2 \leq (1 + C_2\alpha^2 + o_\alpha(1))XV(z)^2. \tag{3.3}$$

3.1. **The first moment.** Partition the primes through z into nonempty blocks

$$\mathcal{P}_j = \{p : z^{2^{-j-1}} < p \le z^{2^{-j}}\}, \qquad 0 \le j \le J,$$

ending when the lower endpoint is below 2. Then $J = O(1+\log\log z)$. By (1.3), the sums $\sum_{p\in\mathcal{P}_j} 1/p$ are bounded by an absolute constant C_0, uniformly in z, j. Moreover,

$$V_j := \prod_{p\in\mathcal{P}_j}(1-1/p) \ge v_0 > 0 \tag{3.4}$$

uniformly, since $-\log(1-1/p) \le 2/p$ for $p \ge 2$.

Choose an absolute integer L_0 so large that $C_0^k/k! \le 2^{-k}$ for $k \ge 2L_0$, and put

$$T = \lceil \log_2(1/\alpha)\rceil + L_0, \qquad k_j = 2T + 2j.$$

For $K_j(n) = \sum_{p\in\mathcal{P}_j} A_p(n)$, the Bonferroni polynomials

$$U_j(n) = \sum_{i=0}^{k_j}(-1)^i\binom{K_j(n)}{i}, \qquad L_j(n) = \sum_{i=0}^{k_j-1}(-1)^i\binom{K_j(n)}{i}$$

satisfy

$$L_j \le \mathbf{1}_{\{K_j=0\}} \le U_j, \qquad U_j \ge 0, \qquad U_j - L_j = \binom{K_j}{k_j}.$$

Telescoping the product, using the nonnegativity of the upper polynomials, gives

$$S_z(n) \ge \prod_j U_j(n) - \sum_j (U_j(n) - L_j(n)) \prod_{i\ne j} U_i(n). \tag{3.5}$$

Replace the variables $A_p(n)$ temporarily by independent Bernoulli variables of means $1/p$. For a single block,

$$\mathbb{E}U_j \ge V_j, \qquad \mathbb{E}(U_j - L_j) \le \frac{C_0^{k_j}}{k_j!} \le 2^{-k_j}.$$

Also $\mathbb{E}U_j - V_j \le \mathbb{E}(U_j - L_j)$, so $\mathbb{E}U_j \le V_j(1 + v_0^{-1}2^{-k_j})$. Independence between blocks and (3.4) show that the expectation of the right side of (3.5) is at least

$$V(z)\left(1 - O\left(\sum_j 2^{-k_j}\right)\right) \ge V(z)(1 - O(\alpha^2)).$$

To transfer this bound to integers, expand (3.5) into products of distinct A_p. Every resulting squarefree modulus m satisfies

$$m \le z^{\sum_{j\ge0} k_j 2^{-j}} = z^{4T+4} \le X^{1/4}$$

when α is sufficiently small. Each coefficient has absolute value at most $J+2$. The Chinese remainder theorem gives exactly m forbidden residue classes modulo m^2 for a product indexed by m, hence its sum over I is $X/m + O(m)$. The total transfer error is bounded by

$$O\left((J+2)\sum_{m\le X^{1/4}} m\right) = O((J+2)X^{1/2}) = o(XV(z)).$$

Thus $\sum_{n\in I} S_z(n) \ge (1 - C_1\alpha^2 - o_\alpha(1))XV(z)$. Translating I by an integer $0 \le j < H$ changes the sum of S_z, which lies between zero and one, by at most $2H$. Since $H = o(XV(z))$, averaging these translates proves (3.2).

3.2. **A uniform two-position bound.** For an integer k, let $a_p(k)$ be the cardinality of the intersection of the forbidden residue sets at n and $n+k$ modulo p^2. Set

$$g_k(p) = \frac{2}{p} - \frac{a_p(k)}{p^2}, \qquad V_k = \prod_{p \le z}(1 - g_k(p)).$$

Thus $g_k(p)$ is the density of the union of these two residue sets, and $1/p \le g_k(p) \le 2/p$.

Lemma 3.2. *For sufficiently small fixed $\alpha > 0$, uniformly in k and in integer intervals J_X of length X,*

$$\sum_{n \in J_X} S_z(n) S_z(n+k) \le (1 + C\alpha^2) X V_k + O(X^{3/5}), \tag{3.6}$$

where C and the implied constant are absolute.

Proof. If $g_k(p) = 1$ for some p, then $V_k = 0$ and the left side is zero. We may therefore suppose $0 < g_k(p) < 1$ for every $p \le z$, and write $g(p) = g_k(p)$. Extend g multiplicatively to squarefree products of primes through z, and put

$$q(r) = \prod_{p \mid r} \frac{g(p)}{1 - g(p)}, \qquad R = \lfloor X^{1/10} \rfloor, \qquad G_R = \sum_{r \le R} q(r).$$

All moduli in this proof are squarefree and supported on primes through z; in particular $g(1) = q(1) = 1$.

Let $F_r(n)$ indicate that the union event occurs for every $p \mid r$. For real weights λ_r supported on $r \le R$, with $\lambda_1 = 1$, the square $(\sum_r \lambda_r F_r(n))^2$ majorizes $S_z(n) S_z(n+k)$. Its main term after summation over J_X is

$$X Q(\lambda), \qquad Q(\lambda) = \sum_{r,s \le R} \lambda_r \lambda_s g([r,s]).$$

Writing $y_t = \sum_{t \mid r} g(r) \lambda_r$, one has

$$Q(\lambda) = \sum_{t \le R} \frac{y_t^2}{q(t)}, \qquad \lambda_1 = \sum_{t \le R} \mu(t) y_t. \tag{3.7}$$

The first identity follows by expanding $1/g((r,s)) = \sum_{t \mid (r,s)} 1/q(t)$, and the second is Möbius inversion. Choose $y_t = \mu(t) q(t) / G_R$. Then $\lambda_1 = 1$, $Q(\lambda) = 1/G_R$, and inversion gives

$$\lambda_r = \frac{\mu(r)}{G_R} \prod_{p \mid r} (1 - g(p))^{-1} \sum_{\substack{s \le R/r \\ (s,r) = 1}} q(s). \tag{3.8}$$

In particular $|\lambda_r| \le 1$. Indeed, the numerator without its sign equals $\sum_{s \le R/r, (s,r)=1} \sum_{e \mid r} q(se)$; the products se are distinct and all at most R, so this is a subsum of G_R.

For $m = [r,s]$, the union conditions occupy $\prod_{p \mid m}(2p - a_p(k)) \le m^2$ residue classes modulo m^2. The Chinese remainder theorem therefore gives

$$\sum_{n \in J_X} F_m(n) = X g(m) + O(m^2).$$

There are at most R^2 pairs (r,s) and $m \le R^2$. Using $|\lambda_r| \le 1$, the total error is $O(R^6)$, and hence

$$\sum_{n \in J_X} S_z(n) S_z(n+k) \le X / G_R + O(R^6). \tag{3.9}$$

For independent Bernoulli variables Z_p with means $g(p)$,

$$G_R V_k = \mathbb{P}\left(\sum_{p\le z} Z_p \log p \le \log R\right).$$

The mean of the sum is $O(\log z)$, and its variance is $O((\log z)^2)$ by (1.5) and $g(p)\le 2/p$. Its second moment is therefore $O((\log z)^2)$. Markov's inequality applied to its square gives $G_R V_k \ge 1 - C'\alpha^2$ for large X. After making α smaller if necessary, $1/G_R \le (1+C\alpha^2)V_k$. Substitution in (3.9), with $R^6 \le X^{3/5}$, proves the lemma. □

3.3. **Averaging the local factors.** For $|k|<H$, put $w_H(k) = (H-|k|)/H^2$, and put $w_H(k)=0$ otherwise. These are the probabilities of the difference of two independent uniform integers in $\{0,\dots,H-1\}$. In particular, $\sum_k w_H(k) = 1$ and $w_H(k)\le 1/H$.

Lemma 3.3. *With the parameters* (3.1),

$$\sum_k w_H(k)\frac{V_k}{V(z)^2} \le (1-\alpha^2)^{-2} + o_\alpha(1). \tag{3.10}$$

Proof. Write

$$R_p(k) = \frac{1-g_k(p)}{(1-1/p)^2} = 1 + \frac{a_p(k)-1}{(p-1)^2}, \qquad v_p(k) = (R_p(k)-1)_+.$$

The function R_p has period p^2, is nonnegative, and is at most $p/(p-1)$. Counting the pairs of forbidden residues gives $\sum_{k \bmod p^2} a_p(k) = p^2$, so R_p has mean one over a period. Also

$$0 \le v_p(k) \le \frac{a_p(k)}{(p-1)^2}, \qquad \frac{1}{p^2}\sum_{k \bmod p^2} v_p(k) \le \frac{1}{(p-1)^2}, \qquad 1+v_p(k) \le \frac{p}{p-1}. \tag{3.11}$$

Choose a sufficiently small absolute $c_1>0$ and put

$$Y = c_1 \log H, \qquad M = \prod_{p\le Y} p^2, \qquad L(k) = \prod_{p\le Y} R_p(k).$$

By (1.4), $M \le H^{1/4}$. The Chinese remainder theorem shows that L has mean one modulo M. A uniform integer in $\{0,\dots,H-1\}$ has residue probabilities $1/M + O(1/H)$; convolving with another probability distribution preserves this error bound. Consequently

$$\sum_k w_H(k)L(k) = 1 + O(M/H). \tag{3.12}$$

Set $Y_0 = H^{1/4}$ and $Y_1 = H^{1-\alpha^2}$. For $Y < p \le Y_0$, the nonnegative function Lv_p has period Mp^2 and, by the Chinese remainder theorem, period mean $O(p^{-2})$. Counting complete periods and at most two incomplete periods in $|k|<H$, and using $w_H \le 1/H$, gives

$$\sum_k w_H(k)L(k)v_p(k) \ll p^{-2} + M/H.$$

By (1.3) and (3.11),

$$\prod_{Y<p\le Y_0}(1+v_p(k)) \ll \frac{\log Y_0}{\log Y}.$$

Telescoping this product and summing the preceding estimate show that its insertion after L increases the weighted mean by at most

$$O\left(\frac{\log Y_0}{\log Y}\left(\frac{1}{Y} + \frac{MY_0}{H}\right)\right) = o(1).$$

For $Y_0 < p \le Y_1$, the same period-counting argument without L gives

$$\sum_k w_H(k) v_p(k) \ll p^{-2} + H^{-1}.$$

The product of $1 + v_p$ in this range is $O_\alpha(1)$. The preceding product, including L, is pointwise $O(\log Y_0)$ by (1.3). A second telescoping estimate therefore bounds the additional weighted mean by

$$O_\alpha\left(\log Y_0 \left(\frac{1}{Y_0} + \frac{Y_1}{H}\right)\right) = o_\alpha(1).$$

Together with (3.12), this proves

$$\sum_k w_H(k) \prod_{p \le Y_1} R_p(k) \le 1 + o_\alpha(1).$$

Finally,

$$\prod_{Y_1 < p \le z} R_p(k) \le \prod_{Y_1 < p \le z} \frac{p}{p-1} = (1 + o_\alpha(1)) \frac{\log z}{\log Y_1}.$$

Since $\log H \sim \eta \log X$,

$$\frac{\log z}{\log Y_1} \longrightarrow \frac{\alpha}{(1-\alpha^2)\eta} = (1-\alpha^2)^{-2}.$$

All factors are nonnegative, so the last pointwise estimate can be multiplied into the preceding weighted bound. This proves (3.10). □

To finish Proposition 3.1, expand the square in (3.1). For each pair of shifts i, j, apply Lemma 3.2 on $I + i$ with $k = j - i$. Averaging the pairs and then using Lemma 3.3 gives

$$\sum_{n \in I} B(n)^2 \le (1 + C\alpha^2) X V(z)^2 \big((1-\alpha^2)^{-2} + o_\alpha(1)\big) + O(X^{3/5}).$$

For small α, $(1-\alpha^2)^{-2} = 1 + O(\alpha^2)$, and $X^{3/5} = o(XV(z)^2)$ by (1.3). This is (3.3); the first moment was proved above.

4. Stable centers and the exceptional set

Lemma 4.1. *Let $\alpha = 2^{-L}$ with fixed $L \ge 2$, and let H be as in (3.1). There is a set $U^* \subset I$ with*

$$|U^*| \ge c_2 d^L X \tag{4.1}$$

for an absolute $c_2 > 0$ and all sufficiently large X, such that every $n \in U^*$ and $0 \le j < H$ satisfy

$$n + j \in I, \qquad A_p(n + j) = 0 \quad (X^\alpha < p \le 2\sqrt{X}). \tag{4.2}$$

Proof. Start with the set counted in Proposition 2.2. Delete its points within H of either endpoint of I, and delete the points meeting any forbidden residue interval enlarged by H at both ends. A prime p contributes at most $O(H(X/p^2 + 1))$ additional deleted points. The total loss is

$$O\left(H + H \sum_{X^\alpha < p \le 2\sqrt{X}} (X/p^2 + 1)\right) \ll H X^{1-\alpha} = o_\alpha(X),$$

because $\eta = \alpha(1-\alpha^2) < \alpha$ and $\alpha \le 1/4$. The remaining set satisfies (4.2), and (4.1) holds with $c_2 = c_0/2$. □

Proof of Theorem 1.1. We first prove the lower bound. Let C_1, C_2 be the constants in Proposition 3.1. Since $d > 1/4$,

$$\frac{(2^{-L})^2}{d^L} = (4d)^{-L} \longrightarrow 0.$$

Choose L sufficiently large, put $\alpha = 2^{-L}$, and set $\rho = c_2 d^L$. We can require $0 < \rho \le 1$ and $\max(C_1, C_2)\alpha^2 \le \rho/16$. Then fix this L and take X sufficiently large to absorb all $o_\alpha(1)$ errors into $\rho/16$. Writing $V = V(z)$, we obtain

$$\sum_{n\in I} B(n) \ge (1-\rho/8)XV, \qquad \sum_{n\in I} B(n)^2 \le (1+\rho/8)XV^2, \qquad |I \setminus U^*| \le (1-\rho)X.$$

Cauchy–Schwarz now gives

$$\begin{aligned}\sum_{n\in U^*} B(n) &\ge \sum_{n\in I} B(n) - \sqrt{|I\setminus U^*| \sum_{n\in I} B(n)^2} \\ &\ge XV\left(1 - \frac{\rho}{8} - \sqrt{(1-\rho)(1+\rho/8)}\right) \ge \frac{\rho}{8}XV.\end{aligned}$$

The last inequality follows from $(1-\rho)(1+\rho/8) \le (1-\rho/4)^2$ for $0 \le \rho \le 1$.

Whenever $n \in U^*$ and a term $S_z(n+j)$ in $B(n)$ equals one, the integer $m = n+j$ lies in I and avoids every prime through z. It also avoids the primes $z < p \le 2\sqrt{X}$ by (4.2). A larger prime has $p^2 > 2X$, so it cannot occur in a representation of m. Thus m is exceptional. For any fixed m, at most H pairs (n, j) satisfy $m = n + j$ with $0 \le j < H$. Therefore

$$E(X) \ge \frac{1}{H} \sum_{n\in U^*} \sum_{j=0}^{H-1} S_z(n+j) = \sum_{n\in U^*} B(n) \ge \frac{\rho}{8} XV(z) \gg \frac{X}{\log X}$$

by (1.3).

For the upper bound, keep one sufficiently small fixed α. For large X, every prime $p \le z$ satisfies $p^2 < X$. Every exceptional integer in I is consequently counted by S_z. In Lemma 3.2, take $k = 0$. Then $S_z(n)^2 = S_z(n)$ and $V_0 = V(z)$, giving

$$E(X) \le \sum_{n\in I} S_z(n) \le (1 + C\alpha^2)XV(z) + O(X^{3/5}) \ll \frac{X}{\log X}.$$

This proves (1.2) for integer X. For real X, replacing X by $\lfloor X \rfloor$ changes the integer interval $(X, 2X]$ by at most two points and changes $X/\log X$ by a factor tending to one. The same two bounds follow after adjusting the constants. □

Acknowledgment

The authors acknowledge assistance from OpenAI's ChatGPT in developing the argument, checking intermediate estimates, and preparing the exposition.

References

[1] P. Erdős, *Some unconventional problems in number theory*, Mathematics Magazine **52** (1979), no. 2, 67–70.
[2] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, Journal für die reine und angewandte Mathematik **78** (1874), 46–62. doi:10.1515/crll.1874.78.46.
[3] P. L. Tchebichef, *Mémoire sur les nombres premiers*, Journal de Mathématiques Pures et Appliquées, sér. 1, **17** (1852), 366–390.