MATHDISCOVERIES
Mathematical Preprint

Working Draft

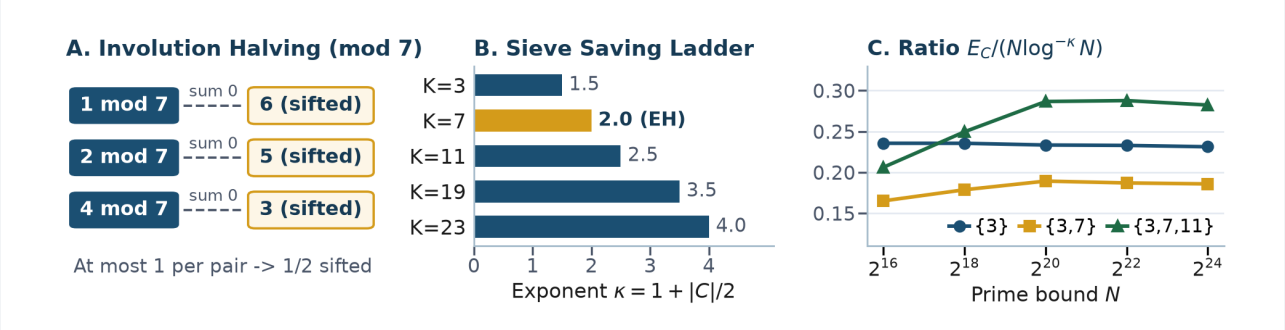
Erdős–Straus: A Sieve Bound on the Type II Branch for Fixed Shifts

Tyler B. Hughes*,†

†Independent Researcher, United States

Ⓢ *Supporting Information: standalone exact-arithmetic verifier (`recompute.py`, `recompute.out`) and trust-boundary ledgers*

Disclosure: AI-assisted working draft directed by Tyler B. Hughes. Not for submission as is. No human mathematician has yet refereed the proof.



ABSTRACT: For any prime $p \equiv 1 \pmod 4$, a shift $c \equiv 3 \pmod 4$ proposes $x_c = (p+c)/4$ in $4/p = 1/x + 1/y + 1/z$; the Type II branch succeeds when coprime d_1, d_2 satisfy $d_1 d_2 \mid x_c$ and $c \mid d_1 + d_2$. We prove an involution lemma: if shift c fails Type II at $p > c$, then the prime-factor residues of x_c mod c avoid inverse pairs $\{a, -a\}$ and lie in one of $2^{\varphi(c)/2}$ half systems. With Montgomery's large sieve ($Q = \sqrt{N}$), Mertens' theorem in progressions, and Rankin's trick, any finite nonempty set C of shifts $c \equiv 3 \pmod 4$ has $E_C(N) \ll_C N(\log N)^{-1-|C|/2}$ primes $p \le N$, $p \equiv 1 \pmod 4$, defeating every $c \in C$ on Type II. Thus the least shift $k(p)$ satisfies $\#\{p \le N : k(p) > K\} \ll_K N(\log N)^{-1-m/2}$ ($m = \lfloor (K+1)/4 \rfloor$), giving $\ll N(\log N)^{-2}$ at $K = 7$. Under Elliott–Halberstam, linear-sieve switching yields $\#\{p \le N : k(p) > 7\} \gg N(\log N)^{-2}$. Exact Python checks verify 81,307 Type II failures below 2^{20} (0 violations) and $E_C(N)$ through 2^{24}. Unconditional lower bounds for $k(p) > 7$ and sharpness for $|C| \ge 2$ remain unsettled. No Lean 4 formalization is claimed; the proof is unrefereed.

Verification Scope (G11): WARN: Human referee: pending — **Full Trust Boundary:** Section 5.
Main results: 0 of 5 in Lean Kernel (0%) · 1 Cert Only · 4 written · 1 open (not counted)
Abstract claims: 0 of 5 in Lean Kernel (0%) · 1 Cert Only · 4 written · 1 open (not counted)

MSC 2020: 11D68, 11N36, 11N13 **Keywords:** Erdős–Straus conjecture, unit fractions, Type II branch, arithmetic large sieve, linear sieve, Elliott–Halberstam conjecture

1. INTRODUCTION AND MAIN RESULTS

The Erdős–Straus conjecture asks whether every integer $n \ge 2$ admits a representation $4/n = 1/x + 1/y + 1/z$ in positive integers x, y, z. Because composite denominators reduce to their prime divisors, the problem concentrates on primes p, and specifically on primes $p \equiv 1 \pmod 4$: every prime $p \equiv 3 \pmod 4$ is settled immediately by $x = (p+1)/4$ and $4/p - 1/x = 1/(px) = 1/(2px) + 1/(2px)$. For $p \equiv 1 \pmod 4$, any three-unit-fraction decomposition with smallest denominator x satisfies $p/4 < x \le 3p/4$, so the integer *shift* $c = 4x - p$ is positive and satisfies $c \equiv 3 \pmod 4$. Writing $x_c = (p+c)/4$, the solutions at shift c split cleanly into two divisor branches [4, 2]: the *Type II* (untwisted) branch succeeds precisely when x_c admits coprime divisors d_1, d_2 with $d_1 d_2 \mid x_c$ and $c \mid d_1 + d_2$, whereas the *Type I* (twisted) branch replaces $c \mid d_1 + d_2$ by $c \mid pd_1 + d_2$. Let $k(p)$ denote the least shift $c \ge 1$ that works on either branch.

A natural analytic question is how rapidly the exceptional prime count shrinks when a prime $p \equiv 1 \pmod 4$ defeats several fixed shifts at once. For a single shift, two-sided counts of order $N(\log N)^{-3/2}$ are known: Iwaniec's half-dimensional sieve theorem on shifted quadratic forms [7] (and independently Fuchs, Hsu, Rickards, Schindler, and Stange [6]) yields $\#\{p \le N : k(p) > 3\} \asymp N(\log N)^{-3/2}$, while Dahan [2] establishes the same order for shift 7 alone and proves an upper bound of shape $N(\log N)^{-1-|P|/2}$ for fixed sets P of witness pairs whose shift varies with p. Here we transpose that fixed-depth picture to arbitrary finite sets of *fixed* shifts, working purely through the Type II branch and Montgomery's arithmetic large sieve [9, 10] `[to check]` without requiring a prime level of distribution.

The structural mechanism is a two-line modular restriction on prime divisors of x_c.

Lemma 1 (Involution Lemma). *Let p be a prime with $p \equiv 1 \pmod 4$, let c be a positive integer with $c \equiv 3 \pmod 4$ and $p > c$, and put $x_c = (p+c)/4$. Then $\gcd(x_c, c) = 1$. Let $T_c(p) \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ be the set of residue classes modulo c attained by the prime factors of x_c. If shift c fails on the Type II branch at p, then $T_c(p)$ contains no additive inverse pair $\{a, -a\}$ modulo c. Consequently, $T_c(p) \subseteq S_c$ for at least one* half system *$S_c \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ containing exactly one element from each of the $\varphi(c)/2$ pairs $\{a, -a\}$.*

Because each failing shift confines the prime factors of x_c to half of the units modulo c, every prime modulus $\ell > \max C$ whose residue modulo c falls outside S_c forbids the congruence $p \equiv -c \pmod{\ell}$, saving half a power of $\log N$ per shift in the large sieve.

Theorem 2 (Fixed-Shift Type II Sieve Upper Bound). *Let C be a finite nonempty set of positive integers satisfying $c \equiv 3 \pmod 4$, and let*

$$E_C(N) := \#\{p \le N \text{ prime} : p \equiv 1 \pmod 4, \text{ every } c \in C \text{ fails Type II at } p\}.$$

Then, for all $N \ge 3$,

$$E_C(N) \ll_C N(\log N)^{-1-|C|/2}.$$

Since defeating both branches at every shift $c \le K$ implies defeating the Type II branch at every admissible shift $c \equiv 3 \pmod 4$ up to K, Theorem 2 yields an immediate tail bound for the least working shift $k(p)$.

Corollary 3 (Least-Shift Tail Upper Bound). *For every integer $K \ge 3$, let $m = \lfloor (K+1)/4 \rfloor$ be the number of integers $c \equiv 3 \pmod 4$ with $3 \le c \le K$. Then*

$$\#\{p \le N \text{ prime} : k(p) > K\} \ll_K N(\log N)^{-1-m/2}.$$

In particular, $\#\{p \le N \text{ prime} : k(p) > 7\} \ll N(\log N)^{-2}$ ($m = 2$), $\#\{p \le N \text{ prime} : k(p) > 11\} \ll N(\log N)^{-5/2}$ ($m = 3$), $\#\{p \le N \text{ prime} : k(p) > 19\} \ll N(\log N)^{-7/2}$ ($m = 5$), and $\#\{p \le N \text{ prime} : k(p) > 23\} \ll N(\log N)^{-4}$ ($m = 6$).

At $K = 7$, the joint failure set $\{p : k(p) > 7\}$ corresponds to a linear sieve (dimension 1) on the primes. Unconditionally, the Bombieri–Vinogradov level $1/2$ stops at sifting parameter $z \approx N^{1/4}$, leaving a parity barrier. Assuming the Elliott–Halberstam conjecture, however, one can sift to $z = N^{1/2-\delta}$ and eliminate survivors with two large bad prime factors via Selberg's upper-bound sieve of dimension $5/2$.

Proposition 4 (Conditional Lower Bound at $K = 7$). *Assume the Elliott–Halberstam conjecture: for every $\varepsilon > 0$ and $A > 0$,*

$$\sum_{q \le N^{1-\varepsilon}} \max_{(a,q)=1} \left| \pi(N;q,a) - \frac{\pi(N)}{\varphi(q)} \right| \ll_{\varepsilon,A} N(\log N)^{-A}.$$

Then $\#\{p \le N \text{ prime} : k(p) > 7\} \gg N(\log N)^{-2}$. Combined with Corollary 3, $\#\{p \le N \text{ prime} : k(p) > 7\} \asymp N(\log N)^{-2}$ under the Elliott–Halberstam conjecture.

While the proofs of Lemma 1, Theorem 2, Corollary 3, and Proposition 4 are purely analytic and use no computation, exact arithmetic confirms the involution restriction, its non-invertibility (negative control), the parity mechanism of Proposition 4, and the empirical scaling of $E_C(N)$ through $N = 2^{24}$.

Proposition 5 (Computational Verification and Empirical Scaling — Cert Only). *The standalone exact-arithmetic verifier `recompute.py` confirms all four statements below with zero discrepancies:*

1. *Across all 40,949 primes $p \equiv 1 \pmod 4$ with $23 < p < 2^{20}$ and shifts $c \in \{3,7,11,15,19,23\}$ (245,694 pairs), there are 81,307 Type II failures and 0 violations of Lemma 1, while the converse of Lemma 1 fails 95,454 times.*
2. *Across all 538,763 primes $p \equiv 1 \pmod 4$ below 2^{24}, every one of the 11,270 primes with $k(p) > 7$ fails on the Type II branch at $c = 3$ and $c = 7$ (0 exceptions; replacing shift 7 with shift 11 yields 7,074 exceptions).*
3. *The exact counts $E_C(N)$ for $C = \{3\}$, $\{3,7\}$, and $\{3,7,11\}$ across $N \in \{2^{16}, 2^{18}, 2^{20}, 2^{22}, 2^{24}\}$ match Table 1; at $N = 2^{24}$, $E_{\{3,7\}}(2^{24}) = \#\{p < 2^{24} : k(p) > 7\} = 11{,}270$, whereas $E_{\{3,7,11\}}(2^{24}) = 4{,}196$ exceeds $\#\{p < 2^{24} : k(p) > 11\} = 4{,}123$ by 73 primes where only Type I works at shift 11.*
4. *Among all primes $p \equiv 1 \pmod{24}$ below 2^{22}, all 18,350 primes with $(p/7) = +1$ have even bad-factor counts in both $(p+3)/4$ and $(p+7)/4$ (0 exceptions and 0 mismatches with $k(p) > 7$), whereas all 18,530 primes with $(p/7) = -1$ have odd bad-factor count in $(p+7)/4$ (0 even counts).*

Conjecture 6 (Unconditional Lower Bound and Exponent Sharpness — Unsettled). *For every finite nonempty set C of positive integers $c \equiv 3 \pmod 4$, does $E_C(N) \asymp_C N(\log N)^{-1-|C|/2}$ hold unconditionally, and in particular does $\#\{p \le N \text{ prime} : k(p) > 7\} \gg N(\log N)^{-2}$ hold without assuming the Elliott–Halberstam conjecture?*

Figure 1 maps the logical dependencies and verification tiers across all six claims. To illustrate Lemma 1 in action on concrete primes (verified verbatim by `recompute.py`), the snippet below extracts the prime-factor residue set $T_c(p) \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ and tests for an additive inverse pair $\{a, -a\}$:

Concept in Action: Involution Test for $T_c(p)$

```
def involution_test(p, c):
    x, res, d = (p + c) // 4, set(), 2
    n = x
    while d * d <= n:
        while n % d == 0:
            res.add(d % c); n //= d
        d += 1
    if n > 1: res.add(n % c)
    hit = any((c - a) in res for a in res if a)
    return x, sorted(res), hit
# (1129, 11)->(285,[3,5,8],True)  # 3+8=11: Type II works
# (1129,  7)->(284,[1,2],False)   # fails (k(1129)=11)
# (  17,  7)->(  6,[2,3],False)   # converse fails: 1+2*3=7
```

Roadmap. Section 2 fixes notation, recalls the two-branch divisor criterion and exact characterizations at shifts 3 and 7, and works through concrete examples. Section 3 proves Lemma 1, Theorem 2, Corollary 3, and Proposition 4, and explains why the lower-bound sieve halts unconditionally at $K = 7$ and conditionally at $K \ge 11$. Section 4 presents the exact computational verification and scaling data for Proposition 5. Section 5 displays the machine-generated Reader's Trust Boundary. Section 6 surveys prior work and open questions, and Section 7 records reproducibility and AI disclosure.

2. DEFINITIONS, NOTATION, AND FIXED-SHIFT SETUP

Throughout this paper, p and ℓ denote rational primes, φ is Euler's totient function, μ is the Möbius function, and $\pi(N;q,a)$ counts primes $p \le N$ satisfying $p \equiv a \pmod q$. Vinogradov notation $f \ll_C g$ means $|f| \le Mg$ for a constant $M > 0$ depending only on C, and $f \asymp g$ means $f \ll g \ll f$.

Suppose an odd prime p satisfies $4/p = 1/x + 1/y + 1/z$ in positive integers $x \le y \le z$. Because $1/x < 4/p \le 3/x$, the

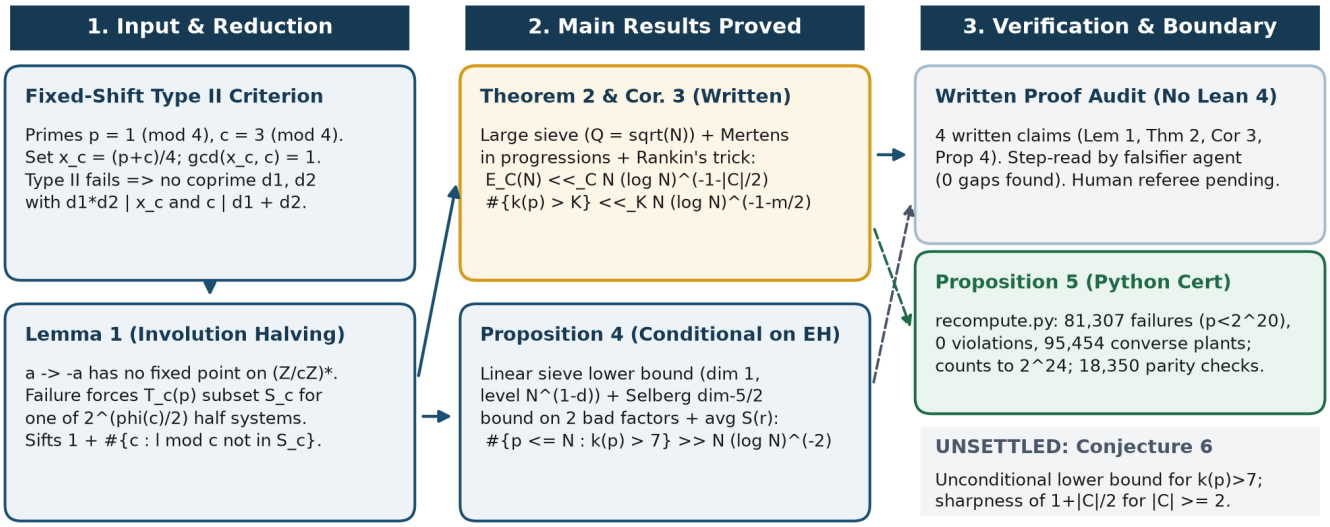


Figure 1. Discovery and proof architecture for this manuscript. Column 1 summarizes the fixed-shift Type II reduction and Lemma 1; Column 2 lists the four written-proof results (Lemma 1, Theorem 2, Corollary 3, and the conditional Proposition 4); Column 3 separates written-proof review status (no Lean 4 formalization; human referee pending), exact computational verification (`recompute.py`, Proposition 5), and the unsettled boundary (Conjecture 6).

smallest denominator satisfies $p/4 < x \le 3p/4$. Setting the *shift* $c := 4x - p$, we have $0 < c \le 2p$, $c \equiv -p \pmod 4$, and

$$x = x_c := \frac{p+c}{4}, \qquad N_c := px_c, \qquad \frac{4}{p} - \frac{1}{x_c} = \frac{c}{N_c}.$$

For $p = 2$, $4/2 = 1/1 + 1/2 + 1/2$ gives $x = 1$ and $c = 2$. For every prime $p \equiv 3 \pmod 4$, shift $c = 1$ yields $x_1 = (p+1)/4$ and $4/p = 1/x_1 + 1/(2px_1) + 1/(2px_1)$. For $p \equiv 1 \pmod 4$, the admissible shifts are positive integers $c \equiv 3 \pmod 4$.

Remark 7 (Two-branch fixed-shift criterion [4, 2]). Let $p \ge 5$ be prime and c a positive integer with $c \equiv -p \pmod 4$ and $c \le 2p$. Because c is odd and $c \equiv -p \not\equiv p \pmod 4$, we have $p \nmid c$, $\gcd(c, N_c) = 1$, and $p \nmid x_c$ (since $x_c \le 3p/4 < p$). By the classical two-unit-fraction divisor rule, $c/N_c = 1/y + 1/z$ has a solution in positive integers y, z if and only if there exist coprime positive integers u, v with $uv \mid N_c$ and $c \mid u + v$, giving $y = (N_c/u)(u+v)/c$ and $z = (N_c/v)(u+v)/c$. Since p divides $N_c = px_c$ to the exact first power, at most one of u, v is divisible by p, partitioning solutions into two branches:

- **Type II (untwisted) branch:** $p \nmid uv$, so there exist coprime positive integers d_1, d_2 with $d_1 d_2 \mid x_c$ and $c \mid d_1 + d_2$. Both y and z are divisible by p while $p \nmid x_c$. Equivalently, since $\gcd(c, x_c) = 1$, there exist integers e_q with $|e_q| \le v_q(x_c)$ (the q-adic valuation of x_c) such that $\prod_{q \mid x_c} q^{e_q} \equiv -1 \pmod c$.
- **Type I (twisted) branch:** $p \mid uv$; writing $\{u, v\} = \{pd_1, d_2\}$, there exist coprime positive integers d_1, d_2 with $d_1 d_2 \mid x_c$ and $c \mid pd_1 + d_2$. Here p divides exactly one of (x_c, y, z).

We define $k(p)$ to be the least shift $c \ge 1$ for which $4/p = 1/x_c + 1/y + 1/z$ succeeds on at least one branch; equivalently, $k(p) = 4x_{\min}(p) - p$, where $x_{\min}(p)$ is the least denominator occurring in any three-unit-fraction decomposition of $4/p$ (catalogued in OEIS A400619 and A400620 [1]).

Remark 8 (Exact characterization at shifts 3 and 7 [2, 3]). At shift $c = 3$, the only units modulo 3 are 1 and $2 \equiv -1$. For a prime $p \equiv 1 \pmod 4$, $k(p) > 3$ holds if and only if $p \equiv 1 \pmod{24}$ and every prime factor of $m_3 = (p+3)/4$ satisfies $q \equiv 1 \pmod 3$: indeed, if $p \equiv 5 \pmod 8$ then $2 \mid m_3$, and if $p \equiv 2 \pmod 3$ then $m_3 \equiv 2 \pmod 3$ has a prime factor $q \equiv 2 \pmod 3$, giving the Type II pair $(d_1, d_2) = (1, q)$ in both cases (and Type I pair $(1, 1)$ when $p \equiv 2 \pmod 3$). Thus at shift 3 the Type I and Type II branches succeed or fail together.

At shift $c = 7$, Dahan [3, Theorem `sylow_and_c7_iff`(b)] shows that for prime $p \equiv 1 \pmod{24}$, shift 7 fails on the Type II branch—and equivalently on both branches—precisely when every prime factor of $m_7 = (p+7)/4$ is a quadratic residue modulo 7 ($q \equiv 1, 2, 4 \pmod 7$). The necessity is immediate: $p \equiv 1 \pmod 8$ implies $2 \mid m_7$, so any prime factor $q \mid m_7$ with $q \equiv 6, 3, 5 \pmod 7$ yields the working Type II pair $(1, q)$, $(1, 2q)$, or $(2, q)$ respectively. Conversely, if every prime factor of m_7 is a quadratic residue modulo 7, then $p \equiv 4m_7 \pmod 7$ is also a quadratic residue, so every divisor of $N_7 = pm_7$ lies in $\{1, 2, 4\} \pmod 7$ and no two sum to $0 \pmod 7$. Hence $k(p) > 7$ holds if and only if $p \equiv 1, 25, 121 \pmod{168}$, every prime factor of m_3 is $\equiv 1 \pmod 3$, and every prime factor of m_7 is $\equiv 1, 2, 4 \pmod 7$. In particular, for every N, $E_{\{3,7\}}(N) = \#\{p \le N : k(p) > 7\}$.

Worked examples. Three small primes illustrate the two branches (checked in `recompute.out`):

- $p = 3{,}361$: $x_3 = (3{,}361 + 3)/4 = 841 = 29^2$, with $29 \equiv 2 \pmod 3$. Taking $(d_1, d_2) = (1, 29)$ gives $3 \mid 1 + 29$ and $4/3{,}361 = 1/841 + 1/974{,}690 + 1/28{,}266{,}010$, so $k(3{,}361) =$

3.

- $p = 73$: $x_3 = 19 \equiv 1 \pmod 3$ fails shift 3, whereas $x_7 = (73+7)/4 = 20 = 2^2 \cdot 5$ has inverse pair $\{2,5\} \bmod 7$; $(d_1, d_2) = (2,5)$ yields $4/73 = 1/20 + 1/292 + 1/730$, so $k(73) = 7$.
- $p = 1{,}129$: $x_3 = 283 \equiv 1 \pmod 3$ (prime) and $x_7 = 284 = 2^2 \cdot 71$ ($2, 71 \in \{1,2,4\} \bmod 7$), so $k(1{,}129) > 7$; at shift 11, $x_{11} = 285 = 3 \cdot 5 \cdot 19$ contains the inverse pair $\{3,8\} \bmod 11$ ($19 \equiv 8 \pmod{11}$), giving $4/1{,}129 = 1/285 + 1/33{,}870 + 1/214{,}510$ and $k(1{,}129) = 11$.

3. PROOFS OF THE MAIN RESULTS

Proof of Lemma 1 (Involution Lemma).

Proof of Lemma 1. Assume p is prime with $p \equiv 1 \pmod 4$, $c \equiv 3 \pmod 4$ is a positive integer with $p > c$, and $x_c = (p+c)/4$. First, $\gcd(x_c, c) = 1$: any prime r dividing both x_c and c divides $4x_c - c = p$, forcing $r = p$, which contradicts $r \le c < p$. Hence every prime divisor $q \mid x_c$ lies in a unit class $q \bmod c \in (\mathbb{Z}/c\mathbb{Z})^\times$, so $T_c(p) \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ is well defined.

Next, consider the negation map $\iota(a) = -a \bmod c$ on $(\mathbb{Z}/c\mathbb{Z})^\times$. Since c is odd, 2 is a unit modulo c, so $a \equiv -a \pmod c$ implies $2a \equiv 0 \pmod c$ and hence $a \equiv 0 \pmod c$, impossible for $a \in (\mathbb{Z}/c\mathbb{Z})^\times$. Thus ι is a fixed-point-free involution, partitioning $(\mathbb{Z}/c\mathbb{Z})^\times$ into $\varphi(c)/2$ unordered pairs $\{a, -a\}$.

Suppose for contradiction that $T_c(p)$ contains both a and $-a$ for some $a \in (\mathbb{Z}/c\mathbb{Z})^\times$. Then there exist prime divisors $q_1, q_2 \mid x_c$ with $q_1 \equiv a \pmod c$ and $q_2 \equiv -a \pmod c$. Because $a \not\equiv -a \pmod c$, the primes q_1 and q_2 are distinct, so $\gcd(q_1, q_2) = 1$, $q_1 q_2 \mid x_c$, and $q_1 + q_2 \equiv a + (-a) \equiv 0 \pmod c$. The pair $(d_1, d_2) = (q_1, q_2)$ therefore witnesses the Type II branch at shift c, contradicting the assumption that shift c fails on the Type II branch at p.

Thus $T_c(p)$ contains at most one element from each of the $\varphi(c)/2$ pairs $\{a, -a\}$. Choosing one representative from every pair not yet hit by $T_c(p)$ produces a half system $S_c \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ with $|S_c| = \varphi(c)/2$ and $T_c(p) \subseteq S_c$. There are $2^{\varphi(c)/2}$ half systems modulo c in total. □

Notice why the converse of Lemma 1 fails: $T_c(p)$ records only residues of *single* prime factors, whereas a Type II witness (d_1, d_2) may use composite divisors. For instance, at $p = 17 > 7$ we have $x_7 = (17+7)/4 = 6 = 2 \cdot 3$, so $T_7(17) = \{2,3\}$ contains no additive inverse pair modulo 7, yet $(d_1, d_2) = (1,6)$ satisfies $7 \mid 1 + 6$ and yields $4/17 = 1/6 + 1/17 + 1/102$. Figure 2 displays the inverse-pair partition for $c \in \{3, 7, 11\}$ alongside the empirical partition of 245,694 pairs (p, c) below 2^{20}.

Proof of Theorem 2 (Fixed-Shift Large-Sieve Bound).

Proof of Theorem 2. Fix a finite nonempty set C of positive integers $c \equiv 3 \pmod 4$. Write $c^* := \max C$ and $\kappa := 1 + |C|/2$. Since $E_C(N) \le N$ trivially, it suffices to prove the bound for all $N \ge N_0(C)$ sufficiently large in terms of C. Put $Q := \sqrt{N}$, and assume $N_0(C)$ is large enough that $Q > c^*$.

Step 1 (Decomposition by half-system tuples). Primes $p \le Q$ contribute at most $\sqrt{N} = o_C(N(\log N)^{-\kappa})$ to $E_C(N)$. Every remaining prime $p \in (Q, N]$ counted in $E_C(N)$ satisfies $p > c^*$ and fails on the Type II branch for every $c \in C$. By Lemma 1, there exists a tuple $\mathbf{S} = (S_c)_{c \in C}$ of half systems $S_c \subseteq (\mathbb{Z}/c\mathbb{Z})^\times$ such that $T_c(p) \subseteq S_c$ for all $c \in C$. Setting

$$A(\mathbf{S}) := \{p \in (Q, N] \text{ prime} : p \equiv 1 \pmod 4, \; T_c(p) \subseteq S_c \text{ for all } c \in C\},$$

we have

$$E_C(N) \le Q + \sum_{\mathbf{S}} |A(\mathbf{S})|, \tag{1}$$

where the sum runs over the $M(C) := \prod_{c \in C} 2^{\varphi(c)/2}$ tuples of half systems, a finite number depending only on C.

Step 2 (Residue classes avoided modulo primes $\ell \le Q$). Fix a tuple $\mathbf{S} = (S_c)_{c \in C}$. For every prime ℓ with $c^* < \ell \le Q$, note that $\gcd(\ell, c) = 1$ for every $c \in C$, so $\ell \bmod c \in (\mathbb{Z}/c\mathbb{Z})^\times$. Define the forbidden set of residue classes modulo ℓ:

$$\Omega_{\mathbf{S}}(\ell) := \{0 \bmod \ell\} \cup \{-c \bmod \ell : c \in C, \; \ell \bmod c \notin S_c\}.$$

We verify that no element $p \in A(\mathbf{S})$ lies in any class of $\Omega_{\mathbf{S}}(\ell)$:

- Because p is prime and $p > Q \ge \ell$, we have $p \not\equiv 0 \pmod \ell$.
- If $c \in C$ satisfies $\ell \bmod c \notin S_c$, then $\ell \bmod c \notin T_c(p)$, so $\ell \nmid x_c = (p+c)/4$. Since $\ell > c^* \ge 3$ is odd, $\gcd(\ell, 4) = 1$, whence $\ell \nmid p + c$, i.e., $p \not\equiv -c \pmod \ell$.

Moreover, the classes listed in $\Omega_{\mathbf{S}}(\ell)$ are pairwise distinct: for every $c \in C$, $0 < c \le c^* < \ell$ implies $-c \not\equiv 0 \pmod \ell$, and for distinct $c_1, c_2 \in C$, $0 < |c_1 - c_2| < c^* < \ell$ implies $-c_1 \not\equiv -c_2 \pmod \ell$. Therefore $A(\mathbf{S})$ avoids exactly

$$\omega_{\mathbf{S}}(\ell) := |\Omega_{\mathbf{S}}(\ell)| = 1 + \#\{c \in C : \ell \bmod c \notin S_c\} \le 1 + |C|$$

residue classes modulo ℓ. Because the elements of C are distinct positive integers congruent to $3 \pmod 4$, we have $c^* \ge 4|C| - 1 \ge |C| + 2$ (as $|C| \ge 1$), so every prime $\ell > c^*$ satisfies $\omega_{\mathbf{S}}(\ell) \le 1 + |C| < \ell$. Set $\omega_{\mathbf{S}}(\ell) := 0$ for primes $\ell \le c^*$.

Step 3 (Montgomery's arithmetic large sieve). By Montgomery's arithmetic large sieve [9] with the Montgomery–Vaughan constant $N - 1 + Q^2$ [10] `[to check]` applied to $A(\mathbf{S}) \subseteq [1, N]$,

$$|A(\mathbf{S})| \le \frac{N - 1 + Q^2}{L(Q)} < \frac{2N}{L(Q)}, \tag{2}$$

where

$$L(Q) := \sum_{m \le Q} \mu^2(m) h(m),$$

$$h(m) := \prod_{\ell \mid m} h(\ell), \qquad h(\ell) := \frac{\omega_{\mathbf{S}}(\ell)}{\ell - \omega_{\mathbf{S}}(\ell)}.$$

(Note that $A(\mathbf{S})$ may avoid additional classes modulo ℓ, which only strengthens (2).)

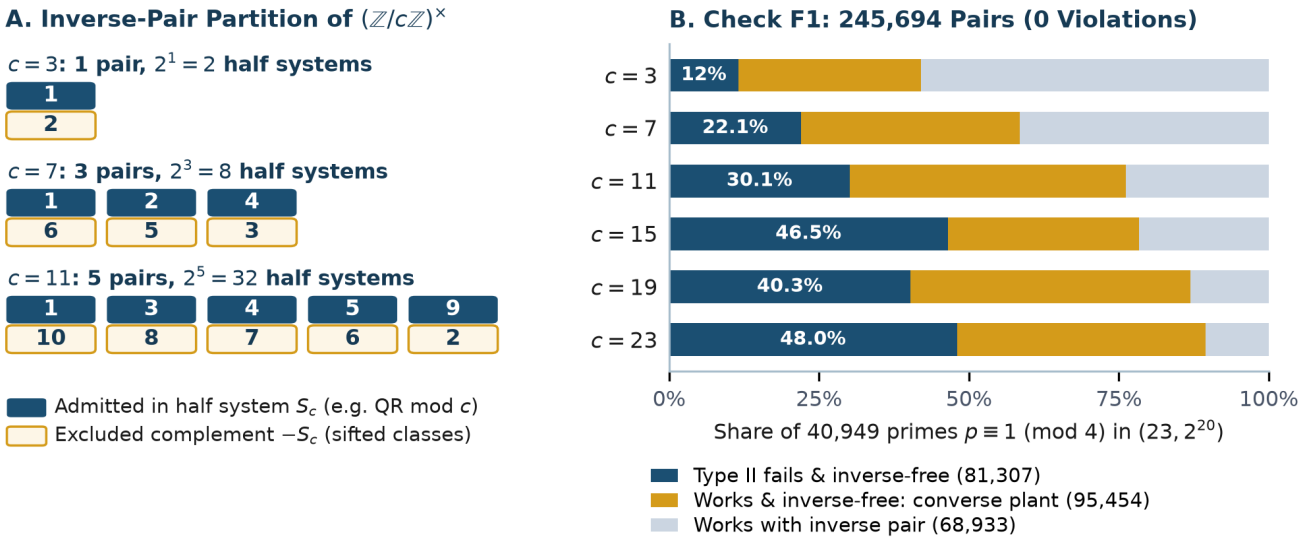


Figure 2. Panel A: Fixed-point-free involution $a \mapsto -a$ on $(\mathbb{Z}/c\mathbb{Z})^\times$ for $c = 3, 7, 11$, partitioning the $\varphi(c)$ units into $1, 3, 5$ pairs and yielding $2^{\varphi(c)/2} = 2, 8, 32$ half systems (quadratic residues shaded navy, excluded complements gold). Panel B: Empirical partition from Check F1 (`recompute.py`) across all 40,949 primes $p \equiv 1 \pmod 4$ in $(23, 2^{20})$ and $c \in \{3, 7, 11, 15, 19, 23\}$ (245,694 pairs): 81,307 Type II failures with 0 violations of Lemma 1, 95,454 converse counterexamples (works yet inverse-free), and 68,933 pairs working via a direct inverse pair.

Step 4 (Lower bound $L(Q) \gg_C (\log Q)^\kappa$ via Mertens and Rankin's trick). For each $c \in C$, the complement $(\mathbb{Z}/c\mathbb{Z})^\times \setminus S_c$ has exact cardinality $\varphi(c)/2$. By Mertens' theorem in arithmetic progressions (a consequence of $L(1,\chi) \neq 0$ for Dirichlet characters modulo c), for every a coprime to c and $z \geq 2$,

$$\sum_{\substack{\ell \leq z \\ \ell \equiv a \pmod c}} \frac{\log \ell}{\ell} = \frac{\log z}{\varphi(c)} + O_c(1),$$

$$\sum_{\substack{\ell \leq z \\ \ell \equiv a \pmod c}} \frac{1}{\ell} = \frac{\log\log z}{\varphi(c)} + O_c(1).$$

Summing over the $\varphi(c)/2$ classes $a \notin S_c$ and over $c \in C$, and adding the prime sums $\sum_{c^* < \ell \leq z} (\log \ell)/\ell = \log z + O_C(1)$ and $\sum_{c^* < \ell \leq z} 1/\ell = \log\log z + O_C(1)$ for $0 \bmod \ell$, gives

$$\sum_{c^* < \ell \leq z} \frac{\omega_{\mathbf{S}}(\ell) \log \ell}{\ell} = \kappa \log z + O_C(1), \tag{3}$$

$$\sum_{c^* < \ell \leq z} \frac{\omega_{\mathbf{S}}(\ell)}{\ell} = \kappa \log\log z + O_C(1), \tag{4}$$

where $\kappa = 1 + |C|/2$ and the implied constants are uniform over the finitely many tuples $\mathbf{S}$. Since $0 \leq \omega_{\mathbf{S}}(\ell) \leq 1 + |C|$ and $\ell \geq c^* + 1 \geq |C| + 3$, we have

$$0 \leq h(\ell) - \frac{\omega_{\mathbf{S}}(\ell)}{\ell} = \frac{\omega_{\mathbf{S}}(\ell)^2}{\ell(\ell - \omega_{\mathbf{S}}(\ell))} \ll_C \frac{1}{\ell^2},$$

so (3) implies

$$\sum_{c^* < \ell \leq z} h(\ell) \log \ell \leq \kappa \log z + B \tag{5}$$

for a constant $B = B(C) \geq 1$ depending only on C.

Put $s := e\kappa + 2$ and choose $z := Q^{1/s}$. Increase $N_0(C)$ if necessary so that $z > c^*$ and $\log z \geq eB$ for all $N \geq N_0(C)$. Let $P := \prod_{c^* < \ell \leq z} \ell$ and $\sigma := 1/\log z$. Every divisor $m \mid P$ is squarefree, and every $m \mid P$ with $m > Q$ satisfies $(m/Q)^\sigma > 1$; hence Rankin's trick gives

$$\begin{aligned} L(Q) &\geq \sum_{\substack{m \mid P \\ m \leq Q}} h(m) \geq \sum_{m \mid P} h(m) - Q^{-\sigma} \sum_{m \mid P} h(m) m^\sigma \\ &= \prod_{c^* < \ell \leq z} (1 + h(\ell)) - Q^{-\sigma} \prod_{c^* < \ell \leq z} (1 + h(\ell)\ell^\sigma). \end{aligned} \tag{6}$$

For every prime $\ell \in (c^*, z]$, put $t := (\log \ell)/(\log z) \in (0, 1]$. By convexity of $t \mapsto e^t$ on $[0, 1]$, we have $\ell^\sigma = e^t \leq 1 + (e-1)t \leq 1 + et$, so

$$\begin{aligned} 1 + h(\ell)\ell^\sigma &\leq 1 + h(\ell) + eh(\ell)t \\ &\leq (1 + h(\ell))(1 + eh(\ell)t) \leq (1 + h(\ell)) \exp(eh(\ell)t). \end{aligned}$$

Multiplying over all primes $\ell \in (c^*, z]$ and applying (5) together with $\log z \geq eB$ yields

$$\begin{aligned} \prod_{c^* < \ell \leq z} (1 + h(\ell)\ell^\sigma) &\leq \exp\left(\frac{e}{\log z} \sum_{c^* < \ell \leq z} h(\ell) \log \ell \right) \\ &\quad \times \prod_{c^* < \ell \leq z} (1 + h(\ell)) \\ &\leq e^{e\kappa + 1} \prod_{c^* < \ell \leq z} (1 + h(\ell)). \end{aligned}$$

Because $Q^{-\sigma} = \exp(-\log Q/\log z) = e^{-s} = e^{-(e\kappa+2)}$, we have $Q^{-\sigma} e^{e\kappa+1} = e^{-1}$, and substituting into (6) yields

$$L(Q) \geq (1 - e^{-1}) \prod_{c^* < \ell \leq z} (1 + h(\ell)).$$

Finally, $h(\ell) \geq \omega_{\mathbf{S}}(\ell)/\ell \geq 0$ and the elementary inequality

$\log(1+u) \geq u - u^2/2$ (valid for all $u \geq 0$) give, via (4),

$$L(Q) \geq (1-e^{-1}) \exp\left(\sum_{c^* < \ell \leq z} \frac{\omega_{\mathbf{S}}(\ell)}{\ell} - \frac{1}{2} \sum_{c^* < \ell \leq z} \frac{\omega_{\mathbf{S}}(\ell)^2}{\ell^2} \right)$$
$$\gg_C (\log z)^\kappa = s^{-\kappa} (\log Q)^\kappa \gg_C (\log N)^\kappa.$$

Step 5 (Conclusion). Combining Step 4 with (2) gives $|A(\mathbf{S})| \ll_C N(\log N)^{-\kappa}$ uniformly for every half-system tuple $\mathbf{S}$. Summing over all $M(C) = \prod_{c \in C} 2^{\varphi(c)/2}$ tuples in (1) completes the proof:

$$E_C(N) \ll_C \sqrt{N} + M(C)\, N(\log N)^{-\kappa} \ll_C N(\log N)^{-1-|C|/2}.$$

□

Proof of Corollary 3 (Least-Shift Tail Bound).

Proof of Corollary 3. Let $K \geq 3$ and $C_K := \{c \in \mathbb{Z} : 3 \leq c \leq K,\ c \equiv 3 \pmod 4\}$, so $|C_K| = \lfloor (K+1)/4 \rfloor = m$. If a prime p satisfies $k(p) > K \geq 3$, then $p \neq 2$ (as $k(2) = 2$) and $p \not\equiv 3 \pmod 4$ (as $k(p) = 1$ for $p \equiv 3 \pmod 4$), forcing $p \equiv 1 \pmod 4$. Furthermore, every shift $c \in C_K$ fails on both branches at p, and in particular fails on the Type II branch. Hence

$$\#\{p \leq N \text{ prime} : k(p) > K\} \leq E_{C_K}(N) \ll_K N(\log N)^{-1-m/2}$$

by Theorem 2. Evaluating $m = \lfloor (K+1)/4 \rfloor$ at $K = 7, 11, 19, 23$ gives $m = 2, 3, 5, 6$ and exponents $-2, -5/2, -7/2, -4$. □

Proof of Proposition 4 and Lower-Bound Barriers.

Proof of Proposition 4. Let $m_3 := (p+3)/4$ and $m_7 := (p+7)/4$. Call a prime ℓ *bad for* m_3 if $\ell \equiv 2 \pmod 3$, and *bad for* m_7 if ℓ is a quadratic non-residue modulo 7 ($\ell \equiv 3, 5, 6 \pmod 7$). By Remark 8, a prime $p > 7$ satisfies $k(p) > 7$ if and only if $p \equiv 1, 25, 121 \pmod{168}$ and neither m_3 nor m_7 has any bad prime factor.

Step 1 (Parity of bad-factor counts). Let $\mathcal{A} := \{p \leq N \text{ prime} : p \equiv 1, 25, 121 \pmod{168}\}$. For every $p \in \mathcal{A}$, we have $m_3 \equiv 1 \pmod 6$ (so $3 \nmid m_3$ and $m_3 \equiv 1 \pmod 3$) and $4m_7 = p + 7 \equiv p \pmod 7$, hence $m_7 \equiv 2p \pmod 7$ is a quadratic residue modulo 7 (since 2 and p are quadratic residues modulo 7; note $2 \mid m_7$ and 2 is not bad for m_7, while $3 \nmid m_7$ since $p + 7 \equiv 2 \pmod 3$). Because the bad primes for m_3 and m_7 are precisely the primes at which the respective quadratic characters take value -1, multiplicativity implies that both m_3 and m_7 have an *even* number of bad prime factors, counted with multiplicity.

Step 2 (Linear-sieve lower bound). Fix $\delta \in (0, 1/10)$ and put $z := N^{1/2-\delta}$. Sift $\mathcal{A}$ by removing, for each prime $\ell < z$ outside $\{2, 3, 7\}$, the congruence $p \equiv -3 \pmod \ell$ whenever ℓ is bad for m_3 and $p \equiv -7 \pmod \ell$ whenever ℓ is bad for m_7. At $\ell = 5$, the two removed classes 2 and 3 mod 5 are distinct and coprime to 5, leaving 2 of 4 coprime classes unsifted; for every prime $\ell > 7$, the classes -3 and -7 mod ℓ are distinct and coprime to ℓ (as $7 - 3 = 4 < \ell$). Let $\rho(\ell) \in \{0, 1, 2\}$ count the removed classes modulo ℓ (with $\rho(2) = \rho(3) = 0$ and $\rho(7) = 0$) and set $g(\ell) := \rho(\ell)/(\ell - 1) < 1$. Because half of all primes are bad for m_3 and half are bad for m_7, Mertens' theorem in progressions gives

$$V(z) := \prod_{\ell < z} (1 - g(\ell)) \asymp (\log z)^{-1} \asymp (\log N)^{-1},$$

and the sifting density has dimension $\kappa = 1$ (a linear sieve).

Under the Elliott–Halberstam conjecture, the primes in $\mathcal{A}$ have level of distribution $D = N^{1-\delta}$ (with remainder $O_{A,\delta}(N(\log N)^{-A})$). The sifting parameter is

$$s := \frac{\log D}{\log z} = \frac{1-\delta}{1/2-\delta} = 2 + \frac{2\delta}{1-2\delta} \in (2, 4).$$

By the linear-sieve lower bound of Iwaniec [8] and Friedlander and Iwaniec [5] [to check], the count of survivors $p \in \mathcal{A}$ whose values m_3 and m_7 have no bad prime factor below z is at least

$$|\mathcal{A}|\, V(z)\, (f(s) - o(1)),$$
$$f(s) = \frac{2e^\gamma \log(s-1)}{s} \qquad (2 \leq s \leq 4).$$

Since $|\mathcal{A}| \sim \frac{3}{\varphi(168)} \frac{N}{\log N} = \frac{1}{16} \frac{N}{\log N}$, $V(z) \asymp (\log N)^{-1}$, and $f(s) \asymp \delta$ as $\delta \to 0^+$, there exists an absolute constant $c_1 > 0$ such that at least $c_1 \delta N (\log N)^{-2}$ primes survive for all $N \geq N_0(\delta)$.

Step 3 (Eliminating survivors with two large bad factors). For $\delta < 1/10$ and N sufficiently large, every survivor satisfies $m_3, m_7 < N < N^{3/2-3\delta} = z^3$. Since every bad prime factor of m_3 or m_7 is at least z, each of m_3 and m_7 has fewer than 3 bad prime factors, and by Step 1 that count is even—hence 0 or 2. If both counts are 0, then $k(p) > 7$.

Consider first the survivors for which m_3 has 2 bad prime factors. Write $m_3 = q_1 q_2 r$, where $z \leq q_1 \leq q_2$ are bad primes for m_3 and $r \geq 1$ has all its prime factors $\equiv 1 \pmod 3$. Then $q_1 q_2 \geq z^2 = N^{1-2\delta}$ implies $r \leq (N+3)/(4z^2) \leq N^{2\delta}$, and $q_1 \leq \sqrt{m_3/r} \leq N^{1/2}$. Fix q_1 and r, and set $Y := (N+3)/(4rq_1)$; note $Y \geq N^{1/2-2\delta}/4$, so $\log Y \asymp \log N$. We bound the number of integers $q_2 \leq Y$ satisfying simultaneously:

1. q_2 is prime (sifting dimension 1),
2. $p = 4rq_1q_2 - 3$ is prime (sifting dimension 1), and
3. $m_7 = rq_1q_2 + 1$ has no bad prime factor below $z_0 := N^{1/10}$ (sifting dimension 1/2, since $z_0 \leq z$).

Applying Selberg's upper-bound sieve of dimension $1 + 1 + 1/2 = 5/2$ on the integers $q_2 \leq Y$ [5] [to check] (which requires no prime distribution hypothesis) bounds the count of such q_2 by

$$\ll \mathfrak{S}(rq_1) \frac{Y}{(\log N)^{5/2}}, \qquad \mathfrak{S}(n) := \prod_{\ell \mid n} \left(1 - \frac{1}{\ell}\right)^{-5/2}.$$

Because $q_1 \geq z$, we have $\mathfrak{S}(rq_1) \leq \mathfrak{S}(q_1)\mathfrak{S}(r) \ll \mathfrak{S}(r)$. Summing over $q_1 \in [z, N^{1/2}]$ gives, by Mertens' theorem,

$$\sum_{\substack{z \leq q_1 \leq N^{1/2} \\ q_1 \equiv 2 \pmod 3}} \frac{1}{q_1} \leq \sum_{z \leq q_1 \leq N^{1/2}} \frac{1}{q_1}$$
$$= \log\left(\frac{1/2}{1/2-\delta}\right) + O\left(\frac{1}{\log N}\right) \ll \delta.$$

Summing $\mathfrak{S}(r)/r$ over $r \le N^{2\delta}$ whose prime factors all satisfy $\ell \equiv 1 \pmod 3$ via the Euler product yields

$$\sum_{\substack{r\le N^{2\delta}\\ \ell\mid r\Rightarrow \ell\equiv 1 \pmod 3}} \frac{\mathfrak{S}(r)}{r} \le \prod_{\substack{\ell\le N^{2\delta}\\ \ell\equiv 1 \pmod 3}} \left(1+\frac{(1-1/\ell)^{-5/2}}{\ell-1}\right) \ll \exp\left(\sum_{\substack{\ell\le N^{2\delta}\\ \ell\equiv 1 \pmod 3}} \frac{1}{\ell}\right) \ll (\delta\log N)^{1/2},$$

since $(1-1/\ell)^{-5/2}/(\ell-1) = 1/\ell + O(\ell^{-2})$ and half the primes are $\equiv 1 \pmod 3$. Multiplying these estimates gives

$$\sum_{q_1,r} \mathfrak{S}(rq_1)\frac{N/(4rq_1)}{(\log N)^{5/2}} \ll \delta\cdot(\delta\log N)^{1/2}\frac{N}{(\log N)^{5/2}} = \delta^{3/2}\frac{N}{(\log N)^2}.$$

Exchanging the roles of m_3 and m_7 (writing $m_7 = q_1q_2r$ with bad primes $q_1, q_2 \ge z$ for m_7, $p = 4rq_1q_2 - 7$, and $m_3 = rq_1q_2 - 1$, where $r \le N^{2\delta}$ has only quadratic-residue prime factors modulo 7) yields the identical upper bound $\ll \delta^{3/2}N(\log N)^{-2}$ for survivors with two large bad factors in m_7.

Step 4 (Conclusion). Combining Step 2 with the two upper bounds in Step 3 gives an absolute constant $c_2 > 0$ such that

$$\#\{p \le N \text{ prime} : k(p) > 7\} \ge (c_1\delta - c_2\delta^{3/2})\frac{N}{(\log N)^2}$$

for all $N \ge N_0(\delta)$. Fixing $\delta := \min(1/20, (c_1/(2c_2))^2) > 0$ makes $c_1\delta - c_2\delta^{3/2} > 0$, proving the proposition. □

Why the argument halts unconditionally and for $K \ge 11$. Unconditionally, Bombieri–Vinogradov supplies only level of distribution $D = N^{1/2-\varepsilon}$, forcing $z < N^{1/4}$ because the linear sieve's sifting limit is $\beta = 2$. Each of m_3 and m_7 can then carry 0 or 2 bad prime factors in a region $[N^{1/4}, N^{1/2}]$ of fixed logarithmic width rather than width δ, so Step 3 does not shrink below Step 2 and the parity problem persists. (By contrast, for a single shift $c = 3$ or $c = 7$, the sieve has dimension 1/2 and sifting limit $\beta = 1$, so level 1/2 reaches $z \approx N^{1/2}$, leaving at most one large bad prime factor, which parity rules out immediately [7, 2].) At $K = 11$, the joint sieve already has dimension 3/2, whose sifting limit exceeds 2; hence even at level $D = N^{1-\delta}$ the sifting bound z stays bounded away from $N^{1/2}$ by a fixed exponent gap, and the switching argument applies only to $K = 7$.

4. COMPUTATIONAL VERIFICATION AND EMPIRICAL PICTURE

Although Theorem 2, Corollary 3, and Proposition 4 rest solely on their written proofs, exact computation provides a direct check of Lemma 1, its strict non-invertibility, the parity hypothesis of Proposition 4, and the finite-range behavior of $E_C(N)$. Note that the large-sieve inequality (2) itself is non-trivial only asymptotically (its constant $M(C) = \prod_{c\in C} 2^{\varphi(c)/2}$ grows rapidly with c, e.g. $M(\{3,7,11\}) = 2\cdot 8\cdot 32 = 512$), so finite counts test the structural steps and scaling rate rather than the explicit constant.

Algorithm and independent cross-validation. The standalone Python script `recompute.py` (standard library only, runtime ≈ 7 s on a single core; output archived in `recompute.out`) constructs a smallest-prime-factor table up to $2^{24}+32$ and evaluates the Type II and Type I branches via exact bitmask dynamic programming over signed prime-power products $\prod_{q\mid x_c} q^{e_q} \bmod c$ with $|e_q| \le v_q(x_c)$ (Remark 7). To rule out encoding errors, `recompute.py` independently cross-validates this bitmask evaluator against brute-force divisor-pair enumeration across all 3,366 pairs (p, c) with prime $p \equiv 1 \pmod 4$, $23 < p < 20{,}000$, and $c \in \{3, 7, 11\}$, finding 0 mismatches.

Table 1. Exact Type II failure counts $E_C(N)$ at $N = 2^{16}, 2^{18}, 2^{20}, 2^{22}$, and 2^{24}, with normalized ratios $E_C(N)/(N\log^{-\kappa} N)$ in parentheses (`recompute.out`). For $C = \{3,7\}$, $E_{\{3,7\}}(N)$ equals $\#\{p < N : k(p) > 7\}$ identically; the last column lists exact $\#\{p < N : k(p) > 11\}$ to separate Type II failure from both-branch failure at shift 11.

N	$E_{\{3\}}$ (κ=1.5)	$E_{\{3,7\}}$ (κ=2)	$E_{\{3,7,11\}}$ (κ=2.5)	#{k>11}
2^{16}	418 (0.2356)	88 (0.1652)	33 (0.2063)	30
2^{18}	1,401 (0.2355)	301 (0.1787)	119 (0.2496)	113
2^{20}	4,742 (0.2334)	1,033 (0.1893)	420 (0.2866)	410
2^{22}	16,407 (0.2329)	3,374 (0.1871)	1,329 (0.2877)	1,305
2^{24}	57,186 (0.2313)	11,270 (0.1859)	4,196 (0.2823)	4,123

Table 2. Per-shift breakdown of Check F1 (`recompute.out`) over all 40,949 primes $p \equiv 1 \pmod 4$ in $(23, 2^{20})$, showing half-system counts $2^{\varphi(c)/2}$, Type II failures, violations of Lemma 1, and converse counterexamples.

c	$\varphi(c)$	$2^{\varphi(c)/2}$	Type II fails	Viol.	Converse fails
3	2	2	4,742	0	12,456
7	6	8	9,031	0	14,941
11	10	32	12,343	0	18,868
15	8	16	19,034	0	13,074
19	18	512	16,497	0	19,117
23	22	2,048	19,660	0	16,998
Total	–	–	81,307	0	95,454

Empirical observations and negative controls. Table 2 records the exact Check F1 breakdown over 245,694 prime-shift pairs: Lemma 1 holds with 0 violations across all 81,307 failures, while the negative-control plant (testing the converse of Lemma 1) fails 95,454 times, confirming that half systems are genuinely a relaxation rather than an equivalence. Table 1 and Figure 3 show the exact failure counts through $N = 2^{24}$:

- At $C = \{3,7\}$, $E_{\{3,7\}}(N)$ equals $\#\{p < N : k(p) > 7\}$ identically at every N, consistent with Remark 8, while replacing shift 7 by shift 11 in Check F2 breaks 7,074 of the 11,270 primes below 2^{24}.
- At $C = \{3,7,11\}$, the third column counts Type II failures (4,196 below 2^{24}), which strictly contain the 4,123 primes with $k(p) > 11$; the remaining 73 primes $(3, 6, 10, 24, 73$ at $2^{16}, 2^{18}, 2^{20}, 2^{22}, 2^{24})$ admit only a Type I solution at shift 11.

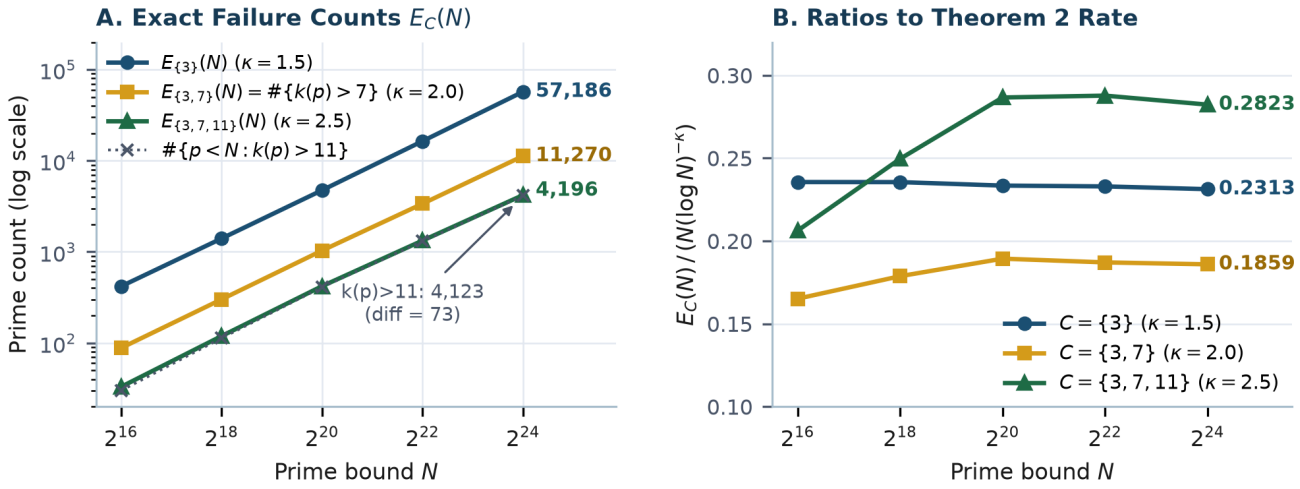


Figure 3. Empirical scaling of Type II failure counts through $N = 2^{24}$ (`recompute.out`). Panel A: Exact counts $E_{\{3\}}(N)$, $E_{\{3,7\}}(N) = \#\{p < N : k(p) > 7\}$, $E_{\{3,7,11\}}(N)$, and $\#\{p < N : k(p) > 11\}$ on a logarithmic vertical scale, noting the 73-prime gap at $N = 2^{24}$. Panel B: Normalized ratios $E_C(N)/(N(\log N)^{-1-|C|/2})$ settling near 0.2313, 0.1859, and 0.2823.

- Across $N = 2^{16}$ through 2^{24}, the normalized ratios of $E_C(N)$ to $N(\log N)^{-\kappa}$ settle near 0.2313, 0.1859, and 0.2823. Because Theorem 2 is an upper bound and $N \leq 2^{24}$ is modest, these ratios agree with the exponent $\kappa = 1 + |C|/2$ without confirming sharpness.
- Finally, Check F4 verifies Step 1 of Proposition 4 across all primes $p \equiv 1 \pmod{24}$ below 2^{22}: all 18,350 primes with $(p/7) = +1$ have even bad-factor counts in both m_3 and m_7 (0 exceptions and 0 mismatches with $k(p) > 7$), whereas all 18,530 primes with $(p/7) = -1$ fail the even-parity condition in m_7 (0 even counts).

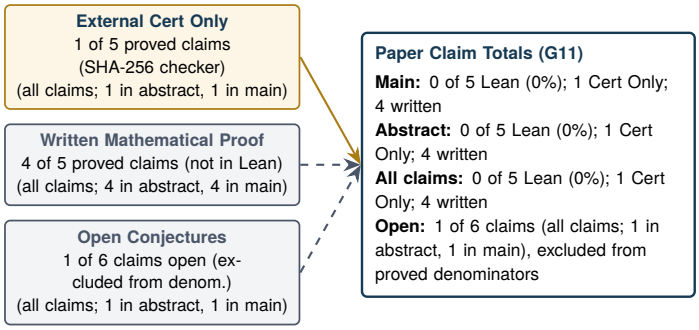
This completes the verification of Proposition 5.

5. FORMAL VERIFICATION & READER'S TRUST BOUNDARY

What You Must Trust to Accept This Paper:

1. **Lean 4 Kernel:** No Lean 4 formalization is claimed in this manuscript.
2. **Written Proofs:** All mathematical arguments rest on standard human-readable proofs.
3. **External Certificates & Written Proofs:** 1 SHA-256-pinned external artifact(s) plus any claims marked Written or Unsettled in Table 3 below.

Reader's Trust-Flow Architecture (Distinct Evidence Paths to Claim Totals)



Anti-Shortcut Audit Strip — No-Lean Disclosure

N/A: Lean 4: Not claimed | N/A: sorry / admit: N/A | N/A: native_decide: N/A | N/A: Escape hatches: N/A | N/A: Library coverage: N/A | N/A: Lean fidelity: N/A | WARN: Human referee: pending

Table 3. Per-Claim Reader's Trust Boundary Ledger (G11 Denominators Derived Mechanically).[a]

Paper Claim	Proof Tier	Lean Decl / Artifact	Actual Axioms & Fidelity	Assumptions & What You Must Trust
Lem. 1: Involution lemma – Type II failure at shift c = 3 (mod 4) for prime p > c confines prime-factor residues T_c(p) of x_c = (p + c)/4 to a half system S_c of size phi(c)/2	Written	Written proof	Lean: none; fidelity: n/a	Written elementary modular-arithmetic proof (Section 3.1); checked by falsifier agent and verified computationally across 245,694 pairs below 2^20; not formalized in Lean 4; unrefereed.
Thm. 2: Fixed-shift Type II sieve upper bound E_C(N) «_C N (log N)^(-1 - |C|/2) for any finite nonempty set C of shifts c = 3 (mod 4)	Written	Written proof	Lean: none; fidelity: n/a	Written analytic proof (Section 3.2) via Lemma 1, Montgomery's arithmetic large sieve (Q = sqrt(N)), Mertens' theorem in progressions, and Rankin's trick; step-read by falsifier agent; not formalized in Lean 4; unrefereed.
Cor. 3: Least-shift tail bound #{p <= N : k(p) > K} «_K N (log N)^(-1 - m/2) for K >= 3, m = floor((K + 1)/4), giving « N (log N)^(-2) at K = 7	Written	Written proof	Lean: none; fidelity: n/a	Written corollary of Theorem 2 (Section 3.3); step-read by falsifier agent; not formalized in Lean 4; unrefereed.
Prop. 4: Conditional lower bound #{p <= N : k(p) > 7} » N (log N)^(-2) assuming the Elliott-Halberstam conjecture	Written	Written proof	Lean: none; fidelity: n/a	Conditional on the Elliott-Halberstam conjecture; written proof (Section 3.4) citing the linear sieve lower bound (Iwaniec 1980 / Opera de Cribro) and Selberg's dim-5/2 upper-bound sieve; step-read by falsifier agent; not formalized in Lean 4; unrefereed.

Paper Claim	Proof Tier	Lean Decl / Artifact	Actual Axioms & Fidelity	Assumptions & What You Must Trust
Prop. 5: Exact Python verification of 81,307 Type II failures (0 violations, 95,454 converse plants) below 2^20, scaling table through 2^24, and 18,350 EH parity checks below 2^22	Cert Only	recompute.py (deb56683f39a) [archived; replay pending]	External cert only; fidelity: n/a	Deterministic exact-arithmetic Python script recompute.py (standard library only, archived stdout recompute.out).
Conj. 6: Unconditional lower bound #{p <= N : k(p) > 7} » N (log N)^(-2) and sharpness of exponent 1 + |C|/2 for |C| >= 2	Unsettled	Open conjecture	Lean: none; fidelity: n/a	Explicitly unsettled problem (excluded from G11 denominators).

[a]Allowed pure-kernel axioms: `propext`, `Classical.choice`, `Quot.sound`. Actual axioms printed above are read directly from verified outputs. Provenance nonce: 953673819627 | Fidelity SHA-256: 3f0614741dde.

6. PRIOR WORK AND OPEN QUESTIONS

Credited literature. Elsholtz and Tao [4] classify Erdős–Straus decompositions into Type I and Type II solutions, determine the average number of solutions over primes up to a log log N factor, and survey earlier density bounds including Vaughan's exceptional-set estimate $N\exp(-c(\log N)^{2/3})$ [13] `[to check]` and Salez's modular verification to 10^{17} [11] `[to check]`. Bello-Hernández, Benito, and Fernández [1] develop an equivalent scaled divisor parametrization in the shift frame $k = 4x - p$ and study greedy survivor records.

The closest antecedents to Theorem 2 are Dahan's two 2026 preprints [2, 3]. In [2], Dahan formulates the fixed-shift criterion with its two branches, characterizes shift 3, proves single-shift upper and lower bounds at shift 7 (Theorem `blind_primes`), and proves Theorem `fixed_depth`: for a fixed finite set P of coprime witness pairs (u, a), the primes $n \le N$ $(n \equiv 1 \pmod{24})$ having no divisor $s \equiv -1 \pmod{4ua}$ of $an + u$ number $\ll_P N(\log N)^{-1-|P|/2}$, via an involution lemma on $x \mapsto -x^{-1} \bmod 4ua$ and Selberg's sieve at Bombieri–Vinogradov level. Because a witness pair (u, a) produces a shift $c = (u+v)/a$ that varies with n, fixed-shift failure is not covered by any finite P; Theorem 2 transposes that mechanism to fixed shifts using the additive involution $a \mapsto -a \bmod c$ and Montgomery's large sieve [9, 10] `[to check]`. In [3], Dahan establishes the exact prime-factor characterization of shifts 3 and 7 (Theorem `sylow_and_c7_iff(b)`) and applies the large sieve to an intersection of a growing number of prime shifts (Theorem `blind_intersection_and_PNR(a)`), which saves only a constant factor when $|C|$ is fixed.

For a single shift, two-sided counts of order $N(\log N)^{-3/2}$ are known unconditionally: at shift 3 via Iwaniec [7, Theorem 1, eq. (1.1)] applied to primitive representations by $\xi^2 + \xi\eta + \eta^2$ with $B = 4, A = -3$ (and independently via Fuchs, Hsu, Rickards, Schindler, and Stange [6, Theorem 1.1(1)]), and at shift 7 via Dahan [2]. Sander [12] `[to check]` uses Iwaniec's half-dimensional sieve to obtain $\gg x(\log x)^{-3/2}$ for one fixed-parameter Type II family $gh/w = t$, which mixes shifts rather than fixing c.

Searches run and unread gaps. Prior-work searches covered arXiv (API sweeps returning 63 distinct entries), OEIS, zbMATH Open API, full-text LaTeX checks of [4, 2, 3, 1, 6], the full EuDML scan of [7], and a 5-query Google Scholar sweep on 2026-11-22. Neither Theorem 2 nor Proposition 4 was found in the sources searched; the method is standard and Theorem 2 is a direct transposition of Dahan's fixed-depth proof to fixed shifts. Items still owed (`[to check]` in `references-checked.md`): the paywalled body of Sander [12] (zbMATH review read; ScienceDirect HTTP 403), full-text re-reads of the standard sieve references [9, 10, 8, 5, 13, 11], and full-text human inspection of two HTTP-403 gated preprints surfaced in the 2026-11-22 Google Scholar sweep: R. Marangoni (Academia.edu, "The Erdős–Straus equation with a fixed denominator") and M. A. Mahran (ResearchGate, "Local Divisor Obstructions and Complementary Parametric Constructions for the Erdos–Straus Equation").

Open questions. Three concrete questions remain unsettled:

1. *Unconditional lower bound for $k(p) > 7$:* Prove $\#\{p \le N : k(p) > 7\} \gg N(\log N)^{-2}$—or even that infinitely many primes satisfy $k(p) > 7$—without assuming Elliott–Halberstam (e.g., via equidistribution of $\{p : k(p) > 3\}$ in arithmetic progressions on average to moduli $N^{1/2-\varepsilon}$).
2. *Sharpness for $|C| \ge 2$:* Determine whether the exponent $1 + |C|/2$ in Theorem 2 is sharp when $|C| \ge 2$, and whether the converse failures of Lemma 1 (from composite divisor products) alter the true exponent at large shifts.
3. *Explicit dependence on C:* Improve the implied constant $M(C) = \prod_{c \in C} 2^{\varphi(c)/2}$ in Theorem 2 so the bound becomes informative at growing $|C|$.

7. DATA AVAILABILITY, REPRODUCIBILITY, AND USE OF AI

All manuscript sources, figure scripts, and verification outputs reside in `papers/erdos-straus-type-ii/draft1/`. Running

```
python3 papers/erdos-straus-type-ii/draft1/recompute.py
```

reproduces `recompute.out` byte-for-byte in under 10 s using only the Python standard library, verifying all worked examples, the 3,366-pair divisor cross-check, Check F1 (81,307 failures, 0 violations, 95,454 converse plants), Check F2 (11,270 primes with $k(p) > 7$), Table 1 through $N = 2^{24}$, and Check F4 (18,350 parity checks). Scripts in `figures/` regenerate all four 300 DPI figures.

Use of AI and review status. AI research agents built and directed by Tyler B. Hughes derived the proofs, performed the independent falsifier step-check and computation, built the figures, and drafted this manuscript. No Lean 4 formalization is claimed in this draft. No human mathematician has yet refereed the proof.

Drafted: November 2026 **Updated:** November 24, 2026

REFERENCES

(1) M. Bello-Hernández, M. Benito, and E. Fernández, A Divisor Parametrization for the Erdős–Straus Conjecture, arXiv:2606.10922v1 (2026).

(2) B. Dahan, Sieve dimension and search depth for the Erdős–Straus conjecture, $n \equiv 1 \pmod{24}$, arXiv:2608.24035v2 (2026).

(3) B. Dahan, Composite witness sieves, Kneser–Plancherel containers, and the exponent 5/7 for the Erdős–Straus conjecture, arXiv:2611.08717v1 (2026).

(4) C. Elsholtz and T. Tao, Counting the number of solutions to the Erdős–Straus equation on unit fractions, *J. Aust. Math. Soc.* **94** (2013), 50–105. doi:10.1017/S1446788712000468.

(5) J. Friedlander and H. Iwaniec, *Opera de Cribro*, AMS Colloquium Publications **57**, Providence, RI, 2010. doi:10.1090/coll/057.

(6) E. Fuchs, C. Hsu, J. Rickards, D. Schindler, and K. E. Stange, Primes represented by shifted quadratic forms: on primitivity and congruence classes, arXiv:2504.20289v1 (2025).

(7) H. Iwaniec, Primes of the type $\varphi(x, y)+A$ where φ is a quadratic form, *Acta Arith.* **21** (1972), 203–234. doi:10.4064/aa-21-1-203-234.

(8) H. Iwaniec, A new form of the error term in the linear sieve, *Acta Arith.* **37** (1980), 307–320. doi:10.4064/aa-37-1-307-320.

(9) H. L. Montgomery, A Note on the Large Sieve, *J. London Math. Soc.* **s1-43** (1968), 93–98. doi:10.1112/jlms/s1-43.1.93.

(10) H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134. doi:10.1112/S0025579300004708.

(11) S. E. Salez, The Erdős–Straus conjecture: New modular equations and checking up to $N = 10^{17}$, arXiv:1406.6307v1 (2014).

(12) J. W. Sander, On $4/n = 1/x + 1/y + 1/z$ and Iwaniec' Half Dimensional Sieve, *J. Number Theory* **46** (1994), 123–136. doi:10.1006/jnth.1994.1008.

(13) R. C. Vaughan, On a problem of Erdős, Straus and Schinzel, *Mathematika* **17** (1970), 193–198. doi:10.1112/S0025579300002886.