MATHDISCOVERIES
Mathematical Preprint

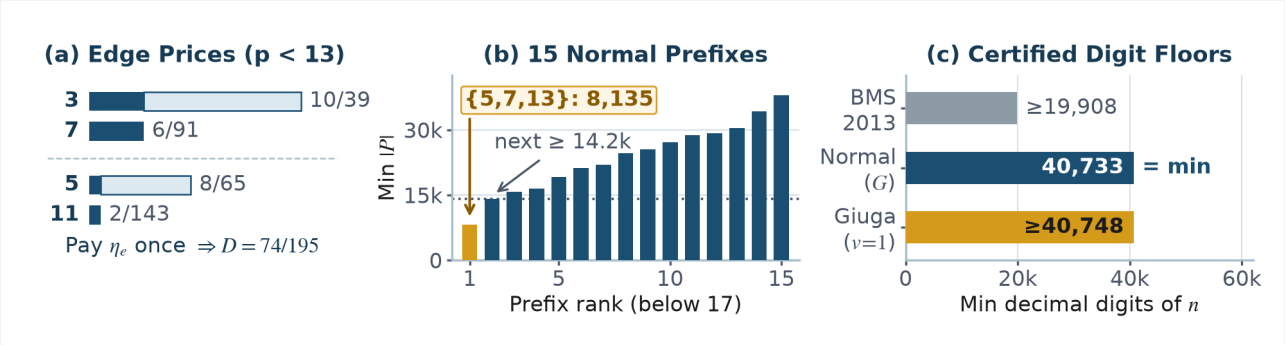
How Many Prime Factors Could a Counterexample to Giuga's Conjecture Have?

Tyler B. Hughes[†]

[†]Independent Researcher, United States

Ⓢ *Supporting Information:* `recompute.py`, `critical-edges.json.xz`, *and* `lean/Giuga/` (*Lean 4 + Mathlib, rev.* `855d12ba1`)

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



ABSTRACT: Giuga conjectured that no composite $n > 1$ satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$. As shown by Giuga, any counterexample's prime divisors form a normal odd prime set with reciprocal sum above one. Nonnegative prices on forbidden pairs bound both factor count and product size. Exact integer certificates across all fifteen conflict-free prefixes below 17, combined with Lean 4 conditional lifts, prove every counterexample has at least 8,138 distinct prime divisors and $n > 10^{40,747}$ (40,748 digits), improving Borwein, Maitland, and Skerritt (4,771 divisors, 19,908 digits). Under normality and reciprocal sum above one alone, the exact minima are 8,135 factors and 40,733 digits; adding the value-one congruences and single-deletion test gives 8,138 factors and 40,748–40,750 digits. Unconditionally inside Lean 4, we formalize an 8,135-prime (40,733-digit) normal witness, an 8,138-prime (40,751-digit) seven-rule ceiling witness, and counterexample bounds of 578 prime divisors and $n > 10^{1,803}$. Existence remains open.

Verification Scope (G11): WARN: Human referee: pending — **Full Trust Boundary:** Section 6.
Main results: 4 of 7 in Lean Kernel (57%) · 2 Lean + Cert · 1 Cert Only · 1 open (not counted)
Abstract claims: 7 of 10 in Lean Kernel (70%) · 2 Lean + Cert · 1 Cert Only · 1 open (not counted)

MSC 2020: 11A41, 11Y11, 90C05 **Keywords:** Giuga's conjecture, normal prime sets, maximum flow, exact integer certificates, Lean 4

1. INTRODUCTION AND MAIN RESULTS

For a prime n, every term in $\sum_{k=1}^{n-1} k^{n-1}$ leaves remainder one after division by n. Their sum therefore leaves remainder $n-1$. Giuga asked whether the same sum can have that remainder for a composite [4, 3].

Conjecture 1 (Giuga's Conjecture, 1950–1951). *No composite integer $n > 1$ satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$.*

A small prime divisor would help a counterexample bring the sum of its reciprocal prime factors above one. The difficulty is that the same divisor rules out many other small primes. For example, 3 excludes 7 because 3 divides $7-1$.

Theorem 2 (Counterexample factor-count lower bound). *If $n > 1$ is composite and $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$, then n has at least 8,138 distinct prime divisors.*

Theorem 3 (Counterexample decimal-digit lower bound). *If $n > 1$ is composite and $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$, then $n > 10^{40,747}$, so n has at least 40,748 decimal digits.*

Both headline bounds improve the published bound of Borwein, Maitland, and Skerritt (4,771 prime divisors and 19,908 decimal digits [3]). In our verification architecture, Theorems 2 and 3 are mixed Lean 4 plus external-certificate results: the `Giuga` Lean 4 + Mathlib library proves the conditional deductions from a fifteen-prefix finite certificate hypothesis, while the standalone exact-integer checker `recompute.py` replays that finite certificate across all fifteen conflict-free prefixes below 17.

Theorem 4 (Exact normal-set minima and local ceiling window). *Among finite sets P of odd primes satisfying $\sum_{p\in P} 1/p > 1$ and $q \nmid r-1$ for all $q < r$ in P, the minimum cardinality is 8,135 and the minimum number of decimal digits of $\prod_{p\in P} p$ is 40,733, both attained by one greedy set G. If one also imposes the value-one congruences and the single-deletion test in Section 4.4, the minimum cardinality becomes 8,138 and the minimum number of decimal digits lies in $\{40{,}748, 40{,}749, 40{,}750\}$ (attained at 40,750 by the explicit set W_{321169}).*

Inside the Lean 4 kernel without external certificate hypotheses, we establish an 8,135-prime normal witness, an 8,138-prime local-rules ceiling witness (demonstrating the limit of any proof using only those seven local conditions), and self-contained counterexample bounds (578 prime divisors and $n > 10^{1,803}$).

Theorem 5 (Unconditional Lean 4 8,135-prime normal witness). *There exists a finite normal set G of odd primes with $|G| = 8{,}135$, $\sum_{p\in G} 1/p > 1$, and $10^{40,732} < \prod_{p\in G} p < 10^{40,733}$ (40,733 decimal digits).*

Theorem 6 (Unconditional Lean 4 seven-rule ceiling witness). *There exists a finite normal set W of odd primes with $|W| = 8{,}138$, $3 \notin W$, $\sum_{p\in W} 1/p > 1$, $\sum_{q\in W\setminus\{p\}} 1/q \le 1$ for every $p \in W$, $|\{p \in W : p \equiv 3 \bmod 4\}| \equiv 0$ or $1 \pmod 4$, $\sum_{p\in W} p \equiv 1 + \prod_{p\in W} p \pmod 8$, and $10^{40,750} < \prod_{p\in W} p < 10^{40,751}$ (40,751 decimal digits).*

Theorem 7 (Unconditional Lean 4 counterexample factor bound). *Every composite integer $n > 1$ satisfying $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod n$ has at least 578 distinct prime divisors.*

Corollary 8 (Unconditional Lean 4 counterexample size bound). *Every composite integer $n > 1$ satisfying $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod n$ satisfies $n > 10^{1,803}$ (at least 1,804 decimal digits).*

Below 13 the odd primes form two forbidden pairs, $(3, 7)$ and $(5, 11)$. Give a prime the bonus $w_p = 1/p - 1/13$ for being smaller than 13. An admissible set can take at most the larger bonus in each pair. Each remaining prime contributes at most $1/13$ to the reciprocal sum. The following calculation bounds the number of prime factors needed to make that sum exceed one.

A Calculation to Try — Verified 7-Line Python Check

```
from fractions import Fraction as F
pairs = [(3, 7), (5, 11)]
def bonus(p):
    return F(1, p) - F(1, 13)
D = sum(max(bonus(q), bonus(r)) for q, r in pairs)
assert D == F(74, 195)
assert 13 * (1 - D) == F(121, 15)  # > 8 factors
```

For a larger graph one vertex belongs to several forbidden pairs. Lemma 11 (Lemma W) explains how to divide its weight among them. We first derive the arithmetic conditions that create the graph, then choose two weight functions on it. The first bounds the count. The second turns an improvement in the count directly into an improvement in the number of digits.

2. FROM A POWER SUM TO A FAMILY OF PRIME SETS

For any finite set P of odd primes put $\sigma(P) = \sum_{p\in P} 1/p$ and $N(P) = \prod_{p\in P} p$, using the empty sum 0 and empty product 1. Call P *normal* if $q \nmid r-1$ for every $q < r$ in P. All logarithms are natural unless a base is shown. For a positive integer N, write $\operatorname{digits}(N) = 1 + \lfloor \log_{10} N \rfloor$.

Proposition 9 (Carmichael–Giuga equivalence). *A composite integer $n \ge 2$ satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod n$ if and only if every prime $p \mid n$ satisfies both*

$$p - 1 \mid (n/p - 1), \qquad p \mid (n/p - 1). \tag{1}$$

Proof. Let p divide a composite n satisfying Giuga's congruence. Include the zero term in its power sum and group the terms by residues modulo p. Each residue occurs n/p times. Summing the $(n-1)$st powers of the nonzero residues gives zero unless $p - 1 \mid n - 1$, when it gives -1 modulo p; this follows by summing the powers of a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Because $n-1 = p(n/p-1)+(p-1)$, the divisibility $p-1 \mid n-1$ holds if and only if $p-1 \mid (n/p-1)$. Thus (1) is necessary. Conversely, the second condition in (1) forces n to be squarefree, and the residue calculation at each prime together with the Chinese remainder theorem recovers the original power-sum congruence. (Formalized in Lean 4 as `Giuga.giuga_iff_carmichael_and_giuga`.) □

An even squarefree composite would have an odd prime divisor p and an even number $p-1$ dividing the odd number $n-1$. Thus every Giuga counterexample n is odd, squarefree, and equals $N(P)$ for its prime-factor set P. If $q \mid r - 1$ for $q, r \in P$, then $q \mid n - 1$ by (1), contradicting $q \mid n$. Hence P is a normal set of odd primes.

Proposition 10 (Unique value). *Every Giuga counterexample n admits a unique integer $v \ge 1$ such that*

$$\sum_{p\in P} n/p = vn + 1, \tag{2}$$

where P is the set of prime divisors of n.

Proof. Modulo any $p \in P$, exactly one term of $\sum_{r\in P} n/r$ survives, and it equals 1 by (1). Because n is squarefree, n divides $(\sum_{p\in P} n/p) - 1$, giving a unique integer v with $\sum_{p\in P} n/p = vn + 1$. Since n is composite and squarefree, $|P| \ge 2$, so the left-hand side is at least 2 and $v \ge 1$. (Formalized in Lean 4 as `Giuga.giuga_exists_value`.) □

Dividing (2) by n gives $\sigma(P) = v + 1/n > 1$ (separately formalized in Lean 4 as `Giuga.giuga_recip_sum_eq` and `giuga_recip_sum_gt_one`).

Theorem 4 starts by retaining only normality and $\sigma(P) > 1$. Keeping the integer v distinguishes a Giuga counterexample from a solution of that relaxed problem.

3. A BOUND ON THE WEIGHT OF COMPATIBLE PRIMES

Fix the primes of P below a chosen split point b and call their set S. Write $T = P \setminus S$ and $h = 1 - \sigma(S)$, so $\sigma(T) > h$. For a cutoff $C \ge b$, let U consist of the primes p with $b \le p < C$ for which $S \cup \{p\}$ is normal. Join $q < r$ in U if $q \mid r - 1$. A normal tail selects an independent set in this finite graph.

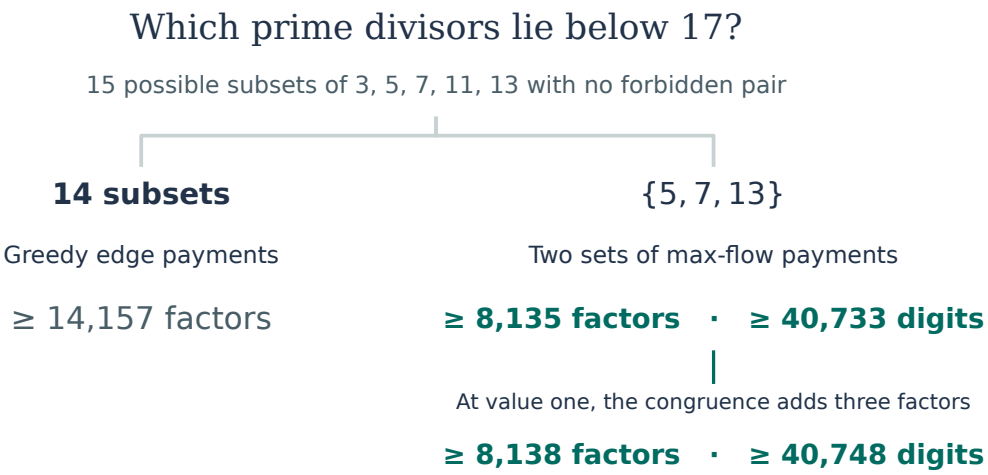


Figure 1. Splitting at 17 leaves one tight case. For the other fourteen, even the smallest certified count gives a product larger than $10^{52,619}$ (and a zero-edge congruence-lifted bound at least $10^{69,620}$). An integer replay proves the displayed lower bounds. Lean 4 unconditionally verifies the 8,135-prime normal witness and the 8,138-prime local-rules ceiling witness together with a self-contained 578-factor ($n > 10^{1,803}$) counterexample bound. At value two or higher, the crossing argument gives 91,476 factors. Existence stays open.

An edge can therefore cover an allowance at both endpoints while being charged at most once to the selected set.

Lemma 11 (Edge payments (Lemma W)). *Let E be a finite set of edges on a finite vertex set U, and assign each edge $e \in E$ a price $\eta_e \geq 0$. For any real vertex weights w_p and any independent set $I \subseteq U$,*

$$\sum_{p\in I} w_p \leq D(w,\eta) := \sum_{e\in E} \eta_e + \sum_{p\in U} \left(w_p - \sum_{e\ni p} \eta_e \right)_+ . \tag{3}$$

Here $(x)_+ = \max(x,0)$ and unlisted edges may be given price zero.

Proof. At each selected vertex $p \in I$, add the incident prices $\sum_{e\ni p} \eta_e$ to the positive residual $(w_p - \sum_{e\ni p} \eta_e)_+$; this sum is at least w_p. Summing over $p \in I$, each edge price η_e appears at most once because I is independent and cannot contain both endpoints of e. Including the nonnegative residuals at unselected vertices $p \in U \setminus I$ only increases the right-hand side. (Formalized in Lean 4 as `Giuga.edge_dual_le_ub_of_independent`.) □

The two disjoint edges in Figure 2 can each be settled by paying the smaller endpoint weight. With overlaps, arbitrarily chosen nonnegative prices still give a proof. To find strong prices, make a left and a right copy of each vertex. Give its source-to-left arc and its right-to-sink arc capacity $(w_p)_+$. For each conflict q, r allow flow from q on the left to r on the right, and in the reverse pairing, with capacity at least the total positive weight. Half the sum of these two flows is a price on $\{q, r\}$. Conservation ensures that the prices incident to p sum to at most $(w_p)_+$. Maximizing the flow maximizes the shared allowance in this construction. Only (3) is needed to check the resulting prices. On the triangle $\{3, 7, 43\}$ each vertex can receive fractional selection $1/2$ although an independent set contains at most one vertex.

Counting factors.

Proposition 12 (Count bound (Lemma W, Refinement 1)). *Let T be a normal set of odd primes $p \geq b$ compatible with a prefix S and satisfying $\sigma(T) > h = 1 - \sigma(S)$. Let $C > 0$, let U contain every tail prime p with $b \leq p < C$ compatible with S, let E be a set of conflict edges between vertices of U, and let $\eta_e \geq 0$ for all $e \in E$. With $w_p = C/p - 1$,*

$$Ch - D(w,\eta) < |T|, \tag{4}$$

and hence $|T| \geq K = \lfloor Ch - D(w,\eta) \rfloor + 1$.

Proof. Every prime $p \in T \setminus U$ satisfies $p \geq C$ and therefore $w_p = C/p - 1 \leq 0$. Applying Lemma 11 to the independent set $T \cap U$ yields

$$Ch - |T| < C\sigma(T) - |T| = \sum_{p\in T} (C/p - 1) \leq \sum_{p\in T\cap U} w_p \leq D(w,\eta).$$

Rearranging gives (4), and integrality of $|T|$ yields $|T| \geq \lfloor Ch - D(w,\eta) \rfloor + 1$. (Formalized in Lean 4 as `Giuga.lemma_w_refinement1`.) □

Pricing a product.

Proposition 13 (Size pricing (Lemma W, Refinement 2)). *Under the hypotheses of Proposition 12, suppose in addition that $K \in \mathbb{N}$ satisfies $|T| \geq K$ and that $\mu, \nu \geq 0$ satisfy $f(C) \leq 0$ for $f(x) = \mu/x + \nu - \log x$. Then for any nonnegative edge prices $\eta'_e \geq 0$ on E,*

$$\mu h + \nu K - D(f,\eta') \leq \sum_{p\in T} \log p. \tag{5}$$

Proof. Since f decreases on $(0,\infty)$ and $f(C) \leq 0$, every prime $p \in T \setminus U$ satisfies $f(p) \leq 0$. Applying Lemma 11 to $T \cap U$ with weights $f(p)$ gives

$$\mu h + \nu K - \sum_{p\in T} \log p \leq \mu\sigma(T) + \nu|T| - \sum_{p\in T} \log p = \sum_{p\in T} f(p) \leq D(f,\eta').$$

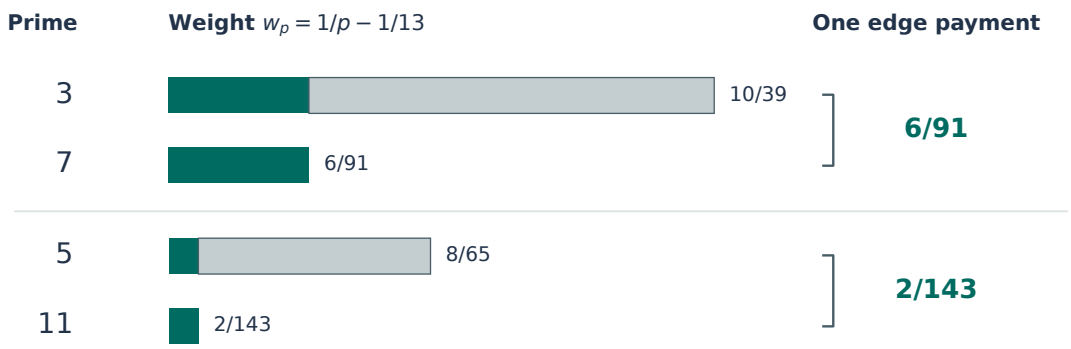


Figure 2. In each pair the dark segment is the edge price at both endpoints. Charge it once. The pale segment at the larger-weight vertex is the only residual to pay. With no edge between 3 and 5, selecting both attains the bound $D = w_3 + w_5 = 74/195$.

Rearranging gives (5). (Formalized in Lean 4 as `Giuga.lemma_w_refinement2`.) □

When $P = S \sqcup T$, adding $\sum_{s\in S} \log s$ to (5) gives $\log N(P) \geq \sum_{s\in S} \log s + \mu h + \nu K - D(f, \eta')$. The coefficient of K in (5) is ν. If arithmetic forces $|P| \equiv 2 \pmod 4$, define the lifted tail count

$$K' = K + ((6 - (|S| + K) \bmod 4) \bmod 4),$$

the least integer $K' \geq K$ with $|S| + K' \equiv 2 \pmod 4$ (formalized as `Giuga.routeALiftK` and `Giuga.routeALiftK_spec`). Replacing K by K' in (5) with the same edge prices η' (the *Route (a) lift*) yields an extra $(K' - K)\nu$ in the lower bound for $\log N(P)$ (formalized as `Giuga.lemma_w_refinement2_route_a`).

What the value adds.

Proposition 14 (Modulo-8 count congruence). *If n is a Giuga counterexample with prime-factor set P and value v satisfying (2), then $|P| \equiv v + 1 \pmod 8$.*

Proof. Write $m = |P|$ and $k_3 = |\{p \in P : p \equiv 3 \bmod 4\}|$. For each $p \in P$, the Legendre symbol $(\frac{n/p}{p})$ equals 1 by (1). Multiplying these symbols over P and applying quadratic reciprocity shows that each unordered pair contributes -1 exactly when both primes are 3 mod 4, so $\binom{k_3}{2}$ is even, or $k_3 \equiv 0, 1 \pmod 4$ (formalized as `Giuga.giuga_reciprocity_rule`).

Every odd square is 1 mod 8. Multiplying (2) by n therefore gives $\sum_{p\in P} p \equiv v + n \pmod 8$ (`Giuga.giuga_residue_mod_8`). Writing $p = 1 + 2a_p$ and expanding the product modulo 8 gives

$$\sum_{p\in P} p - \prod_{p\in P} p \equiv m - 1 - 4\sum_{q<r} a_q a_r \equiv m - 1 - 4\binom{k_3}{2} \pmod 8.$$

Since $\binom{k_3}{2}$ is even, $4\binom{k_3}{2} \equiv 0 \pmod 8$, yielding $m \equiv v + 1 \pmod 8$. (Formalized in Lean 4 as `Giuga.giuga_card_mod_eight`.) □

When $v = 1$, even the weaker congruence $m \equiv 2 \pmod 4$ (`Giuga.odd_giuga_card_mod_four`) raises the lower bound from 8,135 to 8,138 and enters (5) directly.

Lemma 15 (Higher-value crossing (Lemma C)). *Suppose every normal odd prime set P with $\sigma(P) > 1$ satisfies $|P| \geq N_1$, and suppose fewer than N_1 odd primes lie strictly below q. Then every normal odd prime set P with $\sigma(P) > 2$ satisfies $|P| \geq N_1 + q$.*

Proof. Order P increasingly and stop at the first prime $r \in P$ for which the accumulated reciprocal sum exceeds 1; such a first crossing exists because $\sigma(P) > 2$. The crossing prefix P_1 is normal with $\sigma(P_1) > 1$, so $|P_1| \geq N_1$. Since fewer than N_1 odd primes are below q, the largest element $r = \max P_1$ satisfies $r \geq q$. Because r was the first crossing, $\sigma(P_1) \leq 1 + 1/r$, so the remaining tail $P \setminus P_1$ has reciprocal sum strictly greater than $1 - 1/r$. Every prime in $P \setminus P_1$ exceeds r, so each contributes strictly less than $1/r$; thus $|P \setminus P_1| \geq r \geq q$ and $|P| \geq N_1 + q$. (Formalized in Lean 4 as `Giuga.lemma_C_general`.) □

Inside Lean 4, a bitmask sieve and SWAR popcount (`Giuga.odd_prime_card_lt_83341`) prove unconditionally that there are only 8,134 odd primes below $q = 83{,}341$. Whenever $N_1 = 8{,}135$, Lemma 15 therefore forces $|P| \geq 8{,}135 + 83{,}341 = 91{,}476$ for every counterexample with $v \geq 2$ (`Giuga.lemma_C_91476`), and $n \geq 91{,}476! > 10^{40{,}747}$ (indeed $n > 10^{446{,}177}$ by `Giuga.lemma_C_prod_gt_10_pow_446177`).

4. THE FINITE CERTIFICATE AND THE ATTAINING SETS

Use $b = 17$. Every odd prime below b belongs to $\{3, 5, 7, 11, 13\}$. Discard any subset containing a conflict. This yields exactly the fifteen prefixes in Table 1. At each prefix the verifier sieves the primes up to the cutoff, discards conflicts with S, and bounds the contribution of the surviving primes by (3). It needs no list of primes above the cutoff.

Fourteen prefixes. Set $C = 200{,}000$. Give each vertex its initial residual $(C/p - 1)_+$, rounded up to the verifier's grid. Visit q in increasing order and then its admissible neighbors $r > q$ in increasing order. On each edge pay the smaller remaining residual and subtract it from both endpoints. Each payment reduces the sum of residuals by twice the amount paid, so the final value of (3) is the initial sum less all payments. The smallest count obtained this way is 14,157. Distinct positive integers in increasing order have their ith member at least i, so every one of these fourteen cases has $N(P) \geq 14{,}157! > 10^{52{,}619}$. Equally, taking

Table 1. Certified total factor counts for normal sets with $\sigma(P) > 1$, ordered within each column. Each is a lower bound. The greedily constructed set G attains the entry in bold.

All 15 Conflict-Free Prefixes $S \subset \{3,5,7,11,13\}$ Below $b = 17$					
S	$\lvert P\rvert \geq$	S	$\lvert P\rvert \geq$	S	$\lvert P\rvert \geq$
$\{5,7,13\}$	**8,135**	$\{7,13\}$	21,262	$\{3,11\}$	28,703
$\{5,7\}$	14,157	$\{7,11\}$	21,931	$\{13\}$	29,205
$\{7,11,13\}$	15,788	$\{11,13\}$	24,663	$\{11\}$	30,368
$\{3,5\}$	16,459	$\{5\}$	25,501	$\emptyset$	34,194
$\{5,13\}$	19,097	$\{7\}$	27,075	$\{3\}$	37,911

$\mu = 0$, $\nu = \log_{\mathrm{lo}}(200{,}000)$ (where $\log_{\mathrm{lo}}$ denotes the exact-integer lower logarithm defined in Section 4), $C = 200{,}000$, and zero edge prices $\eta' = 0$ in Proposition 13 directly certifies $\log_{10} N(P) \geq 69{,}620 > 40{,}747$ across all fourteen prefixes, matching the per-prefix hypothesis of `Giuga.cor_giuga_route_a_gt_10_pow_40747`.

The remaining prefix. For $S = \{5,7,13\}$ use $C = 325{,}078$. Here U has 16,042 vertices. The certificate stores 10,934 edges with two prices per edge, one for (4) and one for (5). The count bound gives $K = 8{,}132$. At the same prefix the product bound gives $\log_{10} N(P) > 40{,}732.063$. The total count $|S| + K$ is 8,135. When $v = 1$, Proposition 14 forces $|P| \equiv 2 \pmod 8$ (hence $2 \pmod 4$), so the tail must contain at least 8,135 primes. With ν approximately 11.898582, using this tail count in (5) gives $\log_{10} n > 40{,}747.566$. Together with the fourteen prefixes above, Proposition 12, and frontier completeness (`Giuga.lemma_w_frontier_count`), these exact integer inequalities establish the universal normal-set floor `hN1`, the prefix cover `hF`, the per-prefix tail count bounds `hTailK`, and the per-prefix logarithmic bounds `hCert`; combined with Lemma 15 for $v \geq 2$ inside `Giuga.cor_giuga_8138_primes` and `Giuga.cor_giuga_route_a_gt_10_pow_40747`, this proves Theorems 2 and 3.

Integer verification. All stored prices and multipliers are nonnegative integers in units of $1/Q$, $Q = 10^{12}$. Rounded prices need only be legal on their specified edges. For an upper bound on (3), round each vertex weight upward. Round h and prefix logarithms downward. Verify $f(C) \leq 0$ with an upper bound on $\mu/C + \nu$ and a lower bound on $\log C$. For a lower bound on the positive decimal logarithm, divide the lower bound on the natural logarithm by an upper bound on $\log 10$.

All logarithm bounds reduce to rational arithmetic. For $1 \leq y \leq 2$ put $t = (y-1)/(y+1)$, so $0 \leq t \leq 1/3$ and

$$\log y = 2 \sum_{j=0}^{19} \frac{t^{2j+1}}{2j+1} + R,$$

$$0 \leq R \leq \frac{2t^{41}}{41(1-t^2)}.$$

Write $p = 2^{\ell} y$, use this expansion for y and 2, and discard the positive remainder for a lower bound. The checker also rounds downward in each fixed-point multiplication. For $\log 10 = 3\log 2 + \log(5/4)$ it evaluates the upper formula with exact rational numbers, including the remainder. This treats primes near a zero weight in the same direction as every other vertex. The checker rejects a fabricated edge and a multiplier that leaves positive weight beyond the cutoff.

Attainment and the limit of the local conditions. Starting with $\{5,7,13\}$, visit the primes from 17 upward. Accept a prime precisely when it is compatible with every prime already accepted. Stop at the first reciprocal sum greater than one. The final two accepted primes are 321,047 and 321,053, and the latter is the 8,135th member. For this set G, exact integer calculations in `recompute.py` verify

$$\sigma(G \setminus \{321{,}053\}) < 1 < \sigma(G),$$
$$10^{40{,}732} < N(G) < 10^{40{,}733},$$

while the unconditional Lean 4 check in Theorem 5 independently verifies normality, $|G| = 8{,}135$, $\sigma(G) > 1$, and $10^{40{,}732} < N(G) < 10^{40{,}733}$. Together with the fifteen-prefix count and product lower bounds above, this proves the first part of Theorem 4.

A value-one counterexample would have $\sigma(P) = 1 + 1/n$. Deleting any prime then drops the sum below one (`Giuga.giuga_exactness_rule`). Consider the seven-rule local class of finite odd-prime sets P obeying (i) normality, (ii) $3 \notin P$, (iii) $\sigma(P) > 1$, (iv) single-deletion minimality ($\sigma(P \setminus \{p\}) \leq 1$, or strictly < 1 for a true value-one counterexample), and the three value-one congruences

$$|P| \equiv 2 \pmod 8, \qquad k_3 \equiv 0, 1 \pmod 4,$$
$$\sum_{p \in P} p \equiv 1 + N(P) \pmod 8.$$

Any member of this class sets a ceiling on lower bounds derivable solely from these seven local conditions. The count and product bounds for $v = 1$ used only normality, $\sigma(P) > 1$, and $|P| \equiv 2 \pmod 4$, so they apply to this entire class.

For upper bounds, let a single prime vary in the family

$$B = (G \setminus \{97{,}387\}) \cup \{321{,}073, 321{,}109, 321{,}143\},$$
$$W_x = B \cup \{x\}.$$

The witness verified inside Lean 4 (Theorem 6) takes $x = 1{,}999{,}993$. Extending the greedy sequence to its 8,139th member and testing single deletions gives the smaller choice $x = 321{,}169$ with the same deletion 97,387. For each choice `recompute.py` checks normality, $3 \notin W_x$, all three congruences, $k_3 = 4{,}032$, and $0 < \sigma(W_x) - 1 < 1/x$; because $x = \max W_x$, deleting any prime strictly drops the sum below one. (In Lean 4, Theorem 6 proves the non-strict form $\sigma(W \setminus \{p\}) \leq 1$ on $W_{1999993}$.) The integer products are summarized in Table 2.

In particular $10^{40{,}749} < N(W_{321169}) < 10^{40{,}750}$. This proves the final assertion of Theorem 4, also if one adds $3 \notin P$ to the definition of the class. For both sets, the cofactor at 5 violates (1), which requires a remainder of one.

Table 2. Local witnesses $W_x = B \cup \{x\}$ satisfying normality, single-deletion minimality, and all value-one congruences, while failing (1) at $p = 5$.

Last prime x	$\lvert W_x \rvert$	digits$(N(W_x))$	$(N(W_x)/5) \bmod 5$
1,999,993	8,138	40,751	4
321,169	8,138	40,750	2

Unconditional Lean 4 bounds without external certificates. Inside `lean/Giuga/UnconditionalAndDigits.lean`, a self-contained two-prefix certificate below $b = 5$ ($\emptyset$ and $\{3\}$) at cutoff $C = 3{,}000$ is evaluated directly inside the Lean 4 kernel by radix-trie edge accumulation and GMP bitmask sieving, with zero `native_decide`. That internal certificate proves $|P| \geq 575$ for every normal set with $\sigma(P) > 1$ (`Giuga.unconditional_normal_set_575`); applying Proposition 14 and Lemma 15 then yields $|P| \geq 578$ (Theorem 7) and $n > 10^{1{,}803}$ (Corollary 8). Independently, the witnesses G and $W_{1999993}$ in Theorems 5 and 6 are checked inside the kernel via a 102-prime bitmask sieve up to 321,143, binary-tree trial division for 1,999,993, and exact rational summation over the 8,135-prime and 8,138-prime sets.

5. PRIOR WORK, OPEN QUESTIONS, AND DATA AVAILABILITY

Bedocchi [1] credits Giuga with the normal prime-set and reciprocal-sum reduction and computed the greedy sequence whose reciprocal sum first crosses one at 8,135 members. Borwein, Borwein, Borwein, and Girgensohn [2] used that witness, gave the value-one count congruence modulo four, and asked in their fifth open problem whether a particular prefix minimizes the count at every depth in a stated range. Our result establishes their numerical consequence; the intermediate equalities remain a separate question. Borwein, Maitland, and Skerritt [3] reached 4,771 factors and 19,908 digits by distinguishing prefixes through depth 311. In their tail estimate a prime had to be compatible with the prefix, but two primes admitted separately could still exclude each other. Edge prices account for precisely that exclusion. Both Borwein papers were read in full for the source audit. Giuga's original article is known here through later work [to check]. Mavrotheris [5] also records the modulo-eight congruence; the statement was checked in the preprint, whose lattice argument was read only in part [to check]. Prior-work checks focused on the published sequence [4, 1, 2, 3, 5]; an exhaustive post-2013 preprint survey has not yet been logged [to check]. Separately, an independent public Lean 4 formalization of Agoh–Giuga counterexample structure (oddness, squarefreeness, and at least 9 prime factors; S. Schlesinger, `agoh-giuga-conjecture`, checked via web summary [to check]) precedes our Lean 4 library.

Three natural open questions remain beyond Conjecture 1. First, the local minimum under normality, single-deletion minimality, and all value-one congruences is now pinned to $\{40{,}748, 40{,}749, 40{,}750\}$ digits: which of these three values is attained? Second, can the cofactor congruence $N(P)/p \equiv 1 \pmod{p}$ be incorporated into a finite search at several small primes simultaneously? Both local witnesses already fail at $p = 5$. Third, evaluating the full fifteen-prefix certificate inside Lean 4 would move Theorems 2 and 3 from Lean + Cert into the pure kernel.

Reproducibility and Use of AI. Run `python3 recompute.py` beside `critical-edges.json.xz` and `hughes-giuga-draft5.tex`. This standard-library program executes the printed seven-line example, enumerates all fifteen prefixes below 17, verifies the count and Route (a) size bounds across all fifteen cases, and constructs and checks G, $W_{1999993}$, and W_{321169} (under three seconds wall time on an Apple M4 Max). All rounding directions in `recompute.py` are strictly conservative (upper bounds on vertex weights and $\log 10$, lower bounds on prefix budgets and $\log p$), and the script includes fault-injection assertions rejecting fabricated edges, fractional prices, and positive-tail cutoffs.

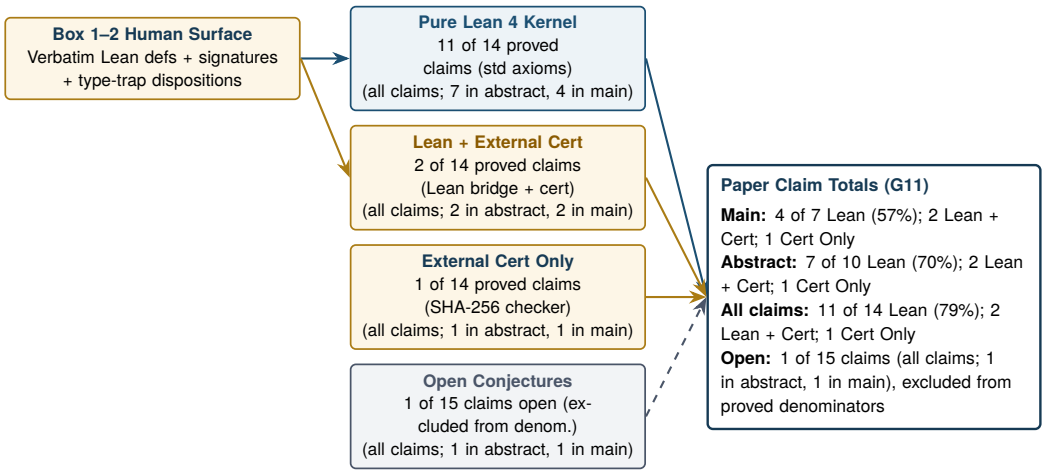
The claim ledger (`claims.md`) maps every numerical assertion to its verification output, and the Lean 4 library `lean/Giuga/` (7 files, 5,001 lines, 128 audited declarations at revision `855d12ba1`, zero `sorry`, zero `native_decide`, using Lean's standard kernel GMP arithmetic for internal bitmask checks) is detailed in Section 6; a standalone Palomar submission package is archived at `github.com/mathdiscoveries/giuga-conjecture-counterexample` (Palomar provides mechanical Lean checking and automated editorial review, not human peer review). AI research agents built and directed by Tyler B. Hughes assisted with the search, proofs, Lean 4 formalization, software, and manuscript. No human mathematician has yet refereed the proof. The reference ledger (`references-checked.md`) identifies the primary-source checks still pending.

6. FORMAL VERIFICATION & READER'S TRUST BOUNDARY

What You Must Trust to Accept This Paper:

1. **Lean 4 Kernel & Toolchain:** leanprover/lean4:v4.35.0; committed axiom receipt anchored to git commit 855d12ba1c80 (independent gate-box kernel replay pending); standard axioms only (propext, Classical.choice, Quot.sound).
2. **Core Definitions & Fidelity (Boxes 1–2):** Verify that the verbatim Lean definitions in Box 1 match Section 2 and that each Lean signature in Box 2 matches its stated theorem.
3. **External Certificates & Written Proofs:** 1 SHA-256-pinned external artifact(s) plus any claims marked Written or Unsettled in Table 4 below.

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



Anti-Shortcut Audit Strip — Source-Level Approx (Gate Replay Pending)

WARN: Committed receipt (gate replay pending) | PASS: sorry/admit: 0 (per committed receipt)
PASS: native_decide: 0 (per committed receipt) | PASS: Custom axioms & meta: 0 (per committed receipt)
PASS: Coverage: 128/128 public theorems (source-level approx) | WARN: Fidelity: 13/13 exact (draft cross-family)
WARN: Witnesses: pending gate replay | WARN: Human referee: pending

Box 1 — Verbatim Lean 4 Custom Definitions (Human Audit Surface)

Giuga.IsGiugaCounterexample (Giuga/Defs.lean:30-31) — Section 1, Conjecture 1

```
def IsGiugaCounterexample (n : ℕ) : Prop :=
  2 ≤ n ∧ ¬ Nat.Prime n ∧ (∑ k ∈ Finset.Ico 1 n, k ^ (n - 1)) ≡ n - 1 [MOD n]
```

Giuga.IsCarmichaelCondition (Giuga/Defs.lean:35-36) — Section 2, eq. (1)

```
def IsCarmichaelCondition (n : ℕ) : Prop :=
  ∀ p, Nat.Prime p → p ∣ n → (p - 1) ∣ (n / p - 1)
```

Giuga.IsGiugaCondition (Giuga/Defs.lean:39-40) — Section 2, eq. (1)

```
def IsGiugaCondition (n : ℕ) : Prop :=
  ∀ p, Nat.Prime p → p ∣ n → p ∣ (n / p - 1)
```

Giuga.IsNormalOddPrimeSet (Giuga/Defs.lean:44-45) — Section 2

```
def IsNormalOddPrimeSet (P : Finset ℕ) : Prop :=
  (∀ p ∈ P, Nat.Prime p ∧ Odd p) ∧ (∀ q ∈ P, ∀ r ∈ P, q < r → ¬ (q ∣ r - 1))
```

Giuga.IsConflictEdge (Giuga/LemmaW.lean:36-37) — Section 3

```
def IsConflictEdge (q r : ℕ) : Prop :=
  q < r ∧ q ∣ r - 1
```

Giuga.IsTailPrime (Giuga/LemmaW.lean:41-42) — Section 3

```
def IsTailPrime (S : Finset ℕ) (p_d x : ℕ) : Prop :=
  Nat.Prime x ∧ Odd x ∧ p_d ≤ x ∧ ∀ s ∈ S, ¬ (s ∣ x - 1)
```

Giuga.IsIndependent (Giuga/LemmaW.lean:46-47) — Section 3, Lemma 11

```
def IsIndependent (E : Finset (ℕ × ℕ)) (A : Finset ℕ) : Prop :=
  ∀ e ∈ E, ¬ (e.1 ∈ A ∧ e.2 ∈ A)
```

Giuga.need (Giuga/LemmaW.lean:32-33) — Section 3

```
noncomputable def need (S : Finset ℕ) : ℝ :=
  1 - ∑ s ∈ S, (1 : ℝ) / (s : ℝ)
```

Giuga.edgeDualUB (Giuga/LemmaW.lean:57-60) — Section 3, eq. (3)

```
noncomputable def edgeDualUB (U : Finset ℕ) (E : Finset (ℕ × ℕ))
    (w : ℕ → ℝ) (η : ℕ × ℕ → ℝ) : ℝ :=
  (∑ e ∈ E, η e) +
    ∑ v ∈ U, max 0 (w v - ∑ e ∈ E.filter (fun e => e.1 = v ∨ e.2 = v), η e)
```

Giuga.routeALiftK (Giuga/UnconditionalAndDigits.lean:1196-1197) — Section 3.2–3.3

```
def routeALiftK (sCard K : ℕ) : ℕ :=
  K + (6 - (sCard + K) % 4) % 4
```

Selected Concrete Sanity Examples (checked in Lean; examples only, not global identity proofs): Giuga.swarPopcountUp_survivorMask (swarPopcountUp 16 survivorMask = 8134); Giuga.swarPopcountUp_mask4211 (swarPopcountUp 16 (survivorMask &&& ((1 «< 2105) - 1)) = 574); Giuga.checkLeaf3000_empty (checkLeaf3000 false 9 312 packedEdges3000Empty 1000000 574 = true); Giuga.checkLeaf3000_three (checkLeaf3000 true 7 108 packedEdges3000Three 666666 586 = true).

Box 2 — Verbatim Main Theorem Signatures, Context Binders & Applicability

Giuga.cor_giuga_8138_primes (Giuga/CeilingAndRules.lean:703-728) src:8cfdbabd156b1a

```
theorem cor_giuga_8138_primes
    (hN1 : ∀ P : Finset ℕ, IsNormalOddPrimeSet P → (1 : ℝ) < ∑ p ∈ P, (1 : ℝ) / (p :
      ↪ ℝ) →
      8135 ≤ P.card)
    {n : ℕ} (hn : IsGiugaCounterexample n) :
    8138 ≤ n.primeFactors.card
```

Assumptions: Conditional on hN1 (every normal odd prime set with reciprocal sum > 1 has >= 8,135 primes, discharged by recompute.py across all 15 prefixes below 17) and hypothetical Giuga counterexample n. Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.cor_giuga_route_a_gt_10_pow_40747 (Giuga/UnconditionalAndDigits.lean:1259-1330) src:9a3a3ae224e41d

```
theorem cor_giuga_route_a_gt_10_pow_40747
    (hN1 : ∀ P : Finset ℕ, IsNormalOddPrimeSet P → (1 : ℝ) < ∑ p ∈ P, (1 : ℝ) / (p :
      ↪ ℝ) →
      8135 ≤ P.card)
    {F : Finset (Finset ℕ)}
    (hF : ∀ S : Finset ℕ, IsNormalOddPrimeSet S → (∀ s ∈ S, s < 17) → S ∈ F)
    (K : Finset ℕ → ℕ)
    (μ ν C : Finset ℕ → ℝ)
    (U : Finset ℕ → Finset ℕ)
    (E : Finset ℕ → Finset (ℕ × ℕ))
    (η : Finset ℕ → ℕ × ℕ → ℝ)
    (hTailK : ∀ P : Finset ℕ, IsNormalOddPrimeSet P →
      (1 : ℝ) < ∑ p ∈ P, (1 : ℝ) / (p : ℝ) →
      K (P.filter (· < 17)) ≤ (P.filter (17 ≤ ·)).card)
    (hCert : ∀ S ∈ F,
      0 ≤ μ S ∧ 0 ≤ ν S ∧ 0 < C S ∧
      μ S / C S + ν S - Real.log (C S) ≤ 0 ∧
      (∀ x, IsTailPrime S 17 x → (x : ℝ) < C S → x ∈ U S) ∧
      (∀ e ∈ E S, e.1 ∈ U S ∧ e.2 ∈ U S ∧ IsConflictEdge e.1 e.2) ∧
      (∀ e ∈ E S, 0 ≤ η S e) ∧
      (40747 : ℝ) * Real.log 10 <
        (∑ s ∈ S, Real.log (s : ℝ)) + μ S * need S +
          ν S * (routeALiftK S.card (K S) : ℝ) -
          edgeDualUB (U S) (E S) (fun x => μ S / (x : ℝ) + ν S - Real.log (x : ℝ)) (η
            ↪ S))
    {n : ℕ} (hn : IsGiugaCounterexample n) :
    10 ^ 40747 < n
```

Assumptions: Conditional on hN1, prefix cover hF, per-prefix tail count bounds hTailK, and depth-6 Route (a) logarithmic certificates hCert (established by recompute.py + critical-edges.json.xz on {5,7,13} and zero-edge C = 200,000 bounds on the other 14 prefixes via Prop. 12 and frontier completeness) and hypothetical Giuga counterexample n. Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.exists_normal_odd_prime_set_8135 (Giuga/Witness8135.lean:1117-1123) src:ff6cc9831e0dce

```
theorem exists_normal_odd_prime_set_8135 :
    ∃ G : Finset ℕ, IsNormalOddPrimeSet G ∧ G.card = 8135 ∧
      (1 : ℚ) < (∑ p ∈ G, (1 : ℚ) / (p : ℚ)) ∧
      (1 : ℝ) < (∑ p ∈ G, (1 : ℝ) / (p : ℝ)) ∧
      10 ^ 40732 < (∏ p ∈ G, p) ∧ (∏ p ∈ G, p) < 10 ^ 40733
```

Assumptions: Closed existential statement with zero free hypotheses; verified unconditionally by pure-kernel reduction. Applicability: Unconditional (closed statement; no outer premise witness needed).

Giuga.exists_ceiling_witness_8138 (Giuga/Witness8135.lean:1171-1189) src:572a573a412ad8

```
theorem exists_ceiling_witness_8138 :
    ∃ W : Finset ℕ,
      IsNormalOddPrimeSet W ∧
      W.card = 8138 ∧
      3 ∉ W ∧
      (1 : ℝ) < (∑ p ∈ W, (1 : ℝ) / (p : ℝ)) ∧
      (∀ p ∈ W, (∑ q ∈ W.erase p, (1 : ℝ) / (q : ℝ)) ≤ 1) ∧
      ((W.filter (fun p => p % 4 = 3)).card % 4 = 0 ∨
        (W.filter (fun p => p % 4 = 3)).card % 4 = 1) ∧
      (∑ p ∈ W, p) ≡ 1 + (∏ p ∈ W, p) [MOD 8] ∧
      10 ^ 40750 < (∏ p ∈ W, p) ∧
      (∏ p ∈ W, p) < 10 ^ 40751
```

Assumptions: Closed existential statement with zero free hypotheses; verified unconditionally by pure-kernel reduction. Applicability: Unconditional (closed statement; no outer premise witness needed).

Giuga.giuga_unconditional_578_primes (Giuga/UnconditionalAndDigits.lean:1002-1024) src:a90fbe4271f3b4

```
theorem giuga_unconditional_578_primes {n : ℕ} (hn : IsGiugaCounterexample n) :
    578 ≤ n.primeFactors.card
```

Assumptions: Zero external hypotheses; applies to any hypothetical Giuga counterexample n (vacuously true if Giuga's conjecture holds). Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.giuga_unconditional_gt_10_pow_1803 (Giuga/UnconditionalAndDigits.lean:1033-1073) src:74bc6bf4982700

```
theorem giuga_unconditional_gt_10_pow_1803 {n : ℕ} (hn : IsGiugaCounterexample n) :
    10 ^ 1803 < n
```

Assumptions: Zero external hypotheses; applies to any hypothetical Giuga counterexample n (vacuously true if Giuga's conjecture holds). Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.giuga_iff_carmichael_and_giuga (Giuga/Defs.lean:222-278) src:acc789bd4fb790

```
theorem giuga_iff_carmichael_and_giuga {n : ℕ} (hn : 2 ≤ n) (hnp : ¬ Nat.Prime n) :
    IsGiugaCounterexample n ↔ IsCarmichaelCondition n ∧ IsGiugaCondition n
```

Assumptions: Any composite natural number n >= 2. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Giuga.giuga_exists_value (Giuga/Defs.lean:389-443) src:2c1bfd89a36f69

```
theorem giuga_exists_value {n : ℕ} (hn : IsGiugaCounterexample n) :
    ∃! v : ℕ, 1 ≤ v ∧ ∑ p ∈ n.primeFactors, n / p = v * n + 1
```

Assumptions: Any hypothetical Giuga counterexample n (vacuously true if Giuga's conjecture holds). Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.edge_dual_le_ub_of_independent (Giuga/LemmaW.lean:154-200) src:15718e83120f51

```
theorem edge_dual_le_ub_of_independent {U A : Finset ℕ} {E : Finset (ℕ × ℕ)}
    {w : ℕ → ℝ} {η : ℕ × ℕ → ℝ}
    (hsub : A ⊆ U) (hind : IsIndependent E A) (hη : ∀ e ∈ E, 0 ≤ η e) :
    (∑ x ∈ A, w x) ≤ edgeDualUB U E w η
```

Assumptions: Any finite graph (U, E), independent subset A subseteq U, real weights w, and nonnegative edge prices eta >= 0. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Giuga.lemma_w_refinement1 (Giuga/LemmaW.lean:457-484) src:cad288cbab1af0

```
theorem lemma_w_refinement1 {S T U : Finset ℕ} {E : Finset (ℕ × ℕ)}
    {p_d : ℕ} {Λ : ℝ} {η : ℕ × ℕ → ℝ}
    (hT : IsNormalOddPrimeSet T)
    (hTail : ∀ x ∈ T, IsTailPrime S p_d x)
    (hneed : need S < ∑ x ∈ T, (1 : ℝ) / (x : ℝ))
    (hΛ : 0 < Λ)
    (hU : ∀ x, IsTailPrime S p_d x → (x : ℝ) < Λ → x ∈ U)
    (hE : ∀ e ∈ E, e.1 ∈ U ∧ e.2 ∈ U ∧ IsConflictEdge e.1 e.2)
    (hη : ∀ e ∈ E, 0 ≤ η e) :
    Λ * need S - edgeDualUB U E (fun x => Λ / (x : ℝ) - 1) η < (T.card : ℝ)
```

Assumptions: Any prefix S, normal tail T of primes >= p_d compatible with S with sum 1/p > need(S), cutoff Lambda > 0, valid conflict graph (U, E), and nonnegative prices eta >= 0. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Giuga.lemma_w_refinement2 (Giuga/LemmaW.lean:517-549) src:0666a5eeaba8d9

```
theorem lemma_w_refinement2 {S T U : Finset ℕ} {E : Finset (ℕ × ℕ)}
    {p_d K : ℕ} {μ ν C : ℝ} {η : ℕ × ℕ → ℝ}
    (hT : IsNormalOddPrimeSet T)
    (hTail : ∀ x ∈ T, IsTailPrime S p_d x)
    (hneed : need S < ∑ x ∈ T, (1 : ℝ) / (x : ℝ))
    (hK : K ≤ T.card)
    (hμ : 0 ≤ μ) (hν : 0 ≤ ν) (hC : 0 < C)
    (hfC : μ / C + ν - Real.log C ≤ 0)
    (hU : ∀ x, IsTailPrime S p_d x → (x : ℝ) < C → x ∈ U)
    (hE : ∀ e ∈ E, e.1 ∈ U ∧ e.2 ∈ U ∧ IsConflictEdge e.1 e.2)
    (hη : ∀ e ∈ E, 0 ≤ η e) :
    μ * need S + ν * (K : ℝ) -
        edgeDualUB U E (fun x => μ / (x : ℝ) + ν - Real.log (x : ℝ)) η ≤
      ∑ x ∈ T, Real.log (x : ℝ)
```

Assumptions: Any prefix S, normal tail T with |T| >= K and sum 1/p > need(S), multipliers mu, nu >= 0 and cutoff C > 0 with mu/C + nu - log C <= 0, valid conflict graph (U, E), and nonnegative prices eta >= 0. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Giuga.giuga_card_mod_eight (Giuga/UnconditionalAndDigits.lean:205-258) src:56cf073a4acde9

```
theorem giuga_card_mod_eight {n v : ℕ} (hn : IsGiugaCounterexample n)
    (hv : ∑ p ∈ n.primeFactors, n / p = v * n + 1) :
    n.primeFactors.card ≡ v + 1 [MOD 8]
```

Assumptions: Any hypothetical Giuga counterexample n and its unique integer value v satisfying sum_{p | n} n/p = v*n + 1. Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

Giuga.lemma_C_general (Giuga/CeilingAndRules.lean:41-163) src:5db21805a655d6

```
theorem lemma_C_general {N₁ q : ℕ}
    (hN1 : ∀ P : Finset ℕ, IsNormalOddPrimeSet P → (1 : ℝ) < ∑ p ∈ P, (1 : ℝ) / (p :
      ↪ ℝ) →
      N₁ ≤ P.card)
    (hq : ((Finset.range q).filter (fun p => Nat.Prime p ∧ Odd p)).card < N₁)
    {P : Finset ℕ} (hP : IsNormalOddPrimeSet P)
    (hsum : (2 : ℝ) < ∑ p ∈ P, (1 : ℝ) / (p : ℝ)) :
    N₁ + q ≤ P.card
```

Assumptions: Any threshold N1, integer q with fewer than N1 odd primes below q, normal-set floor hN1, and normal odd prime set P with sum 1/p > 2. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Table 3. Lean 4 Type-Trap Audit Checklist — Source-Level Approximation (Gate Replay Pending).[a]

Declaration	Hazard	Operand	Category	Audited Disposition & Guard
IsCarmichaelCondition	nat_sub	- 1	intended_convention	Every prime p satisfies p >= 2; all consumers (giuga_iff_carmichael_and_giuga) supply 2 <= n, so p | n implies n / p >= 1 and exact subtraction in N.
IsCarmichaelCondition	nat_div	/ p	intended_convention	Guarded directly by the explicit hypothesis p | n inside the universal quantifier.
IsConflictEdge	nat_sub	- 1	intended_convention	Since q < r in N, r >= 1, so r - 1 is exact subtraction.
IsGiugaCondition	nat_div	/ p	intended_convention	Guarded directly by p | n inside the universal quantifier; all consumers (giuga_iff_carmichael_and_giuga, squarefree_of_giuga_condition) supply 1 <= n.
IsGiugaCondition	nat_sub	- 1	intended_convention	Consumers supply n >= 1 with p | n (giuga_iff_carmichael_and_giuga, squarefree_of_giuga_condition), so n / p >= 1 and n / p - 1 is exact.
IsGiugaCounterexample	real_log_rpow	^ (n - 1)	intended_convention	Standard natural-number power k ^ (n - 1) with n >= 2 (not Real.rpow).
IsGiugaCounterexample	nat_sub	- 1	intended_convention	Explicitly guarded by the first conjunct 2 <= n.
IsNormalOddPrimeSet	nat_sub	- 1	intended_convention	Every element r of P is an odd prime (r >= 3), so r - 1 >= 2 is exact.
IsTailPrime	nat_sub	- 1	intended_convention	Explicitly guarded by Nat.Prime x and Odd x, so x >= 3 and x - 1 is exact.

Declaration	Hazard	Operand	Category	Audited Disposition & Guard
cor_giuga_8138_primes	real_div	(p : ℝ)	intended_convention	Every p in P satisfies Nat.Prime p (hence p >= 3 > 0) under IsNormalOddPrime Set P.
cor_giuga_route_a_gt_10_pow_40747	real_div	(p : ℝ)	intended_convention	Every p in P is an odd prime (p >= 3 > 0) under IsNormalOddPrimeSet P.
cor_giuga_route_a_gt_10_pow_40747	nat_div	/ C	intended_convention	Real division (not Nat division) explicitly guarded by 0 < C S in hCert.
cor_giuga_route_a_gt_10_pow_40747	real_log_rpow	Real.log	intended_convention	Real.log is evaluated at 10 > 0, primes >= 3, C S > 0, and arbitrary vertices x in U S; any non-positive vertex in U S only adds a nonnegative max 0 (...) term to edgeDual UB and cannot weaken the lower bound.
cor_giuga_route_a_gt_10_pow_40747	real_div	(x : ℝ)	intended_convention	On tail primes x in T, x >= 17 > 0; U S is arbitrary and any junk vertex in U S only adds a nonnegative max 0 (...) term to edgeDualUB, so the lower bound remains sound.
edgeDualUB	nat_sub	- ∑	intended_convention	Exact real subtraction inside max 0 (...); source scanner flags '-' over-approximately.
exists_ceiling_witness_8138	real_div	(p : ℝ)	intended_convention	Every p in W is an odd prime (p >= 5 > 0) under IsNormalOddPrimeSet W.
exists_ceiling_witness_8138	real_div	(q : ℝ)	intended_convention	Every q in W.erase p belongs to W, hence is an odd prime >= 5 > 0.
exists_ceiling_witness_8138	nat_mod	% 4	intended_convention	Standard Euclidean remainder modulo 4 matching mathematical congruence mod 4.
exists_normal_odd_prime_set_8135	nat_div	/ (p : ℚ)	intended_convention	Rational division (not Nat division) with prime denominator p >= 3 > 0 under Is NormalOddPrimeSet G.
exists_normal_odd_prime_set_8135	real_div	(p : ℝ)	intended_convention	Every p in G is an odd prime (p >= 3 > 0) under IsNormalOddPrimeSet G.
giuga_card_mod_eight	nat_div	/ p	intended_convention	Every p in n.primeFactors divides n, so n / p is the exact integer cofactor.
giuga_exists_value	nat_div	/ p	intended_convention	Every p in n.primeFactors divides n, so n / p is the exact integer cofactor.
lemma_C_general	real_div	(p : ℝ)	intended_convention	Every p in P is an odd prime (p >= 3 > 0) under IsNormalOddPrimeSet P.
lemma_C_general	finset_range	Finset.range	intended_convention	Intended exclusive upper bound matching the prose statement 'fewer than N1 odd primes strictly below q'.
lemma_w_refinement1	real_div	(x : ℝ)	intended_convention	Every x in T is an odd prime (>= 3 > 0); U is an arbitrary superset of tail primes < Lambda and any non-tail vertex in U only adds a nonnegative max 0 (...) term to edgeDualUB.
lemma_w_refinement1	nat_sub	- edgeDualUB	intended_convention	Exact subtraction in R; source scanner flags '-' over-approximately.
lemma_w_refinement2	real_div	(x : ℝ)	intended_convention	Every x in T is an odd prime (>= 3 > 0); U is an arbitrary superset of tail primes < C and any non-tail vertex in U only adds a nonnegative max 0 (...) term to edge DualUB.
lemma_w_refinement2	nat_div	/ C	intended_convention	Real division (not Nat division) explicitly guarded by hypothesis hC : 0 < C.
lemma_w_refinement2	real_log_rpow	Real.log	intended_convention	Explicitly guarded by 0 < C and Nat. Prime x for all x in T; any non-positive vertex in arbitrary U only adds a nonnegative max 0 (...) term to edgeDual UB.
need	real_div	(s : ℝ)	intended_convention	Defined for arbitrary S : Finset N (the general lemmas hold for arbitrary S); in all paper applications S is a finite set of odd primes (s >= 3 > 0).
routeALiftK	nat_sub	- (sCard + K)	intended_convention	Since (sCard + K) % 4 <= 3 < 6, the difference 6 - (sCard + K) % 4 lies in {3, 4, 5, 6} with zero truncation; verified by routeALiftK_spec.

Declaration	Hazard	Operand	Category	Audited Disposition & Guard
`routeALiftK`	`nat_mod`	`% 4`	intended_convention	Standard Euclidean remainder mod 4; routeALiftK_spec proves sCard + route ALiftK sCard K = 2 (mod 4).
`instDecidableIsIndependent`	`local_instance_or_notation`	`instDecidableIsIndependent`	intended_convention	Trivial decidability instance unfolding Is Independent to Finset universal quantification; no custom reduction or notation.

[a] Covers the specified Lean 4 hazard set (`Nat` subtraction/division/mod, totalized real/rational division, `Real.log`/`rpow`, `Finset.range`, `Classical.choose`, local instances); no finite checklist certifies all semantics.

Table 4. 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
Conj. 1: Giuga conjecture (1950): no composite n > 1 satisfies sum_{k=1}^{n-1} k^(n-1) = -1 (mod n)	Unsettled	Open conjecture	Lean: none; fidelity: n/a	Explicitly open conjecture (predicate defined in Lean as Giuga.IsGiugaCounterexample; excluded from G11 denominators).
Thm. 2: Every Giuga counterexample has >= 8,138 distinct prime divisors	Lean + Cert	`Giuga.cor_giuga_8138_primes` + recompute.py (d178adc45519) [archived; replay pending]	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 conditional deduction from hN1; external exact-integer checker recompute.py + critical-edges.json.xz discharges hN1 across all 15 prefixes below 17.
Thm. 3: Every Giuga counterexample satisfies n > 10^40,747 (>= 40,748 decimal digits)	Lean + Cert	`Giuga.cor_giuga_route_a_gt_10_pow_40747` + recompute.py (d178adc45519) [archived; replay pending]	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 conditional Route (a) lift from hN1, hF, hTailK, and per-prefix certificates hCert; external exact-integer checker recompute.py + critical-edges.json.xz establishes all 15 prefixes (10,934 edge prices on {5,7,13}, zero-edge C = 200,000 bounds >= 69,620 digits on the other 14).
Thm. 4: Normal-set minima 8,135 primes / 40,733 digits; local value-one class minimum 8,138 primes and 40,748–40,750 digits	Cert Only	recompute.py (d178adc45519) [archived; replay pending]	External cert only; fidelity: n/a	External exact-integer checker recompute.py + critical-edges.json.xz certifies lower bounds and W_321169 (40,750 digits); Lean 4 unconditionally verifies witnesses G and W_1999993 (Thms. 5–6) and conditionally proves cardinality exactness from hN1.
Thm. 5: Unconditional Lean 4 8,135-prime normal set G with |G| = 8,135, sum 1/p > 1, 10^40,732 < N(G) < 10^40,733	Lean Kernel	`Giuga.exists_normal_odd_prime_set_8135`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel (zero external certificate hypotheses).
Thm. 6: Unconditional Lean 4 seven-rule ceiling witness W with |W| = 8,138 and 10^40,750 < N(W) < 10^40,751	Lean Kernel	`Giuga.exists_ceiling_witness_8138`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel (zero external certificate hypotheses).
Thm. 7: Unconditional Lean 4 counterexample lower bound >= 578 distinct prime divisors	Lean Kernel	`Giuga.giuga_unconditional_578_primes`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel via internal 2-prefix C = 3,000 radix-trie certificate (zero external hypotheses).
Cor. 8: Unconditional Lean 4 counterexample size bound n > 10^1,803 (>= 1,804 decimal digits)	Lean Kernel	`Giuga.giuga_unconditional_gt_10_pow_1803`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel via internal C = 3,000 certificate and prime-product lower bound.
Prop. 9: Composite n >= 2 is a Giuga counterexample <-> Carmichael and Giuga divisibility conditions hold	Lean Kernel	`Giuga.giuga_iff_carmichael_and_giuga`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel for all composite n >= 2.

Paper Claim	Proof Tier	Lean Decl / Artifact	Actual Axioms & Fidelity	Assumptions & What You Must Trust
Prop. 10: Every Giuga counterexample has a unique integer value v >= 1 with sum_{p ∣ n} n/p = v*n + 1	Lean Kernel	`Giuga.giuga_exists_value`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel over IsGiugaCounterexample.
Lem. 11: Lemma W: Edge-price upper bound sum_{p in I} w_p <= D(w, eta) for any independent set I	Lean Kernel	`Giuga.edge_dual_le_ub_of_independent`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel for any finite graph (U, E), independent set, real weights, and eta >= 0.
Prop. 12: Lemma W (Refinement 1): Count lower bound C*h - D(w, eta) < |T| for w_p = C/p - 1	Lean Kernel	`Giuga.lemma_w_refinement1`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel for any normal tail T compatible with prefix S and cutoff C > 0.
Prop. 13: Lemma W (Refinement 2): Size lower bound mu*h + nu*K - D(f, eta_prime) <= sum_{p in T} log p	Lean Kernel	`Giuga.lemma_w_refinement2`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel for mu, nu >= 0, C > 0 with mu/C + nu - log C <= 0, and |T| >= K.
Prop. 14: Modulo-8 count congruence |P| = v + 1 (mod 8) for every Giuga counterexample	Lean Kernel	`Giuga.giuga_card_mod_eight`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel over IsGiugaCounterexample and its value v.
Lem. 15: Lemma C: Higher-value crossing implies |P| >= N1 + q when sum 1/p > 2	Lean Kernel	`Giuga.lemma_C_general`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	Lean 4 + Mathlib pure kernel for any normal-set floor N1 and threshold q with < N1 odd primes below q.

[a] Allowed pure-kernel axioms: `propext`, `Classical.choice`, `Quot.sound`. Actual axioms printed above are read directly from verified outputs. Provenance nonce: e3a815a4d0a8 | Lean mode: committed_receipt | Closure SHA-256: b03b5a113783 | Git anchor: 855d12ba1c80 | Axioms SHA-256: e10ef18034fc | Fidelity SHA-256: bd56774ba449. External validation receipts: Palomar record.

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

REFERENCES

(1) E. Bedocchi, *Nota ad una congettura sui numeri primi*, Riv. Mat. Univ. Parma (4) **11** (1985), 229–236. Zbl 0598.10018.

(2) D. Borwein, J. M. Borwein, P. B. Borwein and R. Girgensohn, *Giuga's conjecture on primality*, American Mathematical Monthly **103** (1996), 40–50. doi:10.1080/00029890.1996.12004697.

(3) J. M. Borwein, C. Maitland and M. Skerritt, *Computation of an improved lower bound to Giuga's primality conjecture*, Integers **13** (2013), A67. Zbl 1284.11002.

(4) G. Giuga, *Su una presumibile proprietà caratteristica dei numeri primi*, Ist. Lombardo Sci. Lett., Rend., Cl. Sci. Mat. Natur., III. Ser. **14**(83) (1951), 511–518. Zbl 0045.01801.

(5) N. Mavrotheris, *Characteristic-vector congruences for weak primary pseudoperfect and Giuga numbers*, Zenodo preprint (2026). doi:10.5281/zenodo.22085830.