Conjectures.io

Formal proof verified through Conjectures

ERDŐS PROBLEM 18(B): SUMS OF FEW DISTINCT DIVISORS OF $n!$

Abstract. For a practical number N, let $h(N)$ be the least k such that every integer $1 \le m \le N$ is a sum of at most k distinct divisors of N. The accepted Lean submission proves part (b) of Erdős Problem 18: for every $\varepsilon > 0$, $h(n!) < n^{\varepsilon}$ for all sufficiently large n. We explain how the proof works. A radix recursion reduces the factorial bound to representing integers by few divisors of a small factorial. A modular lifting step reduces that to hitting every residue class modulo a power of two. Fourier analysis on $\mathbb{Z}/2^K\mathbb{Z}$, applied to products of digits built from divisors of factorials, reduces this in turn to an exponential-sum decay estimate for products of nonconcentrated odd residues. The submission proves that estimate by an L^2 flattening argument of sum–product type. We give the reductions in full and identify the longer analytic inputs precisely. This paper is an exposition of the accepted artifact and a guide to its complete formal proof.

1. The question and the result

A positive integer N is *practical* if every integer m with $1 \le m \le N$ is a sum of distinct divisors of N. For practical N, write

$$h(N) = \max_{1 \le m \le N} \min\Big\{|D| : \ D \subseteq \{d : d \mid N\},\ \textstyle\sum_{d \in D} d = m\Big\}.$$

Thus $h(N)$ distinct divisors always suffice, and some $m \le N$ needs exactly $h(N)$. Every factorial is practical, so $h(n!)$ is defined for all $n \ge 1$. For example $h(6) = 2$ (the hardest values are $4 = 1 + 3$ and $5 = 2 + 3$) and $h(12) = 3$ (for instance $11 = 1 + 4 + 6$). Part (b) of Erdős Problem 18, as listed in [2], asks whether $h(n!) < n^{o(1)}$. The accepted proof answers this question affirmatively.

Theorem 1.1 (Erdős Problem 18(b)). *For every real $\varepsilon > 0$ there is an integer $n_0(\varepsilon)$ such that for every integer $n \ge n_0(\varepsilon)$, every integer m with $1 \le m \le n!$ is a sum of fewer than n^{ε} distinct divisors of $n!$. Equivalently, $h(n!) < n^{\varepsilon}$ for all $n \ge n_0(\varepsilon)$.*

The threshold $n_0(\varepsilon)$ depends on ε. The proof does not extract an explicit value for it. What the proof actually establishes is the following uniform form.

Theorem 1.2 (Form proved). *For every $0 < p \le 1$ there is a constant $K_p \ge 0$ such that $h(n!) \le K_p + n^p$ for every $n \in \mathbb{N}$.*

Theorem 1.1 follows by taking $p = \min(\varepsilon/2, 1/2)$: eventually $K_p \le n^{\varepsilon}/3$ and $n^p \le n^{\varepsilon}/3$ (Section 8).

Date: 16 November 2026.

Key words and phrases. practical numbers, distinct divisors, factorials, exponential sums, sum–product, Lean.

Submitted by JenW1N. Working proof exposition and source guide prepared with AI assistance from the accepted Lean submission. The longer sum–product and flattening arguments are supplied by the linked formal source. This prose is not itself kernel-verified.

1.1. **The exact formal statement.** The Formal Conjectures source [3] defines h and states the problem as follows. The inner infimum is the least number of distinct divisors of n whose sum is m.

```
noncomputable def practicalH (n : ℕ) : ℕ :=
  Finset.sup (Finset.Icc 1 n) fun m =>
    sInf {k | ∃ D : Finset ℕ, D ⊆ n.divisors ∧ D.card = k ∧
      m ∈ subsetSums D}

theorem erdos_18b : answer(sorry) ↔
    ∀ ε : ℝ, 0 < ε → ∀ᶠ n : ℕ in atTop,
      (practicalH n.factorial : ℝ) < (n : ℝ) ^ ε
```

The committed target asks for a proof with the answer set to *yes*. The submission checks this target type by `rfl` (lines 4–8 of the submitted file):

```
theorem exact_target_type :
    (fcTypeOfName% "Erdos18.erdos_18b") =
      (True ↔ ∀ ε : ℝ, 0 < ε → ∀ᶠ n : ℕ in Filter.atTop,
        (Erdos18.practicalH n.factorial : ℝ) < (n : ℝ) ^ ε) := by
  rfl
```

The final declaration of the submission proves exactly this proposition [S46]. The filter quantifier `∀ᶠ n in atTop` means "for all sufficiently large n". The threshold is chosen after ε, as in Theorem 1.1.

1.2. **Scope and history.** In a problem list presented on 28 June 1974, Erdős defined $f(n)$ as the least integer such that every $1 \le m \le n!$ is a sum of at most $f(n)$ distinct divisors.[1] He wrote that he had proved $f(n) < n$ by a simple induction. He asked whether $f(n) < (\log n)^c$ for an absolute constant c, and added: "I could not even prove $f(n) = o(n)$" [1, Problem 4.33.3]. Theorem 1.1 with $\varepsilon = 1/2$ gives $h(n!) < n^{1/2}$ eventually, hence $h(n!) = o(n)$. It does *not* give the polylogarithmic bound $h(n!) < (\log n)^{O(1)}$, which is part (c) of the modern problem [2]. Nor does it address part (a), on infinitely many practical m with $h(m) < (\log\log m)^{O(1)}$. Throughout, the scope is exactly part (b). We make no claim about priority beyond the cited sources.

1.3. **Small values.** Table 1 lists $h(n!)$ for $n \le 10$, computed exactly by a minimum-count subset-sum over all divisors (and confirmed by exhaustive search for $n \le 5$). The validation script recomputes every entry. These values only illustrate the definition and imply nothing about asymptotics.

n	1	2	3	4	5	6	7	8	9	10
divisors of $n!$	1	2	4	8	16	30	60	96	160	270
$h(n!)$	1	1	2	3	4	5	5	6	7	7
smallest hardest m	1	1	4	17	97	659	3733	33473	362783	2979161

TABLE 1. Exact values of $h(n!)$ for $n \le 10$.

2. Architecture of the proof

Write $\mathrm{len}(R) = \lfloor \log_2 R \rfloor + 1$ for the binary length of $R \ge 1$. The proof has four layers.

(1) *Radix recursion* (Section 3). Passing from $(n - n^\theta)!$ to $n!$ costs only the number of divisors needed for residues below $n!/(n-n^\theta)!$. A potential argument turns this into $h(n!) \le K_p + n^p$, provided every R is a sum of about $\mathrm{len}(R)^{p/4}$ distinct divisors of $F!$ with $F \approx \mathrm{len}(R)^{1+p/16}$.

[1] The printed text reads "divisors of n". The range $m \le n!$ shows that divisors of $n!$ are meant, so $f(n) = h(n!)$.

(2) *Modular lifting* (Section 4). Such local representations follow if, for every large k, every residue class modulo 2^k has a small representative that is a sum of few divisors of a factorial of size polynomial in k.
(3) *Fourier covering* (Sections 5 and 6). Residue classes modulo 2^K are hit by sums of products of elements of a *digit set* A. Each element of A is an odd sum of a few divisors of a factorial. The covering follows from exponential-sum decay for products of elements of A.
(4) *Analytic input* (Section 7). That decay is a *weighted dyadic mixing* estimate for products of nonconcentrated odd residues modulo 2^J. The submission proves it by an L^2 flattening iteration whose single step is a sum–product argument in $\mathbb{Z}/2^J\mathbb{Z}$.

Layers 1–3 are written out in full below. For layer 4 we give the reduction to L^2 flattening and outline the flattening step, which occupies most of the 14,043-line source. Items [S1]–[S48] refer to the source guide in Section 10.

3. The radix recursion

Lemma 3.1 (Radix step [S2])**.** *Let $M \geq 1$ be practical and $q \geq 1$. Suppose every $0 \leq r < q$ is a sum of at most ℓ distinct divisors of qM. Then $h(qM) \leq h(M) + \ell$. In particular, if $m \leq n$ and every $r < n!/m!$ is a sum of at most ℓ distinct divisors of $n!$, then $h(n!) \leq h(m!) + \ell$.*

Proof. Let $1 \leq R \leq qM$ and write $R = qa + r$ with $0 \leq r < q$, so $a \leq M$. Since M is practical, $a = \sum_{d \in D} d$ with D a set of at most $h(M)$ divisors of M ($D = \emptyset$ if $a = 0$). The numbers qd, $d \in D$, are distinct divisors of qM, and each is at least $q > r$. Write r as a sum over a set E of at most ℓ distinct divisors of qM. Every element of E is at most r, so qD and E are disjoint, and R is the sum of the at most $h(M) + \ell$ elements of $qD \cup E$. For the second statement take $M = m!$ and $q = n!/m!$. □

For example, with $n = 9$ and $m = 6$ we have $q = 504$, and every $r < 504$ is a sum of at most 3 distinct divisors of $9!$. The lemma gives $h(9!) \leq h(6!) + 3 = 8$. The true value is 7. The validation script checks the lemma's conclusion for all $1 \leq m < n \leq 9$.

Divisor sums with repetition are easier to manipulate. The next lemma converts them into distinct sums at a small cost in the host.

Lemma 3.2 (Distinctification [S3], [S4])**.** *Let s be a multiset of u divisors of $N \geq 1$. Then $\sum s$ is a sum of at most u distinct divisors of $2^u N$. Moreover $2^u \cdot F! \mid (F + 2u)!$, so a sum of u divisors of $F!$ with repetition is a sum of at most u distinct divisors of $(F + 2u)!$.*

Proof. Induct on u. If s has no repetition, it is already a set of divisors of $N \mid 2^u N$. Otherwise replace two copies of some d by the single element $2d$. The sum is unchanged, and the new multiset has $u - 1$ divisors of $2N$. By induction its sum is a sum of at most $u - 1$ distinct divisors of $2^{u-1} \cdot 2N = 2^u N$. For the second claim, $2^u \mid (2u)!$ and $(2u)!\, F! \mid (F + 2u)!$. □

For instance $9 = 3 + 3 + 3$ uses the divisor 3 of 6 three times. Merging one pair gives $9 = 6 + 3$, a sum of distinct divisors of 12.

Proposition 3.3 (Local bounds give the power bound [S5]–[S8])**.** *Let $0 < p \leq 1$ and set $a = 1 + p/16$ and $b = p/4$. Suppose there is $C > 0$ such that every $R \geq 1$ is a sum of at most $C \operatorname{len}(R)^b$ distinct divisors of $F!$ for some $F \leq C \operatorname{len}(R)^a$. Then there is $K \geq 0$ with $h(n!) \leq K + n^p$ for all n.*

Proof. Put $\theta = 1 - p/4$ and $\gamma = p/8$. For large n let $w = \lfloor n^\theta \rfloor$ and $m = n - w$. Then $n^\theta/2 \leq w < n$, and $Q = n!/m! \leq n^w$. Since $\operatorname{len}(n) \leq n^\gamma$ eventually,

$$\operatorname{len}(Q) \leq w \operatorname{len}(n) + 1 \leq 2n^{\theta+\gamma}.$$

Let $1 \leq R < Q$, so $\operatorname{len}(R) \leq \operatorname{len}(Q)$. The hypothesis supplies $F \leq C(2n^{\theta+\gamma})^a$. The exponent satisfies

$$(\theta + \gamma)a = (1 - \tfrac{p}{8})(1 + \tfrac{p}{16}) = 1 - \tfrac{p}{16} - \tfrac{p^2}{128} < 1,$$

so $F \le n$ for large n. Then $F! \mid n!$ and R is a sum of distinct divisors of $n!$, at most

$$\ell = C(2n^{\theta+\gamma})^b \quad \text{of them, where} \quad (\theta+\gamma)b = \tfrac{p}{4} - \tfrac{p^2}{32} < \tfrac{3p}{4} = \theta + p - 1.$$

Hence $\ell \le \frac{p}{2} n^{\theta+p-1}$ for large n. By Lemma 3.1, $h(n!) \le h(m!) + \frac{p}{2} n^{\theta+p-1}$. Concavity of $x \mapsto x^p$ gives $x^p - y^p \ge p(x-y)x^{p-1}$ for $0 \le y \le x$. Therefore

$$n^p - m^p \ge p\, w\, n^{p-1} \ge \tfrac{p}{2} n^{\theta+p-1}.$$

So there is N_0 such that each $n \ge N_0$ has some $m < n$ with

$$h(n!) - n^p \le h(m!) - m^p.$$

By strong induction, $h(n!) \le K + n^p$ for every n, with $K = \sum_{i<N_0} h(i!)$. □

4. Modular lifting

Definition 4.1 (Dyadic modular bounds [S10])**.** For $a, b > 0$, say that *dyadic modular bounds* hold with exponents (a, b) if there are $D, k_0 \in \mathbb{N}$ and $A, B > 0$ with the following property. For every $k \ge k_0$ there are F, u with $2^k \mid F!$, $F \le Ak^a$, $u \le Bk^b$, such that every residue class modulo 2^k contains an integer $S \le 2^{kD}$ which is a sum of at most u divisors of $F!$, repetitions allowed.

Proposition 4.2 (Lifting [S9], [S11], [S12])**.** *If dyadic modular bounds hold with exponents (a, b), then there are $C, E > 0$ such that every $R \ge 1$ is a sum of at most $E \operatorname{len}(R)^b$ divisors of $F!$ with repetition, for some $F \le C \operatorname{len}(R)^a$. If also $b \le a$, the hypothesis of Proposition 3.3 holds with exponents (a, b).*

Proof. Let $\lambda = 1 - \frac{1}{2(D+1)} < 1$. Choose $C \ge \max(2^{(D+1)(k_0+1)}, A/(1-\lambda^a))$ and $E \ge \max(1, B/(1-\lambda^b))$. We use strong induction on R. If $R < 2^{(D+1)(k_0+1)}$, then $R \mid R!$, so take $F = R$ and one summand.

Otherwise put $k = \lfloor \lfloor \log_2 R \rfloor / (D+1) \rfloor \ge k_0$ and $q = 2^k$. Then $q^{D+1} \le R$ and $k \le \operatorname{len}(R)$. Take the representative $S \equiv R \pmod q$ with $S \le q^D$, a sum of at most $u \le B \operatorname{len}(R)^b$ divisors of $F!$ with $F \le A \operatorname{len}(R)^a$. Since $S \le q^D \le R/q < R$, the integer $T = (R-S)/q$ satisfies $1 \le T \le R/q$. By induction, T is a sum of at most $E \operatorname{len}(T)^b$ divisors of $G!$, where $G \le C \operatorname{len}(T)^a$. Each qd with $d \mid G!$ divides $F!\,G!$, which divides $(F+G)!$, because $q \mid F!$. So $R = S + qT$ is a sum of at most $u + E \operatorname{len}(T)^b$ divisors of $(F+G)!$.

Since $T \le R/2^k$, we have $\operatorname{len}(T) \le \operatorname{len}(R) - k$. Also $\operatorname{len}(R) \le 2(D+1)k$, so $\operatorname{len}(T) \le \lambda \operatorname{len}(R)$. Therefore

$$F + G \le A \operatorname{len}(R)^a + C\lambda^a \operatorname{len}(R)^a \le C \operatorname{len}(R)^a,$$

and similarly for the count. For the last claim, apply Lemma 3.2: R is a sum of at most u distinct divisors of $(F+2u)!$, and $F + 2u \le (C+2E) \operatorname{len}(R)^a$ when $b \le a$. □

5. Covering residues modulo 2^K by Fourier analysis

For a function μ on $\mathbb{Z}/2^K\mathbb{Z}$ write $\widehat{\mu}(x) = \sum_y \mu(y)\, \mathrm{e}(-xy/2^K)$, where $\mathrm{e}(t) = \exp(2\pi i t)$. This is the unnormalized transform used by Mathlib. The *level* $\operatorname{lev}(x)$ of $x \ne 0$ is the j with additive order 2^j, so $1 \le \operatorname{lev}(x) \le K$. For laws μ, ν let $\mu * \nu$ be the additive convolution and $\mu \circledast \nu$ the multiplicative one, which is the law of a product of independent samples. Let $\mu^{\circledast r}$ be the r-fold product law.

Lemma 5.1 (Fourier positivity [S13], [S14])**.** *Let μ satisfy $\widehat{\mu}(0) = 1$ and $\sum_{x \ne 0} |\widehat{\mu}(x)|^s < 1$. Then $\mu^{*s}(y) \ne 0$ for every y. If $|\widehat{\mu}(x)| \le 2^{-t \operatorname{lev}(x)}$ for all $x \ne 0$ and $ts \ge 2$, the hypothesis holds.*

Proof. By inversion, $2^K \mu^{*s}(y) = 1 + \sum_{x \ne 0} \widehat{\mu}(x)^s \mathrm{e}(xy/2^K)$. The sum has modulus less than 1. For the second claim, at most 2^j elements have level j. So the sum is at most $\sum_{j=1}^{K} 2^j 4^{-j} = 1 - 2^{-K}$. □

If every point in the support of μ is the residue of an integer $S \le H$ that is a sum of at most u divisors of $F!$, then every point in the support of μ^{*s} is the residue of an integer $S \le sH$ that is a sum of at most su such divisors [S13].

Proposition 5.2 (Covering from product decay [S15], [S16]). *Let $t > 0$ and $s = \lceil 2/t \rceil$. Let f be a probability law on $\mathbb{Z}/2^K\mathbb{Z}$ supported on odd residues. Let $b, r \ge 1$, and suppose:*

1. *$\widehat{f}(x) = 0$ whenever $2 \le \mathrm{lev}(x) \le b$;*
2. *$|\widehat{f^{\circledast r}}(x)| \le 2^{-t\,\mathrm{lev}(x)}$ whenever $\mathrm{lev}(x) > b$;*
3. *each residue in the support of f is the residue of an integer $S \le 2^K$ that is a sum of at most u divisors of $F!$;*
4. *$2s \le 2^K$.*

Then every residue class modulo 2^K contains an integer $S \le 2^{K(r+1)}$ that is a sum of at most $s(u^r+1)$ divisors of $(rF)!$.

Proof. Let g be the law of $y_1 \cdots y_r + \beta$, where the y_i are independent with law f and $\beta \in \{0,1\}$ is a fair independent bit. Then $\widehat{g}(x) = \widehat{f^{\circledast r}}(x) \cdot \frac{1}{2}(1 + \mathrm{e}(-x/2^K))$, and the last factor has modulus at most 1. If $\mathrm{lev}(x) = 1$, then $x = 2^{K-1}$ and the factor vanishes. If $2 \le \mathrm{lev}(x) \le b$, write $\widehat{f \circledast h}(x) = \sum_z h(z)\widehat{f}(zx)$. Multiplying by a unit preserves the level, so by (1) every term vanishes. Induction on r gives $\widehat{f^{\circledast r}}(x) = 0$. If $\mathrm{lev}(x) > b$, use (2). Thus $|\widehat{g}(x)| \le 2^{-t\,\mathrm{lev}(x)}$ for all $x \ne 0$, and Lemma 5.1 shows that g^{*s} charges every residue.

For representatives, a product $S_1 \cdots S_r$ of integers from (3) expands into at most u^r products of r divisors of $F!$. Each such product divides $(F!)^r$, which divides $(rF)!$. Adding β adds the divisor 1. So each atom of g is represented by an integer at most $2^{Kr}+1$ using at most u^r+1 divisors. Summing s of these gives at most $s(u^r+1)$ divisors and the value $s(2^{Kr}+1) \le 2s\,2^{Kr} \le 2^{K(r+1)}$. □

6. Digit sets built from divisors of factorials

Fix $a > 1$. For large K put $F = \lceil K^a \rceil$ and $b_0 = \lfloor \log_2 F \rfloor$. Then $2 \le b_0 \le K$ and $2^{b_0} \le F$. For $\ell \ge 1$ let

$$D_\ell = \{0\} \cup \{d : \ d \mid F!, \ d < 2^\ell\}.$$

Lemma 6.1 (Many short divisors [S17]–[S19]). *There is $c \in (0, 1/2]$, depending on a, such that for all large K and all $1 \le \ell \le K$ we have $|D_\ell| \ge 2^{c\ell}$.*

Proof. Let $\delta = (a-1)/(4a)$ and $\lambda = \mathrm{len}(F)$, so $2^{\lambda/2} \le F$. Chebyshev's lower bound for the prime-counting function (in Mathlib) gives $\pi(F) \ge F^{1-\delta}$ for large F. Since $F^{1-2\delta} \approx K^{(a+1)/2}$ and $(a+1)/2 > 1$, we get $\pi(F) \ge 2KF^\delta$ for large K. If $\ell \le 4\lambda$, every integer $d \le \min(F, 2^\ell - 1)$ divides $F!$. Hence $|D_\ell| \ge \min(F+1, 2^\ell) \ge 2^{\delta\ell/8}$. If $\ell > 4\lambda$, let $v = \lfloor \ell/(2\lambda) \rfloor \ge 1$, so $\ell \le 4\lambda v$. Products of v distinct primes $\le F$ are distinct divisors of $F!$ smaller than $F^v \le 2^{\lambda v} < 2^\ell$. Since $v \le K$, we have $\pi(F)/(2v) \ge F^\delta$, and so

$$|D_\ell| \ge \binom{\pi(F)}{v} \ge \Big(\frac{\pi(F)}{2v}\Big)^v \ge F^{\delta v} \ge 2^{\delta\lambda v/2} \ge 2^{\delta\ell/8}.$$

Take $c = \min(\delta/8, 1/2)$. □

Now define block endpoints $e_i = \min(K, 2^i b_0)$. Let A_0 be the set of odd integers below 2^{b_0}, and put

$$A_{i+1} = \{x + 2^{e_i} d : \ x \in A_i, \ d \in D_{e_{i+1}-e_i}\}.$$

Let $A = A_{\mathrm{len}(K)}$. Since $2^{\mathrm{len}(K)} > K$, the last endpoint is K.

Lemma 6.2 (Digit-set profile [S20]–[S24]). *For all large K:*

1. *A consists of odd integers in $[0, 2^K)$, and $|A_{i+1}| = |A_i||D_{e_{i+1}-e_i}|$;*

(2) *every element of A is a sum of at most* $\mathrm{len}(K)+1$ *divisors of* $(F+2K)!$*;*
(3) $|A_i| \ge 2^{ce_i}$*;*
(4) *for* $2 \le j \le K$*, every residue class modulo* 2^j *contains at most* $2^{-(c/2)j}|A|$ *elements of* A*;*
(5) *the uniform law* f_A *of* A *modulo* 2^K *has* $\widehat{f_A}(x) = 0$ *whenever* $2 \le \mathrm{lev}(x) \le b_0$.

Proof. (1) Elements of A_i are below 2^{e_i}, so $x + 2^{e_i}d$ determines (x, d), and oddness is inherited from A_0. (2) Elements of A_0 are below $2^{b_0} \le F$, so they divide $F!$. An appended term $2^e d$ with $e \le K$ and $d \mid F!$ divides $2^K F!$, which divides $(F+2K)!$. There are $\mathrm{len}(K)$ appended terms. (3) We have $|A_0| = 2^{b_0-1} \ge 2^{cb_0}$, and widths satisfy $e_{i+1} - e_i \le e_i \le K$, so Lemma 6.1 applies at each step. (4) Induct on i. For A_0 and $2 \le j \le b_0$, the mass of a residue class is 0 or $2^{1-j} \le 2^{-(c/2)j}$. For $j \le e_i$, the appended digits are invisible modulo 2^j, and each x is extended by the same number of digits, so the masses are unchanged. For $e_i < j \le e_{i+1} \le 2e_i$, a residue class modulo 2^j determines $x \in A_i$. Its mass is therefore at most $1/|A_i| \le 2^{-ce_i} \le 2^{-(c/2)j}$. (5) Write $x = 2^{K-j}m$ with m odd and $j = \mathrm{lev}(x) \le b_0$. Appended terms are multiples of 2^{b_0}, so they do not affect $\mathrm{e}(-xy/2^K)$. The transform factors through the uniform law on odd residues modulo 2^j, whose sum $\sum_{t<2^{j-1}} \mathrm{e}(-m(1+2t)/2^j)$ vanishes for $j \ge 2$. □

The remaining hypothesis of Proposition 5.2 is decay of $\widehat{f_A^{\circledast r}}$ above level b_0. If $\mathrm{lev}(x) = j$ and $x = 2^{K-j}m$ with m odd, then

$$\widehat{f_A^{\circledast r}}(x) = \mathbb{E}_{y_1,\dots,y_r \in A}\, \mathrm{e}\big(-m\, y_1 \cdots y_r / 2^j\big),$$

an exponential sum modulo 2^j only [S25]. By Lemma 6.2(4), A satisfies the nonconcentration hypothesis of the following estimate with $g = c/2$, at every modulus 2^j with $j \le K$.

Theorem 6.3 (Weighted dyadic mixing [S26], [S35])**.** *For every* $0 < g \le 1/2$ *there are* $r \ge 1$*,* $t > 0$ *and* J_0 *such that the following holds for every* $J \ge J_0$*. Let* A *be a nonempty finite set of odd natural numbers such that, for each* $2 \le l \le J$*, every residue class modulo* 2^l *contains at most* $2^{-gl}|A|$ *elements of* A*. Then for every odd* m*,*

$$\Big|\mathbb{E}_{y_1,\dots,y_r \in A}\, \mathrm{e}\big(-m\, y_1 \cdots y_r / 2^J\big)\Big| \le 2^{-tJ}.$$

This is proved in the submitted file (Section 7). It is not an additional hypothesis.

Proposition 6.4 (Dyadic modular bounds [S27])**.** *For every* $a > 1$ *and* $b > 0$*, dyadic modular bounds hold with exponents* (a, b).

Proof. Take c from Lemma 6.1, then r, t, J_0 from Theorem 6.3 with $g = c/2$, and $s = \lceil 2/t \rceil$. Let K be large, with $b_0 \ge J_0$. Apply Proposition 5.2 to $f = f_A$ with $b = b_0$, host $F+2K$ and $u = \mathrm{len}(K)+1$. Hypothesis (1) is Lemma 6.2(5). Hypothesis (2) is Theorem 6.3 at $J = \mathrm{lev}(x) > b_0 \ge J_0$, by the display above. Hypothesis (3) is Lemma 6.2(2). Every residue class modulo 2^K thus has a representative $S \le 2^{K(r+1)}$ that is a sum of at most $s((\mathrm{len}(K)+1)^r + 1) \le BK^b$ divisors of $(r(F+2K))!$. Here $r(F+2K) \le 4rK^a$. Finally $2^K \mid (F+2K)!$ by Lemma 3.2, so $D = r+1$ works. □

7. The analytic input

Theorem 6.3 is deduced from a statement about general laws on $\mathbb{Z}/2^J\mathbb{Z}$. Call a nonnegative function ρ on $\mathbb{Z}/2^J\mathbb{Z}$, or on its unit group, (γ, ε)-*nonconcentrated* if for every L with $\varepsilon J < L \le J$, each residue class modulo 2^L has ρ-mass at most $2^{-\gamma L}$. For a law μ and a law w on units, the *averaging step* is

$$S_w\mu = \Big(\sum_u w(u)\, \mu(u^{-1}\,\cdot\,)\Big)^{*2}, \qquad \widehat{S_w\mu}(k) = \Big(\sum_u w(u)\, \widehat{\mu}(uk)\Big)^2.$$

The product iteration is $\nu_0 = f$ and $\nu_{n+1} = \sum_u w_n(u)\,\nu_n(u^{-1}\cdot)$, the law of $y\,u_1\cdots u_n$. Theorem 6.3 is the case $f = w_n = f_A$, which is supported on units and nonconcentrated with $\gamma = g$ once $\varepsilon J \ge 2$.

Theorem 7.1 (Product decay [S34]). *For every $\gamma > 0$ there are $\varepsilon \in (0, 1/4]$, $\tau > 0$, $R \ge 1$ and J_0 such that for $J \ge J_0$, all (γ,ε)-nonconcentrated laws f and $w_0, \dots, w_R$ (the w_n on units), and every unit k: $|\widehat{\nu_{R+1}}(k)| \le 2^{-\tau J}$.*

The proof combines three ingredients. The first two are short.

Lemma 7.2 (Repeated squaring [S29], [S30]). *Let $\tilde f = f * f(-\cdot)$, so that $\widehat{\tilde f} = |\widehat f|^2 \ge 0$, and let $\mu_n = S_{w_{n-1}} \cdots S_{w_0} \tilde f$. Then for all k,*

$$|\widehat{\nu_{R+1}}(k)|^{2^{R+1}} \le \sum_u w_R(u)\,\widehat{\mu_R}(uk).$$

Proof. First, $|\widehat{\nu_n}(k)|^{2^{n+1}} \le \widehat{\mu_n}(k)$ by induction on n. For $n = 0$ this is $|\widehat f|^2 = \widehat{\tilde f}$. For the step, $\widehat{\nu_{n+1}}(k) = \sum_u w_n(u)\widehat{\nu_n}(uk)$. By convexity of $z \mapsto |z|^{2^{n+1}}$ under the probability w_n, this gives $|\widehat{\nu_{n+1}}(k)|^{2^{n+1}} \le \sum_u w_n(u)\widehat{\mu_n}(uk)$. Squaring gives $\widehat{\mu_{n+1}}(k)$. The same convexity step at $n = R$ gives the claim. □

Lemma 7.3 (Bilinear bound [S31]). *If k is a unit, w is a law on units with $\max_u w(u) \le M$, and μ is any function, then*

$$\Big|\sum_u w(u)\,\widehat\mu(uk)\Big|^2 \le 2^J M \sum_x |\mu(x)|^2.$$

Proof. By Cauchy–Schwarz the left side is at most $\sum_u w(u)^2 \cdot \sum_u |\widehat\mu(uk)|^2$. The first factor is at most M. Since $u \mapsto uk$ is injective, Parseval bounds the second by $\sum_x |\widehat\mu(x)|^2 = 2^J \sum_x |\mu(x)|^2$. □

The third ingredient is the long formal input.

Proposition 7.4 (L^2 flattening [S32], [S33]). *For $\gamma > 0$ and $0 < \delta \le 1$ there are $\tau' > 0$, $\varepsilon \in (0, 1/4]$ and J_0 such that for $J \ge J_0$, every (γ,ε)-nonconcentrated law μ and (γ,ε)-nonconcentrated law w on units satisfy*

$$\textstyle\sum_x |S_w\mu(x)|^2 \le \max\big(2^{-(1-\delta)J},\ 2^{-\tau' J}\sum_x |\mu(x)|^2\big).$$

Nonconcentration passes from μ to $S_w\mu$. Consequently, for some R depending only on γ, δ, every iterate μ_R as in Lemma 7.2 has $\sum_x |\mu_R(x)|^2 \le 2^{-(1-\delta)J}$.

Proof of Theorem 7.1 from these inputs. Let $\delta = \min(\gamma/2, 1/2)$, so $\gamma - \delta > 0$. Taking $L = J$ in the nonconcentration of w_R gives $\max_u w_R(u) \le 2^{-\gamma J}$. The symmetrized law $\tilde f$ is again nonconcentrated, so Proposition 7.4 applies to the iterates μ_n. By Lemmas 7.2 and 7.3,

$$|\widehat{\nu_{R+1}}(k)|^{2^{R+2}} \le 2^J \cdot 2^{-\gamma J} \cdot 2^{-(1-\delta)J} = 2^{-(\gamma-\delta)J}.$$

Thus $\tau = (\gamma - \delta)/2^{R+2}$ works. □

7.1. **How the flattening step is proved.** We outline the argument for Proposition 7.4 and point to its formal statements. Write $\mu_v = \mu(v^{-1}\cdot)$. A Fourier identity and Cauchy–Schwarz bound $\sum_x |S_w\mu(x)|^2$ by the average, over independent u, v with law w, of $\sum_x |\mu * \mu_{u^{-1}v}(x)|^2$ [S32]. So it suffices to show the following whenever $\sum_x \mu(x)^2 \ge 2^{-(1-\delta)J}$: the w-average of $\sum_x |\mu * \mu_v(x)|^2$ is at most $2^{-\tau' J}\sum_x \mu(x)^2$ [S36]. Splitting μ into boundedly many dyadic level sets reduces this to sets $A, B \subseteq \mathbb{Z}/2^J\mathbb{Z}$ of size at most $2^{(1-\delta)J}$ and a nonconcentrated set T of units [S37]. For indicator functions, $\sum_x (1_A * 1_{vB})(x)^2$ is the additive energy $E(A, vB)$. The target becomes

$$\Big(\sum_{u\in T} E(A, uB)\Big)^2 \le 2^{-\tau' J}|T|^2|A|^3|B|^3,$$

and the mixed case is reduced to the case $B = A$ [S38].

The saving for $B = A$ is proved by contradiction. If every large subfamily of T contains a multiplier with small energy, the average over T is small [S39]. So suppose instead that many $u \in T$ have $E(A, uA) \geq 2^{-\tau' J}|A|^3$. A Balog–Szemerédi–Gowers argument then gives two things [S40]: a large $B \subseteq A$, and many normalized multipliers S with $|B + sB| \leq K|B|$ for all $s \in S$, where $K = 2^{O(\tau' J)}$. Call such an S a stabilizer of B. Sums and products of stabilizing elements remain stabilizing, at a polynomial cost in K. Since B is nonconcentrated and has density deficit, every stabilizer has size at most $K \cdot 2^{(1-c)J}$ [S41]. On the other hand, S inherits nonconcentration from T, so its residues modulo 2^L are numerous for every $L > \varepsilon J$. A sum–product growth theorem in $\mathbb{Z}/2^J\mathbb{Z}$ then forces the iterated sum–product closure of S to grow by a factor $2^{\sigma J}$ at each step [S43]. After boundedly many steps this exceeds the stabilizer bound, a contradiction [S42]. The growth theorem itself is proved by multi-scale analysis. The set is first regularized into a "dyadic regular tree", with a uniform number of lifts at each block of scales. Entropy-increment arguments then show that either sums, or bounded combinations of products of differences, grow at a positive proportion of scales [S44], [S45].

The paragraph above is a road map, not a proof. Each step is a verified theorem of the submitted file, with constants that depend only on (γ, δ) and not on J. That uniformity is what the order of quantifiers in Theorem 6.3 requires.

8. Assembling the final theorem

Proof of Theorems 1.1 and 1.2. Let $0 < p \leq 1$. Proposition 6.4 gives dyadic modular bounds with exponents $(1 + p/16, p/4)$, and $p/4 \leq 1 + p/16$. Proposition 4.2 supplies the hypothesis of Proposition 3.3, which yields K_p with $h(n!) \leq K_p + n^p$ for all n. This is Theorem 1.2.

Given $\varepsilon > 0$, put $p = \min(\varepsilon/2, 1/2)$, so $0 < p < \varepsilon$. For large n we have $n^p \leq n^\varepsilon/3$ and $K_p \leq n^\varepsilon/3$, hence

$$h(n!) \leq K_p + n^p \leq \tfrac{2}{3} n^\varepsilon < n^\varepsilon.$$

This proves the forward direction of the committed equivalence. The reverse direction concludes `True` and is immediate. □

Remark 8.1 (Conditional routes in the file). The source also contains two conditional deductions, from a set-valued mixing hypothesis and from an optional stronger set estimate (rows [S47], [S48]). Neither hypothesis is asserted as a theorem, and neither deduction is used by the final theorem. The final theorem applies the deduction of row [S28] to the unconditional proof of row [S35], in the declaration of row [S46].

9. Formal verification and provenance

The submission was accepted by the service on 16 September 2026 at 06:43:46 UTC. Production verification run 32 returned `VERIFIED` at 06:47:33 UTC. The run passed the statement comparator, task-commitment, trusted-hash and submission-policy checks, the permitted-axiom check and the Lean kernel check, under `landrun+seccomp`. The allowed axioms were `propext`, `Quot.sound` and `Classical.choice`. Nanoda was disabled. The task was built from Formal Conjectures task revision `8432eac99811`. The human-authorized reward review approved the submission on 16 September 2026 at 20:29:30 UTC under policy v3. No new Lean replay was performed for this paper. The public proof was retrieved on 16 November 2026 and checked byte for byte against the accepted digest. JenW1N is the public solver name attached to the submitted proof. The submitted file contains no third-party license notices.

10. Guide to the complete source

Line numbers below refer to the exact public submitted `Main.lean`, which has 14,043 lines. They count submitted bytes only, without the validator's trusted header and footer. The source checksum is

`4d6ee89617415288e9f127beb3c0e0211c01`
`1f891889fcb43d0e16373bd14088`.

The formal source contains the complete auxiliary development. The prose proofs above give the radix recursion, distinctification, modular lifting, Fourier covering, digit sets, the reduction of Theorem 6.3 to L^2 flattening, and the final parameter deduction. The flattening and sum–product theorems are stated through their verified interfaces and located in the table.

	Declaration and starting line	Mathematical role
S1	`practicalH_le_of_short_sums` (28)	Upper bounds on h from short sums.
S2	`practicalH_radix` (99) `factorial_radix_recurrence` (111)	Lemma 3.1.
S3	`distinctify_divisor_multiset` (177)	Merging repeated divisors.
S4	`factorial_binary_reserve` (157) `factorial_multiset_to_distinct` (243)	$2^u F! \mid (F+2u)!$ and Lemma 3.2.
S5	`eventually_radix_width_bounds` (689)	Width n^θ and $\mathrm{len}(n!/m!)$.
S6	`bounded_of_eventual_potential_decrease` (729)	Potential argument.
S7	`eventual_factorial_potential_decrease` (748)	One radix step with exponent bookkeeping.
S8	`local_bounds_give_power_bound` (812)	Proposition 3.3.
S9	`positive_lifting_of_congruence` (147)	$R = S + qT$ with $1 \le T \le R/q$.
S10	`HasBoundedModularRepresentatives` (313) `DyadicModularBounds` (492)	Definition 4.1.
S11	`bounded_recursive_modular_lifting` (363)	Lifting recursion with budgets.
S12	`dyadic_modular_bounds_give_local_multisets` (498) `dyadic_modular_bounds_give_local_bounds` (557)	Proposition 4.2.
S13	`convolution_pow_support_representatives` (970) `bounded_modular_representatives_of_fourier` (1002)	Positivity and representatives.
S14	`dyadic_fourier_norm_sum_lt_one` (1058) `exists_convolution_power_for_dyadic_decay` (1108)	Level counting in Lemma 5.1.
S15	`dft_smooth_product_zero_at_low_conductor` (1472)	Low levels vanish after smoothing.
S16	`exists_power_modular_representatives_of_product_decay` (1487)	Proposition 5.2.
S17	`shortFactorialDigits` (1525)	The sets D_ℓ.
S18	`eventually_primeCounting_ge_rpow` (1624)	$\pi(F) \ge F^{1-\delta}$ from Chebyshev.
S19	`shortFactorialDigits_uniform_lower` (1673) `shortFactorialDigits_uniform_asymptotic` (1755)	Lemma 6.1.
S20	`binaryAppend` (1804) `binaryBlockSet` (2098)	Digit-set construction.
S21	`BinaryBlockProfile` (2061) `binary_block_set_profile` (2143)	Lemma 6.2(1)–(3).
S22	`binary_append_spread` (2006)	Lemma 6.2(4).
S23	`dft_binary_block_set_low` (2218)	Lemma 6.2(5).
S24	`factorialBlockSet` (2287) `factorial_block_laws` (2348)	Parameters $F = \lceil K^a \rceil$, b_0.
S25	`dft_product_uniform_transfer` (2451)	Reduction to modulus $2^{\mathrm{lev}(x)}$.
S26	`WeightedDyadicMixing` (2472)	Statement of Theorem 6.3.

	Declaration and starting line	Mathematical role
S27	`block_product_decay_of_weighted_mixing` (2482) `dyadic_modular_bounds_of_block_product_decay` (2547)	Proposition 6.4.
S28	`erdos18b_of_weighted_dyadic_mixing` (2580) `erdos18b_of_dyadic_modular_bounds` (827)	Final deduction (Section 8).
S29	`cyclicUnitAveragingStep` (13366) `cyclicUnitProductIter` (13740)	S_w and the product iteration.
S30	`norm_dft_unit_product_dominated` (13745) `norm_dft_unit_product_final_power_le` (13774)	Lemma 7.2.
S31	`norm_dft_unit_mixture_sq_le` (13803)	Lemma 7.3.
S32	`exists_dyadic_averaging_step_flattening` (13413) `exists_dyadic_averaging_step_energy_bound` (13462)	One averaging step in Proposition 7.4.
S33	`exists_dyadic_probability_flattening_iteration` (13540)	Iteration count R in Proposition 7.4.
S34	`exists_dyadic_unit_product_fourier_decay` (13846)	Theorem 7.1.
S35	`weighted_dyadic_mixing` (14011)	Proof of Theorem 6.3.
S36	`exists_dyadic_probability_flattening` (12648) `exists_dyadic_weighted_probability_flattening` (12983)	Energy of $\mu * \mu_v$ averaged over multipliers.
S37	`exists_finite_dyadic_level_decomposition` (12384) `exists_dyadic_set_combination_flattening` (12041)	Dyadic level sets.
S38	`exists_dyadic_average_unit_energy_decay` (11480) `exists_dyadic_average_mixed_energy_decay` (11679)	Saving for $E(A, uA)$ and $E(A, uB)$.
S39	`exists_dyadic_unit_dilate_energy_saving` (11342) `finite_sum_bound_of_hereditary_small_value` (11440)	One good multiplier in every large subfamily.
S40	`finite_bsg_two_sets` (9701) `finite_many_unit_dilates_stabilizer` (10250)	Balog–Szemerédi–Gowers; stabilizer extraction.
S41	`ring_sum_stabilizer_quadratic_closure` (10494) `exists_dyadic_sum_stabilizer_density_bound` (10859)	Closure of stabilizers; size bound.
S42	`exists_dyadic_no_projecting_stabilizer` (11084)	No well-projecting stabilizer.
S43	`exists_dyadic_sum_product_double_growth_of_projection` (10935) `exists_dyadic_ring_quadratic_growth` (11033)	Sum–product growth in $\mathbb{Z}/2^J\mathbb{Z}$.
S44	`exists_general_dyadic_growth_dichotomy` (8478) `exists_dyadic_signed_sum_product_growth` (8753)	Growth dichotomy.
S45	`exists_dyadic_regular_tree` (3612) `exists_uniform_regular_tree_quadratic_amplification` (8186)	Regular trees; amplification.
S46	`target` (14040)	Exact committed target.
S47	`DyadicSetMixing` (2847) `erdos18b_of_dyadic_set_mixing` (2921)	Unused conditional route.
S48	`BourgainDyadicSetEstimate` (2947) `erdos18b_of_bourgain_dyadic_set_estimate` (2983)	Unused optional hypothesis.

References

[1] P. Erdős, *Problems*, Mathematica Balkanica **4** (1974), 203–204, Problem 4.33.3. Presented 28 June 1974 at the problem session of the 5th Balkan Mathematical Congress. Archive scan, printed p. 203.

[2] T. F. Bloom, *Erdős Problem #18*. https://www.erdosproblems.com/18. Retrieved 16 November 2026.

[3] Formal Conjectures contributors, *Erdős Problem 18*, `FormalConjectures/ErdosProblems/18.lean`.

[4] JenW1N, *Accepted Lean submission for Erdős Problem 18(b)*, submitted 16 September 2026, approved 16 September 2026. Complete formal proof; public result and review.