MATHDISCOVERIES
Mathematical Preprint

Working Draft

Odd Perfect Numbers with Equal Non-Special Exponents $r-1$: Exclusion Through 167, with Kernel Proofs Through 83

Tyler B. Hughes
Independent researcher. AI research agents built and directed by Tyler B. Hughes.

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

One branch of the exclusion at $r = 97$

When no parent is special

Coprime divisors

- 36 with weight 1
- 31 with weight 2

Weight gives a lower bound.

Distinct primes forced

$36 + 2 \cdot 31 = 98$

At least 98 divide the candidate, each $\equiv 1$ modulo 97.

The contradiction

$97 > 96$

At most one is special. $v_{97}(N) = 96$ bounds the rest.

ABSTRACT: For each of the 38 odd primes $r \le 167$, we exclude an odd perfect number in which every non-special prime divisor occurs to exponent $r-1$. The special prime is the unique prime divisor whose exponent is odd. Each non-special prime divisor congruent to 1 modulo r contributes one factor of r to the divisor sum, which has only $r-1$ such factors. Chains of divisors force more primes in this residue class than that count permits. For every odd prime r, Lean 4 proves that r cannot have odd exponent in an odd perfect number whose prime exponents are each odd or equal to $r-1$. The kernel proves the complete exclusion for all 22 odd primes through 83. The submitted formalization covers the first 20, through 73; we reconstruct the complete certificates at 79 and 83. For the remaining 16 primes from 89 through 167, the proof combines a written soundness argument with explicit certificates. Three exact-arithmetic checkers accept those certificates. Two share an author, and all use the same mathematical criteria. The general existence of odd perfect numbers remains open.

Verification Scope (G11): WARN: Human referee: pending
Main results: 2 of 3 in Lean Kernel (67%) · 1 Cert Only
Abstract claims: 2 of 3 in Lean Kernel (67%) · 1 Cert Only

Full Trust Boundary: Section 5.

MSC 2020: 11A25, 11Y70 **Keywords:** odd perfect numbers, factor chains, primality certificates, Lean 4

1. INTRODUCTION AND MAIN RESULTS

A number is perfect when it equals the sum of its divisors other than itself, as $6 = 1 + 2 + 3$ does. Every perfect number known is even, and nobody knows whether an odd one exists. A great many conditions that an odd perfect number would have to meet are known; for instance it would exceed 10^{1500} [13] and have at least 10 distinct prime factors [12].

Write $\sigma(n)$ for the sum of all divisors of n, so that $n > 0$ is perfect exactly when $\sigma(n) = 2n$, and $v_q(n)$ for the exponent of the prime q in n. Euler showed that an odd perfect number has the form $N = \pi^{\alpha} m^2$ with π prime, $\pi \nmid m$ and $\pi \equiv \alpha \equiv 1 \pmod 4$; we call π the *special prime*. A line of papers asks what happens when all the other exponents are equal, $v_q(N) = 2\beta$ for every prime $q \neq \pi$ dividing N. When $r = 2\beta + 1$ is prime the cases $r = 3, 5, 7, 11$ were settled by Steuerwald [14], Kanold [7], Hagis and McDaniel [6] and McDaniel and Hagis [11], and $r = 13, 17, 23, 29, 37$ by Cohen and Williams [3]. This paper settles every odd prime $r \le 167$.

Theorem 1 (r is never special). *Let $r \ge 3$ be a prime, and let N be an odd perfect number such that every prime q dividing N has $v_q(N)$ odd or $v_q(N) = r-1$. Then $v_r(N)$ is not odd.*

Kanold proved the stronger congruence $\pi \equiv 1 \pmod r$ when all non-special exponents plus one are positive powers of the same prime r [7] (Section IV). In our setting a congruence for the divisor sum gives a short proof that r cannot be the special prime.

Theorem 2 (The cases $3 \le r \le 83$). *Let r be a prime with $3 \le r \le 83$. There is no odd perfect number N for which some prime π has the property that every prime $q \neq \pi$ dividing N satisfies $v_q(N) = r-1$.*

Theorem 3 (The cases $89 \le r \le 167$). *Let r be a prime with $89 \le r \le 167$. There is no odd perfect number N for which some prime π has the property that every prime $q \neq \pi$ dividing N satisfies $v_q(N) = r-1$.*

The first interval contains 22 odd primes, the second 16.

Prime ranges and proof routes

A candidate is an odd perfect N with all non-special exponents equal to r − 1. Each mark is an odd prime r.



3 to 83 · 22 primes **89 to 167 · 16 primes**

What follows	How the proof works	How it is verified
Main theorem 1 The prime r is never special.	If r were special, removing powers of r from σ(N) = 2N would give 1 ≡ 2 mod r.	**Lean kernel** Every odd prime r.
Main theorem 2 No candidate for 3 ≤ r ≤ 83.	Follow chains of forced prime factors. Close every branch of the search.	**Lean kernel** Through 73, then 79 and 83.
Main theorem 3 No candidate for 89 ≤ r ≤ 167.	Split on the special prime. Each branch exceeds the bound in Proposition 8.	**Certificates + written proof** Three checkers, two authors.
Supporting proposition 8 At most r − 1 primes counted.	Count non-special primes q ≡ 1 mod r in N. Each contributes one factor r to σ(N).	**Written proof** For every candidate.
Supporting proposition 11 $r^{r-1}\Phi_r(r) \mid N$.	The forced factors r^{r-1} and $\Phi_r(r)$ are coprime, so their product divides N.	**Lean kernel** For every candidate.
Supporting proposition 12 Some prime $q \mid \Phi_r(r)$ has $r \mid (q-1)$ but $r^2 \nmid (q-1)$.	The prime factors are 1 modulo r. Their product is 1 + r modulo r².	**Lean kernel** Every odd prime r. No candidate hypothesis.
Open problem	Does any odd perfect number exist?	

Figure 1. Each mark represents one prime parameter. The main theorems give the non-special property and the two exclusion ranges. The supporting propositions identify which divisors a candidate must contain and which congruence holds for every odd prime.

The witness π in the definition need only be prime. Lemma 6 shows that it must coincide with Euler's special prime under the odd-perfect hypothesis. In the submitted Lean package the kernel checks the exclusions through 73. In the extension it also checks the complete certificates for 79 and 83. Above that range the proof uses checked data and the written soundness theorem. Figure 1 shows how the factor chains and the bound fit together.

McDaniel and Hagis bound the number of non-special primes in a residue class [11]. Cohen and Williams turn that bound into exclusions by following divisors of geometric sums [3]. Let $q \neq \pi$ be a prime divisor of N. Then $v_q(N) = r-1$, so q contributes the factor $\Phi(q) = \sigma(q^{r-1}) = 1+q+\cdots+q^{r-1}$ to $\sigma(N)$, and $\Phi(q)$ divides N (Lemma 6); every prime factor of $\Phi(q)$ other than r is congruent to 1 modulo r. Each such non-special prime divisor $q \equiv 1 \pmod r$ of N contributes exactly one factor r to $\sigma(N) = 2N$, while r itself divides N exactly $r-1$ times; so N has at most $r-1$ non-special prime divisors congruent to 1 modulo r (Proposition 8). A factor chain that forces r of them rules the case out. The box below runs the main case of the certificate for $r = 3$, the case of Steuerwald, in which π is none of $3, 13, 61, 97$; it gives a lower bound that contradicts Proposition 8. The three other cases of that certificate, $\pi = 13$, 61 and 97, are needed as well (Section 3).

Concept in Action: the main case of the $r = 3$ certificate

```
def phi(q):
    return q*q + q + 1
assert phi(3) == 13 and phi(13) == 3 * 61
assert phi(61) == 3 * 13 * 97 and phi(97) == 3 * 3169
forced = {13, 61, 97, 3169}
assert all(q % 3 == 1 for q in forced)
print(len(forced) - 1, '>', 3 - 1)
```

Roadmap. Section 2 identifies the exact predicates. Section 3 proves the counting obstruction, explains the coverage of the exceptional branches, and derives a forced divisor valid for every parameter. Section 4 describes the finite data and how to check them. Section 5 records which statements have kernel proofs; Section 6 compares the argument with the published literature.

2. DEFINITIONS, NOTATION, AND SETUP

All numbers are natural numbers. For natural numbers n and q, $v_q(n)$ is Mathlib's `n.factorization q`. For $n > 0$ and q prime it is the usual exponent of q in n, which is 0 when $q \nmid n$. It is 0 whenever $n = 0$ or q is not prime; so $v_q(0) = 0$ for every q, and $v_1(n) = 0$ for every n, although 1 divides every positive integer. In the main results v_q is applied only to a perfect number, and a perfect number is positive. Mathlib calls n perfect when the divisors of n below n add up to n and $n > 0$; for $n > 0$ this is $\sigma(n) = 2n$.

Definition 4. Let r and N be natural numbers.

1. N has *equal exponents* $r-1$ when there is a prime π such that every prime $q \neq \pi$ dividing N has $v_q(N) = r-1$ (`EqualExponents r N`).

2. r is *not special* when every odd perfect N whose prime divisors q each have $v_q(N)$ odd or $v_q(N) = r-1$ has $v_r(N)$ not odd (`NotSpecial r`).
3. For a natural number q, $\Phi_r(q) = \sum_{0\le j<r} q^j$, written $\Phi(q)$ when r is fixed: the empty sum 0 when $r = 0$, and $1 + q + \cdots + q^{r-1}$ when $r \ge 1$. The Lean checker's `T2.phi r q` is defined through $r-1$, so `T2.phi 0 q = 1`; for $r \ge 1$ it equals $\Phi_r(q)$ (`T2.phi_eq`). The two differ only at $r = 0$, which no main theorem admits.

The subtraction $r-1$ is the truncated subtraction of natural numbers; every main theorem statement assumes $r \ge 3$, where it is exact (the internal helper `Opn.geom_gt` admits $r = 2$). Neither definition asks that π divide N or that $\pi \equiv 1 \pmod 4$. The library proves three small facts that show what the predicates mean, each witnessing one predicate only: $2205 = 3^2 \cdot 5 \cdot 7^2$ satisfies `EqualExponents 3` (with $\pi = 5$), $3^{18}\cdot 5 = 1937102445$ satisfies `EqualExponents 19` (with $\pi = 5$), and 6 satisfies `Nat.Perfect`. None of these numbers is both odd and perfect; whether an odd perfect number exists is open, so `NotSpecial r` and the main theorems may hold vacuously (Box 2 in Section 5). Box 1 there also lists two closed checks that the kernel evaluates, `beta1Cert_checked` and `cert5_checked`: the Lean certificate checker accepts the hand-written certificate for $r = 3$ and the certificate for $r = 5$, whose flag records that the case $r = 5 \equiv 1 \pmod 4$ relies on Theorem 1. These instantiate the checker at a fixed r; they are not witnesses for N.

Throughout Section 3, r is an odd prime and $\mathrm{H}(r)$ is the hypothesis: *N is odd and perfect, and N has equal exponents $r-1$ with the prime π.*

3. PROOF OF THE MAIN RESULTS

Divisor sums and forced divisors.

Lemma 5 (Values of Φ). *Let r be an odd prime and $q \ge 2$ an integer.*

(a) *Every prime s dividing $\Phi(q)$ is r or is congruent to 1 modulo r.*

(b) *If $q \equiv 1 \pmod r$, then $\Phi(q) \equiv r \pmod{r^2}$; otherwise $r \nmid \Phi(q)$.*

(c) *$\Phi(q) > q^{r-1}$, $\gcd(\Phi(q), q) = 1$, and $\Phi(q)$ is odd when q is odd.*

Proof. (a) s divides $q^r - 1 = (q-1)\Phi(q)$, so $s \nmid q$ and the order d of q modulo s divides r. If $d = r$, then r divides $s-1$ by Fermat's theorem. If $d = 1$, then $q \equiv 1 \pmod s$, so $\Phi(q) \equiv r \pmod s$ and $s = r$. (b) If $q = 1 + rm$, then $q^j \equiv 1 + jrm \pmod{r^2}$, so $\Phi(q) \equiv r + rm \cdot r(r-1)/2 \equiv r \pmod{r^2}$, since $(r-1)/2$ is an integer. If $r \mid q$, then $\Phi(q) \equiv 1 \pmod r$. Otherwise $(q-1)\Phi(q) = q^r - 1 \equiv q - 1 \not\equiv 0 \pmod r$. (c) $\Phi(q)$ is q^{r-1} plus positive terms, is congruent to 1 modulo q, and for odd q is a sum of r odd numbers. □

Lemma 6 (Forced divisors). *Assume $\mathrm{H}(r)$. Then π divides N to an odd exponent α, $\pi \equiv \alpha \equiv 1 \pmod 4$, $\Phi(q)$ divides N for every prime $q \ne \pi$ dividing N, and $(\pi+1)/2$ divides N.*

Proof. If $\pi \nmid N$, every exponent of N is $r-1$, which is even, so $\sigma(N)$ is a product of odd numbers and cannot equal $2N$. So $\pi \mid N$, and by Euler's theorem (see [4] for a modern statement) the unique prime with an odd exponent is π, with $\pi \equiv \alpha \equiv 1 \pmod 4$. Since σ is multiplicative, $2N = \sigma(\pi^\alpha)\prod_q \Phi(q)$, and each $\Phi(q)$ is odd by Lemma 5(c), so it divides N. As α is odd, $\sigma(\pi^\alpha) = (1+\pi)(1+\pi^2+\cdots+\pi^{\alpha-1})$, so $\pi+1$ divides $2N$ and $(\pi+1)/2$ divides N. □

Lemma 7 (r divides N). *Assume $\mathrm{H}(r)$. Then r divides N.*

Proof. Kanold's fourth-power theorem implies this divisibility (Section III of [7]). We give a direct proof. Suppose $r \nmid N$ and list the primes $q \ne \pi$ dividing N as $q_1 < \cdots < q_t$, with $t \ge 1$ because N is not a prime power. No q_i is congruent to 1 modulo r, for otherwise $r \mid \Phi(q_i) \mid N$ by Lemmas 5(b) and 6. So every prime factor of $\Phi(q_i)$ is congruent to 1 modulo r, divides N, and is no q_j; it is π. Hence $\pi \equiv 1 \pmod r$ and $\Phi(q_i) = \pi^{a_i}$ with $a_i \ge 1$ for each i.

We claim $q_{i+1} > q_i^{r-1}$. Put $P = \pi^{a_i} = \Phi(q_i)$. Since Φ increases, $a_i < a_{i+1}$, so P divides $\Phi(q_{i+1})$ and hence $q_{i+1}^r - 1$; also P divides $q_i^r - 1$. Neither q_i nor q_{i+1} is 1 modulo P: $1 < q_i < P$, and $q_{i+1} \equiv 1 \pmod\pi$ would give $\Phi(q_{i+1}) \equiv r \pmod\pi$, so $\pi \mid r$, which is false. The units modulo the odd prime power P form a cyclic group whose order is divisible by r, so its elements of order r are exactly $q_i, q_i^2, \ldots, q_i^{r-1}$ modulo P. Hence $q_{i+1} \equiv q_i^j \pmod P$ for some $1 \le j \le r-1$. As $0 < q_i^j \le q_i^{r-1} < P$ (Lemma 5(c)) and $q_{i+1} \ne q_i^j$, we get $q_{i+1} \ge q_i^j + P > q_i^{r-1}$.

Since $q_1 \ge 3$ and $q_{i+1} > q_i^2$, we have $q_i - 1 \ge 9^{2^{i-2}}$ for $i \ge 2$. Also $\pi \equiv 1$ modulo both 4 and r, so $\pi \ge 4r+1 \ge 13$. Put $x = 1/9$. For every integer $k \ge 0$, repeated difference of squares gives

$$(1-x)\prod_{j=0}^{k-1}(1+x^{2^j}) = 1 - x^{2^k}.$$

At $k = t-1$ the product bounds $\prod_{i=2}^{t} q_i/(q_i-1)$ by $9/8$, including the empty product. For every prime power the divisor-sum ratio is strictly less than $p/(p-1)$. Multiplying the bounds yields

$$2 = \frac{\sigma(N)}{N} < \frac{13}{12}\cdot\frac{3}{2}\cdot\frac{9}{8} = \frac{117}{64} < 2.$$

□

The Lean theorem `Opn.r_dvd` proves Lemma 7 with the same hypotheses: N odd and perfect, π and r prime with $r \ge 3$, and $v_q(N) = r-1$ for every prime $q \ne \pi$ dividing N.

Proof of Theorem 1. Let N be as in Theorem 1 and suppose $v_r(N) = a$ is odd. If two primes had odd exponents, each would contribute an even factor $\sigma(p^k)$ and 4 would divide $\sigma(N) = 2N$ with N odd; so r is the only one, and every other prime $q \mid N$ has $v_q(N) = r-1$. For a number x write x' for x with every factor r removed. Then $2N' = \sigma(N)' = \sigma(r^a)'\prod_q \Phi(q)'$. Now $\sigma(r^a) \equiv 1 \pmod r$, and $\Phi(q)' \equiv 1 \pmod r$ for each q: when $q \equiv 1 \pmod r$ by Lemma 5(b), since then $\Phi(q) = r \cdot u$ with $u \equiv 1 \pmod r$, and otherwise because $(q-1)\Phi(q) = q^r - 1 \equiv q - 1 \pmod r$. So the right side is 1 modulo r. The left side is $2\prod_q q^{r-1} \equiv 2 \pmod r$ by Fermat's theorem. Hence $r \mid 1$,

a contradiction. For example, with $r = 5$ and $q = 11$, $\Phi(11) = 16105 = 5 \cdot 3221$ and $3221 \equiv 1 \pmod 5$. The Lean declaration `OpnChallenge.notSpecial_of_prime` proves Theorem 1 along these lines. □

The count.

Proposition 8 (At most $r-1$). *Assume* $\mathrm{H}(r)$. *Then* $v_r(N) = r-1$, *and at most* $r-1$ *primes* $q \neq \pi$ *dividing* N *are congruent to* 1 *modulo* r.

Proof. The bound is the case $Q = r$ of the lemma on pp. 25–26 of McDaniel and Hagis [11]. Yamada gives the prime-power version in Lemma 3.1 of [15]. Here the valuation also identifies the entire possible slack. By Lemma 7, $r \mid N$, and by Lemma 6 and Theorem 1, $r \neq \pi$, so $v_r(N) = r-1 = v_r(2N)$. By Lemma 5(b) each prime $q \neq \pi$ with $q \equiv 1 \pmod r$ gives $v_r(\Phi(q)) = 1$. Since $2N = \sigma(\pi^\alpha) \prod_q \Phi(q)$, the number of such q is exactly $r - 1 - v_r(\sigma(\pi^\alpha))$. □

Certificates and their soundness.

Definition 9 (Certificate). A *certificate* for an odd prime r is a finite list of cases. Exactly one is the *main case*; every other case names a prime p and assumes $\pi = p$, while the main case assumes that π is none of its parents. A case lists *parents* in order, each with a reason, and *counted numbers*, each an integer $m \geq 2$ with a count 1 or 2. The certificate must satisfy:

(P) every parent is prime, by trial division below 10^6 and above it by a Pocklington certificate;

(S) every parent q is r, or divides $\Phi(q')$ for an earlier parent q' of the same case, or, in a case $\pi = p$, divides $(p+1)/2$; and no parent of a case $\pi = p$ is p;

(C) every counted number m either divides $\Phi(q)$ for a parent q with $r \nmid m$, or is a parent with $m \equiv 1 \pmod r$; a count 2 comes with a Fermat witness $1 < a < m$ with $a^{m-1} \not\equiv 1 \pmod m$ and m not a perfect power; the counted numbers of a case are pairwise coprime;

(T) the counts of a case add to at least $r+1$, or, in a case $\pi = p$ whose counted numbers are all coprime to p, to at least r;

(E) for every parent $q \neq r$ of the main case with $q \equiv 1 \pmod 4$ there is a case $\pi = q$.

Theorem 10 (Soundness). *If a certificate for an odd prime* r *satisfies* (P), (S), (C), (T) *and* (E), *then no* N *satisfies* $\mathrm{H}(r)$.

Proof. Suppose N satisfies $\mathrm{H}(r)$. By Lemma 7 and Theorem 1, $r \mid N$ and $r \neq \pi$. If π is not a parent of the main case, the main case's assumption holds; otherwise π is a main-case parent with $\pi \equiv 1 \pmod 4$ and $\pi \neq r$, so by (E) some case $\pi = q$ holds. In the case that holds, induction along the parents shows each is a prime dividing N other than π: by (P), by the case's assumption, and by (S) with Lemma 6. Each counted number m then divides N, and its prime factors are congruent to 1 modulo r, by Lemma 5(a) or because m is such a parent. A count of 2 is honest: a Fermat witness shows that m is not prime, and a composite number that is not a perfect power has two distinct prime factors. By coprimality (C), N has at least as many distinct prime factors congruent to 1 modulo r as the counts add to. By (T) that is $r+1$, of which at most one is π, or r none of which is π. Either way N has r such primes other than π, against Proposition 8. □

Primality of a parent. Take a fully factored positive divisor F of $n-1$, with $n \geq 2$ and $F^2 \geq n$. For each prime $p \mid F$, the certificate gives a with

$$a^{n-1} \equiv 1 \pmod n, \qquad \gcd(a^{(n-1)/p} - 1, n) = 1.$$

For a prime $\ell \mid n$ the order of a modulo ℓ divides both $n-1$ and $\ell - 1$, but does not divide $(n-1)/p$. It therefore contains the full p-part of $n-1$. Repeating the argument, with the witness for each p, gives $F \mid \ell - 1$. Every prime divisor of n thus exceeds $\sqrt{n}$, which excludes composite n. Brillhart, Lehmer and Selfridge give this order argument for an even known factor coprime to the cofactor, with the strict cutoff $F > \sqrt{n}$ (Theorem 4 and Corollary 1, p. 623 of [1]). The argument above justifies the precise acceptance test used here.

Completing the small example. When $r = 3$ the box treated the main case. If $\pi = 13$, its half-successor is 7, and $\Phi(7) = 3 \cdot 19$, $\Phi(19) = 3 \cdot 127$ force $7, 19, 127$. If $\pi = 61$, its half-successor is 31, and $\Phi(31) = 3 \cdot 331$; the seed 3 supplies 13. If $\pi = 97$, then $7 \mid (97+1)/2$, and the chain from 3 supplies $13, 61$. In each branch the three displayed primes are non-special and congruent to 1 modulo 3.

Proofs of Theorems 2 and 3. A witness against either theorem supplies N, π satisfying $\mathrm{H}(r)$ in the specified range. For each of the 38 odd primes $r \leq 167$ there is a certificate meeting the conditions of Definition 9. For $r \leq 73$ the certificates are Lean data, and the kernel proves, for each of the 20, that the Lean checker `T2.checkCert` accepts it: for 19 by reducing the whole check directly, and for $r = 71$ by reducing its component checks one at a time and combining them with the proved lemma `checkCert_of_parts` (Section 4). The checker accepts a certificate for $r \equiv 1 \pmod 4$ only when its flag `cited` is set, a flag recording that the proof needs the fact that r is not the special prime. For the 11 primes $r \equiv 3 \pmod 4$ up to 73 the flag is unset and the library's soundness theorem `Opn.sound`, which requires it unset, gives the exclusion. For the nine primes $5, 13, 17, 29, 37, 41, 53, 61, 73$, which are 1 modulo 4, the library uses instead `Opn.sound_given`, which takes `NotSpecial r` as a hypothesis in place of the flag, and discharges that hypothesis with the proved `notSpecial_of_prime` (Theorem 1). The theorem for all 20 primes therefore has no outstanding certificate or number-theoretic hypothesis. For 79 and 83 the extension proves full checker acceptance by assembling the per-case reductions with the same soundness theorem. Both primes are 3 modulo 4, so the unset flag suffices. Enumerating the prime parameters between 73 and 83 completes Theorem 2. For the remaining 16 primes, all three checkers accept each certificate. Eight of these primes are 1 modulo 4: $89, 97, 101, 109, 113, 137, 149, 157$. Theorem 1 supplies the flag's premise. Theorem 3 now follows from Theorem 10. □

A forced divisor before the search.

Proposition 11. *Let r be an odd prime. If N is odd and perfect and has equal exponents $r-1$, then $r^{r-1}\Phi_r(r)$ divides N.*

Proof. By Proposition 8, $v_r(N) = r-1$. Since r is a non-special prime divisor, Lemma 6 gives $\Phi_r(r) \mid N$. The geometric sum is 1 modulo r, so the two divisors are coprime and their product divides N. □

Proposition 12. *Let r be an odd prime. Some prime q divides $\Phi_r(r)$ and satisfies $q \equiv 1 \pmod r$ and $q \not\equiv 1 \pmod{r^2}$.*

Proof. The terms of degree at least two vanish modulo r^2, leaving $\Phi_r(r) \equiv 1 + r \pmod{r^2}$. Every prime factor is 1 modulo r by Lemma 5(a), since r does not divide $\Phi_r(r)$. If all were 1 modulo r^2, multiplying them with their multiplicities would give 1 modulo r^2 as well. □

Together the propositions identify a prime divisor of any hypothetical N for which $r \mid q-1$ but $r^2 \nmid q-1$. This constraint holds before any choices about factorization or the special prime.

4. COMPUTATIONAL VERIFICATION

Finding the certificates. The first Python checker and the Lean kernel both verified the hand-built certificate for $r = 3$. For each larger r, the search starts from $\Phi(r)$, factors $\Phi(q)$ by trial division and the elliptic-curve method, and records primality witnesses. It branches when a parent congruent to 1 modulo 4 could be special. Checking the result requires no search.

Three certificate replays. One author wrote the first two checkers and had read the first before writing the second. The first uses Python integers, Horner's rule for $\Phi(q)$, and `math.gcd`. The second uses libmpdec at 200000 digits with rounding trapped. It evaluates $(q^r-1)/(q-1)$ by exact division, implements Euclid's algorithm and tests perfect powers at prime exponents. Both follow the supplied primality witnesses from each parent and visit only the Pocklington records they need.

The driver `certs/check_all.py` verifies the SHA-256 digest of each program. Both accepted all 18 certificates for $79 \le r \le 167$. The transcript records the input digest and outcome of each of the 36 checks. For the eight inputs flagged $r \equiv 1 \pmod 4$, Theorem 1 supplies the non-special condition.

A separately authored Python checker accepted all 370 cases and rejected an omitted main branch and a false Fermat witness at $r = 167$. It shares the first checker's Python integer arithmetic for cyclotomic sums, greatest common divisors and divisibility. The replay uses `gmpy2.powmod` for modular powers and `gmpy2.is_power` for perfect powers. It allows 1024 iterations per Pollard rho attempt. All three checkers use the same mathematical criteria, Python interpreter and JSON decoder. Table 1 gives the counts replayed by `recompute.py`.

Table 1. The 18 certificates for $79 \le r \le 167$: cases, parents and count of the main case against the $r+1$ needed, Pocklington records stored at the top level of the certificate, the digits of the largest counted number, and the first 12 hexadecimal digits of the certificate's SHA-256 digest.

r	β	cases	par.	count	need	Poc. rec.	digits	SHA-256
79	39	13	27	81	80	68	934	`6578ee03883b`
83	41	12	29	86	84	39	948	`36498927f72f`
89	44	17	30	92	90	84	1393	`a1bcf4a570d6`
97	48	15	32	98	98	62	976	`8331c45f7ef1`
101	50	15	33	102	102	46	1293	`bb32418e1dc0`
103	51	14	35	105	104	54	1763	`a345a7a339e7`
107	53	17	36	108	108	57	4280	`c005940430f8`
109	54	22	38	112	110	185	6503	`9854722fb0ca`
113	56	13	37	116	114	69	1105	`df12ad2f410d`
127	63	21	43	130	128	82	1811	`d7541843d563`
131	65	26	44	133	132	129	7761	`fc6c886b0717`
137	68	25	47	139	138	88	2120	`0dfecfdb5a9f`
139	69	24	46	140	140	90	7721	`2358ed76a1db`
149	74	23	49	150	150	87	8661	`4b6a8f82cde1`
151	75	23	52	153	152	87	2113	`52c5cc297d6e`
157	78	25	52	159	158	137	2113	`5d7aafe1286f`
163	81	32	55	164	164	134	2576	`c30532bccc67`
167	83	33	56	169	168	157	2456	`4b732e684316`

The submitted library. The 29 files of the solution and its verification driver use Lean and Mathlib v4.35.0 [8, 9]. For 19 of the 20 primes through 73, `decide +kernel` checks a whole certificate. For $r = 71$ it checks the component terms separately. The theorem `checkCert_of_parts` combines them into `T2.checkCert cert71 = true`. The axiom inventory of all 1096 public theorems uses only `propext`, `Classical.choice` and `Quot.sound`.

The larger certificates. At 79 and 83, the kernel checks each parent and counted entry from the supplied data. The resulting theorem through 83 has no primality or factorization premises. Its verification driver reports only the same three axioms across 3460 public theorems. Eleven historical build reports extend through 167, but their generated case modules are absent.

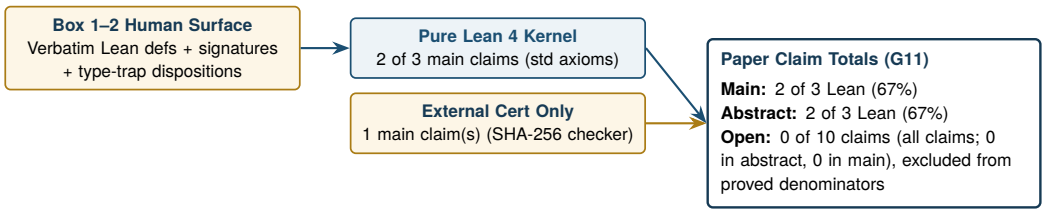
For the 18 files, the kernel checks 33099 entries in 370 branches. The checks cover divisor transitions, residues, pairwise coprimality, total weights and coverage of special parents. Separate proofs establish primality of the 1655 large Pocklington entries and transfer all 16036 ordered parent steps to divisibility of N under the branch hypotheses. For 89 through 167, full acceptance still uses external Fermat and perfect-power checks on weight-two entries.

5. 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 95b05e9119b1 (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:** 2 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 — 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: 3460/3460 public theorems (source-level approx) | WARN: Fidelity: 5/5 exact (draft cross-family)
WARN: Witnesses: pending gate replay | WARN: Human referee: pending

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

OpnChallenge.EqualExponents (Solution.lean:12-14) — Definition 4(1)

```
def EqualExponents (r N : ℕ) : Prop :=
  ∃ π : ℕ, π.Prime ∧
    ∀ q : ℕ, q.Prime → q ∣ N → q ≠ π → N.factorization q = r - 1
```

OpnChallenge.NotSpecial (Solution.lean:18-22) — Definition 4(2)

```
def NotSpecial (r : ℕ) : Prop :=
  ∀ N : ℕ, Odd N → N.Perfect →
    (∀ q : ℕ, q.Prime → q ∣ N →
      Odd (N.factorization q) ∨ N.factorization q = r - 1) →
    ¬ Odd (N.factorization r)
```

Selected Concrete Sanity Examples (checked in Lean; examples only, not global identity proofs): OpnCerts.beta1Cert_checked (T2.checkCert beta1Cert = true); OpnCerts.cert5_checked (T2.checkCert cert5 = true).

Supporting Semantic Closure Index (non-Box-1 helpers): Opn.EqualExponents (Opn/Statement.lean), Opn.NotSpecial (Opn/TheoremG.lean), OpnCerts.EqualExponents (Opn/Certs3To73.lean), OpnCerts.NotSpecial (Opn/Certs3To73.lean).

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

OpnChallenge.notSpecial_of_prime (Solution.lean:25-27) src:d3a48995e58cda

```
theorem notSpecial_of_prime {r : ℕ} (hr : r.Prime) (hr3 : 3 ≤ r) :
    NotSpecial r
```

Assumptions: r prime, 3 <= r; the conclusion constrains a hypothetical odd perfect number. Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

OpnChallenge.no_odd_perfect_equal_exponents_all_primes_le_83 (Opn/Window83.lean:11-22) src:35d1be4f91551b

```
theorem no_odd_perfect_equal_exponents_all_primes_le_83
    (r : ℕ) (hr : r.Prime) (h3 : 3 ≤ r) (h83 : r ≤ 83) :
    ¬ ∃ N : ℕ, Odd N ∧ N.Perfect ∧ EqualExponents r N
```

Assumptions: r prime, 3 <= r <= 83. The value r = 3 meets the parameter hypotheses; existence of an odd perfect number is open. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Opn.r_dvd (Opn/LemmaR.lean:237-396) src:fd3ac56473e9d9

```
theorem r_dvd {N π r : ℕ} (hN : Odd N) (hperf : N.Perfect) (hπ : π.Prime)
    (hr : r.Prime) (hr3 : 3 ≤ r)
    (h : ∀ q, q.Prime → q ∣ N → q ≠ π → N.factorization q = r - 1) :
    r ∣ N
```

Assumptions: N odd and perfect; pi and r prime, 3 <= r; every prime q != pi dividing N has exponent r - 1. The conclusion r | N constrains a hypothetical odd perfect number. Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

EqualExponentCompanion.forcedDivisor (Opn/ForcedDivisor.lean:12-43) src:82f99e05c714e9

```
theorem forcedDivisor {r N : ℕ}
    (hr : r.Prime) (hr3 : 3 ≤ r) (hN : Odd N) (hperf : N.Perfect)
    (hexp : OpnChallenge.EqualExponents r N) :
    r ^ (r - 1) * (∑ i ∈ Finset.range r, r ^ i) ∣ N
```

Assumptions: r prime, 3 <= r; the conclusion restricts a hypothetical odd perfect N satisfying Definition 4(1). Applicability: Hypothetical constraint — vacuously true if no such object exists (carrier status: ordinary_type).

EqualExponentCompanion.primeAtFirstPower (Opn/ForcedDivisor.lean:60-91) src:8ed05c842d5a6b

```
theorem primeAtFirstPower {r : ℕ} (hr : r.Prime) (hr3 : 3 ≤ r) :
    ∃ q : ℕ, q.Prime ∧ q ∣ (∑ i ∈ Finset.range r, r ^ i) ∧
      q % r = 1 ∧ q % (r ^ 2) ≠ 1
```

Assumptions: r prime, 3 <= r; at r = 3 the sum is 13 and the prime 13 meets the conclusion. Applicability: Instantiable — closed instantiation witness PENDING gate-box replay.

Table 2. Lean 4 Type-Trap Audit Checklist — Source-Level Approximation (Gate Replay Pending).[a]

Declaration	Hazard	Operand	Category	Audited Disposition & Guard
`EqualExponents`	`nat_sub`	`- 1`	intended_convention	Theorems 2 and 3 and Proposition 11 require 3 <= r, so r - 1 is exact.
`NotSpecial`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in OpnChallenge.Not Special; Theorem 1 assumes 3 <= r, so it is exact there.
`r_dvd`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in the hypothesis of Opn. r_dvd; the theorem assumes 3 <= r, so it is exact there.
`EqualExponents`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in the library copy Opn. EqualExponents of OpnChallenge.Equal Exponents; the proofs establish 3 <= r from their hypotheses, concrete inputs or checker acceptance.
`NotSpecial`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in the library copy Opn. NotSpecial of OpnChallenge.NotSpecial; the proofs establish 3 <= r from their hypotheses, concrete inputs or checker acceptance.
`EqualExponents`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in the library copy Opn Certs.EqualExponents of OpnChallenge. EqualExponents; the proofs establish 3 <= r from their hypotheses, concrete inputs or checker acceptance.
`NotSpecial`	`nat_sub`	`- 1`	intended_convention	Truncated r - 1 in the library copy Opn Certs.NotSpecial of OpnChallenge.Not Special; the proofs establish 3 <= r from their hypotheses, concrete inputs or checker acceptance.
`forcedDivisor`	`nat_sub`	`- 1`	intended_convention	The exponent r - 1 is exact because r is an odd prime.
`forcedDivisor`	`finset_range`	`Finset.range`	intended_convention	Finset.range r contains exactly the natural indices strictly below r.
`primeAtFirstPower`	`finset_range`	`Finset.range`	intended_convention	Finset.range r contains exactly the natural indices strictly below r.
`primeAtFirstPower`	`nat_mod`	`% r`	intended_convention	The prime r and its square are positive, so these are ordinary residues.
`primeAtFirstPower`	`nat_mod`	`% (r ^ 2)`	intended_convention	The prime r and its square are positive, so these are ordinary residues.

[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 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
Thm. 1: For every prime r >= 3 and every odd perfect N whose prime exponents are each odd or equal to r - 1, v_r(N) is not odd.	Lean Kernel	`OpnChallenge.notSpecial_of_prime`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	r prime with r >= 3. Vacuously true if no odd perfect number exists.
Thm. 2: For every prime r with 3 <= r <= 83 there is no odd perfect N with equal exponents r - 1.	Lean Kernel	`OpnChallenge.no_odd_perfect_equal_exponents_all_primes_le_83`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	r prime with 3 <= r <= 83. The submitted library covers the 20 odd primes through 73. Kernel acceptance of the certificates at 79 and 83 and proved soundness complete the interval.
Thm. 3: For every prime r with 89 <= r <= 167 there is no odd perfect N with equal exponents r - 1.	Cert Only	check_all.py (8e9b6fe0d5ce) [archived; replay pending]; third_check.py (a0141e21a20b) [archived; replay pending]	External cert only; fidelity: n/a	The written soundness theorem applied to the 16 remaining certificates. Three exact checkers accept each file. Two share an author and all share the mathematical criteria. Partial Lean checks do not discharge all weight-two tests.
Lem. 5: Prime factors of Phi(q) are r or 1 mod r; Phi(q) = r mod r^2 when q = 1 mod r and r does not divide Phi(q) otherwise; Phi(q) > q^(r-1), coprime to q, odd for odd q.	Written	Written proof (partial: `Opn.prime_dvd_geom`)	Lean: none; fidelity: n/a	r an odd prime, q >= 2.
Lem. 6: Under H(r): pi divides N to an odd exponent, pi = alpha = 1 mod 4, Phi(q) divides N for every prime q != pi dividing N, and (pi + 1)/2 divides N.	Written	Written proof (partial: `Opn.geom_dvd`)	Lean: none; fidelity: n/a	r an odd prime; N odd and perfect, with a prime pi such that every prime q != pi dividing N has v_q(N) = r - 1 (hypothesis H(r)). Uses Euler's theorem.
Lem. 7: Under H(r), r divides N.	Lean Kernel	`Opn.r_dvd`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	r an odd prime; N odd and perfect, with a prime pi such that every prime q != pi dividing N has v_q(N) = r - 1 (hypothesis H(r)).
Prop. 8: Under H(r), v_r(N) = r - 1 and at most r - 1 primes q != pi dividing N are 1 mod r.	Written	Written proof (partial: `Opn.count_le`)	Lean: none; fidelity: n/a	r an odd prime; N odd and perfect, with a prime pi such that every prime q != pi dividing N has v_q(N) = r - 1 (hypothesis H(r)).
Thm. 10: A certificate meeting (P), (S), (C), (T), (E) for r rules out H(r).	Written	Written proof (partial: `Opn.sound_given`)	Lean: none; fidelity: n/a	r an odd prime; Lemmas 5 to 7, Proposition 8, Theorem 1. Lean counterparts concern the Lean checker T2.checkCert: Opn.sound needs the flag unset (so r = 3 mod 4); Opn.sound_given takes NotSpecial r, which not Special_of_prime proves. Not fidelity-audited here.
Prop. 11: Under the equal-exponent hypothesis, the product of the parameter power and its geometric sum divides N.	Lean Kernel	`EqualExponentCompanion.forcedDivisor`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	r an odd prime; N odd and perfect with equal exponents r - 1 as in Definition 4(1).
Prop. 12: For each odd prime r the geometric sum at r has a prime factor congruent to 1 modulo r and incongruent to 1 modulo r^2.	Lean Kernel	`EqualExponentCompanion.primeAtFirstPower`	Axioms: Classical.choice, Quot.sound, propext; fidelity: exact	r an odd prime.

[a]Allowed pure-kernel axioms: `propext`, `Classical.choice`, `Quot.sound`. Actual axioms printed above are read directly from verified outputs. Provenance nonce: cc652d92406f | Lean mode: committed_receipt | Closure SHA-256: a9b1979ce123 | Git anchor: 95b05e9119b1 | Axioms SHA-256: 96ecb67d1608 | Fidelity SHA-256: 660cd61ddb68.

6. PRIOR WORK AND OPEN QUESTIONS

The historical exclusions in Table 4 concern a fixed common half-exponent β. Steuerwald's condition is that at least one ordinary exponent be at least four [14]. Kanold excludes the all-four case in Section IV of [7]. Hagis and McDaniel exclude the all-six case [6]. Their subsequent theorem also excludes $\beta = 12, 17, 24, 62$, for which $2\beta + 1$ is composite [11].

There are also exclusions for unequal exponents. Hagis and McDaniel (p. 13 of [6]) credit McDaniel [10] [to check] with the case where 3 divides every $2\beta_i + 1$. Yamada states the equivalent condition $\beta_i \equiv 1 \pmod 3$ for all i (p. 303 of [15]). Brown's Theorem 2 excludes the class in which 5 divides every $2\beta_i + 1$ [2]. The latter conclusion also follows from the mixed sieve of Fletcher, Nielsen and Ochem [4]. Under their hypothesis that each $2\beta_i + 1$ is divisible by 3 or 5, their Section 6 excludes $5 \mid N$; when all are divisible by 5, Kanold's theorem forces $5 \mid N$. At prime $2\beta + 1$ these two uniform divisibility classes reach only $r = 3$ and $r = 5$.

Table 4. Prime $r \leq 167$ excluded by results located in the works examined (Section 6).

r	β	source
3	1	Steuerwald 1937 [14]
5	2	Kanold 1941 [7]
7	3	Hagis, McDaniel 1972 [6]
11	5	McDaniel, Hagis 1975 [11]
13, 17, 23, 29, 37	6, 8, 11, 14, 18	Cohen, Williams 1985 [3]

The listed results cover nine of our 38 primes. The remaining 29 include $r = 19$ and 31. Cohen and Williams (p. 73) describe unsuccessful attempts at $\beta = 9, 15, 20, 21, 23$ [3]; their Theorem 1 states all five of their exclusions and Section 3 prints the detailed chains for $\beta = 6, 11$. Brown's historical summary explicitly excepts $\beta = 9$ from its list through 14 [2]. Gallardo and Rahavandrainy say on p. 1 that all cases below $\beta = 20$ are resolved [5]. The list preceding that sentence omits 9 and 15. Both Theorems 1.1 and 1.2 there assume that the special prime is 5, so neither supplies an exclusion for arbitrary special prime at those two values.

Limits of the comparison. We read 15 of 16 cited works in full. The exception is McDaniel's 1970 article [to check]. Its result appears on the opening pages of Hagis and McDaniel's 1972 paper and Yamada's 2005 paper. McDaniel and Hagis formulate the general conjecture in Section 7 of [11]. Yamada improves Kanold's fourth-power divisibility to $t^5 \mid N$ for a common divisor t of all $2\beta_i + 1$ (Theorem 1 of [16]). Proposition 11 gives $r^{r-1} \mid N$ under the narrower equal-exponent, prime-parameter hypothesis. For $r \geq 7$ it implies the fifth-power bound directly.

Beyond the range. The next prime is 173, corresponding to $\beta = 86$. A main branch of the present kind would need a weight of at least 174 and a successful exceptional branch for every eligible parent. The general equal-exponent conjecture, including composite $2\beta + 1$ outside the known classes, and existence of odd perfect numbers remain open.

7. DATA AVAILABILITY, REPRODUCIBILITY, AND USE OF AI

The manuscript, certificate files, checkers, exact-arithmetic replay and kernel replay instructions accompany this draft. The `README.md` gives the build commands and the individual proof targets. The finding library supplies the submitted statements and a separate entry point for the extension. The Palomar package covers the first 20 primes and three predicate examples. Palomar uses mechanical Lean checking and automated editorial review.

AI research agents built and directed by Tyler B. Hughes found the certificates, wrote the proofs and the Lean formalization, checked them, and drafted this manuscript. No human mathematician has yet refereed the proof.

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

REFERENCES

(1) Brillhart, J.; Lehmer, D. H.; Selfridge, J. L. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.* **1975**, *29*, 620–647.

(2) Brown, P. A. More on the nonexistence of odd perfect numbers of a certain form. arXiv:1512.01270, 2015.

(3) Cohen, G. L.; Williams, R. J. Extensions of some results concerning odd perfect numbers. *Fibonacci Quart.* **1985**, *23*, 70–76.

(4) Fletcher, S. A.; Nielsen, P. P.; Ochem, P. Sieve methods for odd perfect numbers. *Math. Comp.* **2012**, *81*, 1753–1776.

(5) Gallardo, L. H.; Rahavandrainy, O. On odd perfect numbers of special forms. arXiv:2304.04109, 2023; journal edition, *Aportaciones Mat. Investig.* **2011**, *20*, 109–115.

(6) Hagis, P., Jr.; McDaniel, W. L. A new result concerning the structure of odd perfect numbers. *Proc. Amer. Math. Soc.* **1972**, *32*, 13–15.

(7) Kanold, H.-J. Untersuchungen über ungerade vollkommene Zahlen. *J. Reine Angew. Math.* **1941**, *183*, 98–109.

(8) de Moura, L.; Ullrich, S. The Lean 4 theorem prover and programming language. In *Automated Deduction, CADE 28*; LNCS 12699, 2021; pp 625–635.

(9) The mathlib Community. The Lean mathematical library. In *Proc. CPP 2020*; ACM, 2020; pp 367–381.

(10) McDaniel, W. L. The non-existence of odd perfect numbers of a certain form. *Arch. Math.* **1970**, *21*, 52–53. [to check]

(11) McDaniel, W. L.; Hagis, P., Jr. Some results concerning the non-existence of odd perfect numbers of the form $p^{\alpha}M^{2\beta}$. *Fibonacci Quart.* **1975**, *13*, 25–28.

(12) Nielsen, P. P. Odd perfect numbers, Diophantine equations, and upper bounds. *Math. Comp.* **2015**, *84*, 2549–2567.

(13) Ochem, P.; Rao, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **2012**, *81*, 1869–1877.

(14) Steuerwald, R. Verschärfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl. *S.-B. Bayer. Akad. Wiss.* **1937**, 69–72.

(15) Yamada, T. Odd perfect numbers of a special form. *Colloq. Math.* **2005**, *103*, 303–307.

(16) Yamada, T. On a theorem of Kanold on odd perfect numbers. *Indian J. Pure Appl. Math.* **2025**, *56*, 1278–1284; arXiv:2312.17059.