How many prime factors could a counterexample to Giuga's conjecture have?

Tyler Hughes [co-author]

AI-assisted research draft. Prepared for mathematical review by the authors before submission.

Abstract

Giuga asked whether a power-sum congruence shared by every prime can hold for a composite integer. The prime divisors of such an integer must have reciprocals summing to more than one, although many pairs of small primes cannot occur together. We prove that every counterexample has at least 8,138 prime divisors and 40,748 decimal digits. The published bound of Borwein, Maitland and Skerritt was 4,771 divisors and 19,908 digits. We attach a nonnegative price to each forbidden pair. An admissible set can collect this price at most once, which bounds both the reciprocal weight it can gain and the product it must pay for that weight. Exact arithmetic on fifteen cases proves that 8,135 factors and 40,733 digits are both attainable and minimal under the reciprocal and pairwise conditions alone. A congruence on the factor count gives the stronger bound for counterexamples. The accompanying integer checker replays the finite inequalities. Lean 4 separately verifies a smaller bound and the original two explicit sets. A smaller local witness is checked by the integer replay. The existence of a composite solution remains open.

MSC 2020 11A41, 11Y11, 90C05. **Keywords** Giuga's conjecture, normal prime sets, maximum flow.

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]. 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 1. *If $n > 1$ is composite and $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n$, then n has at least* 8,138 *distinct prime divisors and $n > 10^{40,747}$.*

Theorem 2. *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*. One set attains both. If one also imposes the value-one congruences and the single-deletion test in Section 4.1, the minimum cardinality becomes* 8,138*. The minimum number of digits under these added conditions lies between* 40,748 *and* 40,750*, inclusive.*

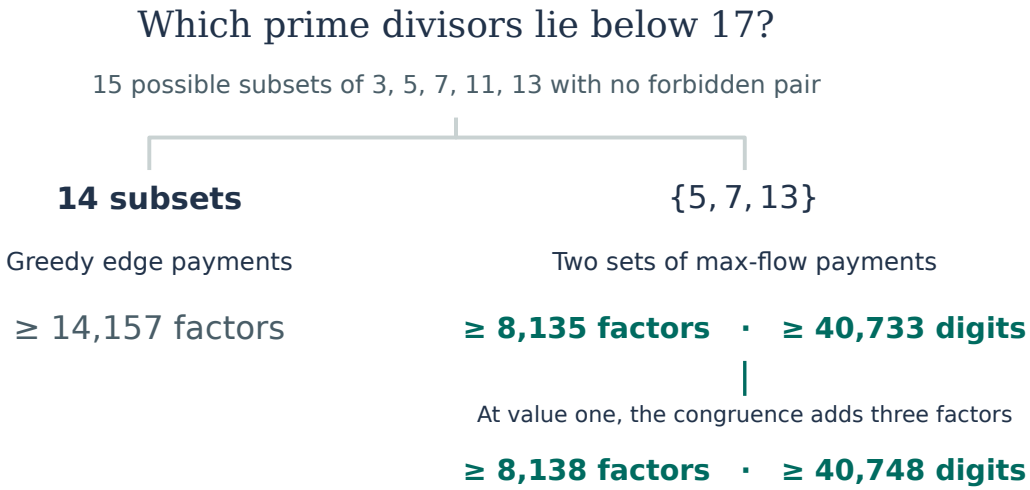


Figure 1. Splitting at 17 leaves one tight case. For the other fourteen, even the smallest certified count gives a product larger than $10^{52{,}619}$. An integer replay proves the displayed lower bounds. Lean checks a set attaining each factor count, and an internal proof gives 578 factors for a counterexample. At value two or higher, the crossing argument gives 91,476 factors. The existence question stays open.

A calculation to try. 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.

```
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)   # more than eight factors
```

For a larger graph one vertex belongs to several forbidden pairs. 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 $\operatorname{digits}(N) = 1 + \lfloor \log_{10} N \rfloor$.

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. Hence every prime divisor satisfies

$$p - 1 \mid n - 1, \qquad n/p \equiv 1 \pmod{p}. \tag{1}$$

Conversely the second condition forces n to be squarefree. The residue calculation at each prime and the Chinese remainder theorem then give the original congruence. An even squarefree composite would have an odd divisor p and an even number $p-1$ dividing the odd number $n-1$. Thus n is odd and $n = N(P)$ for its prime-factor set P. If $q \mid r-1$ for $q, r \in P$, the first condition in (1) would give $q \mid n-1$, contradicting $q \mid n$. This proves normality.

Modulo any $p \in P$, exactly one term of $\sum_{r\in P} n/r$ survives, and it is 1 by (1). Consequently

$$\sum_{p\in P} n/p = vn + 1, \qquad \sigma(P) = v + 1/n, \qquad v \geq 1. \tag{2}$$

The integer v is positive because the sum on the left exceeds one. Theorem 2 starts by retaining only normality and $\sigma(P) > 1$. Keeping the integer v will distinguish a 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 $C \geq b$, let U consist of the primes p with $b \leq p < C$ 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. An edge can therefore cover an allowance at both endpoints while being charged at most once to the selected set.

Lemma W (edge payments)**.** *Assign each edge e a price $\eta_e \geq 0$. For any real vertex weights w_p and independent set $I \subset U$,*

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

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

Proof. At each selected vertex add the incident prices to the positive residual on the right. This covers its entire weight. When these inequalities are summed, each edge price appears at most once because its endpoints cannot both be selected. Including the residuals at unselected vertices can only increase the right-hand side. □

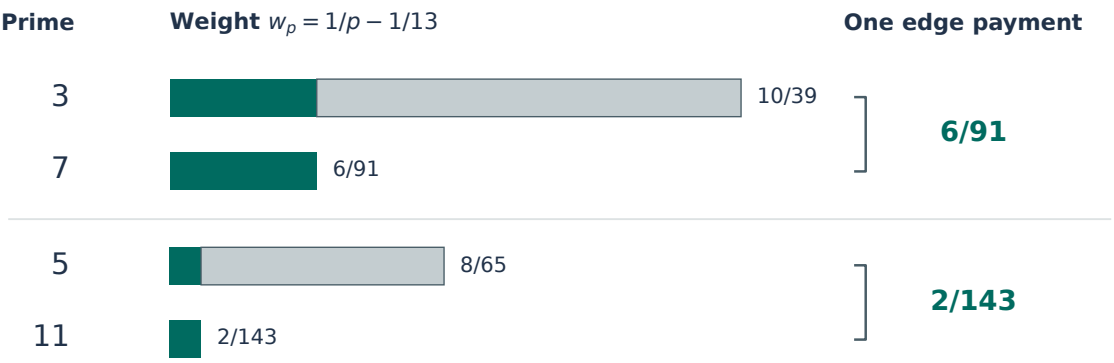


Figure 2. In each pair the dark segment is the edge price at both endpoints. Charge it once. The pale segment at the larger-weight vertex is the only residual to pay. With no edge between 3 and 5, selecting both attains the bound $D = w_3 + w_5 = 74/195$.

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. Take $w_p = C/p - 1$. All primes beyond the cutoff have nonpositive weight, so

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

Thus an upper bound on D gives the integer lower bound

$$|T| \geq K = \lfloor Ch - D(w, \eta) \rfloor + 1. \tag{4}$$

Pricing a product. Choose $\mu, \nu \geq 0$ with $f(C) \leq 0$ for $f(x) = \mu/x + \nu - \log x$. Since f decreases, $\sum_{p \in T} f(p)$ is bounded above by $D(f, \eta')$ for any second price vector η'. Using (4) gives

$$\log N(P) \;\geq\; \sum_{s \in S} \log s + \mu h + \nu K - D(f, \eta'). \tag{5}$$

The coefficient of K is ν. If arithmetic forces three additional factors in the tail, the same prices certify an extra 3ν in the lower bound for $\log N(P)$.

3.1 What the value adds

For an odd squarefree n satisfying (1) and (2), write $m = |P|$ and $k_3 = |\{p \in P : p \equiv 3 \bmod 4\}|$. For each p, the Legendre symbol $(\frac{n/p}{p})$ equals one. Multiply these symbols over P. The two factors associated with each unordered pair contribute -1 exactly when both primes are 3 modulo 4, by quadratic reciprocity. Hence $\binom{k_3}{2}$ is even, or $k_3 \equiv 0, 1 \bmod 4$.

Every odd square is one modulo eight. Multiplication of (2)'s first equality by n therefore gives $\sum_{p \in P} p \equiv v + n \bmod 8$. On writing $p = 1 + 2a_p$, expansion of the product gives

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

It follows that $m \equiv v + 1 \bmod 8$. When $v = 1$, even the weaker condition $m \equiv 2 \bmod 4$ raises the lower bound from 8,135 to 8,138. The smaller congruence suffices in (5).

For $v \geq 2$, order P increasingly and stop at the first prime q for which the accumulated reciprocal sum exceeds one. Such a first crossing exists by (2). The crossing prefix is normal, so it has at least 8,135 members by the finite calculation below. There are only 8,134 odd primes below 83,341, giving $q \geq 83{,}341$. The crossing sum is at most $1 + 1/q$. The remaining sum exceeds $1 - 1/q$. Each remaining reciprocal is smaller than $1/q$, so at least q further primes are needed. This yields $m \geq 91{,}476$, which more than suffices for both assertions of Theorem 1 since $n \geq m!$.

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.

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.

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	$\varnothing$	34,194
$\{5, 13\}$	19,097	$\{7\}$	27,075	$\{3\}$	37,911

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. Thus every one of these cases has $N(P) \geq 14{,}157! > 10^{52{,}619}$. Precise product prices on these prefixes would add nothing to either theorem.

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 $v = 1$ the total must be 2 modulo 4 and the tail must contain at least 8,135 primes. With ν approximately 11.898582, using this tail count in (5) gives $\log_{10} n > 40{,}747.566$. These calculations and the argument for $v \geq 2$ prove Theorem 1.

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

$$\log y = 2\sum_{j=0}^{19} \frac{t^{2j+1}}{2j+1} + R, \qquad 0 \leq R \leq \frac{2t^{41}}{41(1-t^2)}.$$

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.

4.1 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 give

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

Together with the count and product bounds above, this proves the first part of Theorem 2.

A value-one counterexample would have $\sigma(P) = 1 + 1/n$. Deleting any prime then drops the sum below one. Consider the class of normal P with $\sigma(P) > 1$ that obey this single-deletion test and the value-one congruences

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

The count and product bounds for $v = 1$ used only normality, $\sigma(P) > 1$ and $|P| \equiv 2 \bmod 4$, so they apply to this entire class.

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

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

The original witness took $x = 1{,}999{,}993$. 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 the verifier checks normality, all three congruences, $k_3 = 4{,}032$ and $0 < \sigma(W_x) - 1 < 1/x$. As $x = \max W_x$, deleting any prime drops the sum below one. The integer products give the following.

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

In particular $10^{40{,}749} < N(W_{321169}) < 10^{40{,}750}$. This proves the final assertion of Theorem 2, 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.

5 Formal verification in Lean 4

The accompanying library `Giuga` proves the reduction in Section 2, the weighted inequalities in Section 3, the congruence for m modulo eight, and the witness specifications for G and the original $W_{1999993}$. The audit of revision `c8d3c2b1` checked 128 declarations with no `sorry` or `native_decide`. The printed axioms were propositional extensionality, classical choice and quotient soundness.

Two levels of numerical evidence enter these proofs. A certificate for the two prefixes below 5 is evaluated internally. It proves 575 factors under the normal reciprocal conditions, and 578 factors with $n > 10^{1{,}803}$ for any counterexample. The witness proofs also evaluate their finite tests inside Lean. The smaller W_{321169} is verified by the integer checker in this paper. The theorem for 8,138 factors takes the universal 8,135 lower bound as a hypothesis. The formal theorem for $n > 10^{40{,}747}$ takes additional hypotheses for the prefix coverage, tail counts, prices and the corresponding logarithmic inequalities. The original full certificate supplies these data outside the kernel. Section 4 gives a shorter, separate proof of the same numerical conclusion by using the factorial estimate on fourteen prefixes. A timed run of the compact replay took under three seconds on an Apple M4 Max. The README records the interpreter and timings.

6 Prior work and open questions

Bedocchi [1] credits Giuga with the normal prime-set and reciprocal-sum reduction. Bedocchi computed the greedy sequence whose reciprocal sum first crosses one at 8,135 members. Borwein, Borwein, Borwein and Girgensohn [2] used that witness 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. They also gave the value-one count congruence modulo four. 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. 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]. Sorini's working paper [6] identifies its method as heuristic in its title. Its full argument remains unread [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].

The local minimum is now one of 40,748, 40,749, and 40,750 digits. Which of these is the first attained? For counterexamples themselves, can the congruence $N(P)/p \equiv 1 \bmod p$ be incorporated into a finite search at several small p simultaneously? Both local witnesses already fail at $p = 5$. Checking the full fifteen-prefix certificate inside Lean would separately move the largest numerical lower bounds into the kernel.

7 Data availability, reproducibility and use of AI

Run `python3 recompute.py` beside `critical-edges.json.xz`. This standard-library program executes the printed example, enumerates the prefixes, checks the count and size bounds, and constructs the three explicit sets. The README gives hashes, figure scripts, build commands and source locations. The original maximum-flow search had a separate verifier for all fifteen prefixes. A second implementation rechecked the raw prices for $\{5, 7, 13\}$ and $\{5\}$. The compact replay in this paper covers all fifteen cases. AI systems assisted with the search, proofs, software and manuscript. The reference ledger identifies the primary-source checks still pending for the authors.

References

[1] E. Bedocchi, *Nota ad una congettura sui numeri primi*, Rivista di Matematica della Università di Parma (4) **11** (1985), 229–236. Journal PDF.

[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:10.2307/2975213.

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

[4] G. Giuga, *Su una presumibile proprietà caratteristica dei numeri primi*, Istituto Lombardo di Scienze e Lettere, Rendiconti, Classe di Scienze Matematiche e Naturali, vol. 83 (1950/1951). Zbl 0045.01801.

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

[6] L. Sorini, *Un metodo euristico per la soluzione della congettura di Giuga*, Quaderni di Economia, Matematica e Statistica, Università di Urbino, no. 68 (2001). University record.