

On the Almost Perfect Number Conjecture

Structure and Explicit Bounds for Odd Solutions, with a Lean 4 Formalisation

Ibrahim Amin Nicola Shnoudi

Ibrahim.shnoudiest@gmail.com

Research report, 22 October 2026

DOI: <https://doi.org/10.5281/zenodo.23674490>

Abstract

A positive integer n is almost perfect if $\sigma(n) = 2n - 1$. Every power of 2 is almost perfect, and it is conjectured that there are no others. The conjecture is equivalent to the absence of a pair (b, k) with $b > 1$ odd and $(2^k - 1) \cdot \sigma(b^2) = 2^k \cdot b^2 - 1$. It is not proved here. The report establishes the following results and states precisely what is missing.

- The odd part of an almost perfect number that is not a power of 2 has at least three distinct prime factors (formally verified in Lean 4 for the divisor function of Mathlib). The two-prime exclusion holds for every level $N \geq 2$, for integer variables and for all exponents.
- Odd almost perfect numbers: every odd almost perfect number has at least eight distinct prime factors; the previous bound, six, is Kishore's (1978–1981). Every prime factor of $\sigma(n)$ of an odd almost perfect number n is $\equiv \pm 1 \pmod{8}$ (formally verified). The proof of the bound is an exhaustive search over all exponents in which every discarding step is one of five lemmas, formally verified; seven prime factors take seconds, eight take about 18 hours of computing time, and the hardest cases are the chains of Fermat primes 3, 5, 17, 257, 65537. If moreover $n = b^2$ with b squarefree, then b has a prime factor greater than $1.6 \cdot 10^{30}$ and n has more than $4.3 \cdot 10^{27}$ distinct prime factors, and bounds of the same kind hold whenever one of 3, 5, 7 divides $e + 1$ for every exponent e of n ; in all these cases the sum over all admissible primes is expected to converge to a value below $\log 2$ (0.613 for squarefree roots, 0.621, 0.624 and 0.527 for $d = 3, 5, 7$), so that such numbers are not expected to exist; the same method raises the corresponding bound for quasiperfect numbers with squarefree root from about $4 \cdot 10^8$ (Yamada) to $6.5 \cdot 10^{12}$.
- Three prime factors: two regimes, exponent one in the positive regime, explicit bounds for every prime power and a complete decision procedure for each k . Run with exact arithmetic, it excludes all three-prime counterexamples for every $k \leq 16$ and all squarefree ones for every $k \leq 20$.
- A result for all k at once: no squarefree three-prime counterexample has component quotient $D_s \leq 500,000$. The proof combines a Pell equation that does not depend on k , a 2-adic splitting of its orbits, a lower bound for linear forms in two 2-adic logarithms and an exhaustive computation.
- Any number of prime factors: renormalisation reduces the conjecture at even levels to the absence of primitive solutions (formally verified); every counterexample with ω distinct prime factors satisfies $b^2 < (5\omega N)^M$ with $M = 4^\omega - 1$; for exponents at least 2 only finitely many k occur for a fixed component quotient; and every counterexample has $b > 10^{10}$.
- The squarefree case does not depend on primality. It concerns the integral points of the K3 surfaces $(N - 1)\Phi(x)\Phi(y)\Phi(z) = N(xyz)^2 - 1$ with $\Phi(t) = t^2 + t + 1$, whose only solution with $x \leq N$ is the chain (N, N^3, N^9) and which have no other solution for $N \leq 1,000$ or $N = 2^k$, $k \leq 15$. Fibring over x gives curves of genus one; Hilbert symbols remove most of them, and a 2-cover descent proves that several everywhere locally soluble prime slices have no rational point.

- The last step. With all exponents equal to 2, the last two bases of a solution, and of any spooof factorisation, give an integral point on a curve of genus one with a Pell form. There is no odd integer solution of $\prod \Phi(x_i) = 2 \prod x_i^2 - 1$ with $|x_i| \geq 3$ and at most eight bases of either sign, without any bound on the bases. As a statement about the family of curves, for lists with one further base the curve has no rational point outside a set of bases of density zero (proved with the Chebotarev density theorem and Selberg's sieve).

The remaining gap is stated in Section 14. For three primes it is uniform control, in N and x , of the integral points of these genus-one curves, or equivalently of the 2-adic valuations of fundamental solutions of the Pell equations $X^2 - dY^2 = -(3D + 1)(D - 1)$. Every route tested ends at the same second-order behaviour of Φ at one corner of the threefold of all (x, y, z, N) (Remark 11.10A). Beyond three primes, primitive solutions must be excluded at every even level. For odd almost perfect numbers with squarefree root it is an upper bound for the admissible primes within a factor of about 1.5 of their true number, whereas upper-bound sieves give the factor 2 already for the primes alone; by Lemma 11.29C this amounts to a level of distribution of about 0.87 for the primes in arithmetic progressions, beyond the level $1/2$ of the Bombieri–Vinogradov theorem and within the Elliott–Halberstam conjecture.

1. Introduction

1.1 The problem and known results

For a positive integer n let $\sigma(n)$ be the sum of its divisors. Since $\sigma(2^m) = 2^{m+1} - 1$, every power of 2 satisfies $\sigma(n) = 2n - 1$; such numbers are called almost perfect. The almost perfect number conjecture asserts that there are no others. It belongs to the circle of problems around odd perfect numbers and quasiperfect numbers ($\sigma(n) = 2n + 1$) [7].

An odd almost perfect number greater than 1 has at least six distinct prime factors (Kishore [1, 2]); Theorems 11.11 and 11.19 raise this bound to eight. Hence, in the notation of Section 2, the case $k = 1$ with at most seven prime factors is settled, and Sections 6–9 concern even almost perfect numbers. An even almost perfect number that is not a power of 2 has the form $2^r b^2$ with b odd and composite (Antalan and Tagle [3]); moreover $3 \nmid b$, $2^{r+1} < b$ and $(\sigma(b^2) - b^2) \mid b^2 - 1$ (Antalan and Dris [4]). For deficient-perfect numbers ($\sigma(n) = 2n - d$ with $d \mid n$) the case of two prime factors [5] and the odd case with three prime factors [6] are settled; see [10]. None of these results covers even almost perfect numbers with three distinct prime factors, and we found no such result in the literature.

1.2 Organisation

Section 2 reduces the conjecture to the single equation (2.1). Section 3 collects necessary conditions and the renormalisation principle, Section 4 proves the component lemma, by which each prime power of b is determined by the rest of b , and Section 5 gives the Z -form. Section 6 excludes two prime factors. Sections 7 and 8 treat three prime factors for each k , and Section 9 gives a sieve valid for all k . Section 10 shows that the squarefree case is a problem on integral points of K3 surfaces and of their genus-one fibres, independent of primality. Section 11 treats any number of prime factors and the geometry, proves that an odd almost perfect number has at least eight distinct prime factors, bounds from below the largest prime factor and the number of prime factors of one with squarefree root or with exponents in certain families and explains why such numbers are not expected to exist, and describes the descent from one prime to the next, the near-solutions, the spooof factorisations and the curve of the last two bases. Sections 12 and 13 document the computations and the formal verification, and Section 14 states the remaining gap. Appendix A lists coefficients used in Section 8.6 and Appendix B records the verification of this report. A companion document lists every formally verified statement with its Lean 4 declaration and reproduces the complete source, and a supplementary archive contains the Lean project and every program used for a computation, with its logs.

1.3 Conventions

Every theorem, lemma, proposition, corollary and computation, and every remark that asserts a new fact, carries one status label; a remark without a label explains or summarises statements labelled elsewhere. Formally verified: proved in Lean 4 with Mathlib, with no sorry and only the axioms propext, Classical.choice and Quot.sound; the Lean name is given. Proved: a complete proof is written here but not formalised. Cited: a published theorem used as stated. Computed: an exhaustive verification of a finite range in exact integer arithmetic; Section 12 states on which theorems each elimination rests. Heuristic: a plausibility argument, never used in a proof. A remark that calls a route closed either exhibits objects that satisfy every condition the route uses or shows that the route is a reformulation of the equation. Statements printed in blue are the principal results of this report, for which we found no counterpart in the literature, together with the statements of the remaining gap.

Symbol	Meaning
$\sigma(n), s(n)$	sum of the positive divisors of n ; aliquot sum $\sigma(n) - n$
N, q	$N = 2^k$ and $q = N - 1$; in Section 3.1, Theorem 6.4 and Sections 10–11, N is any integer ≥ 2 (the level)
$b, \omega(b)$	odd part of $n = 2^{k-1}b^2$; number of distinct prime factors of b
$\Phi(t), \delta_t$	$t^2 + t + 1 = \sigma(t^2)$; $t - N$ for a prime t of b
$f_N(v)$	the potential $N \cdot v^2 - (N - 1)\sigma(v^2)$ (Lemma 3.7, Section 3.1)
Δ, D_t	for $m = b/t^e$: $\Delta = f_N(m)$ and the component quotient $D_t = N \cdot m^2 - t \cdot \Delta$ (Theorem 4.1)
Z_t, C_s	$\sigma(t^{2e-1})$ and $q \prod_{t \in S} t - N \prod_{t \in S} (t - 1)$ (Section 5)
$C_2(i, j), C_3, L_2, L_3$	pair and triple coefficients (Section 7)
$(P), (M)$	the positive and negative regimes (Theorem 7.2)
P, S	pr and $p + r$ for $b = prs$ (Section 8)
$(E3); K, L$	the integer equation of Section 10; for fixed x , $K = (N - 1)\Phi(x)$ and $L = N \cdot x^2$

2. Reduction to a single equation

Throughout, p, r, s, t denote odd primes, b an odd positive integer, $N = 2^k$ and $q = N - 1$. For a prime t with $t^e \parallel b$ put $\delta_t = t - N$, and write $\Phi(t) = t^2 + t + 1 = \sigma(t^2)$.

Lemma 2.1 (shape). If $\sigma(n) = 2n - 1$, then $n = 2^a b^2$ with $a \geq 0$ and b odd. [proved; its two steps are formally verified: central ($\sigma(m)$ is odd for the odd part m) and `exp_even_of_sigma_odd`]

Proof. $\sigma(n) = 2n - 1$ is odd. Write $n = 2^a m$ with m odd; then $\sigma(m)$ is odd. For an odd prime t , $\sigma(t^e)$ is a sum of $e + 1$ odd numbers and is odd exactly when e is even. Hence $m = b^2$ ■

Lemma 2.2 (central equation). For $n = 2^a b^2$ with b odd, put $k = a + 1$. Then $\sigma(n) = 2n - 1$ if and only if

$$q \cdot \sigma(b^2) = N \cdot b^2 - 1. \quad (2.1)$$

[formally verified: central] *Proof.* $\sigma(n) = (2^{a+1} - 1)\sigma(b^2) = q \cdot \sigma(b^2)$ and $2n - 1 = N \cdot b^2 - 1$ ■

Theorem 2.3. The conjecture holds if and only if (2.1) has no solution with $b > 1$. A solution (b, k) with $b > 1$ is called a counterexample; $k = 1$ corresponds to odd and $k \geq 2$ to even almost perfect numbers. Equivalently, $q \cdot (\sigma(b^2) - b^2) = b^2 - 1$. [proved; the direction from $\sigma(n) = 2n - 1$ to (2.1) is formally verified: central; every power of 2 is almost perfect: `pow_two_isAlmostPerfect`]

The generalised equation $(N - 1) \cdot \sigma(m) = N \cdot m - 1$ with an arbitrary integer $N \geq 2$ is used repeatedly; it says that the aliquot sum $\sigma(m) - m$ divides $m - 1$ with quotient $N - 1$ (Section 11.1).

3. Necessary conditions

In this section (b, k) is a counterexample.

Lemma 3.1 (coprimality). $\gcd(b, \sigma(b^2)) = 1$. [proved] Proof. A common prime divides $q \cdot \sigma(b^2) = N \cdot b^2 - 1$ and b , hence 1 ■

Lemma 3.2. b is not a prime power. [formally verified: not_prime_pow] Proof. If $b = t^e$, then $\sigma(b^2) \equiv 1 \pmod{t}$, and (2.1) modulo t gives $q \equiv -1$, so $t \mid N$, impossible for odd t ■

Lemma 3.3 (congruences). $8q \mid b^2 - 1$, $\sigma(b^2) \equiv 1 \pmod{8}$, and more precisely $\sigma(b^2) - 1 = N(b^2 - 1)/q$, so $v_2(\sigma(b^2) - 1) = k + v_2(b^2 - 1) \geq k + 3$. [proved; the congruence $\sigma(b^2) \equiv 1 \pmod{8N}$ is formally verified: sigma_sq_mod_eightN]

Proof. From (2.1), $q(\sigma(b^2) - b^2) = b^2 - 1$, so $q \mid b^2 - 1$, and $8 \mid b^2 - 1$ with q odd. Then $\sigma(b^2) - 1 = (b^2 - 1)(1 + 1/q) = N(b^2 - 1)/q$ ■

A selection rule modulo 8. Since $\Phi(t) \equiv 3, 5, 7, 1 \pmod{8}$ for $t \equiv 1, 3, 5, 7 \pmod{8}$ and $(\mathbb{Z}/8)^\times$ is a Klein four-group, the condition $\prod \Phi(t) \equiv 1 \pmod{8}$ for a squarefree b with three primes allows exactly the residue patterns $\{7, 7, 7\}$, $\{1, 3, 5\}$, $\{1, 1, 7\}$, $\{3, 3, 7\}$ and $\{5, 5, 7\}$ for (p, r, s) modulo 8 [computed by enumeration]; Lemma 10.18 refines this modulo 2^k . Like every congruence condition it follows from the equation (Remark 3.14); it serves to prune searches.

Lemma 3.4 (abundancy). $\sigma(b^2)/b^2 < 1 + 1/q$ and $\sum_{t \mid b} 1/t < 1/q$; every prime factor of b satisfies $t \geq N + 1$. [proved; used in formally verified form]

Proof. $\sigma(b^2)/b^2 = 1 + (b^2 - 1)/(q \cdot b^2) < 1 + 1/q$. Since $\sigma(t^{2e})/t^{2e} > 1 + 1/t$, multiplicativity gives $1 + \sum 1/t < \prod (1 + 1/t) < 1 + 1/q$. So $t > q$, and as t is odd and q odd, $t \geq N + 1$ ■

Lemma 3.5 (sandwich). (i) $\prod_{t \mid b} (1 + 1/t) < N/q$. (ii) $\prod_{t \mid b} t/(t - 1) > (N^2 + N + 1)/N^2$. [proved]

Proof. (i) is Lemma 3.4. (ii) $\sigma(t^{2e})/t^{2e} < t/(t - 1)$, so $\prod t/(t - 1) > \sigma(b^2)/b^2 = 1 + (b^2 - 1)/(qb^2)$, which increases with b ; since $b > N$, it exceeds $1 + (N + 1)/N^2$ ■

Lemma 3.6 (window for the smallest prime). If b has $\omega \geq 2$ distinct prime factors and p is the smallest, then $p \leq \omega N - 1$. [proved]

Proof. By Lemma 3.5(ii), $(p/(p - 1))^\omega > 1 + 1/N + 1/N^2$. If $p - 1 \geq \omega N$, then $(p/(p - 1))^\omega \leq (1 + 1/(\omega N))^\omega < e^{1/N} < 1 + 1/N + (e - 2)/N^2$, because $(e^u - 1 - u)/u^2$ increases for $0 < u \leq 1$ and equals $e - 2$ at $u = 1$; a contradiction. So $p \leq \omega N$, and p is odd while ωN is even ■ The argument uses only $\sigma(t^{2e})/t^{2e} < t/(t - 1)$ and therefore holds for integer variables as well, with the conclusion $p \leq \omega N$.

Lemma 3.7 (splitting identity; potential). For odd v put $f(v) = N \cdot v^2 - q \cdot \sigma(v^2)$ and $E(v) = \sigma(v^2) - v^2$. For coprime m, u , $f(mu) = f(m) \cdot \sigma(u^2) - N \cdot m^2 \cdot E(u)$ (a polynomial identity). If (b, k) is a counterexample and $b = mu$, then $f(m)\sigma(u^2) - N \cdot m^2 E(u) = 1$; consequently $f(m) \geq 1$ for every unitary divisor m of b and $\gcd(f(m), N \cdot m) = 1$. [formally verified: splitting]

Proof. $\sigma(m^2 u^2) = \sigma(m^2) \sigma(u^2)$ and $q \cdot \sigma(m^2) = N \cdot m^2 - f(m)$ give $f(mu) = N \cdot m^2 u^2 - (N \cdot m^2 - f(m)) \sigma(u^2)$, and $f(b) = 1$ by (2.1) ■

The potential f starts at $f(1) = 1$ and ends at $f(b) = 1$. Adding one prime power changes it by $f(m \cdot t^e) - f(m) + Z_t(t \cdot f(m) - N \cdot m^2)$, with $Z_t = \sigma(t^{2e-1})$.

Theorem 3.8 (monotonicity of the potential). Let m be a unitary divisor of b , $u = b/m$ and $t^e \parallel u$. If u has a prime factor $t' \neq t$ with $t' \leq t^2 - 1$, then $f(m \cdot t^e) > f(m)$. Hence, adding the primes of b in decreasing order, the potential increases strictly at every step except the last, where $f(m_{\omega-1}) - 1 = Z_p D_p$ with p the smallest prime and D_p the component quotient of Section 4. [proved]

Proof. By Lemma 3.7, $f(m) = (1 + N \cdot m^2 E(u))/\sigma(u^2) > N \cdot m^2 (1 - 1/A)$ with $A = \sigma(u^2)/u^2 > (1 + 1/t)(1 + 1/t') \geq t/(t - 1)$ when $t' \leq t^2 - 1$. So $t \cdot f(m) > N \cdot m^2$ and the increment is positive. At the last step $u = p^\alpha$ and Theorem 4.1 gives $t \cdot f(m) - N \cdot m^2 = -D_p$ ■

3.1 Renormalisation and primitive solutions

Throughout this subsection $N \geq 2$ is any integer (the level), and $f_N(v) = N \cdot v^2 - (N - 1)\sigma(v^2)$. A solution at level N is an odd $v > 1$ with $f_N(v) = 1$; a counterexample is a solution at level 2^k .

Proposition 3.9 (recursion of the potential). For coprime m, u , $f_N(mu) = f_N(m) \cdot u^2 - (N - 1)\sigma(m^2) \cdot (\sigma(u^2) - u^2)$. [formally verified: pot_mul, pot_recursion_int]

Theorem 3.10 (renormalisation). Let m, u be coprime and $f_N(m) = 1$. Then $f_N(mu) = 1$ if and only if $f_{N'}(u) = 1$ with $N' = N \cdot m^2$: mu solves the equation at level N exactly when u solves it at level $N \cdot m^2$. [formally verified: renormalise, renormalise_int]

Proof. $f_N(m) = 1$ means $(N - 1)\sigma(m^2) = N \cdot m^2 - 1$. Since $\sigma(m^2 u^2) = \sigma(m^2)\sigma(u^2)$, the equation $(N - 1)\sigma(m^2)\sigma(u^2) = N \cdot m^2 u^2 - 1$ becomes $(N \cdot m^2 - 1)\sigma(u^2) = (N \cdot m^2)u^2 - 1$ ■

Call a solution b at level N primitive if $f_N(m) \neq 1$ for every unitary divisor $1 < m < b$. By Theorem 3.10 every solution factors as $b = m_1 m_2 \cdots m_r$, where m_i is a primitive solution at level $N_i = N(m_1 \cdots m_{i-1})^2$. All these levels are even when N is even. The trivial integer chain $(N, N^3, N^9, \dots)$ of Section 10 is exactly the case where every piece is a single integer $m_i = N_i$.

Corollary 3.11 (an induction on ω). For an even level N there is no solution with one prime factor (the proof of Lemma 3.2 gives $t \mid N$, while the proof of Lemma 3.4, valid at every level, gives $t > N - 1$, so $t = N$, which is even) and none with two (Theorem 6.4, valid for every N). Hence every solution at an even level with at most five distinct prime factors is primitive. More generally, if for some ω_0 there is no primitive solution with $\omega \leq \omega_0$ prime factors at any even level, then there is no solution at all with $\omega \leq \omega_0$ at any even level. [proved]

Proof. If m is a proper unitary divisor with $f_N(m) = 1$, then m is a solution at level N and $u = b/m$ is a solution at the even level $N \cdot m^2$, each with fewer prime factors than b ; one of them has at most two prime factors when $\omega \leq 5$, which is impossible. The general statement follows by induction on ω ■

Remark 3.12 (renormalisation and the conjecture). The absence of solutions at even levels (Conjecture SQ, Conjecture 11.4) is equivalent to the absence of primitive solutions at every even level, and induction on ω through renormalisation is exact. Two features are essential. The deficit 1 is needed: for the analogous two-variable equation with deficit $M \neq 1$ non-trivial solutions exist (Remark 10.11). And the levels $N \cdot m^2$ are not powers of 2, so an induction needs results valid at every even level; among the three-prime results, Theorems 7.2 and 8.4 and the Pell form hold for every $N \geq 2$, and Theorem 7.3 holds for every even $N \geq 4$.

Remark 3.13 (the descent problem). The inductive target is the following: a solution at an even level has a proper unitary divisor m with $f_N(m) = 1$. By Theorem 3.8 no prefix in decreasing order has this property. Since $1 = f_N(m)u^2 - (N - 1)\sigma(m^2)E(u)$ for every split $b = mu$, $f_N(m)$ is the inverse of u^2 modulo $(N - 1)\sigma(m^2)$, and the problem asks for a split in which this inverse equals 1; no mechanism forcing this is known. Conversely, if $f_N(m) = 1$, then u solves the equation at level $N \cdot m^2$ (Theorem 3.10), and Lemma 3.4 at that level gives $t \geq N \cdot m^2 + 1$ for every prime t of u : an imprimitive solution has a gap in its primes, as the trivial chain does [proved]. For even N the potential of an odd number is odd, so at a primitive solution $f_N(d) \geq 3$ for every unitary divisor $1 < d < b$.

Remark 3.14 (the congruences of the splits are the equation). For a split $b = mu$ the recursion gives $u^2 f_N(m) \equiv 1$, that is $N \cdot b^2 \equiv 1 \pmod{(N - 1)\sigma(m^2)}$, a consequence of (2.1). Conversely, take the ω splits $m = b/t^e$. If the numbers $\sigma(t^{2e})$ are pairwise coprime, the moduli have least common multiple $(N - 1)\sigma(b^2)$, so $N \cdot b^2 - 1 = \lambda(N - 1)\sigma(b^2)$ with an integer λ ; here $\lambda > 0$, and $\sigma(b^2) > b^2$ gives $\lambda < N/(N - 1) \leq 2$, so $\lambda = 1$ and (2.1) is recovered. Thus the family of split congruences is equivalent to (2.1), and a contradiction derived from it is a contradiction derived from the equation. Combined with size information the congruences are what Proposition 10.19 uses. [proved]

Remark 3.15 (the Möbius identity). For $b = prs$ and any integers, $\sum_{d|b} \mu(b/d) \cdot f_N(d) \cdot (b/d)^2 = -(N-1)(p+1)(r+1)(s+1)$, since $f_N(d)/d^2 = N - (N-1) \prod_{t|d} (1+x_t)$ with $x_t = 1/t + 1/t^2$ [formally verified: mobius_three]. With $f_N(b) = 1$ and the exact values $f_N(t) = \delta_t(t+1) + 1$ and $f_N(b/t) = 1 + D_t(t+1)$ (Theorem 4.1), it becomes one linear relation among D_p , D_r and D_s , which is again equivalent to the equation. The divisor lattice carries no information beyond integrality, and by Remark 3.14 integrality conditions are equivalent to the equation.

4. The component lemma

Theorem 4.1 (component lemma). Let (b, k) be a counterexample, $t^e \parallel b$, $m = b/t^e$, $w = t^{2e}$, $S = \sigma(w)$, and put $\Delta = N \cdot m^2 - q \cdot \sigma(m^2)$ and $D = N \cdot m^2 - t \cdot \Delta$. Then D is odd and $1 \leq D < \Delta$, so $t = \lfloor N \cdot m^2 / \Delta \rfloor$ and $D = N \cdot m^2 \bmod \Delta$, and

$$w \cdot D = q \cdot \sigma(m^2) - t + 1, N \cdot m^2 = D \cdot S + t, t^2 D < N \cdot m^2. \quad (4.1)$$

[formally verified: component, component_div, component_quotient_odd]

Proof. Write (2.1) as $q \cdot \sigma(m^2) \cdot S = N \cdot m^2 \cdot w - 1$, and use $(t-1)S = t \cdot w - 1$. The first identity of (4.1), multiplied by $(t-1)^2$, is a polynomial consequence of these two relations, and the second follows from the first in the same way. Since $S > w$, $q \cdot \sigma(m^2) \cdot S = N \cdot m^2 \cdot w - 1 < N \cdot m^2 S$, so $\Delta \geq 1$. For $D \geq 1$: if $D < 0$, then $N \cdot m^2 = D \cdot S + t \leq t - S < 0$, impossible; if $D = 0$, then $N \cdot m^2 = t$, impossible because N is even and t is odd. Hence $D \geq 1$. Since $N \cdot m^2$ is even and t is odd, $N \cdot m^2 = D \cdot S + t$ forces $D \cdot S$, and hence D , to be odd. Finally $w \geq t^2$ and $w \cdot D = q \cdot \sigma(m^2) - t + 1 < N \cdot m^2$ give $t^2 D < N \cdot m^2$. For $D < \Delta$: from $D \cdot S + t = N \cdot m^2 = D + t \cdot \Delta$ and $S - 1 = t \cdot Z_t$, with $Z_t = \sigma(t^{2e-1}) \geq 1$, one gets $\Delta = D \cdot Z_t + 1 > D$ ■

Remark (where parity enters). Parity of N is used only to exclude $D = 0$. For an odd parameter N the case $D = 0$, $N \cdot m^2 = t$, does occur: it gives the trivial solutions $m = 1$, $b = t^e$, $N = t$ of the generalised equation.

The quantity $D = D_t$ is the component quotient at t . Each prime power of b is determined by the rest of b . For $e = 1$ the first identity of (4.1) reads $D_t t^2 + t - 1 = (N \cdot b^2 - 1) / \Phi(t)$, so D_t is close to $N \cdot b^2 / t^4$.

The smallest prime $p = N + 1$. If $N + 1$ is prime and is the smallest prime of b , Theorem 4.1 at p together with $(t-1)\sigma(t^{2e}) = t \cdot t^{2e} - 1$ gives $(N^2 - 1)\sigma(m^2) = N^2 m^2 + D_p$ with $D_p \geq 1$ and $m = b/p^a$ [formally verified: component_combo, fermat_reduction]. So m solves the generalised equation at level N^2 up to an overshoot D_p . With D_p free this reduced equation has solutions; an argument in this case must use the link $D_p \cdot \sigma(p^{2a}) = N \cdot m^2 - p$ between D_p and the prime power.

4.1 Rigidity and Pell form

Proposition 4.2. $t^{2e} D_t \equiv 1 - t \pmod{q}$ and $\sigma(t^{2e}) D_t \equiv -t \pmod{N}$; since $t > q$ is prime to q and $\sigma(t^{2e})$ is odd, both coefficients are invertible, hence D_t is determined modulo qN by t and e . [congruences formally verified: D_congr_q, D_congr_N]

Proposition 4.3. If k is even, $D_t \equiv 1 - t \pmod{3}$, so $D_t \neq 1$. If k is odd and $e = 1$, $D_t \neq 1$. [formally verified: D_mod_three, D_ne_one_even, D_ne_one_odd]

Proposition 4.4 (Pell form). If $t \parallel b$, then with $D = D_t$ and $m = b/t$, $(2Dt + D + 1)^2 - D \cdot N \cdot (2m)^2 = -(3D + 1)(D - 1)$. [formally verified: pell_form] Proof. Multiply $N \cdot m^2 = D(t^2 + t + 1) + t$ by $-4D$ and expand ■

Proposition 4.5 (residues of the primes for odd k). Let b be squarefree and (b, k) a counterexample with k odd and $k \geq 3$ (for $k = 1$ see Section 1.1). Then every prime $t \mid b$ satisfies $t \equiv 2 \pmod{3}$ and $t \equiv 5$ or $7 \pmod{8}$, that is $t \equiv 5$ or $23 \pmod{24}$, and the number of primes $t \equiv 5 \pmod{8}$ is even. For three primes, (p, r, s) is congruent modulo 24 to $(23, 23, 23)$ or to a permutation of $(5, 5, 23)$; in particular $t - N \equiv 15$ or $21 \pmod{24}$ for each prime t of b . [proved; residue enumeration computed]

Proof. For k odd, $N \equiv 2$ and $q \equiv 1 \pmod{3}$. If $3 \mid b$, then $q \cdot \sigma(b^2) = N \cdot b^2 - 1 \equiv 2 \pmod{3}$, whereas every $\Phi(t)$ is $\equiv 0$ or $1 \pmod{3}$; so $3 \nmid b$ and $b^2 \equiv 1 \pmod{3}$, hence $N \cdot b^2 - 1 \equiv 1 \pmod{3}$ and $3 \nmid \sigma(b^2) = \prod \Phi(t)$; since $3 \mid \Phi(t)$ exactly when $t \equiv 1 \pmod{3}$, every $t \equiv 2 \pmod{3}$. Let ℓ be a prime dividing $\Phi(t)$. Then $\ell \neq 3$, $t^3 \equiv 1$ and $t \not\equiv 0 \pmod{\ell}$, so $t \equiv t^4 = (t^2)^2$ is a square modulo ℓ . Reducing (2.1) modulo ℓ gives $N \cdot b^2 \equiv 1$, and with $t^2 \equiv t$ this gives $N \cdot (b/t)^2 \equiv t \pmod{\ell}$. Hence $N = 2^k$ is a square modulo ℓ , and since k is odd, $(2/\ell) = 1$, that is $\ell \equiv \pm 1 \pmod{8}$. So $\Phi(t) \equiv \pm 1 \pmod{8}$. As $\Phi(t) \equiv t + 2 \pmod{8}$ for odd t , this gives $t \equiv 5$ or $7 \pmod{8}$. Finally $\prod \Phi(t) = \sigma(b^2) \equiv 1 \pmod{8}$ (Lemma 3.3), and $\Phi(t) \equiv 7$ exactly when $t \equiv 5 \pmod{8}$, so the number of such t is even. Since $N \equiv 0 \pmod{8}$ and $N \equiv 2 \pmod{3}$, $t - N \equiv t \pmod{8}$ and $t - N \equiv 0 \pmod{3}$ ■

That every prime factor of $\sigma(b^2)$ is $\equiv \pm 1 \pmod{8}$ for odd k also follows directly from $N \cdot b^2 - 1 = 2(Mb)^2 - 1$ with $N = 2M^2$; the new points are the condition modulo 3 and the combination of the two. Like every congruence condition (Remark 3.14) the statement excludes nothing by itself, since primes $\equiv 5$ and $\equiv 23 \pmod{24}$ are plentiful; it prunes searches, and it does not use primality.

Remark 4.6 (prime factors of $\Phi(t)$). Nothing derived from the equation bounds the prime factors of $\Phi(t)$ from above, and $\Phi(t)$ may be prime: among the 3,409 primes $p \equiv 5$ or $23 \pmod{24}$ in $(2^{21}, 2^{21} + 2 \cdot 10^5)$, the residue classes allowed by Proposition 4.5 for odd k , 348 have $\Phi(p)$ prime [computed]. In that case the only information at $\ell = \Phi(t)$ is $N(b/t)^2 \equiv t \pmod{\Phi(t)}$, which is the component identity of Theorem 4.1. Lower bounds for the greatest prime factor of $\Phi(t)$ therefore give nothing.

Remark 4.7 (the split for even k). For $k = 2h$ put $A = 2^h$, so $N = A^2$. Then (2.1) reads $(Ab - 1)(Ab + 1) = (A - 1)(A + 1)\sigma(b^2)$ [formally verified: even_k_split], and every prime factor of q and of $\sigma(b^2)$ is assigned to one of the coprime factors $Ab \mp 1$. The split is realised exactly by the trivial integer chain: for $b = A^2$, $(A^3 - 1)/(A - 1) = \Phi(A)$, $(A^3 + 1)/(A + 1) = \Phi(-A)$ and $\Phi(A^2) = \Phi(A)\Phi(-A)$ [formally verified: phi_sq]. So the split pattern is not contradictory, and an argument must use that the t are odd. The relation between the two factors is not of S -unit type, since nothing restricts the prime factors of $\sigma(b^2)$.

Proposition 4.8 (the side of a prime factor is a square root of the component congruence). Let $k = 2h$, $A = 2^h$ and $b = \text{prs}$. Then $\Phi(p) \mid (A \cdot rs - p^2)(A \cdot rs + p^2)$, whether or not p or $\Phi(p)$ is prime, and every prime $\ell \mid \Phi(p)$ divides $A \cdot rs - p^2$ or $A \cdot rs + p^2$. Moreover $\ell \mid A \cdot rs - p^2$ if and only if $\ell \mid Ab - 1$, and $\ell \mid A \cdot rs + p^2$ if and only if $\ell \mid Ab + 1$. [first two statements formally verified: split_sides, split_sides_prime; the last one proved]

Proof. $(A \cdot rs)^2 - p^4 = (A^2(rs)^2 - p^2) - p(p - 1)\Phi(p)$, and the equation gives $A^2(rs)^2 - p = \Phi(p) \cdot (p \cdot q\Phi(r)\Phi(s) - A^2(rs)^2(p - 1))$, which is the component congruence $N(rs)^2 \equiv p \pmod{\Phi(p)}$ of Theorem 4.1. For the last statement, $p^3 \equiv 1 \pmod{\ell}$ gives $Ab = A \cdot p \cdot rs \equiv p(\pm p^2) = \pm 1 \pmod{\ell}$ exactly when $A \cdot rs \equiv \pm p^2$ ■

So the allocation of the prime factors of $\Phi(p)$ to the two sides $Ab \mp 1$ is the choice, prime by prime, of a square root of $N(rs)^2 \equiv p$ modulo $\Phi(p)$: a reformulation of the component congruences, which adds no constraint of its own (Remark 3.14).

Remark 4.9 (quadratic reciprocity between the primes). Reducing (2.1) modulo each prime gives the cross conditions $q\Phi(r)\Phi(s) \equiv -1 \pmod{p}$, $q\Phi(p)\Phi(s) \equiv -1 \pmod{r}$ and $q\Phi(p)\Phi(r) \equiv -1 \pmod{s}$. Their Legendre symbols give three relations $(-q/p)(\Phi(r)/p)(\Phi(s)/p) = 1$ and its analogues, and by Jacobi reciprocity $(\Phi(r)/p)$ equals $\pm(p/\Phi(r)) = \pm \prod_{\ell \mid \Phi(r)} (p/\ell)$. The equation determines only (p^2/ℓ) at such ℓ , through $N(ps)^2 \equiv r \pmod{\Phi(r)}$ (Theorem 4.1), and not (p/ℓ) ; so the six symbols $(\Phi(x)/y)$, $x \neq y$, satisfy three relations, and no further relation among them follows from the equation [heuristic]. Jacobi reciprocity holds for all odd integers, so this route does not use primality, and the cross conditions together with the component congruences modulo $\Phi(p)$, $\Phi(r)$, $\Phi(s)$ reconstruct (2.1) by the argument of Remark 3.14. The cubic analogue is Remark 10.25C.

Remark 4.10 (the exact 3-adic valuation). For every integer t , $v_3(\Phi(t)) = 1$ if $t \equiv 1 \pmod{3}$ and 0 otherwise; in particular $9 \nmid \Phi(t)$ [formally verified: phi_not_dvd_nine]. So for squarefree b , $v_3(\sigma(b^2)) = m$, the number of primes of b that are $\equiv 1 \pmod{3}$. For $k = 2h$ the lifting-the-exponent lemma gives $v_3(2^k -$

$1) = 1 + v_3(h)$, hence $v_3(N \cdot b^2 - 1) = 1 + v_3(h) + m$, and this valuation sits entirely in one of the coprime factors $2^h b \mp 1$. For odd k , $m = 0$ by Proposition 4.5. [proved] This is the equation at the prime 3; it holds for all integers t and, since local conditions are satisfiable (Section 11.4), gives no contradiction on its own.

5. The Z-form

For $t^e \parallel b$ put $Z_t = \sigma(t^{2e-1})$, so that $t^{2e} = 1 + (t-1)Z_t$ and $\sigma(t^{2e}) = 1 + t \cdot Z_t$; $Z_t = (t+1)X_t$ with $X_t = 1$ exactly when $e = 1$. For a set S of primes of b let $C_S = q \prod_{t \in S} t - N \prod_{t \in S} (t-1)$, so $C_\emptyset = -1$ and $C_{\{t\}} = -\delta_t$.

Theorem 5.1 (Z-form). $q \cdot \sigma(b^2) - (N \cdot b^2 - 1) = \sum_S C_S \prod_{t \in S} Z_t + 1$. [formally verified for two and three primes: `zform_two`, `zform_three`; proved for all ω] Proof. Expand $q \prod (1 + tZ_t) - N \prod (1 + (t-1)Z_t)$ ■

Proposition 5.2 (Plücker relations). For disjoint S and distinct primes i, j outside S , $C_{S \cup \{i\}} C_{S \cup \{j\}} - C_{S \cup \{i, j\}} C_S = q N \prod_{t \in S} t(t-1)$. In δ -variables $C_{ij} = qN - \delta_i \delta_j$ and $C_{ijk} = qN(2N - 1 + \delta_i + \delta_j + \delta_k) - \delta_i \delta_j \delta_k$. [proved; $|S| = 0$ formally verified: `plucker_pair`] Proof. With $\alpha = q \prod_S t$ and $\beta = N \prod_S (t-1)$, the left side is $\alpha \beta (i - (i-1))(j - (j-1)) = \alpha \beta$ ■

6. Two distinct prime factors

Here $b = p^a r^b$ with $N+1 \leq p < r$, $C = C_{pr} = N(p+r-1) - pr$, $\delta_p = p - N$, $\delta_r = r - N$.

Theorem 6.1 (exponent collapse). For any integer $N \geq 2$, if (2.1) holds for $b = p^a r^b$ with $N+1 \leq p < r$, then $\alpha = \beta = 1$. [formally verified: `two_prime_short_exponents`]

Proof. By Theorem 5.1 the equation reads $C \cdot Z_p Z_r = \delta_p Z_p + \delta_r Z_r$, equivalently $(C \cdot Z_p - \delta_r)(C \cdot Z_r - \delta_p) = \delta_p \delta_r$. So $C \geq 1$, both factors are ≥ 1 and $\leq \delta_p \delta_r$. From $C \cdot Z_r \leq \delta_p(\delta_r + 1) < \delta_p(r+1)$ one gets $C \cdot X_r < \delta_p < r^2$, forcing $X_r = 1$; similarly $C \cdot X_p < \delta_r < r < p^2$, forcing $X_p = 1$, where $r < p^2$ because $C \geq 1$ gives $r(p-N) < N(p-1)$, so $r < Np < p^2$ ■

Theorem 6.2. For every integer $N \geq 2$ and integers $N+1 \leq p < r$, $(N-1)\Phi(p)\Phi(r) \neq N \cdot p^2 r^2 - 1$. No primality is used. [formally verified: `squarefree_two_general`]

Proof. Put $w = p+r-1$, $A = C(N+1) + 3q$ and $c_0 = C^2 - 3q - 1$. The equation is equivalent to $w(A-w) = c_0$, and the Z-form gives $1 \leq C \leq N-1$. If $c_0 < 0$, then $w > A$ and $-c_0 \geq w > A > 3q \geq -c_0$; if $c_0 > 0$, then $0 < w < A$, so $c_0 = w(A-w) \geq A-1$, that is $C^2 - C(N+1) - 6q \geq 0$, which forces $C > N+1$; if $c_0 = 0$, then $C^2 = 3N-2$, and $9(r-p)^2$ lies strictly between P^2 and $(P+1)^2$ with $P = C^3 + C^2 + 3C - 2$ ■

Theorem 6.3 (main theorem). No counterexample has $\omega(b) \leq 2$. Hence an almost perfect number is a power of 2 or has an odd part with at least three distinct prime factors. [formally verified for the divisor function of Mathlib: `not_two_primes`, `odd_part_one_or_three_primes`, `almostPerfect_classification`]

Theorem 6.4 (two primes, any exponents, any N). Let $n = p^e r^f$ solve the generalised equation $(N-1)\sigma(n) = N \cdot n - 1$ with $N \geq 2$ and $N+1 \leq p < r$ (exponents of n , not of b). Then $(e, f) \in \{(1, 1), (2, 1)\}$. For even N the pattern $(1, 1)$ is impossible, because $\sigma(n) = (p+1)(r+1)$ is even while $N \cdot n - 1$ is odd, and the pattern $(2, 1)$ forces r to be even; so for even N there is no two-prime solution with any exponents. (For even N this also follows at once from parity, as in Proposition 11.2: $N \cdot n - 1$ is odd, so $\sigma(n)$ is odd, and since n is odd every exponent of n is even, which excludes both patterns.) [formally verified: `pattern11_even_N`, `pattern12_impossible`, `pattern31_impossible`, `pattern32_impossible` (with the window $p \leq 2N$ of Lemma 3.6), `squarefree_two_general`, `pattern21_even_N`]

Proof. The Z-form with $Z_t = \sigma(t^{e-1})$ gives $(C \cdot Z_p - \delta_r)(C \cdot Z_r - \delta_p) = \delta_p \delta_r$ with $C \geq 1$ and both factors ≥ 1 . Then $C \cdot Z_r \leq \delta_p(\delta_r + 1) < pr$, so $f \geq 3$ ($Z_r > r^2$) would give $r < p$; and $C \cdot Z_p \leq \delta_r(\delta_p + 1) < rp$, so $e \geq 4$ ($Z_p > p^3$) would give $r > p^2$, contradicting $r < Np < p^2$ ($C \geq 1$ gives $r(p-N) < N(p-1)$, so $r < Np$). Hence $f \leq 2$ and $e \leq 3$. For $(1, 2)$, $Z_p = 1$ and $Z_r = r+1$, so $(C - \delta_r)(r+1) = \delta_p$ with $0 < \delta_p < r+1$, which is impossible. $(2, 2)$ is Theorem 6.2. For $(3, 1)$, $K = C - \delta_p \geq 1$, $r = N + K(1 + p + p^2)$, and $K(1 + \delta_p(1 + p + p^2)) = N^2 -$

p is impossible because the left side exceeds $p^2 > N^2$. For (3, 2), with $Z_p = 1 + p + p^2$ and $R = r + 1$, the Z -form reads $R(C \cdot Z_p - \delta_r) = \delta_p Z_p$; since $C \geq 1$, $Z_p \leq \delta_r R / (R - \delta_p) < R^2 / (R - \delta_p)$. From $C \geq 1$, $R \leq Np / \delta_p$, and on $[p + 1, Np / \delta_p]$ the function $R^2 / (R - \delta_p)$ is bounded by its endpoint values $(p + 1)^2 / (N + 1) < Z_p$ and $N^2 p^2 / (\delta_p (Np - \delta_p^2)) < p^2 < Z_p$, the last inequality being $(\delta_p - 1)N^2 + \delta_p^2 N - \delta_p^3 > 0$; this is a contradiction. In Lean the convexity step is replaced by an explicit polynomial certificate. For (2, 1), $r = N + K(p + 1)$ with $K = (N^2 - p) / (1 + \delta_p(p + 1))$, and r is even when N is even ■

For odd N both surviving patterns occur. The pattern (1, 1) is equivalent to $(p - N + 1)(r - N + 1) = N^2 - N + 1$ and has prime solutions, for example $(p, r) = (7, 11)$ for $N = 5$, $(13, 47)$ for $N = 11$ and $(19, 107)$ for $N = 17$. For the pattern (2, 1), with $\delta = p - N$, K is an integer exactly when $1 + \delta(N + \delta + 1)$ divides $\delta^4 + 2\delta^3 + 4\delta^2 + 3\delta + 1$. Enumerating, for every $\delta \leq 3,000$, the divisors $d \equiv 1 \pmod{\delta}$ of this polynomial gives all 3,019 integer points with $\delta \leq 3,000$ (N up to about $2.7 \cdot 10^{10}$); 3,009 have even N , and each of the ten with odd N has p or r divisible by one of 3, 5, 7, 13, 31, 43, 113. A direct enumeration of all $N \leq 10^5$ finds 63 integer solutions, none with p and r both prime [computed]. So, for two primes larger than N , Conjecture 11.4 is equivalent to the absence of prime points on this family with odd N .

7. Three distinct prime factors: identities, regimes and bounds

Here $b = p^\alpha r^\beta s^\gamma$ with $N < p < r < s$, $x = p^{2\alpha}$, $y = r^{2\beta}$, $z = s^{2\gamma}$, $L_2 = (p - 1)(r - 1)$, $L_3 = (p - 1)(r - 1)(s - 1)$, $C_2(i, j) = N(i + j - 1) - ij = qN - \delta_i \delta_j$ and $C_3 = q \cdot prs - N \cdot L_3$.

Proposition 7.1. (L1) For even N , all $C_2(i, j)$ and C_3 are odd. (L2) $C_3 = s \cdot C_2(p, r) + N \cdot L_2$. (L3) Equation (2.1) is equivalent to $C_3 \cdot xyz = q(pr \cdot xy + ps \cdot xz + rs \cdot yz) - q(px + ry + sz) + q - L_3$; consequently $C_3 \geq 1$ and $C_3 \cdot xyz < q(pr \cdot xy + ps \cdot xz + rs \cdot yz)$. [formally verified: C2_C3_odd, C3_link, L3_identity, L3_bounds]

Dividing (L3) by xyz gives $C_3 = q(rs/x + ps/y + pr/z) - q(p/(yz) + r/(xz) + s/(xy)) + (q - L_3)/(xyz)$. Inequalities from the abundancy alone bound the exponents from below, since a larger exponent makes its term smaller; upper bounds can only come from exactness. Theorems 7.2 and 7.3 and Lemmas 7.4 and 7.5 extract them.

Theorem 7.2 (two regimes). For any exponents, $C_2(p, s) \leq -1$ and $C_2(r, s) \leq -1$. Hence exactly one of: (P) $C_2(p, r) \geq 1$; (M) all three pair coefficients are ≤ -1 . Moreover $p \geq N + 1$. [formally verified for Mathlib's σ : three_prime_one_positive_sigma gives $C_2(p, s) \leq 0$ and $C_2(r, s) \leq 0$, and three_prime_pair_negative_sigma the strict form, by the parity of Proposition 7.1 (L1)]

Theorem 7.3 (exponent one in regime (P)). If $N \geq 4$ and $C_2(p, r) \geq 1$, then $\alpha = 1$. [formally verified for Mathlib's σ : three_prime_exponent_sigma; $k = 1$ is covered by Kishore]

Lemma 7.4 (one prime power is small). $z \leq 3q \cdot pr$, or $y \leq 3q \cdot ps$, or $x \leq 3q \cdot rs$. [formally verified: three_prime_lemmaE] Proof. Otherwise each term of the bound in Proposition 7.1 is smaller than $xyz/(3q)$ times q , so $C_3 \cdot xyz < xyz$ ■

Lemma 7.5 (a second prime power is small, all three cases). (K_z) $x < 2q \cdot rs \cdot z$ or $y < 2q \cdot ps \cdot z$; (K_y) $x < 2q \cdot rs \cdot y$ or $z < 2q \cdot pr \cdot y$; (K_x) $y < 2q \cdot ps \cdot x$ or $z < 2q \cdot pr \cdot x$. [formally verified: K_gen, three_prime_lemmaK]

Proof. With c the distinguished prime, w its power and (a, u) , (b', v) the others, (L3) rearranges to $uv(C_3 w - q \cdot ab') = q(cw - 1)(au + b'v - 1) - L_3$. As $L_3 \leq c(au + b'v - 2)$ and $cw - 1 \geq c + 1$, the right side is positive and smaller than $q \cdot cw(au + b'v)$; hence $uv < 2q \cdot cw \cdot \max(au, b'v)$ ■

Theorem 7.6 (all prime powers bounded). With $T_1 = 3q \cdot rs$ and $T_2 = 2q \cdot rs \cdot T_1$, one of x, y, z is at most T_1 , a second at most T_2 , and all three are below $N \cdot T_1 T_2 = 18N \cdot q^3 r^3 s^3$. [formally verified: three_prime_exponent_caps] Proof. Lemma 7.4, then Lemma 7.5 in the case where that component is distinguished; the third component w satisfies $w < \sigma(w) < N \cdot m^2$ by Theorem 4.1 ■

Theorem 7.7 (regime (P): a bound on s). Let $\alpha = 1$ and $Q = C_2 p^2 - qr$. Then $(sQ + N \cdot L_2 p^2)yz = (p^3 - 1)q(ry + sz - 1) - L_3$, $Q < 0$, and $s(qr - C_2 p^2) < N \cdot L_2 p^2$. [formally verified: alpha_one_bounds]

Proof. With $\alpha = 1$, $x = p^2$ and $\sigma(x) = \Phi(p)$, the difference of the two sides of (★) $(sQ + N \cdot L_2 p^2)yz = (p^3 - 1)q(ry + sz - 1) - L_3$ is L_3 times the residual of (2.1) [checked by exact evaluation], so (★) holds on every solution. If $Q \geq 0$, (★) gives $N \cdot L_2 yz < qp(ry + sz)$. If $ry \geq sz$ this forces $N \cdot L_2 z < 2qpr$, impossible since $z \geq (r + 1)^2$. Otherwise $N \cdot L_2 y < 2qps$, and Theorem 4.1 at s gives $s^2 < N \cdot p^2 y$; together $N \cdot L_2^2 y < 4q^2 p^4$, hence $(p - 1)^2 y < 4Np^2 < 4p^3$, contradicting $y \geq (p + 1)^2$ and $(p - 1)^2(p + 1)^2 \geq 4p^3$ for $p \geq 5$. So $Q < 0$, and the left side of (★) is positive because the right side is ■

In regime (M), $C_3 = N \cdot L_2 - g \cdot s \geq 1$ with $g = -C_2(p, r) \geq 1$, so $s \leq (N \cdot L_2 - 1)/g$. [immediate from the formally verified C3_link and L3_bounds]

Theorem 7.8 (finite decision procedure, all exponents). For each $k \geq 2$ every three-prime counterexample lies in an explicit finite set: (p, r) in the sandwich window of Lemma 3.5; in regime (P) $\alpha = 1$, $qr - C_2 p^2 \geq 1$, $s \leq S := (N \cdot L_2 p^2 - 1)/(qr - C_2 p^2)$ and $y < 2q^2 p^6 r \cdot S$; in regime (M) $s \leq (N \cdot L_2 - 1)/g$ and x, y below the caps of Theorem 7.6 with s replaced by its bound; the remaining prime power is fixed by Theorem 4.1. [proved; every ingredient is formally verified]

Proof of the bound on y. Rewrite (★) as $y \cdot (z(sQ + N \cdot L_2 p^2) - (p^3 - 1)qr) = (p^3 - 1)q(sz - 1) - L_3$. The right side is positive, so the bracket is at least 1 and $y < (p^3 - 1)q \cdot sz$. Since $sQ + N \cdot L_2 p^2 \geq 1$, (★) also gives $yz < qp^3(ry + sz)$. If $sz \geq ry$ this gives $y < 2qp^3 s$; otherwise it gives $z < 2qp^3 r$, and then $y < (p^3 - 1)q \cdot sz < 2q^2 p^6 rs$. In both cases $y < 2q^2 p^6 r \cdot S$. In both regimes $s = \lfloor N \cdot m^2 / \Delta \rfloor$ is non-decreasing in α and β , so the exponent loops stop as soon as $\Delta \leq 0$ or s exceeds its bound, and γ is determined by the identities of Theorem 4.1 ■

Computation 7.9. An implementation of Theorem 7.8 with exact GMP arithmetic finds no three-prime counterexample with any exponents for every $k \leq 16$ ($k = 16$: 696,695,221 prime pairs, $2.30 \cdot 10^{10}$ exponent combinations). [computed; see Section 12] Theorem 7.7 alone removes almost every pair of regime (P), for example 99,103 of 99,106 at $k = 14$. The procedure also covers the cases $\alpha = \beta = 1$, $\gamma \geq 2$, which the squarefree searches do not test. Its cost grows by a factor of about 4 to 7 from one value of k to the next.

8. Three primes, squarefree: the exact structure

Let $b = prs$ be squarefree, $P = pr$, $S = p + r$, $D = D_s$, and $\Delta = N \cdot P^2 - q\Phi(p)\Phi(r) = f(pr)$.

8.1 Pell form

By Theorem 4.1 at s , $N \cdot P^2 = D\Phi(s) + s$ and $q\Phi(p)\Phi(r) = D \cdot s^2 + s - 1$; hence $\Delta = D(s + 1) + 1$ and

$$\Delta^2 - (D + 1)\Delta + D^2 = D \cdot N \cdot P^2. \quad (8.1)$$

Proposition 8.1 (Pell-orbit form). (b, k) is a counterexample if and only if (i) $\Delta = P^2 - q(S^2 + (P + 1)S + 1 - P)$; (ii) $X := 2\Delta - D - 1$ satisfies $X^2 - DN(2P)^2 = -(3D + 1)(D - 1)$; (iii) $D \mid \Delta - 1$ and $s = (\Delta - 1)/D - 1$. [formally verified: delta_PS_form, pell_form, squarefree_of_pell]

Proof. (i) follows from $\Phi(p)\Phi(r) = P^2 + PS + S^2 - P + S + 1$ and $N - q = 1$. (ii) and (iii) are (8.1) and $\Delta = D(s + 1) + 1$. Conversely, if $\Delta = D(s + 1) + 1$ and (ii) holds, then $X = 2Ds + D + 1$ and $X^2 + (3D + 1)(D - 1) = 4D(D\Phi(s) + s)$, so (ii) reads $4D(N \cdot P^2 - D\Phi(s) - s) = 0$. With $h_1 = N \cdot P^2 - D\Phi(s) - s$ and $h_2 = \Delta - D(s + 1) - 1$ one has, identically, $q\Phi(p)\Phi(r)\Phi(s) - (N \cdot P^2 s^2 - 1) = (s + 1)h_1 - \Phi(s)h_2$, so $h_1 = h_2 = 0$ gives (2.1) ■ Thus the whole squarefree three-prime case is a solution (X, Y) of a generalised Pell equation, with $Y = 2P$, such that the quadratic (i) has an integer root S with $S^2 - 4P$ a perfect square and such that p, r and s are primes. The two regimes play no role in this formulation.

Condition (i) is a quadratic in S whose discriminant is $q((N + 3)P^2 + 6qP - 3q - 2X - 2D - 2) = q^2(2S + P + 1)^2 - 4q \cdot E_i$, where $E_i = \Delta - P^2 + q(S^2 + (P + 1)S + 1 - P)$ with $2\Delta = X + D + 1$, so that (i) is $E_i = 0$; a square discriminant is therefore the integrality of S , and $S^2 - 4P = (r - p)^2$. Equivalently, as a quadratic in s for fixed (p, r) , $\Delta s^2 - B \cdot s - (B + 1) = 0$ with $B = q\Phi(p)\Phi(r)$, whose discriminant $B^2 + 4\Delta(B + 1) = (B +$

$2\Delta)^2 - 4\Delta(\Delta - 1)$ must be a square; this is the same condition. [formally verified: discriminant_S, squarefree_three_quartic]

Lemma 8.2 (reduction modulo q). $s(P^2 - D) \equiv 1$ and $(P^2 - D)(P^2 - D - 1) \equiv D \pmod{q}$. These follow from $b^2 \equiv 1 \pmod{q}$ and the definition of D , and are satisfiable modulo q for every residue of s . [formally verified: pell_congruence_mod_q]

Proof. As $N \equiv 1 \pmod{q}$, $\Delta \equiv P^2$ and $N \cdot P^2 \equiv P^2$, so the identities $\Delta = D(s + 1) + 1$ and $N \cdot P^2 = D\Phi(s) + s$ give $P^2 \equiv D(s + 1) + 1$ and $P^2 \equiv D\Phi(s) + s$. Subtracting, $Ds^2 \equiv 1 - s$, hence $s(P^2 - D) \equiv s(Ds + 1) \equiv 1$. Further $(P^2 - D)^2 \equiv (Ds + 1)^2 = D \cdot Ds^2 + 2Ds + 1 \equiv D(s + 1) + 1 \equiv P^2$, and $(P^2 - D)^2 - P^2 = (P^2 - D)(P^2 - D - 1) - D$ ■ The stronger congruence $(P^2 - D)(P^2 - D - 1) \equiv 0 \pmod{q}$ is not a consequence of (i) and (ii): it holds exactly when $q \mid D$, that is when $s \equiv 1 \pmod{q}$, and the point $N = 4$, $D = 2$, $P = 2$, $S = 0$, $X = 11$ satisfies (i) and (ii) but not this congruence [formally verified: strong_congruence_iff_dvd, strong_congruence_fails]. For every residue s prime to q , the values $D \equiv (1 - s)s^{-2}$ and $P \equiv \pm s^{-1}$ satisfy every reduction modulo q (Section 11.4).

Lemma 8.3 (the square case). If $D \cdot N$ is a perfect square, then $D^3 > (4/9)N \cdot P^2$, hence $D > 2s/3$; in regime (P) this never happens. [formally verified: pell_square_bound, positive_regime_not_square]

Proof. Write $DN = M^2$. By (ii), $(MY - X)(MY + X) = (3D + 1)(D - 1) > 0$ with $Y = 2P$ and $X > 0$, so $MY - X \geq 1$ and $MY + X \leq (3D + 1)(D - 1) < 3D^2$. Squaring $2MP < 3D^2$ gives $4DN \cdot P^2 < 9D^4$. Since $N \cdot P^2 > D \cdot s^2$ by Theorem 4.1, $D^2 > 4s^2/9$. In regime (P), Theorem 8.4 gives $D < N$, while $P > N^2$; then $4N^5 < 4N \cdot P^2 < 9D^3 < 9N^3$, which is impossible ■

Pell orbits for fixed (N, D) . If $D \cdot N$ is not a perfect square, the admissible products $P = pr$ lie in finitely many orbits of solutions of $X^2 - DN \cdot Y^2 = -(3D + 1)(D - 1)$ under the units of $\mathbb{Z}[\sqrt{(DN)}]$, and along each orbit Y grows geometrically with ratio at least $2\sqrt{(DN)}$; so an interval $[Y_1, Y_2]$ contains at most $1 + \log(Y_2/Y_1)/\log(2\sqrt{(DN)})$ values per orbit [proved; standard theory of the generalised Pell equation [15, 16]]. This bounds the number of candidates for each D but excludes none, and the number of admissible D grows with N . Section 9 turns this structure into a sieve for fixed D that is uniform in k . For each N this gives an algorithm for regime (M) that needs no bound on D_s : for each admissible D , compute the classes of the Pell equation from the continued fraction of $\sqrt{(DN)}$, run through the orbit points with $2N^2 < Y$ below the bound of Proposition 9.1, and test (i) and (iii); each D costs a period computation of length $O(\sqrt{(DN)} \cdot \log(DN))$.

8.2 The reduced-pair Z-form

Removing the smallest prime leaves a generalised two-variable equation. Put $M = N \cdot p^2$, $B = f(p) = M - q\Phi(p)$, $G = M(r + s - 1) - B \cdot rs$, $\varepsilon_r = B \cdot r - M$, $\varepsilon_s = B \cdot s - M$. As polynomial identities:

$$G(r + 1)(s + 1) - \varepsilon_r(r + 1) - \varepsilon_s(s + 1) - (B - 1) = q\Phi(p)\Phi(r)\Phi(s) - (N(prs)^2 - 1),$$

$$D_s = G(r + 1) - \varepsilon_s, \quad D_r = G(s + 1) - \varepsilon_r, \quad B - 1 = (p - N)(p + 1),$$

and on solutions $D_r D_s = (B - 1)G + \varepsilon_r \varepsilon_s$. [formally verified: reduced_pair_zform, reduced_pair_D, reduced_pair_B, reduced_pair_factor] For $B = 1$, that is $p = N$, this is the identity $(C \cdot Z_p - \delta_r)(C \cdot Z_r - \delta_p) = \delta_p \delta_r$ of Theorem 6.1, and the single term $(B - 1)G$, with $B - 1 = (p - N)(p + 1) \geq p + 1$, is what prevents the two-prime argument from closing the three-prime case. With $u = r + 1$, $v = s + 1$, $E = M + B$, $\kappa = 2B - G$, $X = \kappa u - E$ and $Y = \kappa v - E$, the first identity becomes $B \cdot X^2 - G \cdot XY + B \cdot Y^2 = \kappa(E^2 - (B - 1)\kappa) - \kappa^2 \cdot (\text{residual of } (2.1))$ [formally verified: reduced_pair_binary]. So a solution is a representation of $\kappa(E^2 - (B - 1)\kappa)$ by the binary form $(B, -G, B)$ of discriminant $G^2 - 4B^2$. In these variables the squarefree three-prime case asks that $G(r + 1)(s + 1) - \varepsilon_r(r + 1) - \varepsilon_s(s + 1) = B - 1$ have no integer solution with $p < r \leq s$ when $p > N$.

8.3 The positive regime

Theorem 8.4. In regime (P), $D \cdot (p - N)^2 < N$. [formally verified: delta_upper, positive_pair_bound] Hence $p - N < \sqrt{(N/2)}$ (as $D \geq 2$), and for fixed $(p - N, D)$ at most one pair (p, r) is possible. [proved]

Proof. Write $a = p - N$ and $c = r - N$, so $ac = qN - C_2$. Exactly, $\Delta = 1 + a(p + 1) + c(r + 1) - C_2(p + 1)(r + 1)$ [formally verified: delta_pair_form], hence $a\Delta = a^2(p + 1) + a + (r + 1)(qN - C_2(1 + a(p + 1)))$. Since $C_2 \geq 1$, the last factor is at most $N^2 - N - 1 - aN - a^2 - a$, and a direct comparison gives $a\Delta < N \cdot pr$. By (8.1), $\Delta^2 = D \cdot N \cdot P^2 + (D + 1)\Delta - D^2 > D \cdot N \cdot P^2$, since $\Delta > D$. Hence $D \cdot N \cdot P^2 a^2 < a^2 \Delta^2 < N^2 P^2$ ■ Uniqueness of the pair. For fixed (N, a, D) , Δ is a quadratic polynomial in c with leading coefficient $aN + a^2 + a + 1$, and the function $h(c) = \Delta(c) - (D + 1)/2 - p(N + c)\sqrt{(DN)}$ is convex with $h(0) < -N^4$. By (8.1) a solution satisfies $-1 < h(c) \leq 0$, and convexity forces $c = \lfloor R \rfloor$, where R is the positive root of h . So each pair (a, D) gives at most one candidate pair (p, r) , and regime (P) reduces to $O(N)$ candidates for each N instead of $O(N^2)$. The argument uses $D < N$ and therefore applies to regime (P) only.

8.4 The negative regime

In regime (M), with $g = \delta_p \delta_r - qN \geq 1$, $\Delta = 1 + \delta_p(p + 1) + \delta_r(r + 1) + g(p + 1)(r + 1)$, and $\sqrt{(DN)} \approx g + \delta_r/p$. The component quotient D can be of order N^3 , and no bound on D uniform in k is known. This is where the squarefree three-prime case remains open; Section 9 reduces it to large D . From $C_3 = N \cdot L_2 - g \cdot s \geq 1$ one obtains $s < N \cdot L_2/g$, and the upper bound of Proposition 7.1 places s , up to lower-order terms, in the window $(N \cdot L_2/(g + qr/p^2), N \cdot L_2/g)$. Proposition 4.2 then leaves $O(N)$ possible values of D_s rather than one, so the localisation of Section 8.3 does not reduce the search. Since $s = (\Delta - 1)/D - 1$ is determined by (p, r, D) , an interval $L < s < U$ containing a single integer is equivalent to knowing D , so a sharper window for s is the same problem as a bound on D_s .

8.5 A norm condition on C_3

Theorem 8.5 (conic fibration). With W and X affine in the symmetric functions of the δ 's and $T(c) = N(N - 1)(c - 3N)^2 + 3N + 1$, every squarefree three-prime solution satisfies $(3N + 1)(W^2 - 4) = (N - 1)(3X^2 + 4N(C_3 - 3N)^2)$. [formally verified: conic_norm_identity, conic_norm] For fixed C_3 (local solvability by Hilbert symbols and the Hasse–Minkowski theorem [11]) the conic has a rational point if and only if $(3N + 1)T(C_3)$ is a norm from $\mathbb{Q}(\sqrt{-3})$ (k even) or $\mathbb{Q}(\sqrt{-6})$ (k odd) [proved, Hasse–Minkowski]. This decides rational solvability only; it says nothing about integral points or primes, and is a filter on C_3 , not an exclusion of solutions. Its integral content is $(3X)^2 \equiv (2u)^2 \pmod{3N + 1}$, $u = C_3 - 3N$. [formally verified: conic_divisibility]

Proof of the norm criterion. A conic $aW^2 + bX^2 = c$ has a rational point if and only if $(ac, bc)_v = 1$ at every place v [11]; this is the same condition as $(-ab, ac)_v = 1$, since $(x, -x)_v = 1$. Here $a = 3N + 1$, $b = -3(N - 1)$ and $c = 4T(C_3)$. With $A = (3N + 1)T(C_3)$, removing square factors and using $(A, -A)_v = 1$, the symbol becomes $(A, 3(N - 1)(3N + 1))_v$. Now $A = (3N + 1)^2 + (3N + 1)(N - 1) \cdot N \cdot u^2$. If $N = M^2$, then $A = x^2 + (3N + 1)(N - 1)y^2$ with $x = 3N + 1$ and $y = Mu$, so $(A, -(3N + 1)(N - 1))_v = 1$ and the symbol equals $(A, -3)_v$; if $N = 2M^2$, the same argument with $2(3N + 1)(N - 1)$ gives $(A, -6)_v$ ■ For $N \in \{8, 16, 32, 64, 256\}$ and every $C_3 \leq 3,000$ the criterion agrees with a direct computation of the Hilbert symbols, and the proportions of values of C_3 that it excludes are 66.8%, 47.7%, 69.1%, 65.9% and 47.8%; these are proportions of impossible values of C_3 , not of excluded solutions. The Hilbert-symbol routine was validated against a brute-force test of local solvability of $z^2 = ax^2 + by^2$ for all squarefree $a, b \in [-30, 30]$ (5,776 cases, no disagreement) [computed].

8.6 Regime (P): exact division and an exclusion near the top, for every k

In regime (P) put $a = p - N \geq 1$, $c = r - N$ and $j = C_2(p, r) = qN - ac \geq 1$. Then $a \cdot r = aN + qN - j$, so every quantity of the pair (p, r) is a polynomial in N with coefficients in $\mathbb{Z}[a, j]$.

Lemma 8.5A (scale of r in regime (P)). $r > q(N + a)/(a + 1)$; in particular $r > N^2/(2a)$ for $N \geq 4$ (for $a = 1$ because r is odd and $N^2/2$ is even). [proved] Proof. By Lemma 3.4, $1/r < 1/q - 1/p - 1/s < 1/q - 1/p = (a + 1)/(q(N + a))$ ■

Proposition 8.6 (exact division). Let $A = a^2\Delta$, with $\Delta = N(\text{pr})^2 - q\Phi(p)\Phi(r)$. Then A is a monic quartic in N : $A = N^4 - (aj - a + 2)N^3 + (1 - 2j - 2a^2j)N^2 + (a^3 - a - a^3j - a^2j + aj^2 + 2j)N + A_0(a, j)$, and $a^2 \cdot N \cdot (\text{pr})^2 = Q \cdot A + R$, where $Q = N^3 + (3a + aj)N^2 + (2aj + 3a^2 + 4a^2j + a^2j^2)N + Q_0(a, j)$ and $R = R_3N^3 + R_2N^2 + R_1N + R_0$ has degree 3 in N , with explicit coefficients in $\mathbb{Z}[a, j]$ (listed in the Lean module RegimeP). Moreover $(aj)^4 \leq R_3 \leq 82(aj)^4$, $-22(aj)^5 \leq R_2 \leq 83(aj)^5$, $-111(aj)^6 \leq R_1 \leq 55(aj)^6$, $-114(aj)^7 \leq R_0 \leq 33(aj)^7$. [formally verified: regimeP_division, bound_R0-bound_R3, bound_R3_low]

Theorem 8.7 (exclusion near the top of regime (P)). Let (b, k) be a squarefree three-prime counterexample in regime (P), with $N \geq 2^{21}$. Then $(p - N) \cdot C_2(p, r) > (N/100)^{1/4}$. [formally verified: regimeP_top_bounds, regimeP_sandwich, regimeP_top_exclusion; its hypothesis is derived from the component identity $N(\text{pr})^2 = s\Delta + D$ by rpA_eq ($A = a^2\Delta$) and regimeP_hcomp]

Proof. Theorem 4.1 at s gives $N(\text{pr})^2 = s\Delta + D$ with $D \geq 1$, and Theorem 8.4 gives $a^2D < N$. Multiplying by a^2 , $a^2N(\text{pr})^2 = s \cdot A + a^2D$, and Proposition 8.6 gives $(s - Q) \cdot A = R - a^2D$. If $w = aj$ satisfies $100w^4 \leq N$ and $N \geq 2^{21}$, then $10^5w \leq N$, and the coefficient bounds give $R \geq w^4N^3(1 - 10^{-3}) \geq N$ and $R \leq 0.83 \cdot N^4 < (1 - 10^{-4})N^4 \leq A$. Hence $0 < R - a^2D < A$, so the integer $s - Q$ lies strictly between 0 and 1, a contradiction ■ For $k \leq 20$ there is no squarefree three-prime counterexample at all (Section 12), so Theorem 8.7 holds for every k .

Remark 8.8 (the range of Theorem 8.7). To leading order $a^4\Delta \approx a(a(N - aj) - (a + 1)^2)N^3$, so with $V = a(N - aj) - (a + 1)^2$ one has $s \approx aN^4/V$ and $D \approx V^2/(a^4N)$. Small aj is the top of the range of D (D close to N/a^2), which Theorem 8.7 removes; Theorem 9.6 removes the bottom ($D \leq 500,000$). For larger aj the quotient $s - Q$ is a non-zero integer $m \approx R/A$, and the condition $R - mA \in (0, N)$ allows a bounded number of j for each m : a finite search for each k , not a contradiction.

Proposition 8.9 (the window fixes the quotient). In the setting of Theorem 8.7 (without the size hypothesis on aj), put $E = a^2D$. Then $0 < E < N < A$, and $E = R \bmod A$, $s = Q + \lfloor R/A \rfloor$. Hence, for each triple (N, a, j) , the integer $m = s - Q$ is uniquely determined, and a counterexample exists only if two numerical coincidences hold: (i) $R \bmod A < N$, and (ii) $D(s + 1) = \Delta - 1$ with $s = Q + \lfloor R/A \rfloor$ and $D = (R \bmod A)/a^2$. [formally verified: regimeP_m_determined, with its hypothesis supplied by rpA_eq and regimeP_hcomp]

Proof. $a^2N(\text{pr})^2 = s \cdot A + E$ with $0 \leq E < A$, and $a^2N(\text{pr})^2 = Q \cdot A + R$; so $R = E + A(s - Q)$, and Euclidean division by A gives the claim ■

Remark 8.10 (congruences on m). Reducing modulo N and modulo q determines a^2D modulo qN , which is Proposition 4.2, and since $a^2D < N$ its residue modulo N determines it. The component identity $\Phi(s)D \equiv -s \pmod{N}$, with $s \equiv Q(0) + m$, gives the cubic congruence $a^2(Q(0) + m) + (R(0) - mA(0)) \cdot \Phi(Q(0) + m) \equiv 0 \pmod{N}$, a filter on m modulo 2^k . As $m = \lfloor R/A \rfloor$ is fixed by (N, a, j) , this is a test for each (a, j) , not a contradiction for all of them; congruences alone cannot give one (Section 11.4).

Proposition 8.11 (regime (P) as integral points on a family of quartic curves). Put $G(N, a, j) = (A + N(aP)^2)^2 - 4A(A - a^2)$, with $A = a^2\Delta$ and $aP = (N + a)(aN + qN - j)$ as in Proposition 8.6. Every squarefree three-prime counterexample in regime (P) gives an integral point (j, y) on the curve $C_{N,a}$: $y^2 = G(N, a, j)$, with $y = a^2(\Delta + N(\text{pr})^2 - 2D)$. As a polynomial in j , G has degree 4 and leading coefficient $(L - 2M)(L + 2M)$, where $L = N(N + a)^2 + M$ and $M = aN + a^2 + a + 1$. [identity formally verified: regimeP_quartic, with $A = a^2\Delta$ supplied by rpA_eq; degree and leading coefficient checked by exact expansion] For every tested pair (N, a) ($N = 2^{21}, 2^{22}, 2^{25}, 2^{30}$; $a = 1, 2, 5, 11$) the quartic is squarefree and its leading coefficient is not a square, so $C_{N,a}$ has genus one [computed].

Proof. Relation (8.1), $\Delta^2 - (D + 1)\Delta + D^2 = DN(\text{pr})^2$, says that D is a root of $X^2 - (\Delta + NP^2)X + \Delta^2 - \Delta$; its discriminant times a^4 is G , and its square root is $a^2(\Delta + NP^2 - 2D)$ ■

Remark 8.12 (regime (P) as a family of curves). For fixed k and a the counterexamples of regime (P) are integral points on the genus-one curve $C_{N,a}$, finitely many by Siegel's theorem, and there are fewer than $\sqrt{(N/500,001)}$ such curves for each k . As a polynomial in N for fixed (a, j) , G is monic of degree 14 and Runge's method applies, which gives Theorem 8.7 where N is large compared with aj . As a polynomial in j for fixed (N, a) , its leading coefficient $(L - 2M)(L + 2M)$ is not a square and Runge's method does not apply. In the middle of the range, where aj and $N - aj$ are both of order N , there is no small parameter, and an argument valid for every k must control the integral points of the whole family $C_{N,a}$: the same kind of uniformity as in Section 9.

Lemma 8.13 (the budget of the two larger primes). Let $b = prs$ be a squarefree three-prime counterexample with $p < r < s$, $a = p - N$ and $M = f_N(p) = a(p + 1) + 1$. Then, exactly, $q\Phi(p) \cdot (\Phi(r)\Phi(s) - r^2s^2) = M \cdot r^2s^2 - 1$, that is $x_r + x_s + x_r x_s = (M - 1/(rs)^2)/(q\Phi(p))$ with $x_t = 1/t + 1/t^2$. Consequently $q\Phi(p)/M < r < 2q\Phi(p)/(M - 1) + 2$. [identity: Proposition 3.9 with $m = p$, $u = rs$; lower bound formally verified: budget_lower; upper bound proved]

Proof. The identity is Proposition 3.9 with $f_N(prs) = 1$. Since $\Phi(r)\Phi(s) - r^2s^2 > (r + 1)s^2$, it gives $q\Phi(p)(r + 1) < M r^2$, hence $q\Phi(p) < Mr$. For the upper bound put $\beta = (M - 1/(rs)^2)/(q\Phi(p)) > (M - 1)/(q\Phi(p)) = 2e$. Since $x_s < x_r$, $\beta < 2x_r + x_r^2$. If $r \geq 1/e + 2$, then $x_r \leq e - e^2 + 4e^3$, so $2x_r + x_r^2 < 2e$ for $e < 1/20$; here $e = a(p + 1)/(2q\Phi(p)) < 1/N$, so $e < 1/20$ for $k \geq 5$, and smaller k are excluded by the computations of Section 12. This is a contradiction ■

Remark 8.14 (the budget and the reduced pair). Lemma 8.13 sharpens Lemma 8.5A, since $q\Phi(p)/M > qp^2/M > q(N + a)/(a + 1)$, and it holds in both regimes. Its budget M is the quantity $B = f_N(p)$ of Section 8.2, whose excess $B - 1 = a(p + 1)$ is the obstruction term there. In regime (P), together with $r < N(p - 1)/a$ (that is, $C_2(p, r) \geq 1$), it leaves for r an interval of length about $N/a^2 + 1$, which is the content of Theorem 8.4; within it s is determined by r , and one numerical coincidence remains (Proposition 8.9).

9. A uniform-in- k result: the 2-adic Pell sieve

Every result on three primes in Sections 7 and 8 holds for each k separately. This section gives statements valid for all k at once, at the price of fixing the component quotient $D = D_s$ at the largest prime. It uses the shape $N = 2^k$ in an essential way.

Proposition 9.1 (the Pell equation does not depend on k). Let $b = prs$ be a squarefree three-prime counterexample with $k \geq 5$, $X = 2\Delta - D - 1$, $c = (3D + 1)(D - 1)$, $t = lk/2j + 1$ and $Y = 2^t P$. Then $X^2 - d \cdot Y^2 = -c$ with $d = D$ for even k and $d = 2D$ for odd k ; $v_2(Y) = t$ exactly; and $2^{5t-4} < Y < 2^{7t}$. [Pell forms formally verified: pell_even, pell_odd; bounds proved]

Proof. Write $N = M^2$ (k even) or $N = 2M^2$ (k odd); then $2M = 2^t$ and Proposition 8.1(ii) becomes $X^2 - D(2MP)^2 = -c$, respectively $X^2 - 2D(2MP)^2 = -c$. P is odd, so $v_2(Y) = t$. $P > N^2$. By Lemma 3.5(ii) and $p \geq N + 1$, $(r/(r - 1))^2 > 1 + 1/(N(N + 1))$, so $r \leq 2N^2 + 2N + 1$; with $p \leq 3N - 1$ (Lemma 3.6), $P < 7N^3$ for $N \geq 8$. Substituting $N = 2^{2t-2}$ or 2^{2t-1} gives the bounds ■

For fixed D , all k are governed by one Pell equation; a counterexample at level k is a solution with $v_2(y) = t$ and $5t - 4 < \log_2 y < 7t$, so $v_2(y) > (\log_2 y)/7$. Along an orbit y_n grows geometrically while $v_2(y_n)$ grows only slowly; this is the source of uniformity.

Theorem 9.2 (fixed D). Fix $D \geq 2$ and put $c = (3D + 1)(D - 1)$. (a) If $-c$ is not a square in $\mathbb{Q}_2$, then $2t \leq v_2(c) + 2$. (b) If d is a perfect square, Lemma 8.3 gives $N^5 < 9D^3/4$. (c) In every case only finitely many k are possible, effectively. [proved; (c) by Theorem 9.4]

Proof of (a). $X^2 + c = dY^2$ with $2^t \mid Y$ gives $X^2 \equiv -c \pmod{2^{2t}}$; a 2-adic integer is a square if and only if, after removing an even power of 2, it is $\equiv 1 \pmod{8}$ ■

Theorem 9.3 (2-adic splitting). Let ε be the fundamental unit of norm 1 of $\mathbb{Z}[\sqrt{d}]$ and $\alpha \cdot \varepsilon^n = x_n + y_n \sqrt{d}$ an orbit of solutions. If $\varepsilon^m = 1 + 2^w \eta$ with $\eta \in \mathbb{Z}[\sqrt{d}]$, then for every index v , $y_{v+mj} = \sum_{i \geq 0} C(j, i) 2^{wi} \gamma_i$ with γ_0

$= y_v$ and $\gamma_i \in \mathbb{Z}$ (a finite sum for $j \geq 0$, a convergent series in $\mathbb{Z}_2$ for $j < 0$). Hence if $v_2(y_v) < w$, then $v_2(y_n) = v_2(y_v)$ on the whole class $n \equiv v \pmod{m}$; otherwise the class splits into two classes modulo $2m$, for which $\varepsilon^{2m} \equiv 1 \pmod{2^{w+1}}$. Running the splitting to depth H gives $v_2(y_n) \leq H + 1$ for every n outside the classes still unsplit at depth H . [proved]

Theorem 9.4 (closure by linear forms in two 2-adic logarithms). With $\beta = \alpha/\bar{\alpha}$, $y_n = \bar{\alpha}\varepsilon^{-n}(\beta(\varepsilon^2)^n - 1)/(2\sqrt{d})$, so $v_2(y_n) \leq v_2(c) + v_2(\beta(\varepsilon^2)^n - 1)$. If β is not an algebraic integer, β and ε^2 are multiplicatively independent, and the estimate of Bugeaud and Laurent [13] applies. In the form of Theorem H of [14] it reads: if α_1, α_2 are multiplicatively independent algebraic numbers with $v_p(\alpha_1) = v_p(\alpha_2) = 0$ (v_p normalised by $v_p(p) = 1$), $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$, b_1, b_2 are positive integers, $\log A_i \geq \max\{h(\alpha_i), (\log p)/D\}$ and $b' = b_1/(D \log A_2) + b_2/(D \log A_1)$, then $v_p(\alpha_1^{b_1}\alpha_2^{b_2} - 1) \leq (24p(p^D - 1)D^4/((p - 1)(\log p)^4)) \cdot \max\{\log b' + \log \log p + 0.4, 10(\log p)/D, 10\}^2 \cdot \log A_1 \cdot \log A_2$. Here $p = 2$, $D = 2$, $\alpha_1 = \beta$, $b_1 = 1$, $\alpha_2 = \varepsilon^{\pm 2}$ and $b_2 = |n|$, and the term $10(\log 2)/2 < 10$ can be dropped from the maximum. This gives $v_2(\beta(\varepsilon^2)^n - 1) \leq K \cdot \max\{\log b' + \log \log 2 + 0.4, 10\}^2 \cdot \log A_1 \cdot \log A_2$, with $K = 24 \cdot 2 \cdot (2^2 - 1) \cdot 2^4/(\log 2)^4 \approx 9.98 \cdot 10^3$, $\log A_1 \geq \max\{h(\beta), (\log 2)/2\}$, $\log A_2 = \log \varepsilon$ and $b' = 1/(2 \log A_2) + |n|/(2 \log A_1)$. This grows like $(\log |n|)^2$, while Proposition 9.1 needs $v_2(y_n) > (|n| \cdot \log_2 \varepsilon - C')/7$. So there is an explicit n_0 beyond which no orbit index can give a counterexample. [proved, using the cited estimate; all computations use $10^4 \cdot K$ as a safety margin]

Algorithm for one pair (D, d). (1) All fundamental solutions of $X^2 - dY^2 = -c$, by the continued-fraction method of Lagrange, Matthews and Mollin [15], applied to $-c/f^2$ for every $f^2 \mid c$. (2) No solution: the pair is excluded. (3) $-c$ not a 2-adic square: enumerate the boundedly many relevant t . (4) Otherwise compute n_0 , run the splitting of Theorem 9.3 until every unsplit class has least $|n| \geq n_0$ (or the tree terminates), and test every solution with $t \leq H + 1$ in the window of Proposition 9.1 against Proposition 8.1(i). Validation: for $D \leq 200$ the method reproduces exactly the orbits of a brute-force enumeration within Nagell's bound, and for 60 random $D \leq 20,000$ it recovers all solutions with $y < 3 \cdot 10^5$.

Computation 9.5 (D ≤ 100,000). Of the 199,998 pairs (D, parity of k) with $2 \leq D \leq 100,000$: 156,188 have no Pell solution; in 11,299, $-c$ is not a 2-adic square; in 3,429 the 2-adic tree terminates; 28,544 are closed by Theorem 9.4 after splitting; 538 have d a square. The window of Proposition 9.1 was met 1,284,588 times, and no candidate satisfies Proposition 8.1(i). No case of an integral β and no excessive depth occurred. [computed] As an independent cross-check for $D \leq 200$, a brute-force enumeration of all fundamental solutions within Nagell's bound generated every orbit point with $y < 2^{28,010}$ (2,917,991 points): 424 lie in the valuation window, 68 also give an odd P in $(\mathbb{N}^2, 7\mathbb{N}^3)$ and an integral s , all with $k \leq 34$, and none satisfies Proposition 8.1 (i).

Computation 9.5A (100,000 < D ≤ 500,000). The procedure of Computation 9.5 was run on the next range with a faster implementation of two of its steps: $c = (3D + 1)(D - 1)$ is factored through its two factors with a sieve of smallest prime factors, and square roots modulo prime powers are computed by the Tonelli–Shanks algorithm and Hensel lifting; the iteration cap of the continued-fraction step was raised from $2 \cdot 10^4$ to $4 \cdot 10^5$, with a warning if it is reached. The faster implementation reproduces the output of the original one exactly on $201 \leq D \leq 1,000$ (88,084 window points) and on $150,001 \leq D \leq 150,300$, and the square roots agree on 3,000 random cases. Of the 800,000 pairs (D, parity of k) with $100,000 < D \leq 500,000$: 644,776 have no Pell solution; in 39,904, $-c$ is not a 2-adic square; in 12,606 the 2-adic tree terminates; 102,046 are closed by Theorem 9.4 after splitting; 668 have d a square. The window of Proposition 9.1 was met 1,253,360 times, and no candidate satisfies Proposition 8.1 (i). No integral β , no excessive depth and no warning occurred. [computed]

Theorem 9.6. For every k there is no squarefree three-prime counterexample with $D_s \leq 500,000$. [proved, conditional on Computations 9.5 and 9.5A and on the searches $k \leq 20$ of Section 12, and using the cited estimate [13, 14]; from Propositions 4.3, 9.1 and Theorems 9.2–9.4] Proof. $D_s = 1$ is excluded by Proposition 4.3; $k \leq 20$ by the squarefree searches of Section 12.1; for $k \geq 5$ a square d forces $k \leq 10$ by Theorem 9.2(b); all other pairs by Computation 9.5 ($D \leq 100,000$) and Computation 9.5A ($100,000 < D \leq 500,000$) ■

Corollary 9.7. Every squarefree three-prime counterexample satisfies $s < \text{pr} \cdot \sqrt{(N/500,001)}$ (since $D_s s^2 < N(\text{pr})^2$), and in regime (P) also $p - N < \sqrt{(N/500,001)}$ (Theorem 8.4). [proved, conditional as Theorem 9.6] Since the searches of Section 12 already exclude $k \leq 20$, the bounds are of interest for $k \geq 21$.

Remark 9.8 (where the 2-adic method stops, line by line). (i) Theorem 9.4 bounds the orbit index n by an explicit $n_0(D)$, which depends on D through $h(\beta)$ and $\log \varepsilon$. It is uniform in k for fixed D , but $n_0(D)$ is not bounded uniformly in D . (ii) For a given k the relevant D go up to about $9N^3 \approx 2^{6t}$, and the window of Proposition 9.1 has logarithmic width $(2t + 4) \cdot \log 2$. When $\log \varepsilon_d$ exceeds this width, each orbit meets the window in at most one point, $n = 0$ or a neighbour of it. The linear-form bound then has nothing to act on, because it controls large n and not the fundamental solution itself. Among 179,630 values $d \in \{D, 2D\}$ with $10^4 \leq D < 10^5$, only 4,603 (2.6%) have a fundamental unit small enough, with a generous margin, for two orbit points to fit in the window for the smallest relevant t [computed]. The proportion decreases as D grows, since units of small height are rare. (iii) So for almost all D near the top of the range, the question is not about linear forms in logarithms. It is whether a fundamental solution of $X^2 - dY^2 = -(3D + 1)(D - 1)$ can have $v_2(Y) = t$ exactly with $2^{5t-4} < Y < 2^{7t}$, together with Proposition 8.1 (i). This is a question about the 2-adic valuations of fundamental solutions across the whole family of D , for which no general theory is known to us.

Remark 9.8A (where the window points fail). Each point of an orbit in the valuation window of Proposition 9.1 (valuations up to 60) was classified by the first condition of Proposition 8.1 that it violates, in the order: $P \in (N^2, 7N^3)$; $D \mid \Delta - 1$ with $2\Delta = X + D + 1$; the real root S^* of (i) at least $2\sqrt{P}$; the discriminant of (i) a square. For $2 \leq D \leq 3,000$ there are 96,844 failures of the range of P , 168,020 of $D \mid \Delta - 1$, 11,064 of the size of S^* , and 26,084 points that satisfy all of these and fail only because the discriminant of (i) is not a square. These last points occur at a rate of about 1.2 per value of D near $D = 2 \cdot 10^4$, 0.1 near $2 \cdot 10^5$ and 0.05 near $4 \cdot 10^5$, roughly as $1/D$, so that their number up to D grows like $\log D$; in the samples with $D \geq 2 \cdot 10^4$ all of them have $k \leq 14$. Their discriminants are squares modulo 4 and modulo 8 in every case, and modulo 3, 5, 7, 9, 11, 13 and 2^j ($j \geq 4$) both residues and non-residues occur [computed]. So the valuation window does not exclude a counterexample by itself, and no local condition excludes the last step: the final exclusion is the non-squareness of one discriminant, that is, the absence of an integral point on a curve of genus one (Proposition 8.11, Theorem 10.13). A uniform treatment of the squarefree three-prime case therefore needs uniform control of integral points on a family of curves of genus one; uniform control of the 2-adic valuations of fundamental solutions would not suffice [heuristic].

Remark 9.9 (the hypotheses of Theorem 9.4, and the integral case). Theorem H of [14] (from [13]) applies to two multiplicatively independent algebraic numbers that are units at the prime above 2 under consideration. (i) ε^2 is a unit of the ring of integers, so it has valuation 0 at every finite place. (ii) $\beta = \alpha/\bar{\alpha}$ has valuation $v_{\mathfrak{P}}(\alpha) - v_{\mathfrak{P}}(\bar{\alpha})$ at a prime $\mathfrak{P}$ above 2. This is 0 unless 2 splits in $\mathbb{Q}(\sqrt{d})$. If it is not 0, then $v_2(\beta(\varepsilon^2)^n - 1) = \min(v_{\mathfrak{P}}(\beta), 0)$ or a bounded quantity for every n , and $v_2(y_n) \leq v_2(c)$ directly. (iii) If β is not an algebraic integer, β and ε^2 are multiplicatively independent: a relation $\beta^a = \varepsilon^{2b}$ with $a \neq 0$ would make β integral over $\mathbb{Z}$. (iv) If β is an algebraic integer, then β is a unit of the maximal order $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{d})$, of norm 1, since $N(\beta) = 1$. The order $\mathbb{Z}[\sqrt{d}]$ ($d = D$ or $2D$ need not be squarefree) has finite unit index $\mu = [\mathcal{O}_K^\times : \mathbb{Z}[\sqrt{d}]^\times]$, and the norm-one units of $\mathbb{Z}[\sqrt{d}]$ are exactly $\pm \varepsilon^{\mathbb{Z}}$ by the definition of ε . Hence $\beta^\mu = \pm \varepsilon^j$ for some $j \in \mathbb{Z}$. Only the finiteness of μ is used (μ divides 3 when d is squarefree, but not in general). Then $\beta^\mu(\varepsilon^2)^{\mu n} - 1 = \pm \varepsilon^{2\mu n + j} - 1$. By Theorem 9.3 (equivalently, the lifting-the-exponent lemma in $\mathbb{Q}_2(\sqrt{d})$), $v_2(\pm \varepsilon^\mu - 1) \leq C_d + \log_2(|\mu| + 1)$ for an explicit constant C_d . Since $\beta(\varepsilon^2)^n - 1$ divides $\beta^\mu(\varepsilon^2)^{\mu n} - 1$ in $\mathcal{O}_K$, the same bound holds for $v_2(\beta(\varepsilon^2)^n - 1)$ with $m = 2\mu n + j$. Three details complete the argument: (a) If $z = \beta(\varepsilon^2)^n$ satisfies $z^\mu = 1$, then $z = \pm 1$, since K is real. If $z = 1$, then $y_n = 0$, which is not a point of the window. If $z = -1$, then $z - 1 = -2$ and v_2 is bounded. Otherwise $z^\mu - 1 \neq 0$ and the divisibility applies. (b) When 2 splits in K , the bound is applied at each of the two primes above 2. (c) For fixed D the orbits are finitely many, given by the finite list of fundamental solutions of step (1) of the algorithm ([15, 16]). Each orbit has its own β , its own j (computable from $\beta^\mu = \pm \varepsilon^j$) and its own C_d . The bound is therefore uniform over all orbits for that D , with constant max over the finite list, and Theorem 9.4 and this remark are statements

for fixed D only. No uniformity in D is claimed: that is exactly the open question of Remark 9.8. So the integral case is closed without linear forms, with a bound that grows only like $\log n$. In Computation 9.5 no integral β occurred. [proved]

Coverage of Computations 9.5 and 9.5A. For each pair (D, d) , every orbit of solutions of $X^2 - dY^2 = -c$ comes from one of the fundamental solutions listed in step (1). That list is complete by [15, 16] and was cross-validated by brute force for $D \leq 200$ and on random $D \leq 20,000$. For each orbit, every residue class of the index n produced by the splitting of Theorem 9.3 ends in one of three ways: (a) the class has constant valuation $v_2(y_n) \leq H + 1$, and all its members with y_n in the window of Proposition 9.1 are enumerated and tested exactly against Proposition 8.1 (i); (b) the class terminates, with no member of valuation t in the window; (c) the least $|n|$ in the class is at least $n_0(D)$ of Theorem 9.4, computed with $10^4 \cdot K$, so no member can satisfy $v_2(y_n) > (\log_2 y_n)/7$. The window was met 1,284,588 times in Computation 9.5 and 1,253,360 times in Computation 9.5A, and every such point failed Proposition 8.1 (i). Pairs with no solution, with $-c$ not a 2-adic square, or with d a square are closed by Theorem 9.2. Hence every k and every $D \leq 500,000$ is covered by a proved bound or an exact test.

9.1 Higher exponents: finiteness in k for fixed D , for any number of primes

Proposition 9.10 (the curves of Section 9.1 are nonsingular). For integers $e \geq 1$ and $D \geq 1$ put $S_e(T) = 1 + T + \dots + T^{2e} = \sigma(T^{2e})$ and $F_{D,e}(T) = D \cdot S_e(T) + T$. For every real $D > 0$, $F_{D,e}$ has a repeated complex root if and only if $D = D^*(e)$, where $D^*(e) = x_0((2e - 1)x_0 + 2e)/(2e + 1)$ and x_0 is the unique positive root of $x^{2e+1}((2e - 1)x + 2e) = 2x + 1$. For $e \geq 2$ one has $1 < D^*(e) < 2$. Consequently, for every $e \geq 2$ and every integer $D \geq 1$, $F_{D,e}$ has no repeated root. [proved; the elimination and the exclusion of every integer $D \geq 1$ are formally verified: `double_root_quadratic`, `quadratic_root_real`, `sixteen_pow_bound`, `no_double_root`]

Proof. Write $S = S_e$. Then $(T - 1)S(T) = T^{2e+1} - 1$ and, differentiating, $(T - 1)S'(T) + S(T) = (2e + 1)T^{2e}$. Let $\theta \in \mathbb{C}$ be a double root ($\theta \neq 0$ and $\theta \neq 1$, since $F(0) = D$ and $F(1) = (2e + 1)D + 1$), so that $D \cdot S(\theta) + \theta = 0$ and $D \cdot S'(\theta) + 1 = 0$. Multiplying the two identities for S by D and substituting gives

$$(i) (2e + 1)\theta^{2e}D = 1 - 2\theta, \quad (ii) D(\theta^{2e+1} - 1) = -\theta(\theta - 1),$$

and $(2e + 1) \cdot (ii) - \theta \cdot (i)$ eliminates θ^{2e} : $(2e + 1)D = (2e - 1)\theta^2 - 2e\theta$. This elimination holds in every commutative ring (`double_root_quadratic`). The relation is not an equation for θ alone: it links θ to D . Eliminating D instead of θ^{2e} gives $S(\theta) - \theta S'(\theta) = 0$, an equation of degree $2e$ in θ (for $e = 2$: $1 - \theta^2 - 2\theta^3 - 3\theta^4 = 0$). The two routes agree: substituting the quadratic relation into (i) gives $\theta^{2e+1}((2e - 1)\theta - 2e) = 1 - 2\theta$, and one checks from $(T - 1)S = T^{2e+1} - 1$ and $(T - 1)S' = (2e + 1)T^{2e} - S$ that $T^{2e+1}((2e - 1)T - 2e) - (1 - 2T) = -(T - 1)^2(S(T) - TS'(T))$ identically. For real $D > 0$ this quadratic in θ has discriminant $4e^2 + 4(4e^2 - 1)D > 0$, so θ is real (`quadratic_root_real`: if $\theta = u + vi$, the imaginary part gives $(2(2e - 1)u - 2e)v = 0$, and $v \neq 0$ would make the real part $-(2e - 1)(u^2 + v^2) - (2e + 1)D < 0$); its two roots have product $-(2e + 1)D/(2e - 1) < 0$. If $\theta > 0$, then (i) gives $\theta < 1/2$, and $\theta((2e - 1)\theta - 2e) < 0 < (2e + 1)D$, a contradiction. Hence $\theta = -x$ with $x > 0$ and

$$(9.1) \quad (2e + 1)D = (2e - 1)x^2 + 2ex, \quad (2e + 1)x^{2e}D = 1 + 2x.$$

Eliminating D gives $x^{2e+1}((2e - 1)x + 2e) = 2x + 1$. By Descartes' rule of signs this equation has exactly one positive root x_0 , and the first equation of (9.1) expresses D as the increasing function $g(x) = x((2e - 1)x + 2e)/(2e + 1)$; hence $D = g(x_0) = D^*(e)$. Conversely, at $D = D^*(e)$ and $\theta = -x_0$ the identities (i) and (ii) hold, and reading the computation backwards ($\theta \neq 1$) gives $D \cdot S(\theta) + \theta = 0$ and $D \cdot S'(\theta) + 1 = 0$, so $-x_0$ is a double root.

It remains to show that no integer $D \geq 1$ satisfies (9.1) when $e \geq 2$. If $D \geq 2$, the first equation forces $x > 1$, since for $0 < x \leq 1$ its right-hand side is at most $4e - 1 < 2(2e + 1)$; then $x^{2e} \geq x$ and $(2e + 1)x^{2e}D \geq 10x > 1 + 2x$, contradicting the second equation. If $D = 1$, the quadratic $(2e - 1)x^2 + 2ex - (2e + 1)$ equals $-0.08e - 1.36 < 0$ at $x = 3/5$ and $0.88e - 1.64 > 0$ at $x = 4/5$, so $3/5 < x < 4/5$. Then $1 + 2x > 11/5$, while $(2e + 1)x^{2e} < (2e + 1)(16/25)^e \leq 5 \cdot (16/25)^2 = 2.048 < 11/5$, because $(2e + 3) \cdot (16/25) \leq 2e + 1$ for $e \geq 2$. This

again contradicts the second equation. Finally, let $x_1 < x_2$ be the positive points where $g = 1$ and $g = 2$, and $h(x) = x^{2e+1}((2e-1)x + 2e) - 2x - 1 = (2e+1)g(x)x^{2e} - 2x - 1$. The two estimates just made give $h(x_1) < 0 < h(x_2)$; since h is negative before x_0 and positive after it, $x_1 < x_0 < x_2$, that is $1 < D^*(e) < 2$ ■ (The case analysis is formally verified in any ordered field: `no_double_root`, with `sixteen_pow_bound` for the inequality $(2e+1)(16/25)^e \leq 2.048$.)

Numerically, $D^*(2) \approx 1.0899$, $D^*(3) \approx 1.1948$, $D^*(4) \approx 1.2798$, $D^*(5) \approx 1.3477$, $D^*(6) \approx 1.4030$, $D^*(7) \approx 1.4489$, $D^*(8) \approx 1.4875$ [computed; F and F' vanish at $-x_0$ to within 10^{-15}]. For $e = 1$ the value is $D^*(1) = 1$: indeed $F_{1,1}(T) = T^2 + 2T + 1 = (T+1)^2$. Thus the only integer at which any member of the family degenerates is $D = 1$ for $e = 1$, which is the conic case treated by the Pell sieve at the beginning of this section.

Theorem 9.11 (higher exponents). Fix integers $D \geq 1$ and $e \geq 2$, and put $F(t) = D \cdot \sigma(t^{2e}) + t = D(1 + t + \dots + t^{2e}) + t$. Then there are only finitely many k , all bounded effectively in terms of D and e , for which some counterexample (b, k) , with any number of prime factors, has a prime power $t^e \parallel b$ whose component quotient is $D_t = D$. [proved, using Proposition 9.10 and Baker's theorem on hyperelliptic equations [17]; the reduction to the curve is formally verified: `higher_exponent_curve_even`, `higher_exponent_curve_odd`]

Proof. Theorem 4.1 at t gives $N \cdot m^2 = D \cdot \sigma(t^{2e}) + t$ with $m = b/t^e$. If k is even, $N = M^2$ and $(Mm)^2 = F(t)$. If k is odd, $N = 2M^2$ and $(2Mm)^2 = 2F(t)$. In both cases (t, Y) is an integral point on $Y^2 = F(t)$ or $Y^2 = 2F(t)$. These curves do not depend on k . The polynomial F , and hence $2F$, has degree $2e \geq 4$ and, by Proposition 9.10, no repeated root, so it has at least three simple roots. By Baker's theorem [17], $|t|$ and $|Y|$ are bounded by an effective constant $B(D, e)$. Since $2^{\lfloor k/2 \rfloor}$ divides Y , also $k \leq 2 \cdot \log_2 B(D, e) + 1$ ■

Remark 9.12. Theorem 9.11 is the analogue, for exponents $e \geq 2$, of Theorem 9.2 (c). For $e = 1$ the curve is a conic with infinitely many points and 2-adic arguments are needed, whereas for $e \geq 2$ it has genus $e - 1 \geq 1$ and finitely many integral points. The theorem applies at every prime with exponent at least 2, for any number of prime factors, and it does not use primality. Like Theorem 9.2 it is a statement for fixed D , with an effective but very large bound $B(D, e)$.

Remark 9.13 (the role of Proposition 9.10). A discriminant argument shows only that, for each e , the curves are singular for finitely many D . Proposition 9.10 shows that this set contains no integer when $e \geq 2$, so Theorem 9.11 needs no hypothesis or computation. (For $e \leq 6$ the resultant $\text{Res}_t(F, F')$ factors as $D^{2e-1} \cdot P_e(D)$, with $P_e(0) = -(2e-1)^{2e-1}$ and leading coefficient $(2e+1)^{2e-1}$ [computed].) For $e = 1$ the discriminant is $-(3D+1)(D-1)$, the constant of the Pell equations of this section, since $4D \cdot F_{D,1}(t) = (2Dt + D + 1)^2 + (3D+1)(D-1)$. The bound $B(D, e)$ grows with D and no bound on D_t is known, so Theorem 9.11 does not close the gap of Remark 9.8.

9.2 A constraint on D valid for every k

Theorem 9.14 (D_s modulo powers of 2). Let $b = \text{pr}s$ be a squarefree three-prime counterexample, $D = D_s$, $c = (3D+1)(D-1)$. Then one of the following holds. (i) $-c$ is a square in $\mathbb{Q}_2$. (ii) $D \equiv 1 \pmod{2^{k-3}}$ and $s \equiv -1 \pmod{2^{\lceil (k-3)/2 \rceil}}$. (iii) $3D \equiv -1 \pmod{2^{k-3}}$ and $s \equiv 1 \pmod{2^{\lceil (k-3)/2 \rceil}}$. In particular, since D is odd (Theorem 4.1), $D \equiv 1 \pmod{4}$, and, writing $D = 4n+1$, either $-n(3n+1)$ is a square in $\mathbb{Q}_2$ or case (ii) or (iii) holds. [proved, using the searches $k \leq 20$ of Section 12; the parity of D , the case $D \equiv 3 \pmod{4}$ and the congruences for s are formally verified: `component_quotient_odd`, `pell_D_three_mod_four`, `deep_case_one`, `deep_case_third`]

Proof. By the searches of Section 12.1, $k \geq 21$, so Proposition 9.1 applies with $t = \lfloor k/2 \rfloor + 1 \geq 11$. If $-c$ is not a 2-adic square, Theorem 9.2 (a) gives $v_2(c) \geq 2t - 2 = 2\lfloor k/2 \rfloor \geq k - 1$. The bound in Theorem 9.2 (a) depends only on $v_2(c)$, not on D , so this step is uniform in D . Since $(3D+1) - 3(D-1) = 4$, the two factors cannot both be divisible by 8, so one of them has valuation at least $k-3$. Theorem 4.1 at s gives $N(\text{pr})^2 = D \cdot \Phi(s) + s$, so 2^k divides $D \cdot \Phi(s) + s$. If $D \equiv 1 \pmod{2^{k-3}}$, then $(s+1)^2 = D \cdot \Phi(s) + s - (D-1)\Phi(s) \equiv 0 \pmod{2^{k-3}}$. If $3D+1 \equiv 0 \pmod{2^{k-3}}$, then $(s-1)^2 = (3D+1)\Phi(s) - 3(D \cdot \Phi(s) + s) \equiv 0 \pmod{2^{k-3}}$. For

$D \equiv 3 \pmod{4}$, write $D = 4m + 3$: then $c = 4(6m + 5)(2m + 1)$ and $v_2(c) = 2 < k - 1$, and directly $X^2 + c \equiv 0 \pmod{64}$ has no solution, because with $X = 2x$ it reduces to $x^2 + 12m^2 + 5 \equiv 0 \pmod{16}$, which fails for all residues of x modulo 8 and m modulo 2 ■

Remark 9.15 (what Theorem 9.14 gives, and a barrier). (1) Theorem 9.14 is the first constraint on D_s that holds for every k and every D : together with the parity of D (Theorem 4.1) it excludes all even D and all $D \equiv 3 \pmod{4}$, and the admissible D form a 2-adic set of density $1/48$, up to the classes (ii) and (iii), whose density 2^{4-k} tends to 0 [density computed for $D \leq 2^{22}$: 0.020833]. Computations 9.5 and 9.5A also treat even D , which Theorem 4.1 excludes directly. Theorem 9.14 does not bound D , and at odd primes there is no local obstruction (Section 11.4). (2) A bound on D cannot come from the sizes and the component identities alone. The equation $q(x+1)(y+1)(z+1) = Nxyz - 1$ has the same shape, the same sizes and the same component lemma ($N \cdot xy = D'(z+1) - 1$); its integer solutions with $N = 2^k$, $N \leq x \leq 4N$ and $x < y < z$ have D' as large as $0.90N^2$, $0.94N^2$, $0.97N^2$ and $1.09N^2$ for $k = 7, 9, 11, 13$ [computed]. So a bound on D_s must use Φ , oddness or primality. Since $D_s \approx \Delta^2/(N(\text{pr})^2)$ with $\Delta = f_N(\text{pr})$, a bounded D_s means a pair (p, r) whose potential is within a bounded factor of its least possible size $\text{pr}\sqrt{N}$, whereas typical pairs have Δ of order $(\text{pr})^2$: bounding D is a reformulation of most of the squarefree three-prime case.

10. The primality-free core of the squarefree case

10.1 The integer equation (E3)

The splitting identity of Lemma 3.7 is pure algebra, so the squarefree three-prime equation is the case of prime variables of the integer equation

$$(N - 1)\Phi(x)\Phi(y)\Phi(z) = N(xyz)^2 - 1, \quad 2 \leq x \leq y \leq z, \quad (\text{E3})$$

whose solutions are the integral points of the Wehler K3 surface $S_N \subset (\mathbb{P}^1)^3$ of tridegree $(2, 2, 2)$; see [8] for heights on such surfaces. It has the trivial solution (N, N^3, N^9) , for which $\Phi(N)\Phi(N^3)\Phi(N^9) = \sigma(N^{26})$.

Proposition 10.1 (integers). (i) In two variables, $(M - 1)\Phi(y)\Phi(z) = M(yz)^2 - 1$ with $2 \leq y \leq z$ and $M \geq 2$ holds only for $(y, z) = (M, M^3)$. (ii) Every solution of (E3) has $x \geq N$. (iii) If $x = N$, then $(y, z) = (N^3, N^9)$. [formally verified: two_var_integer, chain_first_pos, chain_first_eq_N]

Proof. (i) If $y < M$, then $y^2 - (M - 1)(y + 1) < 0$ and $M(yz)^2 - (M - 1)\Phi(y)\Phi(z) = z^2(y^2 - (M - 1)(y + 1)) - (M - 1)\Phi(y)(z + 1) < 0$. If $y = M$, the equation becomes $(z - M^3)(z + 1) = 0$. If $M < y < z$, Theorem 6.2 applies (it does not use primality). If $y = z > M$, reducing modulo y gives $y \mid M$, which is impossible. (ii) If $x < N$, then $f_N(x) < 0$ and, by Proposition 3.9 applied twice, $f_N(xyz) < 0 \neq 1$. (iii) For $x = N$ the equation is the two-variable equation with $M = N^3$, since $(N - 1)\Phi(N) = N^3 - 1$, and (i) applies ■

Computation 10.2. There is no solution of (E3) with $N < x$ for every $N \leq 1,000$ ($3.02 \cdot 10^9$ pairs (x, y)) and for $N = 2^k$, $k \leq 15$ ($1.81 \cdot 10^{10}$ pairs); the same enumeration finds 114 solutions of the exponent-one analogue $(N - 1)(x + 1)(y + 1)(z + 1) = N \cdot xyz - 1$ with $N < x \leq y \leq z$ and $N \leq 60$ (one of them, $N = 17$, $(35, 35, 233)$, has $x = y$), e.g. $N = 5$, $(7, 11, 385)$. [computed] Two controls validate the program: with $x = N$ it returns (N, N^3, N^9) for every $N \leq 60$, and the exponent-one count above.

Computation 10.2A (integer solutions with any number of factors). Replace the primes by integers $t_1 \leq \dots \leq t_w$, repetitions allowed: $q \cdot \prod \Phi(t_i) = N \cdot (\prod t_i)^2 - 1$. The procedure of Theorem 11.8A applies with all exponents equal to 1 (each factor lies in an explicit window determined by the previous ones, the gap $N \cdot m^2 - q \cdot \prod \Phi$ stays positive, and the last factor is a root of a quadratic), so for each (N, w) the enumeration is complete. For $w \leq 4$ and $2 \leq N \leq 8$, and for $w \leq 5$ and $N = 2$, the only solutions are the prefixes of the trivial chain $(N, N^3, N^9, \dots)$ [computed; up to $2.0 \cdot 10^9$ nodes per case; a Python and a C implementation agree for $N \leq 7$; with $t + 1$ in place of $\Phi(t)$ the program finds the known solutions of the exponent-one equation, for example $(7, 11, 385)$ for $N = 5$ and $(35, 35, 233)$ for $N = 17$]. Moreover

[proved]: if for every level N every such solution contains the factor N , then, since $f_N(N) = 1$, Theorem 3.10 (an identity valid for integer factors) shows that the other factors solve the equation at level N^3 , and induction makes every solution a prefix of the trivial chain. This hypothesis is therefore equivalent to Conjecture 10.3.

Conjecture 10.3 (integer Φ -chains). For all $N \geq 2$ and $\omega \geq 1$, the only integers $2 \leq x_1 \leq \dots \leq x_\omega$ with $(N - 1)\prod \Phi(x_i) = N\prod x_i^2 - 1$ are $x_1 = N$, $x_2 = N^3$, $x_3 = N^9$, ...; equivalently, all potentials $f_N(x_1 \dots x_j)$ equal 1. Since the chain contains N^3 , which is not prime, and every prime factor of b exceeds N , the conjecture implies that no almost perfect number $2^{k-1}b^2$ has a squarefree odd part $b > 1$, whatever the number of prime factors of b . It holds for $\omega \leq 2$ (Proposition 10.1), and it is verified for $\omega = 3$ when $N \leq 1,000$ or $N = 2^k$ with $k \leq 15$ (Computation 10.2), for $\omega = 4$ when $N \leq 8$, and for $\omega = 5$ when $N = 2$ (Computation 10.2A).

Remark 10.4 (what a proof has to use). The data of Computation 10.2 locate the decisive property. The search covers all integers x, y, z , odd and even, and all levels $N \leq 1,000$, odd and even. It finds no solution of (E3) with $x > N$, while the same enumeration finds 114 solutions of the exponent-one analogue with factors $x + 1$ instead of $\Phi(x)$. Three conclusions follow. (i) Primality is not what excludes solutions: the squarefree case behaves the same for composite values. (ii) Parity of N and of the variables is not what excludes them either; parity enters the proofs only to exclude $D = 0$, that is the first step $x = N$ of the trivial chain (Theorem 4.1, Proposition 10.1). (iii) What separates (E3) from its solvable exponent-one analogue is that $\Phi(x) = (x - \omega)(x - \omega^2)$ is a norm from $\mathbb{Z}[\omega]$. The equation reads $q \cdot N(\beta) = N(x_1 \dots x_\omega)^2 - 1$ with $\beta = \prod (x_i - \omega)$, a product of linear Eisenstein integers. A proof valid for every k is therefore most likely to come from a global property of β , beyond the local data described in Remarks 10.6 and 10.7, applied to this special shape, rather than from properties of primes. The smallest open case is Conjecture 10.3 for three variables with $x > N$. The contrast with the exponent-one analogue is the Fano/Calabi–Yau dichotomy of Section 11.3; near infinity it appears at second order (Remark 11.10A).

10.2 The Eisenstein element

Proposition 10.5 (the Eisenstein element and its content). For integers x, y, z put $P = xyz$, $S = x + y + z$, $T = xy + yz + zx$ and $\beta = (x - \omega)(y - \omega)(z - \omega)$. Then $\beta = A - C\omega$ with $A = P - S - 1$ and $C = T + S$, and $N(\beta) = A^2 + AC + C^2 = \Phi(x)\Phi(y)\Phi(z)$ [formally verified: `eisenstein_norm`]. Each factor $x - \omega$ is primitive (its ω -coefficient is -1). For a prime $\ell \neq 3$, ℓ divides both A and C if and only if there are two of the variables, say $u \neq v$, with $\ell \mid \Phi(u)$ and $uv \equiv 1 \pmod{\ell}$, that is, u and v reduce to the two distinct primitive cube roots of unity modulo ℓ . [proved; checked on 3,000 random triples]

Proof. $\ell \equiv 1 \pmod{3}$ splits as $\pi \bar{\pi}$ in $\mathbb{Z}[\omega]$, with $\pi = (\ell, \omega - \rho)$ for a cube root of unity $\rho \neq 1 \pmod{\ell}$. Then $\pi \mid u - \omega$ exactly when $u \equiv \rho$, and $\bar{\pi} \mid u - \omega$ exactly when $u \equiv \rho^2 \pmod{\ell}$. A primitive factor is not divisible by ℓ , so $\ell \mid \beta$ exactly when π and $\bar{\pi}$ divide different factors, that is when $u \equiv \rho$ and $v \equiv \rho^2 = \rho^{-1}$. Primes $\ell \equiv 2 \pmod{3}$ are inert and never divide Φ ■

Remark 10.6 (what the Eisenstein shape adds). (i) In the coordinates (S, T, P) the equation becomes the single norm equation $A^2 + AC + C^2 = (NP^2 - 1)/(N - 1)$, the ternary normal form of the squarefree equation [formally verified: `squarefree_three_ternary`]; requiring $X^3 - SX^2 + TX - P$ to have integer roots only returns to the original variables. (ii) Beyond its norm, the shape of β gives the content $\gcd(A, C)$ of Proposition 10.5 and the residues of β modulo small Eisenstein integers (for three odd variables $\beta \equiv 1 \pmod{2}$, so A is odd and C even): local data. (iii) With $\gamma = \beta - P = -(1 + S) - (T + S)\omega$ the equation becomes $q \cdot (P(T - S - 2) + N(\gamma)) = P^2 - 1$, so $q \cdot N(\gamma) \equiv -1 \pmod{P}$, the global form of the cross conditions of Remark 4.9. The size $|\gamma| \approx P/q$ is the natural one, since $|\beta - P|/P = O(1/N)$ for factors larger than N ; the content of the relation lies in its exactness (Remark 10.8).

Remark 10.6A (why the two-variable argument does not extend). For three variables put $e_1 = x + y + z$, $u = e_2 - e_1$, $C_3 = N(u + 1) - e_3$, so that C_3 is the coefficient of Theorem 5.1, and $A' = (N + 1)C_3 + 3(N - 1)e_1 - (3N^2 - 1)$. Then, identically, $u(A' - u) - (C_3 - 2N + 1)^2 + 3(N - 1)e_1^2 + N^2 - N + 1 = -(N(xyz)^2 - 1$

– $(N - 1)\Phi(x)\Phi(y)\Phi(z)$), so (E3) is equivalent to $u(A' - u) = (C_3 - 2N + 1)^2 - 3(N - 1)e_1^2 - (N^2 - N + 1)$ [identity checked at 20,000 random integer points]. This is the exact analogue of the relation $w(A - w) = C^2 - 3q - 1$ in the proof of Theorem 6.2. There the right side depends only on the pair coefficient C , which the Z -form confines to $1 \leq C \leq N - 1$, so it is too small for the left side and the case closes by size. In three variables the right side contains the term $-3(N - 1)e_1^2$, which is large and is not controlled by C_3 ; the equation then only expresses that A' is close to u , and no contradiction follows from sizes. Any extension of Theorem 6.2 must control e_1 jointly with C_3 , which is again the second-order problem of Remark 11.10A.

Remark 10.7 (content and ideal factorisation of β). Let $\ell \neq 3$ divide $\gcd(A, C)$ through the pair (p, r) of Proposition 10.5, so $\ell \mid \Phi(p)$, $\ell \mid \Phi(r)$ and $pr \equiv 1 \pmod{\ell}$. Then $\ell^2 \mid \Phi(p)\Phi(r)$, hence $\ell^2 \mid N \cdot b^2 - 1$, and the equation modulo ℓ gives $N \cdot s^2 \equiv 1 \pmod{\ell}$ for the third prime. These conditions are consistent with primes even modulo ℓ^2 : for $(N, \ell) = (16, 7), (32, 7), (64, 13), (256, 19)$ the prime triples $(23, 53, 149), (37, 53, 109), (107, 113, 307), (277, 311, 1571)$ have $\ell \mid \gcd(A, C)$, $N \cdot s^2 \equiv 1 \pmod{\ell}$, and satisfy (2.1) modulo ℓ^2 [computed]. More generally, $\mathbb{Z}[\omega]$ is a principal ideal domain, and at a prime $\ell \equiv 1 \pmod{3}$ the factorisation of β records only which of the two primes above ℓ divides each factor $x - \omega$, that is, which primitive cube root of unity x is modulo ℓ , with multiplicities fixed by x modulo powers of ℓ . So the ideal factorisation of β is a collection of local data, which are satisfiable (Section 11.4); the global invariants of β are its norm, which is the equation, and its argument (Remark 10.9) [proved].

Remark 10.8 (the Vieta partner of P). With $D' = T - S - 2$, $G = N(\gamma)$ and $M = P - qD'$, the relation of Remark 10.6 (iii) is equivalent to $P \cdot M = qG + 1$ [formally verified: vieta_partner]; hence $0 < M < P$, $M \equiv P \pmod{q}$, and $M = (T - S) + 3N - 2 - C_3$ [checked by exact evaluation]. In the coordinates (S, T, P) the equation is the quadratic $X^2 - qD' \cdot X - (qG + 1) = 0$ in $X = P$, whose second root is $-M$. The partner point $(S, T, -M)$ is not the (S, T, P) of a triple of positive integers, and none of the three Vieta involutions of the ternary quadric preserves integral roots and positivity in general, since each changes the discriminant of the cubic; so no Vieta descent is available.

Remark 10.9 (length and direction of β). The equation fixes the length, $|\beta|^2 = P^2 + (P^2 - 1)/q$, and the direction $\theta = \sum \arctan(\sqrt{3}/(2u + 1))$ over $u \in \{x, y, z\}$, with $\tan \theta = \sqrt{3} \cdot C/(2A + C)$, satisfies $\theta \approx \sqrt{3}/(2q)$ to first order. For real $x, y > N$ the equation has a real root z whenever $f_N(xy) > 0$, so the real solutions with $N < x \leq y < z$ form a two-dimensional family; a grid of (x, y) gives 669, 686, 691 and 691 real solutions for $N = 16, 64, 1024$ and 2^{20} , and on it $N \cdot \theta$ lies in $[0.847, 0.875]$ for $N = 16$ and tends to $\sqrt{3}/2$ [computed]. Every inequality between length and direction valid for real variables holds on this family, so a contradiction must use integrality; in these coordinates the only integral information is $\tan \theta \in \sqrt{3} \cdot \mathbb{Q}$, which holds for every integer triple.

Remark 10.10 (the factors of q). By Lemma 3.3, $q \mid P^2 - 1$, so $P \equiv \varepsilon \pmod{q}$ for a square root ε of 1, and the sign of P modulo each prime $\ell \mid q$ decides on which side of $(Ab - 1)(Ab + 1)$ the factor ℓ lies (Remark 4.7). No such distribution is excluded by local information or by primality: for $k = 6$ (four square roots of 1 modulo 63) and $k = 8$ (eight modulo 255) every ε is realised by primes $N < p < r < s$ with $prs \equiv \varepsilon \pmod{q}$ and $\prod \Phi(t) \equiv 1 \pmod{8N}$, for example $(67, 79, 379), (71, 191, 311), (79, 167, 199)$ and $(113, 241, 359)$ for $k = 6$ [computed]. The order of x modulo every prime factor $\ell \neq 3$ of $\Phi(x)$ is 3 for every integer x , so this information does not use primality either.

10.3 Fibration over one variable

Remark 10.11 (the two-variable deficit equation). Fixing the smallest variable x turns (E3) into $K \cdot \Phi(y)\Phi(z) = L \cdot (yz)^2 - 1$ with $L = N \cdot x^2$, $K = (N - 1)\Phi(x)$ and deficit $M = L - K = f_N(x)$ (Proposition 3.9). An exhaustive search over $L < 4,000$ and $2 \leq M < L$ finds 2,158 solutions. Of these, 1,761 form the renormalisation family $z = L \cdot y^2$, which occurs exactly when $K\Phi(y) = L \cdot y^2 - 1$ (Theorem 3.10); the other 397 all have $M/K \geq 0.053$ [computed]. Since $L = (M \cdot X - 1)/E$ with $X = \Phi(y)\Phi(z)$ and $E = X - (yz)^2$, the deficit is determined modulo E by the pair (y, z) , with $M/K \approx 1/y + 1/z$; for (E3) it must moreover equal $f_N(x)$ and fit $L = N \cdot x^2$, the same numerical coincidence as in Proposition 8.9.

Remark 10.12 (the deficit scale). For (E3), $M \approx (x - q)x$ and $K \approx Nx^2$, so $M/K^{2/3}$ is of order $(x - q)/N$, between 0 and about 2. The 397 solutions of Remark 10.11 outside the renormalisation family have $M/\sqrt{K} \geq 1.62$ and $M/K^{2/3} \geq 0.52$, attained by $(L, M, K, y, z) = (964, 49, 915, 31, 52)$ [computed]. So solutions outside the family occur at the scale of (E3), and no lemma of the form “small deficit implies the family” excludes (E3) beyond the thin range $x - q \lesssim \sqrt{N}$. Only two solutions of the search have the shape $(L, K) = (Nx^2, (N - 1)\Phi(x))$, both from the trivial chain, $(N, x, y, z) = (2, 8, 2, 512)$ and $(3, 27, 3, 19683)$; a second search, over $A = K \leq 3,000$ and $B = M$, finds 630 solutions of $A\Phi(y)\Phi(z) = (A + B)(yz)^2 - 1$ with $D \geq 1$ at the last variable, none of the form $((N - 1)\Phi(x), f_N(x))$ [computed]. A proof of (E3) must use the link between K and L through x .

Theorem 10.13 (fibration of (E3) over one variable). Fix $N \geq 2$ and an integer x , and put $K = (N - 1)\Phi(x)$, $L = N \cdot x^2$, $E = 4L - 3K$ and $C' = 3KL + 4L - 3K$. (i) Every integer solution (y, z) of the two-variable equation $L(yz)^2 - K\Phi(y)\Phi(z) = 1$, in particular every solution (x, y, z) of (E3) with this x , gives an integral point $(\pi, V) = (yz, (y + 2)(z + 2) - 3)$ on the conic $K \cdot V^2 = E \cdot \pi^2 + 6K \cdot \pi - 3K - 4$, equivalently $U^2 - K \cdot E \cdot V^2 = 4C'$ with $U = E \cdot \pi + 3K$. The pairs (y, z) themselves are the integral points of the curve $L(yz)^2 = K\Phi(y)\Phi(z) + 1$ of bidegree $(2, 2)$, which has arithmetic genus one and double covers the conic through $(y, z) \mapsto (\pi, V)$. (ii) Hence if the conic has no rational point, that is, if the Hilbert symbol $(C', KE)_\ell = -1$ at some prime ℓ , no solution of (E3) has this value of x , whatever y, z and D . (iii) For an odd prime $\ell \nmid 3(N - 1)x$: if $\ell \nmid N$ and ℓ divides $\Phi(x)$ to an odd power, $(C', KE)_\ell = (N/\ell)$; if $\ell \nmid KE$ and ℓ divides C' to an odd power, $(C', KE)_\ell = (-K(3K + 4)/\ell)$; if ℓ divides E but not $3KC'$, the symbol is 1, because $4C' = (3K)^2 + (3K + 4)E$. A prime ℓ dividing both N and $\Phi(x)$ does not occur on a solution: modulo ℓ , (E3) reads $-\Phi(x)\Phi(y)\Phi(z) \equiv -1$, so $\gcd(N, \Phi(x)) = 1$ and such slices are excluded directly. [proved; the identities of (i) are formally verified: `slice_conic`, `slice_conic_norm`]

Proof. (i) Put $\sigma = y + z$. The equation reads $M\pi^2 - K(\pi\sigma + \sigma^2 - \pi + \sigma + 1) = 1$ with $M = L - K$. As a quadratic in σ its discriminant must be the square of $K(2\sigma + \pi + 1) = K \cdot V$, which gives $K \cdot V^2 = (K + 4M)\pi^2 + 6K\pi - 3K - 4$ with $K + 4M = E$. Multiplying by E and completing the square gives $U^2 - KE \cdot V^2 = 9K^2 + (3K + 4)E = 4C'$. (ii) A conic with an integral point has rational points, which exist exactly when the Hilbert symbols are 1 at every place (Hasse–Minkowski [11]); here $KE > 0$ for $x > N$. (iii) If $\ell \mid \Phi(x)$ and $\ell \nmid (N - 1)x$, then $\ell \nmid L$, $E \equiv 4L$ and $4C' \equiv 16L \pmod{\ell}$, so the symbol is $(4L/\ell)^v = (N/\ell)^v$ with $v = v_\ell(K)$. If $\ell \mid C'$ and $\ell \nmid KE$, then $\ell \mid 3K + 4$ and $E \equiv -9K^2/(3K + 4) \pmod{\ell}$, so $KE \equiv -K(3K + 4) \cdot (3K/(3K + 4))^2$. The last case is immediate from the identity ■

For an actual solution the condition at the primes of $\Phi(x)$ always holds, since N is a square modulo every prime factor of $\Phi(x)$ (proof of Proposition 4.5). The conditions at the primes of C' are new; they move with x . The same test applied to the curve itself at finitely many small primes, by searching for solutions modulo ℓ that lift by Hensel’s lemma, uses integrality and removes further values of x .

Computation 10.14 (slices that survive). For every $N \leq 120$ and every x with $N < x \leq 3N + 2$ (Lemma 3.6 for integer variables gives $x \leq 3N$), the conic of Theorem 10.13 was tested by Hilbert symbols, and the curve was then tested for $\mathbb{Z}_\ell$ -points at the primes $\ell \leq 47$. For $N = 3, 5, 7, 8, 13, 14, 15, 17, 21, 23, 31, 35, 59, 91$ no value of x survives, so for these N , (E3) has no non-trivial solution, proved without enumerating y or z . For $N = 2^k$, out of the integers x in $(N, 3N + 2]$, the number of surviving slices is 0, 8, 3, 40, 4, 105, 35, 520, 82, 1,333 for $k = 3, \dots, 12$, that is at most 4.6% for odd k and 16–31% for even k . Restricted to primes x (and, for odd k , to $x \equiv 5$ or $23 \pmod{24}$, Proposition 4.5) the survivors are 0, 1, 1, 16, 3, 34, 8, 107, 15, 339 out of 1, 9, 3, 26, 13, 82, 35, 267, 130, 906 admissible primes. For the single slice $x = N + 1$ and every $N \leq 1,500$, the conic has no rational point for 1,402 values of N and has one for 97 values (72 even, 25 odd, among them $N = 4, 256$ and $1,024$); $K \cdot E$ is never a square [computed]. So this slice is not excluded by local conditions uniformly in N . Validation: the test rejects none of the 2,158 known solutions of the two-variable deficit equation (Remark 10.11), and the Hilbert-symbol routine agrees with a brute-force search for rational points on all 2,640 conics $U^2 - dV^2 = C$ with $2 \leq d < 40$, $|C| \leq 40$ [computed].

Remark 10.15 (what the fibration achieves). It treats all D at once, and it combines the two kinds of information that Remark 9.15 shows to be necessary: local conditions at primes that move with x , and the archimedean bound $N < x \leq 3N$, which makes the set of slices finite. A purely local argument cannot exclude solutions, since the full equation is solvable modulo every prime power, but each slice may be obstructed at a different prime. A fixed proportion of slices survives, larger for even k , where N is a square and the conditions at the primes of $\Phi(x)$ are void. A surviving slice is a curve of genus one with points everywhere locally; its integral points are finite (Siegel) and, for $N \leq 1,000$, decided by Computation 10.2. For each N the fibration reduces (E3) to a short list of genus-one curves: 3 prime slices for $k = 7$, 8 for $k = 9$ and 15 for $k = 11$.

Remark 10.16 (the surviving slices as curves). Put $A = Ly^2 - K\Phi(y)$. The equation of a slice is $Az^2 - K\Phi(y)z - (K\Phi(y) + 1) = 0$, so $(2Az - K\Phi(y))^2 = Q(y)$ with $Q(y) = KE \cdot y^4 + (4KL - 6K^2)y^3 + (4KL - 9K^2 + 4L - 4K)y^2 - (6K^2 + 4K)y - (3K^2 + 4K)$ [formally verified: slice_quartic]; $A \neq 0$ at a solution, since $A \cdot z^2 = K\Phi(y)(z + 1) + 1 > 0$. The invariants of Q are $I = 81K^4 - 144K^3L + 144K^3 + 16K^2L^2 - 248K^2L + 16K^2 + 32KL^2 - 32KL + 16L^2$ and an explicit J of degree 6, and $4I^3 - J^2 = 6912 \cdot K^2 \cdot G(K, L)$, where G has degree 6 in K and 5 in L and leading part $81K^6(L - 1)^2(L^2 + L + 1)$. The following was checked [computed]. (1) $G(K, L) \neq 0$ on all 3,776 slices of (E3) with $N \leq 60$, so each is a smooth curve of genus one with Jacobian $Y^2 = X^3 - 27I \cdot X - 27J$. (2) The cubic $X^3 - 27IX - 27J$ has no rational root on these slices or on 300 random pairs (K, L) , so the Jacobians have no rational 2-torsion, and a descent must be a full 2-descent over a cubic field that changes from slice to slice. (3) $(y, z) \mapsto (1/y, 1/z)$ maps the curve of (K, L) onto that of $(-K/L, 1/L)$, and $G(K, L) = L^{10}G(-K/L, 1/L)$. (4) The 13 surviving prime slices with $N \leq 512$ ($N = 16$: $x = 37$; $N = 32$: 71; $N = 128$: 173, 293, 317; $N = 512$: 557, 743, 911, 1013, 1103, 1319, 1367, 1487) have no rational point $y = u/v$ with $|u|, v \leq 300$ on the quartic model, while the expected point is found on 300 control curves; their rational points are decided in Remark 10.25B. (5) The branch locus $B(y) = My^4 - 2Ky^3 - 3Ky^2 - 2Ky - (K + 1)$ of the double cover of the conic has no rational root and no quadratic factor on all 1,716 slices with $N \leq 40$. (6) For a given N the integral points of every slice lie in the window $K/M < y \leq 2K/M + O(1)$, which Computation 10.2 enumerates for all x when $N \leq 1,000$ and $N = 2^k$, $k \leq 15$; in particular the 13 slices above have no integral point. The structural question is whether the link $L - K = f_N(x)$ forces an obstruction on every surviving slice.

Remark 10.17 (the slice equation in reciprocal and Markov form). Write $f = L - K = f_N(x)$. (1) Dividing by $K(yz)^2$ gives the exact identity $f/K = 1/y + 1/z + 1/y^2 + 1/z^2 + 1/(yz) + 1/(y^2z) + 1/(yz^2) + 1/(y^2z^2) + 1/(K(yz)^2)$; hence $y, z > K/f$, and $\gcd(K, L) = 1$. (2) Reducing modulo y and modulo z gives the cross conditions $y \mid K\Phi(z) + 1$ and $z \mid K\Phi(y) + 1$ (Remark 4.9), which follow from $yz \mid K(y^2 + z^2 + y + z + 1) + 1$ and are equivalent to it when $\gcd(y, z) = 1$. On a solution $K(y^2 + z^2 + y + z + 1) + 1 = yz(g - K)$ with $g = fyz - K(y + z) > 0$, so the slice equation is the Markov-type equation $K(y^2 + z^2) - c \cdot yz + K(y + z) + K + 1 = 0$ with $c = g - K$ [formally verified: slice_markov]. (3) Identically, $(fy - K)(fz - K) = K^2 + fg$ [formally verified: slice_factor]. (4) Vieta jumping in y sends y to $y^* = w/K$ with $w = (K\Phi(z) + 1)/y$ and $w \equiv y^{-1} \pmod{K}$, so y^* is never an integer, and the classical descent is not available. The solutions of the two-variable deficit equation fill the whole window $K/f < y \leq 2K/f + O(1)$ (for the 397 solutions outside the renormalisation family, yf/K ranges over $[1.09, 4.13]$) [computed], so a narrower window must use that $(K, f) = ((N - 1)\Phi(x), f_N(x))$ (Remark 10.12).

10.4 Congruences and size

Lemma 10.18 (2-adic balance). Let b be odd and squarefree with prime factors $t_1, \dots, t_\omega$, let (b, k) be a counterexample, and let $r = \min v_2(t_i + 1)$. If $r < k$, the number of i with $v_2(t_i + 1) = r$ is even. For three primes x, y, z it is exactly two; if $v_2(x + 1) = v_2(y + 1) = r < c = v_2(z + 1)$, then $x + y + 2 \equiv 0 \pmod{2^{r+d}}$ with $d = \min(c - r, r, k - r)$. [proved] For the smallest prime, $v_2(x + 1) \geq k$ with $N < x < 3N$ forces $x = 2N - 1$ or $x = 3N - 1$.

Proof. Modulo N , (2.1) gives $\prod \Phi(t_i) \equiv 1$. Write $\Phi(t) = 1 + A_t$ with $A_t = t(t + 1)$, so $v_2(A_t) = v_2(t + 1) \geq 1$ for odd t . In $\prod(1 + A_{t_i}) - 1$ every product of two or more A 's has valuation at least $2r > r$, so the valuation

is that of the sum of the A 's of valuation r , which is r when their number is odd. That contradicts $\prod \Phi \equiv 1 \pmod{2^k}$ when $r < k$. For the refinement write $x + 1 = 2^r u$ and $y + 1 = 2^r v$ with u, v odd. Then $A_x + A_y = 2^r(2^r(u^2 + v^2) - (u + v))$, and all other terms have valuation at least $\min(c, 2r)$. Hence $2^r(u^2 + v^2) \equiv u + v \pmod{2^d}$, and since $d \leq r$, $u + v \equiv 0 \pmod{2^d}$. ■ For odd k this contains the parity statement of Proposition 4.5 (the case $r = 1$). A randomised test on 33,000 triples with $\prod \Phi \equiv 1 \pmod{2^k}$, $3 \leq k \leq 13$, found no exception [computed].

Proposition 10.19 (congruences and size). Let $b > 1$ be odd, $X = \sigma(b^2)$ and $E = f_N(b) = Nb^2 - qX$, and suppose b, N and q pairwise coprime. The conditions of (2.1) modulo b (the cross conditions of Remark 4.9), modulo N ($\prod \Phi \equiv 1$, Lemma 10.18) and modulo q ($b^2 \equiv 1$) together are equivalent to $bNq \mid E - 1$ [the combination is formally verified: `congruences_combine`; the converse is immediate]. Hence (b, k) is a counterexample if and only if these congruences hold and $1 \leq E \leq bNq$; this step is elementary, since an integer $E \equiv 1 \pmod{bNq}$ with $1 \leq E \leq bNq$ equals 1 [formally verified: `local_archimedean_split`]. The content of the proposition is the combination of the three congruences; it is a reformulation of (2.1), not a reduction of it. Since $N/q - \sigma(b^2)/b^2 = E/(qb^2)$, the size condition says that $\sigma(b^2)/b^2$ lies below N/q by at most N/b .

Remark 10.20 (what congruences can and cannot do). All congruence information, including Lemma 10.18, the cross conditions of Remark 10.17 and every condition of Section 4, is contained in $E \equiv 1 \pmod{bNq}$; what remains is one archimedean inequality, $E \leq bNq$, whereas for a typical b the potential is of order b^2 . Congruences cannot replace this inequality. For $N = 2^k$ with $k = 4, 5, 6, 7$, taking x in $(N, 3N)$, y in the window of Remark 10.17 and $z \geq y$ running over the divisors of $K\Phi(y) + 1$ with $y \mid K\Phi(z) + 1$, there are 354, 900, 4,056 and 8,194 triples satisfying the cross conditions; 117, 215, 684 and 901 of them also satisfy $\prod \Phi \equiv 1 \pmod{2^k}$, and none satisfies (2.1) [computed]. A proof must control how closely $\sigma(b^2)/b^2$ can approach N/q .

Remark 10.21 (the size condition alone is satisfiable). For $N = 2^k$, $k = 4, \dots, 9$, a search over z within a few units of the real root of $E(z) = 0$ finds at least 7, 41, 160, 531, 1,582 and 4,849 triples of primes $N < x < y < z$ with $0 < E \leq bNq$. The smallest positive potentials found are $E = 1,021,759$ for $(31, 53, 79)$ at $k = 4$ and $E = 4,738,519$ for $(251, 383, 809)$ at $k = 7$, where $E/(bNq) \approx 3.75 \cdot 10^{-6}$ and $E < b$; none has $E = 1$ [computed]. So both halves of Proposition 10.19 are satisfied separately by many prime triples, and a counterexample is a triple that satisfies both. Any statement of the form “ $0 < E$ implies $E > bNq$ ” for all prime triples is false; a valid statement must assume the congruences, and then it is equivalent to the conjecture for three primes.

10.5 Squares against non-squares, and the slice family

Remark 10.22 (squares against non-squares: genus zero against genus one). The divisibility $s(n) \mid n - 1$ of Proposition 11.1 has many solutions when n is not a square: below $4 \cdot 10^8$ there are 532 that are not prime powers (520 with two prime factors, 10 with three and 2 with four, all squarefree), and the sieve of Computation 11.3 to $2 \cdot 10^{10}$ shows the same pattern [computed]; for $n = b^2$ with b odd there is none below 10^{20} (Computation 11.6). (1) Two primes. For $n = pr$ the condition reads $(p - Q)(r - Q) = \Phi(Q)$, so every factorisation of $\Phi(Q)$ gives a solution, for example $77 = 7 \cdot 11$ from $\Phi(4) = 21 = 3 \cdot 7$; for $n = b^2$ the two-prime equation has only the trivial chain (Proposition 10.1 (i), Theorem 6.3). (2) Three primes. Fixing the smallest prime p , the non-square equation becomes $(Mr - K)(Ms - K) = K^2 + M(K + 1)$ with $K = Q(p + 1)$ and $M = (Q + 1)p - K$, a hyperbola: each slice has genus zero, and its integral points come from factorisations. Of the twelve solutions with at least three primes, three are renormalisations of smaller ones, for example $97,783 = 7 \cdot (61 \cdot 229)$ with $Q = 6$, and nine are primitive, for example $32,562,419 = 113 \cdot 127 \cdot 2269$ with $Q = 58$ [computed]. For b^2 the slices are the genus-one curves of Theorem 10.13. So two proved differences separate the square case from the non-square case: the two-prime equation is rigid, and every slice has genus one instead of zero. What is missing is a way to show that a curve of genus one with the coefficients $K = (N - 1)\Phi(x)$, $L = Nx^2$ has no integral point with $y, z > x$, uniformly in N and x .

Remark 10.23 (the slice family has no visible special structure). A uniform argument would need a property of the family of Remark 10.22 that general genus-one curves lack. Five were tested, and none is present [computed]: (1) rational 2-torsion on the Jacobian (Remark 10.16 (2)); (2) torsion of any order (on all 1,520 slices with $N < 40$, and on 400 random pairs (K, L) , the greatest common divisor of $\#E(\mathbb{F}_p)$ over 25 primes of good reduction is 1); (3) special factors of $G(K, L)$ (divisibility by $N, q, x, \Phi(x), x + 1, M$ or $4L - 3K$ occurs only on a small proportion of slices); (4) obvious rational points (a point with $y = -1$ exists exactly when $K^2 + 4M(K + 1)$ is a square, a point at infinity exactly when $K(4L - 3K)$ is a square, and neither occurs on the 159,200 slices with $N < 400$); (5) splitting of the branch locus (Remark 10.16 (5)). Within these tests the slices behave like a generic two-parameter family of curves of genus one, for which uniform control of integral points in a prescribed region is of the type addressed by uniformity conjectures. Each single N is decided by a finite computation (Theorem 7.8, Computation 10.2).

Remark 10.24 (primality of the coordinates). For the conjecture only prime points on the slice curves matter, a weaker target than all integral points. Two facts limit what primality can add: (E3) has no non-trivial solution for $N \leq 1,000$ even for composite values (Computation 10.2), and the non-square analogue has solutions in primes (Remark 10.22). The natural quadratic condition, $(-K(3K + 4)/y) = 1$ from the discriminant of the slice equation modulo y , is equivalent to the solvability of $K\Phi(z) \equiv -1 \pmod{y}$, since the discriminant of $K(z^2 + z + 1) + 1$ is $-K(3K + 4)$; so it follows from the cross condition and is the symbol at the primes of C' in Theorem 10.13 (iii). For $N = 2^k$, $k = 5, \dots, 10$, the prime triples with $N < x < 3N$, y in the window of Remark 10.17, $z \geq y$ and both cross conditions number 1, 3, 6, 8, 12 and 27; all satisfy both Legendre conditions, and none satisfies $\prod \Phi \equiv 1 \pmod{2^k}$ [computed].

Remark 10.25 (local solubility of the surviving prime slices). For each of the 13 slices of Remark 10.16 (4), solubility of $w^2 = Q(y)$ over $\mathbb{Q}_p$ was decided with the local solubility routine of Cremona's eclib (with NTL 11.6) at $p = 2, 3$ and at every prime dividing $K, G(K, L)$ or the leading coefficient $K(4L - 3K)$, after complete factorisation of $G(K, L)$ (46 to 73 digits). At every other prime the reduction is a smooth curve of genus one whose $\mathbb{F}_p$ -points lift, and real points exist because the leading coefficient is positive. All 13 curves are everywhere locally soluble [computed; the routine was validated on 11a1, 37a1, 389a1 and 5077a1, and it accepts all 60 tested slices that contain known solutions of the two-variable equation]. Each curve is therefore a 2-covering of its Jacobian in the 2-Selmer group, and it has a rational point if and only if its class lies in the image of $E(\mathbb{Q})$; this is decided by the descent of Remark 10.25B. Their integral points are excluded by Remark 10.16 (6).

Remark 10.25A (integer solutions with negative coordinates). Three operations produce integer solutions from solutions: inserting an entry -1 , since $\Phi(-1) = 1$; splitting a square m^2 into $(m, -m)$, since $\Phi(m^2) = \Phi(m)\Phi(-m)$ (Remark 4.7); and, more generally, replacing an entry x by a block $(y_1, \dots, y_r)$ with $\prod y_i = \pm x$ and $\prod \Phi(y_i) = \Phi(x)$. For positive integers no block with $r \geq 2$ exists, because $\Phi(a)\Phi(b) - \Phi(ab) = a^2b + ab^2 + a^2 + b^2 + a + b > 0$ for $a, b \geq 1$. For non-zero integers the blocks of two elements are exactly the operations above: $\Phi(a)\Phi(b) - \Phi(-ab) = (a + b)(a + 1)(b + 1)$, and $\Phi(a)\Phi(b) = \Phi(ab)$ has no solution, since with $s = a + b$ it forces $(s - 2) \mid 6$ and none of the remaining values of s gives integers a, b [proved]. An exhaustive search over non-zero integers, of the two-variable equation with $|y| \leq 2 \cdot 10^6$ and $M \leq 40$ and of (E3) with $|x|, |y| \leq 3,000$ for $N \leq 30$ and $|x|, |y| \leq 1,000$ for $30 < N \leq 120$, finds only prefixes of the trivial chain modified by these operations [computed]. The primitive blocks found are sporadic factorisations of values of Φ : $(2, -3, -3)$ for $x = 18$, from $\Phi(2)\Phi(-3)^2 = 7^3 = \Phi(18)$, the sporadic solution $x = 18$ of the Nagell-Ljunggren equation, which gives the solution $(-3, -3, 2)$ at $N = 18$; $(2, -4, -4, -6)$ for $x = -192$, with $\Phi(-192) = 7 \cdot 13^2 \cdot 31$; and $(2, -3, -4, -15, -27)$ for $x = 9,720$, with $\Phi(9,720) = 7^2 \cdot 13 \cdot 19 \cdot 37 \cdot 211$ (searches over blocks of three, four and five elements with entries up to 50,000, 700 and 60 in absolute value) [computed]. Every block with at least two elements has a negative entry, so blocks never occur in positive solutions. The structural form of Conjecture 10.3, that every integer solution is a prefix of the trivial chain modified by blocks, has Conjecture 10.3 as its positive part [heuristic].

Remark 10.25B (rational points on the slices). Let $w^2 = g(y) = ay^4 + by^3 + cy^2 + dy + e$ be the quartic model of a slice (Remark 10.16), with invariants $I = 12ae - 3bd + c^2$, $J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$ and Jacobian $E: Y^2 = X^3 - 27IX - 27J$. With the classical covariants g_4, g_6 (syzygy $27g_6^2 = g_4^3 - 48Ig_4^2g_6 - 64Jg_4^3$) the map $X = 3g_4/(4g)$ is a 2-covering of E . In $A = \mathbb{Q}[\theta]/(\theta^3 - 27I\theta - 27J)$ one has $3g_4 - 4\theta g = c_0 q(y)^2$ with $c_0 = 9b^2 - 24ac - 4a\theta$ and q quadratic over A (verified for every curve used), so every rational point gives $X - \theta \equiv c_0$ modulo squares, and the curve has a rational point only if c_0 lies in the subgroup of $A^\times/A^{\times 2}$ generated by the classes $X(P) - \theta$ of a basis of $E(\mathbb{Q})/2E(\mathbb{Q})$. When the 2-descent ellrank of PARI/GP 2.18.1 (validated on 11a1, 37a1, 389a1 and 5077a1) proves the rank and returns that many independent points, saturated at 2 (the torsion is trivial in all cases), the following is a proof that the curve has no rational point: for every product $c_0 \prod (X(P_i) - \theta)^{e_i}$ there is a prime $p > 10^6$, not dividing the discriminant of the cubic, and a root t of the cubic modulo p at which the quadratic character of the product is -1 . No conclusion is drawn when fewer points than the proved rank are returned. Controls: the slices $x = N$ for $N = 16, 32$ and 64 , which contain points of the trivial chain, are recognised as having rational points. Results [computed; each negative answer is a proof with explicit witness primes]. (i) The prime slices $(N, x) = (16, 37), (32, 71)$ and $(512, 1103)$, with Jacobians of rank 3, 1 and 1, and $(64, x)$ for $x = 71, 79, 83, 107$ and 157 are everywhere locally soluble and have no rational point: they violate the Hasse principle, and their classes are non-zero elements of the Tate–Shafarevich groups of their Jacobians. For $N = 16$ and 32 every other prime x with $N < x \leq 3N + 2$ gives a conic without rational points (Theorem 10.13), so at these levels no prime slice has a rational point, although integrality is not used. (ii) This is not a property of every slice. The composite slice $(16, 46)$ is everywhere locally soluble, has a Jacobian of rank 4 and contains the rational point $(y, z) = (-982,937/517,647, 943,664,688/283,101,187)$, checked exactly. For the prime slices $(64, 73)$ and $(64, 131)$ the 2-Selmer group has dimension 3, two independent points are known and the root number is -1 ; by the 2-parity theorem (Monsky; Dokchitser–Dokchitser) the 2^∞ -Selmer corank is 3, so if $\text{III}(E)[2^\infty]$ is finite the rank is 3, the 2-Selmer group equals the image of $E(\mathbb{Q})$, and these slices have rational points [proved conditionally on the finiteness of $\text{III}(E)[2^\infty]$; no point was found up to height 10^7 on a reduced model]. (iii) Undecided cases: for $N = 64$, eleven of the 26 primes x with $N < x \leq 3N + 2$ (ten give conics without rational points); for $N = 128$, the three prime survivors $x = 173, 293$ and 317 (rank between 1 and 3, 0 and 4, 1 and 3); for $N = 512$, $x = 557$ (rank 2, one independent point found), $x = 1367$ (rank between 1 and 3) and $x = 743, 911, 1013, 1319, 1487$ (beyond the available memory of 7 GB). (iv) A global obstruction thus excludes many slices already at the level of rational points, including prime slices that escape every local test, but under the standard finiteness conjecture it does not exclude all of them: integrality of y and z must be used [heuristic, resting on the conditional statement for $(64, 73)$].

Remark 10.25C (cubic reciprocity, and the form a reciprocity argument must take). For a solution (t_1, t_2, t_3) of (E3) let $\chi_j = (\cdot/(t_j - \omega))_3$ be the cubic Jacobi symbol modulo $t_j - \omega$ in $\mathbb{Z}[\omega]$. For a prime $\ell \mid \Phi(t_j)$, the prime of $\mathbb{Z}[\omega]$ above ℓ that divides $t_j - \omega$ has residue field $\mathbb{F}_\ell$ with $\omega \mapsto t_j$, so $\chi_j(a)$ is computed prime by prime as $a^{(\ell-1)/3} \bmod \ell$, read as a power of t_j . Grouping the cubic symbols of t_i at the primes of $\Phi(t_j)$, with their multiplicities, therefore gives one symbol $\chi_j(t_i)$ for each ordered pair. (i) What the equation forces. Since $t_j - \omega$ divides β (Proposition 10.5), (E3) gives $N \cdot P^2 \equiv 1$ modulo $t_j - \omega$, hence $\chi_j(P) = \chi_j(N)$ for each j : three conditions, each on a product of the variables. At a prime t_i the equation is the cross condition of Remark 4.9, a congruence between rational integers. For odd k every $t_i \equiv 2 \pmod{3}$ (Proposition 4.5), so it is inert in $\mathbb{Z}[\omega]$, and every rational integer prime to t_i is a cube modulo t_i because $3 \nmid t_i - 1$; the equation at t_i therefore carries no cubic information. By cubic reciprocity [28], $\chi_j(t_i)$ equals, up to an explicit unit factor, the symbol of $\alpha = t_j - \omega$ modulo $t = t_i$, which is $(\bar{\alpha}/\alpha)^{(t+1)/3} \bmod t$. It depends on the argument of α modulo t and not on its norm; since the norm-one subgroup of $\mathbb{F}_{t^2}^\times$ has order $t + 1$, divisible by 3, the cross conditions, which fix only norms, leave it free [proved]. (ii) A witness. Cubic reciprocity holds for every triple, so a contradiction derived from it would require that no triple satisfies the three conditions of (i). For $N = 128$ the primes 197, 2,399 and 4,877, which are $\equiv 5, 23$ and $5 \pmod{24}$, satisfy all three: $\Phi(197) = 19 \cdot 2,053$, $\Phi(2,399) = 433 \cdot 13,297$ and $\Phi(4,877) = 23,790,007$ is prime, and

$\chi_j(N \cdot P^2) = 1$ for $j = 1, 2, 3$. They do not satisfy (E3). Among 3,000 random prime triples for each of $k = 7, 9$ and 11 , with all primes $\equiv 5$ or $23 \pmod{24}$ and the smallest below $3N$, 107, 111 and 115 satisfy all three conditions, against 111 expected for three independent conditions of probability $1/3$; the same program confirms the three conditions on the solution (2, 8, 512) at $N = 2$ [computed]. So cubic symbols combined by reciprocity cannot exclude anything by themselves. This is the cubic analogue of Remark 4.9, and it closes the route. (iii) What remains. A reciprocity argument evaluates, at a point, local invariants whose sum vanishes by a global law; a contradiction needs the local values to be forced by local integrality. That is an integral Brauer–Manin obstruction [25, 26]. Unlike the obstruction to rational points of Remark 10.25B, it is not excluded by the existence of rational points on the slices, and the trivial chain is removed by requiring x, y and z to be odd at the place 2. The natural setting is the affine scheme $\mathcal{U}_N = \text{Spec } \mathbb{Z}[x, y, z]/(F)$ with $F = N(xyz)^2 - 1 - (N - 1)\Phi(x)\Phi(y)\Phi(z)$, or a slice $\mathcal{C}_{N,x} = \text{Spec } \mathbb{Z}[y, z]/(F)$, base-changed to $\mathbb{Z}[\omega]$ so that cubic cyclic algebras are defined, together with the 3-primary part of the Brauer group of its generic fibre and the adelic integral points with odd 2-adic coordinates; Brauer groups of surfaces can be computed effectively in principle [27]. Whether this group contains a class that obstructs integral points, already on one slice such as $(N, x) = (64, 73)$, which has rational points if III is finite, is open; the group may also be too small to give an obstruction [heuristic]. (iv) Two observations on this programme. First, on a single slice the open curve has a trivial Brauer group over $\mathbb{Q}$, so every class is algebraic (integral Brauer–Manin obstructions on curves are studied in [26]); an obstruction on one slice can at most re-prove what Computation 10.2 already decides, and only a class defined uniformly over the family can give something new. Second, the most natural uniform class does not obstruct. For an even level $N = A^2$ the factorisation $(A \cdot xyz - 1)(A \cdot xyz + 1) = (N - 1)\Phi(x)\Phi(y)\Phi(z)$ of Remark 4.7 gives the quaternion algebra $\alpha = (-3, A \cdot xyz - 1)$; its zeros on the affine surface lie where some coordinate is a primitive cube root of unity, whose residue fields contain $\sqrt{-3}$, so α is unramified there. Its local invariant vanishes at every odd prime $\ell \nmid 3(N - 1)$ (such ℓ dividing $A \cdot xyz - 1$ divide some Φ and are $\equiv 1 \pmod{3}$) and at 2 ($A \cdot xyz - 1$ is a unit and $-3 \equiv 1 \pmod{4}$), and at the real place on the component $y, z > 0$, where $A \cdot xyz - 1 > 0$; so for $N = 4$ and $N = 64$, where every prime of $N - 1$ other than 3 is $\equiv 1 \pmod{3}$, only the place 3 can contribute. On the slices $(N, x) = (64, 71), (64, 73), (64, 79), (64, 131), (4, 5), (4, 7)$ and $(4, 11)$, integral 3-adic points with $y \in [-200, 200]$ give both values ± 1 of the 3-adic symbol, and the 2-adic symbol is always 1 [computed with PARI/GP]. So α gives no obstruction, in agreement with Remark 4.10, and no easy Brauer–Manin obstruction is available.

11. The generalised equation, many prime factors, geometry

11.1 The family A059046

Proposition 11.1. For $m \geq 2$, the aliquot sum $\sigma(m) - m$ divides $m - 1$ with quotient $N - 1$ if and only if $(N - 1)\sigma(m) = N \cdot m - 1$. This is OEIS A059046; its non-prime-power terms form A059047 [12]. A counterexample is an odd square b^2 in A059047 whose quotient is a Mersenne number. [proved]

Proposition 11.2 (parity). Let $m \geq 2$ solve $(N - 1)\sigma(m) = N \cdot m - 1$ with $N \geq 3$. Then every prime factor of m exceeds $N - 1$, so m is odd. If N is even, $m = b^2$ is an odd square. If some prime has odd exponent in m , then N is odd. [proved]

Proof. Since $\sigma(m)/m = (N \cdot m - 1)/((N - 1)m) < N/(N - 1)$, every prime $t \mid m$ satisfies $1 + 1/t < \sigma(m)/m < 1 + 1/(N - 1)$, so $t > N - 1 \geq 2$: m is odd. If N is even, $N \cdot m - 1$ is odd, so $\sigma(m)$ is odd, which for odd m means that m is a square. If some prime t has odd exponent e , then $\sigma(t^e)$ is even, so $N \cdot m - 1 = (N - 1)\sigma(m)$ is even and N is odd ■

Computation 11.3. A sieve over all $m \leq 2 \cdot 10^{10}$ finds 2,741 non-prime-power terms of A059047; all are squarefree, with N odd, so that the quotient $N - 1$ is even (2,720 with two, 19 with three, 2 with four prime factors). A four-prime search finds the new term $189,297,459,739 = 31 \cdot 59 \cdot 181 \cdot 571,811$ ($N = 19$). [computed]

Conjecture 11.4 (squarefree law). Every non-prime-power solution of the generalised equation is squarefree. It implies Conjecture SQ: the generalised equation has no solution $m = b^2$ with $b > 1$ other than the powers b of a prime N . Conjecture SQ implies the almost perfect number conjecture.

The family A059047 begins 77, 611, 1073, 2033, ... and arose in te Riele's construction of hyperperfect numbers [12]. A weaker statement than Conjecture 11.4, the exponent-one principle (every non-trivial solution of the generalised equation has a prime of exponent exactly one), also implies the almost perfect number conjecture, since for $N = 2^k$ all exponents of $m = b^2$ are even; it holds for two primes and every N (Theorem 6.4).

Remark 11.5 (where the solutions would hide). For a squarefree three-prime $b = xyz$ the equation is equivalent to $N = (X - 1)/(X - P^2)$ with $X = \Phi(x)\Phi(y)\Phi(z)$ and $P = xyz$, and more generally, for any odd b , to $N - 1 = (b^2 - 1)/(\sigma(b^2) - b^2)$. So the whole problem is the divisibility $s(b^2) \mid b^2 - 1$, where $s(m) = \sigma(m) - m$ is the aliquot sum (Proposition 11.1). The value of the quotient plays no visible role: Computation 10.2 shows that the integer equation (E3) has no non-trivial solution for any level $N \leq 1,000$, odd or even. The decisive question is therefore whether $s(b^2)$ can divide $b^2 - 1$ at all when b is not a prime power. This is Conjecture SQ (Conjecture 11.4).

Computation 11.6 (squares up to 10^{20}). For every odd b with $3 \leq b \leq 10^{10}$, $\sigma(b^2)$ was computed from a segmented factorisation sieve with 128-bit arithmetic, and the divisibility $s(b^2) \mid b^2 - 1$ was tested exactly. It holds exactly for the odd prime powers b (for which $s(b^2) \mid b^2 - 1$ always) and for no other b . Hence no odd non-prime-power square $m \leq 10^{20}$ lies in OEIS A059046 with any quotient. In particular every counterexample to the almost perfect number conjecture, with any number of prime factors and any k , has odd part $b > 10^{10}$. [computed; the program reproduces the count of odd prime powers below 10^6 and 10^8 as a check] The search quoted in [4] covers a larger range (Section 14.2).

11.2 Any number of prime factors

Theorem 11.7 (finiteness for fixed k and ω). For every k and ω there are only finitely many counterexamples with $\omega(b) = \omega$. [proved; not uniform in k ; made effective by Theorem 11.8A] Proof. Suppose there are infinitely many, $b_1, b_2, \dots$ with $b_n \rightarrow \infty$, primes $t_{n,1} < \dots < t_{n,\omega}$ and exponents $e_{n,i}$. Passing to a subsequence, each prime $t_{n,i}$ is eventually constant or tends to infinity, and so is each exponent. By (2.1), $\sigma(b_n^2)/b_n^2 = N/q - 1/(q \cdot b_n^2) \rightarrow N/q$. On the other side, $\sigma(t^{2e})/t^{2e}$ tends to 1 when $t \rightarrow \infty$ (it lies between 1 and $t/(t-1)$), to $t/(t-1)$ when t is fixed and $e \rightarrow \infty$, and is constant otherwise. Hence $\prod_{\text{fixed}} \sigma(t^{2e})/t^{2e} \cdot \prod_{e \rightarrow \infty} t/(t-1) = N/q$. If the exponent of some fixed prime tends to infinity, the left side is a fraction whose numerator $\prod \sigma(t^{2e}) \cdot \prod t$ is odd, so in lowest terms its numerator is odd, while N/q has the even numerator 2^k : a contradiction. Otherwise $q \cdot \sigma(B^2) = N \cdot B^2$ for the product B of the fixed prime powers. If $B = 1$ this says $q = N$. Otherwise every prime of B exceeds q (Lemma 3.4), so $\gcd(q, N \cdot B^2) = 1$ forces $q = 1$, that is $k = 1$, and then $\sigma(B^2) = 2B^2$ is impossible because $\sigma(B^2)$ is odd ■ The proof does not extend to $k \rightarrow \infty$: when all primes tend to infinity together with N , the first-order limit equation $\sum 1/\theta_i = 1$ for $t_i = \theta_i N$ has solutions, so compactness alone cannot give uniformity in k . Arguments of this type go back to Dickson; no priority is claimed. For $\omega \leq 3$ the results of Sections 6 and 7 make the statement effective, and Theorem 11.8A gives an explicit bound for every ω .

Proposition 11.8. With ω primes, $w_i = t_i^{2e_i}$, $T = \prod t_i$, $L_\omega = \prod (t_i - 1)$, $C_\omega = qT - N \cdot L_\omega$: (i) $C_\omega \geq 1$ for even N ; (ii) $C_\omega = t_\omega C_{\omega-1} + N \cdot L_{\omega-1}$; (iii) some $w_i < \omega \cdot q \cdot \prod_{j \neq i} t_j$. [proved; $\omega = 4$ formally verified: L4_identity, four_prime_bounds]

Proof. (i) With $W = \prod w_i$, $\sigma(w) = (tw - 1)/(t - 1) < tw/(t - 1)$ gives $N \cdot W - 1 = q \prod \sigma(w_i) < qTW/L_\omega$, so $C_\omega \cdot W > -L_\omega > -W$ and $C_\omega \geq 0$; C_ω is odd for even N . (ii) is an expansion. (iii) For $u_i = t_i w_i$, $\prod (u_i - 1) \geq \prod u_i - \sum_i \prod_{j \neq i} u_j$. Since $q \prod (u_i - 1) = L_\omega (N \cdot W - 1) < N \cdot L_\omega \cdot W$, this gives $C_\omega \cdot W < q \cdot \sum_i (T/t_i) (W/w_i)$. As $C_\omega \geq 1$, some term satisfies $W < \omega \cdot q \cdot (T/t_i) (W/w_i)$, which is (iii) ■ For $\omega = 3$, (i) is Proposition 7.1, (ii) is the bound on s in regime (M), and (iii) is Lemma 7.4.

Theorem 11.8A (an effective bound for every ω). Let $N \geq 2$ be even, $q = N - 1$, and let $b > 1$ be odd with $q \cdot \sigma(b^2) = N \cdot b^2 - 1$ and $\omega(b) = \omega$. Then $b^2 < (5\omega N)^M$ with $M = 4^\omega - 1$. In particular every counterexample (b, k) with $\omega(b) = \omega$ satisfies $b^2 < (5\omega \cdot 2^k)^M$, and Theorem 11.7 is effective for every ω . The proof is a procedure that determines the prime powers of b in exactly 2ω steps, with explicitly bounded choices at each step. [proved; the parity step is formally verified: `gap_odd`, `gap_ne_zero`]

Proof. For odd x write $h(x) = \sigma(x^2)/x^2$; h is multiplicative on coprime arguments, and for a prime power, $h(t^e) = (t/(t-1))(1 - t^{-(2e+1)})$, so $1 < h(t^e) < t/(t-1)$. By the equation, $h(b) = N/q - 1/(q \cdot b^2) < N/q \leq 2$. A state is a pair (m, S) in which m is a unitary divisor of b whose prime powers are known and S is a set of primes of b not dividing m whose exponents e_i are not yet known; v denotes the part of b coprime to m and to the primes in S . The procedure keeps the invariant that every prime of v exceeds every prime of m and of S . Put $\Pi = \prod_{t \in S} t$, $\Pi' = \prod_{t \in S} (t-1)$, $\Lambda = m^2 \Pi$, $X = q \cdot \sigma(m^2) \cdot \Pi$ and $g = N \cdot m^2 \Pi' - q \cdot \sigma(m^2) \Pi$. Since N is even and q , $\sigma(m^2)$ and Π are odd, g is odd, so $g \neq 0$; and since $h(m) \leq h(b) < 2$ and $q < N$, $X < 2N\Lambda$. The procedure starts at $m = 1$, $S = \emptyset$, $\Lambda = 1$, and ends at $m = b$, $S = \emptyset$.

Step A ($g > 0$, and (m, S) is not the end state). Then $v \neq 1$. This is clear if $S = \emptyset$. If $S \neq \emptyset$ and $v = 1$, then $h(b) = h(m) \prod_{t \in S} h(t^{e_i}) < h(m) \Pi / \Pi'$, so $1/(q \cdot b^2) = N/q - h(b) > N/q - h(m) \Pi / \Pi' = g/(q \cdot m^2 \Pi') \geq 1/(q \cdot m^2 \Pi')$, which contradicts $b^2 \geq m^2 \Pi^2 > m^2 \Pi'$. Let t' be the smallest prime of v and $j \leq \omega$ the number of primes of v . Then $h(v) = h(b)/(h(m) \prod_{t \in S} h(t^{e_i})) > h(b) \Pi' / (h(m) \Pi) = 1 + (g - m^2 \Pi' / b^2) / X \geq 1 + 8/(9X)$, because $b \geq m \Pi v$ with $v \geq 3$ gives $m^2 \Pi' / b^2 < 1/9$. On the other side $h(v) < (t'/(t'-1))^j \leq \exp(j/(t'-1))$, and $h(v) < h(b)/h(m) < 2$. Since $\log(1+y) \geq y/2$ for $0 < y < 1$, $j/(t'-1) > 4/(9X)$, that is $t' < 1 + 9jX/4 < 1 + 4.5\omega N\Lambda \leq 5\omega N\Lambda$. The next state is $(m, S \cup \{t'\})$, with $\Lambda' = \Lambda t' < 5\omega N\Lambda^2$.

Step B ($g < 0$). Then $S \neq \emptyset$, because for $S = \emptyset$ the inequality $g < 0$ says $h(m) > N/q > h(b) \geq h(m)$. Since $h(v) \geq 1$, $\prod_{t \in S} h(t^{e_i}) \leq h(b)/h(m) < N/(q \cdot h(m))$, that is $\prod_{t \in S} (1 - t^{-(2e_i+1)}) < N \cdot m^2 \Pi' / (q \cdot \sigma(m^2) \Pi) = 1 - |g|/X \leq 1 - 1/X$. As $1 - \prod(1 - y_i) \leq \sum y_i$ for $0 \leq y_i \leq 1$, some $t \in S$ satisfies $t^{2e_i+1} < |S| \cdot X < 2\omega N\Lambda$. The next state is $(m \cdot t^{e_i}, S \setminus \{t\})$, with $\Lambda' = \Lambda \cdot t^{2e_i-1} < 2\omega N\Lambda^2$.

Every step A adds a prime of b to S and every step B moves one from S into m , so after exactly 2ω steps all primes are found and all exponents fixed: $m = b$, $S = \emptyset$ and $\Lambda = b^2$. With $C = 5\omega N$ every step gives $C\Lambda' < (C\Lambda)^2$, and $C\Lambda = C$ at the start, so $C \cdot b^2 < C^L$ with $L = 2^{2\omega} = M + 1$, that is $b^2 < C^M$ ■

For $m = 1$ and S the set of all primes, the inequality $g < 0$ of step B is Proposition 11.8 (i) and its conclusion is Proposition 11.8 (iii); Theorem 11.8A combines this exponent step with the prime step of the method used for odd perfect numbers with a fixed number of prime factors (Pomerance [20]; Heath-Brown [21]), the parity of g taking the place of the condition $\sigma(n)/n \neq a/b$ used there. The bound is polynomial in N for fixed ω . It is not uniform in k : in step A the gap g can be as small as 1 while X grows with N , which is the multi-scale structure behind the remark after Theorem 11.7. A bound on b independent of k for fixed ω would reduce each ω to a finite computation, because $b > N$.

Computation 11.8B (the procedure as a program). The procedure of Theorem 11.8A was implemented in C with exact multiprecision arithmetic, branching over every admissible choice: in step A over all primes t' allowed by the lower bound for $h(v)$ and by $h(v) - 1 > 1/t'$ (with every exponent of S at least 1), and in step B over every $t \in S$ and every exponent with $t^{2e_i+1} \cdot |g| < |S| \cdot X$. When one prime remains ($j = 1$), $v = t^{e'}$ and $1/t' < h(v) - 1 < 1/(t' - 1)$; the last prime is then located by exponent boxes, in which each exponent of S is either fixed in $\{1, \dots, E\}$ or only known to exceed E . Bounding $h(m) \prod_{t \in S} h(t^{e_i})$ from below (exponent $E + 1$) and from above (the limit $t/(t-1)$), and using $b^2 \geq m^2 \prod_{t \in S} t^{2e_i} \cdot t'^2$, each box gives an explicit interval for t' . In a box with all exponents fixed the interval contains at most a few integers, and each prime candidate is tested exactly through $t'^{2e'} = (K' - t' + 1)/(K't' - N \cdot m'^2(t' - 1))$, where $m' = b/t^{e'}$ and $K' = q \cdot \sigma(m'^2)$ (Theorem 4.1); the intervals of the other boxes are short and are scanned by the general procedure. The program finds no solution for $\omega = 3$ with any exponents and every $k \leq 15$ ($k = 15$: $1.5 \cdot 10^8$ nodes), for $\omega = 4$ with any exponents and every $k \leq 7$ ($k = 7$: $1.4 \cdot 10^9$ nodes), and for $\omega = 5$ with any exponents and $k \leq 2$ [computed]. For $\omega = 3$ this is a second check of Computation 7.9 ($k \leq 16$) by a different method; for $\omega = 4$ and $\omega = 5$ it covers all exponents, which Computation 11.9 does not.

Validation: the same program for the exponent-one equation $(N - 1)\sigma(n) = N \cdot n - 1$ finds 77 ($N = 5$), the four-prime terms $54,375,629 = 7 \cdot 11 \cdot 547 \cdot 1291$ ($N = 5$) and $128,807,153 = 23 \cdot 109 \cdot 191 \cdot 269$ ($N = 17$), the three-prime solutions $43 \cdot 647 \cdot 6301$ and $43 \cdot 613 \cdot 13679$ ($N = 41$) and $149 \cdot 463 \cdot 659$ ($N = 97$); solutions containing the prime $p = N$, which occur only for odd N , are outside its scope, because a branch with $g = 0$ (impossible for even N) is not followed [computed]. The source and the logs are distributed with this report.

Computation 11.9. When p , r and s appear to the first power, the deficit left by their abundancies bounds the next prime: with $\Delta(p) = N \cdot p^2 - q\Phi(p)$ and $\Delta(pr) = N \cdot p^2 r^2 - q\Phi(p)\Phi(r)$, one has $r \in (q\Phi(p)/\Delta(p), 3.5 \cdot q\Phi(p)/\Delta(p) + 1]$ and $s \in (q\Phi(p)\Phi(r)/\Delta(pr), 2.03 \cdot q\Phi(p)\Phi(r)/\Delta(pr) + 3]$, the factor 2.03 absorbing the term $1/(q \cdot b^2)$; $p \leq 4N - 1$ by Lemma 3.6, and the largest prime t , with any exponent, is determined by Theorem 4.1 [proved]. For $b = p \cdot r \cdot s \cdot t^v$ there is no counterexample for any $k \leq 10$ ($k = 8$: $3.8 \cdot 10^8$ triples; $k = 9$: $1.7 \cdot 10^8$; $k = 10$: $4.1 \cdot 10^9$, including one triple with $t > 2^{63}$ checked separately with exact integers) [computed]. Validation: the same windows applied to the exponent-one equation recover the known four-prime terms of A059047, $54,375,629 = 7 \cdot 11 \cdot 547 \cdot 1291$ ($N = 5$) and $128,807,153 = 23 \cdot 109 \cdot 191 \cdot 269$ ($N = 17$), and find the term of Computation 11.3. Cases in which one of p , r , s has a higher exponent need the four-prime analogue of Theorems 7.7 and 7.8.

11.3 Geometry

Regarding the primes as variables, the generalised equation with exponents f_i of m defines a hypersurface of multidegree $(f_1, \dots, f_\omega)$ in $(\mathbb{P}^1)^\omega$ with canonical class $\mathcal{O}(f_1 - 2, \dots, f_\omega - 2)$. All $f_i = 1$ is the Fano case (solutions are plentiful), all $f_i = 2$ (b squarefree) the Calabi–Yau case (a genus-one curve for $\omega = 2$, a K3 surface for $\omega = 3$), and larger exponents give positive canonical class in those directions, where the Lang–Vojta philosophy predicts that integral points are sparse. This explains why higher exponents collapsed quickly and the squarefree case is the hardest. For $N = 4, 8, 16$ the K3 surface is smooth [computed]. The three Vieta involutions map an integral point to an integral point only when the potential of the other two variables is ± 1 , which happens along the trivial chain and fails at any solution with $x > N$. More precisely, for a solution with $x > N$ the second root in z of $c \cdot z^2 - Qz - (Q + 1) = 0$, with $c = f_N(xy)$ and $Q = (N - 1)\Phi(x)\Phi(y)$, is $-(Q + 1)/(cz) \in (-1, 0)$, and similarly in the other variables, while along the trivial chain the partner of N^9 is -1 . A non-trivial solution would therefore be an isolated integral point, not connected by these involutions to the degenerate points $(N, N^3, -1)$ and $(N, -1, -1)$.

Proposition 11.10 (genus of the fibres). For $D \geq 2$ and $k \leq 300$, the curve $C_{N,D}$ defined by $\Delta(p, r)^2 - (D + 1)\Delta(p, r) + D^2 = DN(pr)^2$ has every component of geometric genus ≥ 1 , so it has finitely many integral points (Siegel). This is weaker than Theorem 7.8 and does not give uniformity. [proved; discriminant condition certified by Sturm sequences] Proof. Let $E_{N,D}$ be the curve in (X, P, S) -space defined by (i) and (ii) of Proposition 8.1. For $D \geq 2$ the conic $X^2 - 4DN \cdot P^2 = -(3D + 1)(D - 1)$ is smooth, hence rational over $\mathbb{Q}$. Condition (i) is quadratic in S with discriminant $q((N + 3)P^2 + 6qP - 3q - 2X - 2D - 2)$ (Section 8.1), so $E_{N,D}$ is the double cover of the conic branched where this vanishes. There $X = ((N + 3)P^2 + 6qP - 3q - 2D - 2)/2$, and substitution gives the quartic $f(P) = ((N + 3)P^2 + 6qP - 3q - 2D - 2)^2 - 16DN \cdot P^2 + 4(3D + 1)(D - 1)$. The branch curves do not meet at infinity, so $E_{N,D}$ has genus 1 exactly when f has four distinct roots. The discriminant of f is a polynomial $R(N, D)$ of degree 12 in N and 6 in D (obtained by exact interpolation and checked at 40 random points); for every $k \leq 300$ a Sturm sequence over $\mathbb{Q}$ shows that $R(2^k, D)$ has no real root $D \geq 2$. The map $(p, r) \mapsto (pr, p + r)$ is finite of degree 2, so each component of $C_{N,D}$ maps onto $E_{N,D}$ and has genus at least 1 by Riemann–Hurwitz ■ Theorem 7.8 already gives an effective finite search for each N , uniformly in D , and effective forms of Siegel’s theorem grow far too fast in N and D to give uniformity.

Remark 11.10A (integral points on surfaces: what the general theorems give). For fixed N let $X_N \subset (\mathbb{P}^1)^3$ be the closure of $(E3)$. It has tridegree $(2, 2, 2)$, so it is a K3 surface, and the complement of the affine surface is $D = D_x + D_y + D_z$, where $D_x = X_N \cap \{x = \infty\}$ is the curve $N(yz)^2 = (N - 1)\Phi(y)\Phi(z)$, irreducible over $\mathbb{Q}$ for every $N \geq 2$ [proved: as a polynomial in z its coefficients $y^2 - (N - 1)(y + 1)$ and

$(N - 1)\Phi(y)$ are coprime, since the first takes the value $N\omega^2 \neq 0$ at a root ω of Φ , and its discriminant $(N - 1)\Phi(y)((N + 3)y^2 - 3(N - 1)y - 3(N - 1))$ is not a square in $\mathbb{Q}[y]$, because the irreducible factor $\Phi(y)$ does not divide the last factor, whose value at ω is $4N\omega^2$. Each of these curves is a fibre of a projection, so it is nef of Iitaka dimension 1 but not big. The coefficient of $x^2y^2z^2$ is 1, so $D_x \cap D_y \cap D_z = \emptyset$, while $D_x \cap D_y$ consists of the two conjugate points with $z^2 - (N - 1)(z + 1) = 0$. With $r = 3$ components of which at most $m = 2$ meet, Levin's higher-dimensional Runge theorem [22] (Theorem 4 (a) there) applies ($m \cdot |S| = 2 < 3$ for $S = \{\infty\}$) and places the integral points on an effectively computable proper closed subset. Here the Runge argument is the bound on the smallest coordinate (Lemma 3.6 for integer variables); on each slice the points at infinity form two Galois orbits, which gives the window of Remark 10.17. So for each N the general theory reproduces the reduction already used and adds nothing. The theorems of Corvaja and Zannier [23] (at least four ample components in general position) and of Heier and Levin [24] (for surfaces, at least seven effective divisors in general position [24, Thm. 1.8]) need more boundary components than the three present here and do not apply. Uniformity in N would need the same arguments on the threefold of all (x, y, z, N) . There the coefficient of $N \cdot x^2y^2z^2$ vanishes, so all four boundary components meet at the point $(\infty, \infty, \infty, \infty)$, $m = r = 4$, and the Runge condition fails. The same holds for the exponent-one equation $(N - 1)(x + 1)(y + 1)(z + 1) = N \cdot xyz - 1$, whose coefficient of $N \cdot xyz$ also vanishes and which has many solutions. Near this corner both equations reduce to the first-order equation $\sum 1/\theta_i = 1$ for $x_i \approx \theta_i N$, and they first differ in the second-order terms: $\log(\Phi(x)/x^2) = 1/x + 1/(2x^2) + \dots$, against $\log(1 + 1/x) = 1/x - 1/(2x^2) + \dots$ [the boundary statements are computed exactly; the conclusion is heuristic]. A uniform argument of Runge type would therefore have to resolve this corner and use the second-order behaviour of Φ , in agreement with Remark 10.4. The corner is populated: the trivial chain (N, N^3, N^9) is an integral point of the threefold for every N , whose coordinates have heights $h(N)$, $3h(N)$ and $9h(N)$, so no inequality $h(P) \leq \alpha \cdot h(N) + O(1)$ with $\alpha < 1$ holds for its integral points, for any of the usual heights on the threefold. A height or Vojta-type argument must therefore use $x > N$, positivity or primality, and cannot rest on integrality alone [proved].

11.4 The limits of local arguments

All congruence conditions above (Propositions 4.2, 4.3, Lemma 8.2, the norm conditions of Theorem 8.5) are consequences of the component equations, and those are solvable modulo every prime power: for $\ell \nmid qN$, Proposition 4.2 does not constrain D_t modulo ℓ , and D_t can be chosen so that $D_t\Phi(t) + t \equiv N \cdot u^2 \pmod{\ell}$; for $\ell \mid q$, $D_t \equiv (1 - t)t^{-2}$, and then $\ell \mid D_t - 1$ is equivalent to $t^2 + t - 1 \equiv 0$, while $\ell \mid 3D_t + 1$ is equivalent to $t^2 - 3t + 3 \equiv 0$, which is solvable exactly when -3 is a square modulo ℓ , the condition that the norm form requires. Local information re-encodes local solvability. A purely local obstruction therefore cannot exist; local information must be combined with archimedean sizes, as in Theorem 8.4 and Section 9.

11.5 A heuristic

Given all prime powers of b but the largest, Theorem 4.1 fixes the largest prime and D ; success requires one further exact equality of probability about $1/\Delta$. Summing gives an expected number of counterexamples with ω prime factors of order $(\log N)/N^{\omega-1}$ for each k , a convergent series. [heuristic] For $\omega = 3$ the measured sum at $k = 11$ is about $2 \cdot 10^{-9}$, in agreement with this order.

11.6 Odd almost perfect numbers

For $k = 1$, equation (2.1) reads $\sigma(b^2) = 2b^2 - 1$: an odd almost perfect number $n > 1$ is a square $n = b^2$, because $\sigma(n) = 2n - 1$ is odd. Kishore [1, 2] proved that b has at least six distinct prime factors. This subsection raises the bound to seven (Theorem 11.11) and then to eight (Theorem 11.19). The method is the procedure of Theorem 11.8A at $N = 2$, organised as an exhaustive search in which every discarding step is one of Lemmas 11.12–11.15, applied to exact integers. For testing, the equation is generalised to $J \cdot \sigma(n) = K \cdot n - d$ with $n = b^2$, b odd, J odd, K even and $d \geq 1$; the case $(J, K, d) = (1, 2, 1)$ is that of odd almost perfect numbers, and $(J, K, d) = (N - 1, N, 1)$ is equation (2.1) at level N .

Theorem 11.11 (seven prime factors). Every odd almost perfect number $n > 1$ has at least seven distinct prime factors. [computed (Computation 11.16); the search rests on Lemmas 11.12–11.15, whose identities and inequalities are formally verified]

Notation. For a prime power $p^a \parallel b$ put $V = p^{2a}$, so that $\sigma(V) = (pV - 1)/(p - 1)$, and $x = 1/(pV)$. For a set of prime powers of b with product m write $s = J \cdot \sigma(m^2)$. For a set R of further primes of b write $\Pi = \prod_R p$, $M = \prod_R (p - 1)$ and $G = s \cdot \Pi - K \cdot m^2 \cdot M$.

Lemma 11.12 (parity). G is odd; in particular $G \neq 0$. [formally verified: oddsearch_parity] Proof. s and Π are odd, and $K \cdot m^2 \cdot M$ is even ■

Lemma 11.13 (closed systems). Suppose that $s \cdot \prod_R \sigma(V_p) = K \cdot m^2 \cdot \prod_R V_p - d$, and put $V = \prod_R V_p$. (i) $s \cdot \Pi \cdot (1 - \prod_R (1 - x_p)) = G + d \cdot M/V$. (ii) If $G > 0$, then $G \cdot p \cdot V_p \leq |R| \cdot s \cdot \Pi$ for some $p \in R$. (iii) If $G < 0$, then $V \cdot |G| < d \cdot M$. (iv) If $R = \{p\}$, then $V_p \cdot G = s - d(p - 1)$. [formally verified: closed_identity, closed_pos, closed_neg, closed_one] Proof. Multiplying the equation by M and dividing by V gives $s \cdot \Pi \cdot \prod (1 - x_p) = K \cdot m^2 \cdot M - d \cdot M/V$, which is (i). Since $0 < 1 - \prod (1 - x_p) \leq \sum x_p$, (i) gives (iii) when $G < 0$; when $G > 0$ it gives $\sum x_p > G/(s\Pi)$, hence (ii). (iv) is (i) for one prime ■

Lemma 11.14 (the last prime). Let U be a set of primes u of b with exponents at least $B(u)$, and let t be a further prime of b , larger than every other, such that $s \cdot \prod_U \sigma(V_u) \cdot \sigma(V_t) = K \cdot m^2 \cdot \prod_U V_u \cdot V_t - d$. Form Π , M and G over U , and put $C_2 = K \cdot m^2 \cdot M$, $X = \sum_U u^{-(2B(u)+1)}$ and $P_V = \prod_U u^{2B(u)}$. (i) $t \cdot G + C_2 + (t - 1) \cdot d \cdot M/(V_t \cdot \prod_U V_u) = s \cdot t \cdot \Pi \cdot (1 - (1 - x_t) \cdot \prod_U (1 - x_u))$. (ii) If $G < 0$ and $t \geq t_0$, then $C_2/(|G| + s \cdot \Pi \cdot (t_0^{-3} + X)) \leq t$ and $t \cdot |G| < C_2 + d \cdot M/(t \cdot P_V)$. (iii) If $G > 0$, then $G < s \cdot \Pi \cdot (x_t + \sum_U x_u)$; hence $t^3 \leq 2s \cdot \Pi/G$, or $u \cdot V_u \leq 2|U| \cdot s \cdot \Pi/G$ for some $u \in U$. (iv) If $U = \emptyset$ and $(J, K, d) = (1, 2, 1)$, then $t = \lfloor 2m^2/(2m^2 - \sigma(m^2)) \rfloor$. [formally verified: last_identity, last_upper, last_lower, last_pos; (iv) is Theorem 4.1 at $N = 2$: component] Proof. (i) is Lemma 11.13 (i) for $U \cup \{t\}$, rewritten. Its left side is positive, and $V_t \geq t^2$; this gives the upper bound in (ii). Its right side is at most $s \cdot t \cdot \Pi \cdot (x_t + \sum_U x_u)$, with $x_t \leq t^{-3}$ and $x_u \leq u^{-(2B(u)+1)}$; this gives the lower bound in (ii) and gives (iii). The lower bound may be iterated, t_0 being replaced by the bound just obtained ■

Lemma 11.15 (the next prime). Suppose that the primes of b below q are known, those of m with their exponents and those of a set U with exponents at least $B(u)$, and that $r \geq 2$ primes of b remain, the smallest being q . Then (i) $s \cdot \prod_U \sigma(u^{2B(u)}) < K \cdot m^2 \cdot \prod_U u^{2B(u)}$, and (ii) $(q/(q - 1))^r \cdot \prod_U u/(u - 1) > (K \cdot m^2 - d/L)/s$ with $L = \prod_U u^{2B(u)} \cdot q^{2r}$. [the ratio bounds are formally verified: ratio_lt, ratio_mono, prod_ratio_le_pow] Proof. Each factor $\sigma(V)/V$ of a prime p with exponent at least B satisfies $\sigma(p^{2B})/p^{2B} \leq \sigma(V)/V < p/(p - 1)$, and the equation gives $\Pi \sigma(V)/V = (K \cdot m^2 - d/\Pi V)/s$ ■

The search. The primes of b are chosen in increasing order. A new prime enters with the condition $a \geq 1$ on its exponent, and Lemma 11.15 (ii) bounds it as long as $K \cdot m^2 \cdot \prod_U (u - 1) > s \cdot \prod_U u$. When this inequality fails, the exponent of a prime $u \in U$ is split into the cases $a = B(u)$ and $a \geq B(u) + 1$, or into all its admissible values when Lemma 11.15 (i) bounds it on its own; by Lemma 11.12 the limiting comparison is never an equality, so the splitting ends. When one prime remains, Lemma 11.14 applies: for $G < 0$ the primes t of the window (ii) are tried, after splitting exponents of U until the window has width at most 30; for $G > 0$ alternative (iii) is followed. With all primes known, Lemma 11.13 fixes the exponents one at a time, and the last one exactly. A branch is discarded only by Lemmas 11.12–11.15, so the search returns every solution with the prescribed number of distinct primes, and each solution returned is checked by evaluating σ .

Computation 11.16. For $(J, K, d) = (1, 2, 1)$ the search finds no solution with $\omega(b) \leq 6$. For $\omega \leq 5$ it takes less than one second, which confirms Kishore's theorem. For $\omega = 6$ it visits 144,512 prime-selection states, 5,568,577 last-prime states and 4,534,707 closed systems, with 2,446,710 exponent splittings; the largest window for t has width 30. Two implementations of the procedure, in Python and in C with GMP, both in exact integer arithmetic, give identical counts for every $\omega \leq 6$; the C run for $\omega = 6$ takes 12 seconds. With window widths 5, 100 and 1,000 in place of 30 the search follows different trees and again finds no solution. Validation. (a) For $(J, K) \in \{(1, 2), (3, 4), (5, 6), (7, 8), (15, 16)\}$ the solutions with $b \leq 3 \cdot 10^6$ and

$1 \leq d \leq 10^7$ were tabulated by direct factorisation. For every pair (d, ω) with $\omega \leq 4$ in these tables, and for 60 random pairs per ratio, 6,349 cases in all, both programs return exactly the tabulated solutions with $n \leq 9 \cdot 10^{12}$. (b) The same holds for the 359 pairs with $(J, K) = (1, 2)$, $\omega = 5$ and $d \leq 10^{10}$, and for the 8 pairs with $\omega = 6$ and $d \leq 10^{13}$, each of which has a solution with six distinct primes. (c) For random b with three or four distinct primes, largest prime up to $3 \cdot 10^4$ and exponents up to 3, with J and K chosen so that $K \cdot b^2 - J \cdot \sigma(b^2)$ is a small positive d , the search recovers every planted b in the runs that finish within the time limit (40 of 40 for three primes, 30 of 30 for four). [computed]

Remark 11.17. Quasiperfect numbers ($\sigma(n) = 2n + 1$) are also odd squares, with abundancy $2 + 1/n$ in place of $2 - 1/n$. For them $\omega \geq 7$ was proved by Hagsis and Cohen [7] and $\omega \geq 8$ by Toyohara, Yao and Tao [29], who decide the last prime by a discriminant criterion. For odd almost perfect numbers the last prime and its exponent are determined directly by the component lemma (Lemma 11.14 (iv)). The case $\omega = 7$ is settled by Theorem 11.19 below, with the help of Lemma 11.18.

Lemma 11.18 (quadratic residues). Let b be an integer and q a prime with $q \mid K \cdot b^2 - d$. Then $K \cdot d$ is a square modulo q . In particular, if $n = b^2$ is an odd almost perfect number, every prime factor q of $\sigma(n)$ satisfies $q \equiv \pm 1 \pmod{8}$, and so does every prime factor of $\sigma(p^{2a})$ for each prime power $p^{2a} \parallel n$. [formally verified: qr_general, qr_two, oap_sigma_prime_mod8] **Proof.** Modulo q , $K \cdot b^2 \equiv d$, hence $K \cdot d \equiv (K \cdot b)^2$. For $(K, d) = (2, 1)$, q divides $\sigma(n) = 2b^2 - 1$, which is odd; so q is odd and 2 is a square modulo q , which holds exactly when $q \equiv \pm 1 \pmod{8}$. Since σ is multiplicative, $\sigma(p^{2a})$ divides $\sigma(n)$ ■

This is the analogue for $\sigma(n) = 2n - 1$ of Cattaneo's observation that every divisor of $\sigma(n)$ of a quasiperfect number is $\equiv 1$ or $3 \pmod{8}$ [31]; for squarefree b and odd $k \geq 3$ the same argument gives Proposition 4.5, and Lemma 11.23 below is its case $k = 1$. In the search, $s = J \cdot \sigma(m^2)$ is the product of J and the values $\sigma(V)$ of the prime powers fixed so far; after the primes of $J \cdot K \cdot d$ are removed from s , every prime factor q of the remainder s' must satisfy $(K \cdot d/q) = 1$. A branch is discarded when the Jacobi symbol $(K \cdot d/s')$ equals -1 , or when s' has a prime factor $q \leq 3,000$ with $(K \cdot d/q) = -1$. The test is applied at every prime-selection state and every last-prime state, and at every splitting of an exponent into $a = B(u)$ and $a \geq B(u) + 1$. For example $\sigma(3^8) = 9,841 = 13 \cdot 757$ with $13 \equiv 5 \pmod{8}$, so $3^8 \parallel n$ is impossible; among the exponents $3^{2a} \parallel n$ with $a \leq 40$, Lemma 11.18 excludes all except possibly $a = 6, 8$ and 18 (a product of primes $\equiv \pm 1 \pmod{8}$ is itself $\equiv \pm 1 \pmod{8}$, so a factor $\equiv \pm 3 \pmod{8}$ of $\sigma(3^{2a})$ left after trial division already suffices).

Theorem 11.19 (eight prime factors). Every odd almost perfect number $n > 1$ has at least eight distinct prime factors. [computed (Computation 11.20); the search rests on Lemmas 11.12–11.15 and 11.18, whose identities, inequalities and congruences are formally verified]

Computation 11.20. For $(J, K, d) = (1, 2, 1)$ and $\omega(b) = 7$, the search of Section 11.6 is partitioned at its fourth prime: the 577 states reached when the four smallest primes of b have been chosen, with the exponent conditions then in force, are run separately. Each state is a different set of four smallest primes, and the union of the states is the whole search. A state may be split further by distributing its leaf units (the blocks of 2^{21} consecutive integers in which the sixth prime is sieved, and the last-prime states) by their index modulo 8 or 32; the union of the parts is the state, which was confirmed on two states by comparing the sums of the counts with a single run. The C program uses GMP for every comparison that decides a branch; a candidate last prime $t < 2^{64}$ is tested by trial division and the Miller–Rabin test with the bases 2, 325, 9375, 28178, 450775, 9780504 and 1795265022, which is deterministic below 2^{64} , and for larger t every odd integer of the window is tested by Lemma 11.13, without a primality test. Result: no state has a solution. With the final program, which applies Lemma 11.18 as described above, the 577 states take 18.1 hours of running time; the largest is the state with smallest primes 3, 5, 17, 257 (16.6 hours, in 32 parts). An earlier computation with versions of the program that do not use Lemma 11.18 completed 575 of the 577 states, again with no solution, in about 73 hours of running time; it confirms the theorem for those states independently of Lemma 11.18. Validation. (a) The final program returns exactly the tabulated solutions with $n \leq 9 \cdot 10^{12}$ in all 6,414 cases of the tables of Computation 11.16 with $d \leq 10^{12}$:

6,049 cases with $(J, K) \in \{(1, 2), (3, 4), (5, 6), (7, 8), (15, 16)\}$ and $\omega \leq 4$, 359 with $\omega = 5$ and 6 with $\omega = 6$; so does the program with Lemma 11.18 applied only at the selection and last-prime states. (b) Lemma 11.18 holds for all 18,334 prime factors of $\sigma(n)$ over all tabulated solutions. (c) The parameter values used (windows enumerated at width at most 10, deferred splittings to depth 24) were validated in the same 6,414 cases before use. [computed]

Remark 11.21 (Fermat primes). The hardest states lie along the chain of Fermat primes $F_j = 2^t + 1$ with $t = 2^j$. Choosing at each step the smallest prime that keeps the abundancy below 2 gives 3, 5, 17, 257, 65537, because $F_j/(F_j - 1) = 1 + 1/(F_j - 1)$ and $(F_j - 1)^2 = F_{j+1} - 1$ give $\prod_{j < m} F_j/(F_j - 1) = 2(1 - 1/(F_m - 1))$; the chain stops at F_5 , which is composite. Of the 577 states of Computation 11.20, the two with the longest ranges for the sixth prime are those with smallest primes 3, 5, 17, 257 and 3, 5, 17, 269: before Lemma 11.18 these ranges had total lengths $4.6 \cdot 10^{11}$ and $7.0 \cdot 10^{13}$, against at most $1.7 \cdot 10^{11}$ for every other state; with it, $9.7 \cdot 10^{10}$ and $1.6 \cdot 10^8$. In the second state 99.6% of the range came from the single configuration $3^8 \cdot 5^8 \cdot 269^4 \cdot 17^{2e} \cdot 4153^{2f}$ ($e \geq 5, f \geq 2$) with the sixth prime in $[1.9 \cdot 10^{13}, 8.9 \cdot 10^{13}]$, which Lemma 11.18 removes at once because $13 \mid \sigma(3^8)$. In the first state one of the largest remaining configurations contains all five Fermat primes, with exponents not yet fixed, and its sixth prime ranges up to $8.6 \cdot 10^9 \approx 2^{33}$. The near-solutions of $\sigma(n)/n = 2 - 1/n$ are therefore organised around this chain; whether this can be turned into a structural statement for every ω is open.

Remark 11.22 (a condition modulo 3). If $3 \mid n$, then $\sigma(n) = 2n - 1 \equiv 2 \pmod{3}$. Since $\sigma(3^{2a}) \equiv 1$, $\sigma(q^{2e}) \equiv 1$ for $q \equiv 2 \pmod{3}$ and $\sigma(q^{2e}) \equiv 2e + 1$ for $q \equiv 1 \pmod{3}$, every prime $q \equiv 1 \pmod{3}$ with $q^{2e} \parallel n$ has $e \not\equiv 1 \pmod{3}$ (otherwise $3 \mid \sigma(n)$, against $(n, \sigma(n)) = 1$ and against Lemma 11.18), and an odd number of them have $e \equiv 2 \pmod{3}$. In particular some prime $q \equiv 1 \pmod{3}$ divides n to an exponent $2e \geq 4$. In the two states of Remark 11.21 the four smallest primes are $\equiv 0$ or $2 \pmod{3}$, so this prime is among the three largest. [proved]

11.7 Squarefree roots and exponent families

In this subsection $n = b^2$ is an odd almost perfect number with b squarefree, so that $\sigma(n) = \prod_{p \mid b} \Phi(p)$. Put $f(p) = \log(\Phi(p)/p^2) = \log(1 + 1/p + 1/p^2)$. Since $\sigma(n)/n = 2 - 1/n$, the primes of b satisfy $\sum_{p \mid b} f(p) = \log(2 - 1/n)$. A prime p is called admissible if every prime factor of $\Phi(p)$ is $\equiv \pm 1 \pmod{8}$. Yamada [33] treated the corresponding case of quasiperfect numbers.

Lemma 11.23 (residues for a squarefree root). Let $n = b^2$ be an odd almost perfect number and p a prime with $p \parallel b$. Then p is admissible and $p \equiv 5$ or $23 \pmod{24}$. [formally verified: oap_squarefree_residue, residue24, mod8_of_prime_factors, sigma_prime_sq] Proof. $\Phi(p) = \sigma(p^2)$ divides $\sigma(n)$, so every prime factor of $\Phi(p)$ is $\equiv \pm 1 \pmod{8}$ by Lemma 11.18, and so is their product $\Phi(p)$. Since $\Phi(p) \equiv p + 2 \pmod{8}$ for odd p , $p \equiv 5$ or $7 \pmod{8}$. If $p \equiv 1 \pmod{3}$, then $3 \mid \Phi(p)$, which is excluded because $3 \not\equiv \pm 1 \pmod{8}$; and $\Phi(3) = 13 \equiv 5 \pmod{8}$. Hence $p \equiv 2 \pmod{3}$ ■

Theorem 11.24 (squarefree root). Let $n = b^2$ be an odd almost perfect number with b squarefree. Then the largest prime factor of b is greater than $1.6 \cdot 10^{30}$, and n has more than $4.3 \cdot 10^{27}$ distinct prime factors. [proved, with Computation 11.25 and the explicit estimate for primes in arithmetic progressions of Bennett, Martin, O'Bryant and Rechnitzer [32] (cited)]

Computation 11.25. (a) For every prime $p \leq 2 \cdot 10^9$, $\Phi(p)$ is factored by a segmented sieve over the primes $\ell \leq 2 \cdot 10^9 + 1$ with $\ell \equiv 1 \pmod{6}$, using the two roots of $x^2 + x + 1$ modulo ℓ ; the cofactor that remains is 1 or a prime greater than $2 \cdot 10^9$. Exactly 7,650,927 primes $p \leq 2 \cdot 10^9$ are admissible, and $S_0 = \sum f(p)$ over them is 0.4629427 to seven decimals. An independent program that factors every $\Phi(p)$ completely (Pollard's rho method and a deterministic Miller–Rabin test) finds the same admissible primes up to 10^7 (60,007 primes, sum 0.4397927) and no admissible prime $p \not\equiv 5, 23 \pmod{24}$ below 10^5 . (b) In $(2 \cdot 10^9, 8 \cdot 10^9]$ there are 24,301,954 primes $p \equiv 5, 23 \pmod{24}$ such that $\Phi(p)$ has no prime factor $\ell \leq 10^6$ with $\ell \equiv 1 \pmod{3}$ and $\ell \equiv 3, 5 \pmod{8}$; they include every admissible prime of this interval, and the sum T of $f(p)$ over them is 0.0056552 to seven decimals. On $(10^5, 10^7]$ this sieve agrees with direct trial division. (c) The

same programs, with the condition $\pm 1 \pmod{8}$ replaced by $1, 3 \pmod{8}$, give for quasiperfect numbers 11,078,663 admissible primes up to $2 \cdot 10^9$ with sum 0.5667729, 35,186,949 primes in $(2 \cdot 10^9, 8 \cdot 10^9]$ with sum 0.0081883, and up to 10^7 the independent factorisation gives 86,712 primes with sum 0.5332355. Every sum is accumulated in double or extended precision and increased by 10^{-7} before use. [computed]

Proof (Theorem 11.24). By Lemma 11.23 every prime of b is admissible. Let $q = 5928 = 24 \cdot 13 \cdot 19$. The roots of $x^2 + x + 1$ are 3, 9 modulo 13 and 7, 11 modulo 19, and $13 \equiv 5, 19 \equiv 3 \pmod{8}$; hence an admissible prime $p > 19$ lies in one of the residue classes $p \equiv 5, 23 \pmod{24}$, $p \not\equiv 3, 9 \pmod{13}$, $p \not\equiv 7, 11 \pmod{19}$, which form a set C of 320 of the $\varphi(q) = 1,728$ classes prime to q . Let $\theta_c(x)$ be the sum of $\log p$ over the primes $p \leq x$ in these classes. By [32, Thm. 1.2], $|\theta(x; q, a) - x/\varphi(q)| < x/(840 \log x)$ for every $x \geq 8 \cdot 10^9$ and every a prime to q , so $\theta_c(x) = \alpha x + E(x)$ with $\alpha = 320/1728$ and $|E(x)| \leq \beta x/\log x$, $\beta = 320/840$. Put $Y = 8 \cdot 10^9$. Since $f(p) < 1/p + 1/p^2$, partial summation with $g(t) = 1/(t \log t)$ gives, for $P > Y$, $\sum_{p \in C, Y < p \leq P} f(p) < \alpha(\log \log P - \log \log Y) + \beta/\log^2 P + \beta(1/\log Y + 3/(2 \log^2 Y)) + 1/(Y - 1)$. Let W be the set formed by the admissible primes up to $2 \cdot 10^9$, the 24,301,954 primes of Computation 11.25 (b) and the primes greater than Y in the classes C ; every prime of b lies in W . Adding S_0 and T , the sum $U(P)$ of f over the elements of W up to P satisfies $U(P) < \log 2 - 10^{-12}$ for every $P \leq P_0 = \exp(69.607)$, and $P_0 > 1.6 \cdot 10^{30}$. Since b has at least eight distinct prime factors, all at least 5 (Theorem 11.19, Lemma 11.23), $n \geq (5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29)^2 > 10^{16}$. Since f decreases and $\sum_{p|b} f(p) = \log(2 - 1/n) > \log 2 - 10^{-12}$, the primes of b cannot all lie below P_0 . Moreover any k elements of W contribute at most the sum of f over the k smallest elements of W , which is at most $U(P_0)$ when k does not exceed the number of elements of W up to P_0 ; hence $\omega(b)$ exceeds that number. That number is at least $7,650,927 + 24,301,954 + (\theta_c(P_0) - \theta_c(Y))/\log P_0$, and by the same estimate $\theta_c(P_0) - \theta_c(Y) \geq \alpha(P_0 - Y) - \beta(P_0/\log P_0 + Y/\log Y)$, which gives more than $4.3 \cdot 10^{27}$ ■

Theorem 11.26 (quasiperfect numbers with squarefree root). Let $N = m^2$ be a quasiperfect number, $\sigma(N) = 2N + 1$, with m squarefree. Then the largest prime factor of m is greater than $8 \cdot 10^{14}$, and N has more than $6.5 \cdot 10^{12}$ distinct prime factors. This improves the bounds 9,457,308,739 and 406,550,054 of Yamada [33, Thm. 1.3]. [proved, with Computation 11.25 (c) and [32] (cited); the residue condition is formally verified: `qp_squarefree_residue`, `qp_prime_mod8`, `mod8_13_of_prime_factors`]

Proof. A prime factor q of $\sigma(N) = 2m^2 + 1$ is odd, and by Lemma 11.18 with $(K, d) = (2, -1)$, -2 is a square modulo q , so $q \equiv 1$ or $3 \pmod{8}$ (Cattaneo [31]). For $p \mid m$, $\Phi(p)$ divides $\sigma(N)$, so $\Phi(p) \equiv 1$ or $3 \pmod{8}$ and $p \equiv 1$ or $7 \pmod{8}$. The proof of Theorem 11.24 applies with the data of Computation 11.25 (c), with $q = 728 = 8 \cdot 7 \cdot 13$ (the roots of $x^2 + x + 1$ are 2, 4 modulo 7 and 3, 9 modulo 13, and $7 \equiv 7, 13 \equiv 5 \pmod{8}$), which leaves 80 of the 288 classes prime to q , and with the target $\log 2$, since $\sigma(N)/N = 2 + 1/N > 2$. It gives $P_0 = \exp(34.330) > 8 \cdot 10^{14}$ and the stated number of prime factors ■

Remark 11.27 (the size of the gap). The admissible sums $S(X) = \sum_{p \leq X} f(p)$ over admissible primes p are 0.4510718, 0.4540662, 0.4577788, 0.4604252 and 0.4629427 at $X = 10^8, 2 \cdot 10^8, 5 \cdot 10^8, 10^9$ and $2 \cdot 10^9$. The admissible primes are cut out by a sieve of dimension $3/2$ (the primes, and for $\Phi(p)$ the primes $\ell \equiv 1 \pmod{3}$ with $\ell \equiv \pm 3 \pmod{8}$, each removing two classes), so their number up to x is expected to be of order $x/(\log x)^{3/2}$ and $S(X)$ to approach its limit like $(\log X)^{-1/2}$. The increments fit $S(X) = S_\infty - c(\log X)^{-1/2}$: on each of the four intervals, c lies between 0.701 and 0.703 and S_∞ between 0.6145 and 0.6147. Since $S_\infty < \log 2 = 0.6931$, odd almost perfect numbers with squarefree root are not expected to exist. [heuristic] The law $(\log x)^{-1/2}$ also holds far beyond the computed range: among 20,000 consecutive primes after each of $x = 10^6, 10^8, \dots, 10^{18}$, with admissibility decided as in Computation 11.29A, the proportion of admissible primes multiplied by $(\log x)^{1/2}$ is constant within sampling error, with mean $B = 0.346 \pm 0.003$ (Computation 11.29A); $2B = 0.693$ agrees with c within sampling error, and the limit obtained from B is 0.613 ± 0.002 . A proof along these lines needs an upper bound for the admissible primes beyond $8 \cdot 10^9$ within a factor of about 1.5 of their true number; the explicit upper-bound sieve of dimension $3/2$ in [33] has the constant 18.56 in place of about 0.70. With $q = 24$ alone, Theorem 11.24 holds with $2.0 \cdot 10^{24}$ and $8.9 \cdot 10^{21}$. For quasiperfect numbers our count of admissible primes below 2^{29} is 3,285,697, against

3,285,696 in [33, (32)], and the product of $\Phi(p)/p^2$ over them is 1.7501432, in agreement with the value 1.75014319434 of [33, (30)]. If b is not squarefree, a prime with exponent 4 or more in n may contribute up to $\log(p/(p-1))$, for example $\log(3/2) = 0.405$ for $p = 3$, which exceeds the remaining gap $\log 2 - S_0 - T \approx 0.22$; the argument then gives no conclusion.

Theorem 11.28 (exponent families). Let n be an odd almost perfect number and $d \in \{3, 5, 7\}$, and suppose that d divides $e + 1$ for every exponent e with $p^e \parallel n$. Then the largest prime factor of n and the number $\omega(n)$ of its distinct prime factors satisfy: for $d = 3$, the largest prime factor is greater than $8 \cdot 10^{28}$ and $\omega(n) > 2 \cdot 10^{26}$; for $d = 5$, greater than $2 \cdot 10^{21}$ and $\omega(n) > 10^{19}$; for $d = 7$, greater than $3 \cdot 10^{19}$ and $\omega(n) > 2 \cdot 10^{17}$. The case $d = 3$ contains the squarefree roots ($e = 2$) and every n whose exponents are all $\equiv 2 \pmod{6}$. [proved, with Computations 11.25 and 11.29 and [32] (cited); the divisibility and residue conditions are formally verified: `geom_dvd`, `oap_family_dvd`, `oap_family_mod8`, `oap_family3_residue`, `oap_family5_residue`, `oap_family7_residue`]

Proof. Let $p^e \parallel n$ with $e + 1 = dk$. Then $(p^d - 1)/(p - 1) = 1 + p + \dots + p^{d-1}$ divides $1 + p + \dots + p^e = \sigma(p^e)$, hence $\sigma(n)$, so every prime factor of $(p^d - 1)/(p - 1)$ is $\equiv \pm 1 \pmod{8}$ by Lemma 11.18, and so is the number itself. Call such primes d -admissible. For $d = 3$ they are the admissible primes of Lemma 11.23, so $p \equiv 5, 23 \pmod{24}$; for $d = 5$, $p \equiv 3, 7 \pmod{8}$ and $p \not\equiv 1 \pmod{5}$; for $d = 7$, $p \equiv 1, 7 \pmod{8}$. A prime $\ell \equiv \pm 3 \pmod{8}$ divides $(p^d - 1)/(p - 1)$ exactly when p has order d modulo ℓ , or $\ell = d$ and $p \equiv 1 \pmod{\ell}$. The contribution of p to $\log(\sigma(n)/n)$ is $\log(\sigma(p^e)/p^e) < g(p) = \log(p/(p-1)) < 1/p + 1/(p(p-1))$, whatever e is. The argument of Theorem 11.24 therefore applies with g in place of f and with these data: for $d = 3$, the sum of g over the admissible primes up to $2 \cdot 10^9$ is 0.4710684 and over the candidates of Computation 11.25 (b) at most $T + 10^{-12}$, with the 320 classes modulo 5,928; for $d = 5$ and $d = 7$, the sums of Computation 11.29 up to $8 \cdot 10^9$, with the 36 of the 160 classes modulo $440 = 8 \cdot 5 \cdot 11$ that satisfy the conditions above and in which p does not have order 5 modulo 11, and with the 44 of the 112 classes modulo $232 = 8 \cdot 29$ in which $p \equiv 1, 7 \pmod{8}$ and p does not have order 7 modulo 29. The estimate [32, Thm. 1.2] gives $P_0 = \exp(66.617)$, $\exp(49.331)$ and $\exp(44.866)$ for $d = 3, 5, 7$, and the stated numbers of prime factors ■

Computation 11.29. For $d = 5$ and $d = 7$ a segmented sieve over all primes $p \leq 8 \cdot 10^9$ keeps those in the classes modulo 8 given above for which no prime $\ell \leq 10^6$ with $\ell \equiv \pm 3 \pmod{8}$ divides $(p^d - 1)/(p - 1)$. This set contains every d -admissible prime up to $8 \cdot 10^9$. For $d = 5$ it has 43,542,578 elements and the sum of g over it is 0.5175017; for $d = 7$, 74,967,114 elements and 0.4247876 (to seven decimals; increased by 10^{-7} before use). For $d = 3, 5, 7, 9, 11$ the program agrees with direct evaluation of $(p^d - 1)/(p - 1)$ modulo every such $\ell \leq 10^4$ for all primes $p \leq 3 \cdot 10^5$. [computed]

Computation 11.29A (admissible proportions). The program `adm.gp` decides whether a prime p is d -admissible from the prime factors of $(p^d - 1)/(p - 1)$: trial division to 10^6 ; a composite cofactor C with $(2/C) = -1$ has a prime factor $\equiv \pm 3 \pmod{8}$; otherwise C is factored completely. (a) Exact sums of g over the d -admissible primes: for $d = 3$ up to 10^5 and 10^7 (60,007 primes up to 10^7 , the count of Computation 11.25 (a)); for $d = 5$ up to 10^5 and 10^7 (56,155 primes, sum 0.4605016); for $d = 7$ up to 10^5 and 10^6 (10,137 primes, sum 0.2772461). (b) The proportion of d -admissible primes among consecutive primes after x : for $d = 3$ (20,000 primes) at $x = 10^6, 10^8, \dots, 10^{18}$, 0.0939, 0.0810, 0.0717, 0.0669, 0.0597, 0.0563, 0.0542; for $d = 5$ (10,000 primes) at $x = 10^6, 10^8, \dots, 10^{14}$, 0.0907, 0.0762, 0.0674, 0.0590, 0.0597; for $d = 7$ (10,000 primes) at $x = 10^6, 10^7, \dots, 10^{10}$, 0.1264, 0.1164, 0.1097, 0.1053, 0.0897. [computed]

Remark 11.29B (the exponent families are not expected to exist). For $d \in \{3, 5, 7\}$ the d -admissible primes are cut out by a sieve of dimension $1/2$ on the primes: a prime $\ell \equiv 1 \pmod{d}$ with $\ell \equiv \pm 3 \pmod{8}$ removes the $d - 1$ residue classes of order d , and such ℓ form a proportion $1/(2(d-1))$ of the primes. Their proportion among the primes near x should therefore be $B_d/(\log x)^{1/2}$. Computation 11.29A (b) confirms this: proportion $\cdot (\log x)^{1/2}$ is constant within sampling error ($\chi^2 = 1.45, 3.62$ and 7.75 on 6, 4 and 4 degrees of freedom), with means $B_3 = 0.346 \pm 0.003$, $B_5 = 0.328 \pm 0.005$ and $B_7 = 0.464 \pm 0.006$, and the

model reproduces every exact increment of Computation 11.29A (a) and Computation 11.25 (a) within 2%. The sum of g over the d -admissible primes greater than X is then $2B_d/(\log X)^{1/2}$ up to terms of lower order, and the sums of g over all d -admissible primes are expected to be 0.621 ($d = 3$), 0.624 ($d = 5$) and 0.527 ($d = 7$), each with a statistical error below 0.004, all below $\log 2 = 0.693$. The supersets of Computation 11.29 have larger sums because they are sieved only by primes $\ell \leq 10^6$. Since every prime p of n contributes less than $g(p)$, odd almost perfect numbers in which one of 3, 5, 7 divides $e + 1$ for every exponent e are not expected to exist; this includes every n whose exponents are all $\equiv 2 \pmod{6}$, all $\equiv 4 \pmod{10}$ or all $\equiv 6 \pmod{14}$. [heuristic] The argument needs a common d : when the exponents are of different types, each prime is restricted only by the condition for its own exponent, and the union of these sets of primes is not controlled by the sieve.

Lemma 11.29C (an even number of bad primes). Call a prime ℓ bad if $\ell \equiv \pm 3 \pmod{8}$. Let $p \equiv 5$ or $23 \pmod{24}$ be a prime. Then the number of bad prime factors of $\Phi(p)$, counted with multiplicity, is even. Consequently p is admissible if and only if $\Phi(p)$ has no bad prime factor $\ell \leq p$. More generally, if $\sigma(p^{d-1}) \equiv \pm 1 \pmod{8}$, then $\sigma(p^{d-1})$ has a bad prime factor if and only if it has one at most $\sigma(p^{d-1})^{1/2}$. [proved]

Proof. Since p is odd, $\Phi(p) \equiv p + 2 \pmod{8}$, so $\Phi(p) \equiv 7$ or $1 \pmod{8}$ for $p \equiv 5$ or $7 \pmod{8}$, and the Jacobi symbol $(2/\Phi(p))$ is 1. It is the product of $(2/\ell)$ over the prime factors ℓ of $\Phi(p)$ with multiplicity, and $(2/\ell) = -1$ exactly for the bad ℓ , so their number is even; 3 does not divide $\Phi(p)$ because $p \equiv 2 \pmod{3}$. If $\Phi(p)$ has a bad prime factor, it therefore has two, counted with multiplicity, and the smaller is at most $\Phi(p)^{1/2} < p + 1$. The general statement is the same argument ■ For the 6,520 primes $p \equiv 5, 23 \pmod{24}$ below $3 \cdot 10^5$, the 2,647 admissible ones are exactly those for which $\Phi(p)$ has no bad prime factor $\ell \leq p$, and no $\Phi(p)$ has an odd number of bad prime factors [computed].

Remark 11.29D (the level of distribution that the argument needs). By Lemma 11.29C the admissible primes are the primes $p \equiv 5, 23 \pmod{24}$ for which $\Phi(p)$ avoids the bad residue classes modulo every bad $\ell \leq p$: a sieve of dimension $1/2$ on the sequence of primes, with sifting range $z = p$ instead of $\Phi(p)^{1/2}$. Among the primes $p \equiv 5, 23 \pmod{24}$ below $2 \cdot 10^6$, those for which $\Phi(p)$ has no bad prime factor up to $z = x^\theta$ number 1.839, 1.313, 1.082 and 1.000 times the admissible ones for $\theta = 1/4, 1/2, 3/4$ and 1 [computed]. If the primes have level of distribution θ in arithmetic progressions, an upper-bound sieve of dimension $1/2$ with level x^θ and sifting range $z = x$ ($s = \theta$) gives, by the function $F(s) = 2e^{\gamma/2}(\pi s)^{-1/2}$ of the half-dimensional sieve for $0 < s \leq 2$ (Iwaniec [41]), $F(\theta)/F(2) = (2/\theta)^{1/2}$ times the expected number of admissible primes, since $F(2)$ describes the complete sifting of the numbers $\Phi(p)$ of size about x^2 . The Bombieri–Vinogradov theorem [39] gives $\theta = 1/2$ and the factor 2, in agreement with Remark 11.33G; the Elliott–Halberstam conjecture [40] would give $\theta = 1$ and the factor $2^{1/2} \approx 1.41$. With $S(2 \cdot 10^9) = 0.4629$ (Remark 11.27) and the fitted limit 0.6146, the argument of Remark 11.27 closes with a factor f as soon as $S(2 \cdot 10^9) + f \cdot (0.6146 - 0.4629) < \log 2$, that is $f < 1.52$, which corresponds to $\theta > 0.87$; an exact computation up to 10^{18} , where the fit gives $S \approx 0.506$, would allow $f < 1.72$, that is $\theta > 0.67$. The best unconditional levels known are $1/2$ in general and, for special weights and fixed residue classes, about $3/5$, which give the factors 2 and about 1.83. [heuristic] So, under the Elliott–Halberstam conjecture with explicit error terms, the abundancy argument would exclude odd almost perfect numbers with squarefree root; unconditionally it is blocked by the level of distribution of the primes, not by the computation.

Remark 11.30 (other families and equal exponents). For $d = 11$ and $d = 13$ the argument gives no bound: $\sigma(5^{10}) = 12,207,031$ is a prime $\equiv 7 \pmod{8}$, $\sigma(3^{12}) = 797,161$ and $\sigma(7^{12}) = 16,148,168,401$ are primes $\equiv 1 \pmod{8}$, and the sums of $\log(\sigma(p^{d-1})/p^{d-1})$ over the primes $p < 400$ for which no factor $\equiv \pm 3 \pmod{8}$ of $(p^d - 1)/(p - 1)$ was found are 0.417 for $d = 11$ and 0.675 for $d = 13$. If all exponents of n are equal to $2a$, Theorem 11.28 applies when one of 3, 5, 7 divides $2a + 1$. The smallest common exponent not covered by Theorem 11.28 is $2a = 10$; for $2a = 16$ the abundancy alone gives no contradiction, since $\sigma(3^{16}) = 1,871 \cdot 34,511$, $\sigma(5^{16}) = 409 \cdot 466,344,409$, $\sigma(7^{16}) = 14,009 \cdot 2,767,631,689$ and $\sigma(11^{16}) = 50,544,702,849,929,377$ (a prime) have all their prime factors $\equiv \pm 1 \pmod{8}$, and $\prod_{p \in \{3, 5, 7, 11\}} \sigma(p^{16})/p^{16} = 2.406 > 2$. Such exponents require a search as in Section 11.6. [computed]

Proposition 11.31 (descent). Let $b > 1$ be odd, take its distinct prime factors $t_1, \dots, t_\omega$ in any order, and let T_i be the power of t_i that divides b^2 exactly. Put $m_0 = 1$ and let m_i be the part of b formed by $t_1, \dots, t_i$, so that $m_i^2 = m_{i-1}^2 T_i$; put $d_i = 2m_i^2 - \sigma(m_i^2)$, $D_i = 2m_{i-1}^2 - d_{i-1}t_i$ and $s_i = (T_i - 1)/(t_i - 1)$. Then (i) $d_{i-1} - d_i = D_i s_i$ for every i , so $d_0 = 1$ and $\sum D_i s_i = 1 - d_\omega$; for an odd almost perfect number b^2 , $\sum D_i s_i = 0$, with $D_1 = 2 - t_1 < 0$. (ii) If b^2 is an odd almost perfect number and $t \parallel b$, then $m = b/t$ and $D = 2m^2 - d_{mt}$, where $d_m = 2m^2 - \sigma(m^2)$, satisfy $D(t + 1) = d_m - 1$, $D \cdot \Phi(t) = 2m^2 - t$ and $D \geq 1$; moreover $D \equiv 3 \pmod{8}$, and $D \equiv 0 \pmod{3}$ if $3 \nmid b$. In particular $D \equiv 3 \pmod{24}$ when b is squarefree, since then $3 \nmid b$ by Lemma 11.23. [proved; the identities and the congruences are formally verified: descent_step, last_prime_quotient, last_prime_D_mod8, last_prime_D_mod3, oap_squarefree_residue]

Proof. (i) $\sigma(T_i) = T_i + s_i$ and $(t_i - 1)s_i = T_i - 1$, so $d_i = 2m_{i-1}^2 T_i - \sigma(m_{i-1}^2)(T_i + s_i)$, and the identity follows by expanding with $\sigma(m_{i-1}^2) = 2m_{i-1}^2 - d_{i-1}$. Summing gives the telescoping sum, and $d_0 = 2 - 1 = 1$. (ii) The equation $\sigma(m^2)\Phi(t) = 2m^2 t^2 - 1$ gives both identities. If $D \leq 0$, then $2m^2 = D\Phi(t) + t \leq t - \Phi(t) < 0$, and $D = 0$ would make $t = 2m^2$ even; so $D \geq 1$. By Lemma 11.23, $t \equiv 5$ or $7 \pmod{8}$ and $t \equiv 2 \pmod{3}$; since m is odd, $2m^2 \equiv 2 \pmod{8}$, and if $3 \nmid m$ then $2m^2 \equiv 2 \pmod{3}$. Reducing $D \cdot \Phi(t) = 2m^2 - t$ modulo 8 and modulo 3 gives the congruences ■

Remark 11.32 (near-solutions). Among the odd $b \leq 10^8$, only $b = 3003 = 3 \cdot 7 \cdot 11 \cdot 13$ has $1 \leq 2b^2 - \sigma(b^2) \leq b$; its defect is $819 = 3^2 \cdot 7 \cdot 13$. There are 1,547 odd $b \leq 10^8$ with $1 \leq 2b^2 - \sigma(b^2) \leq b^{3/2}$, and 1,098 of them are $3003 \cdot t$ with t prime. The reason is the identity $2m^2 x^2 - \sigma(m^2)\Phi(x) = d_m$ at $x = 2m^2/d_m$: when d_m divides $2m^2$, the integer $x = 2m^2/d_m$ keeps the defect unchanged, and primes t close to x keep it small. For $m = 3003$, $x = 22,022 = 2 \cdot 7 \cdot 11^2 \cdot 13$, which is not prime. For $m = 1$ and $d = 1$ this integer step is $x = 2$ and gives the chain 2, 8, 512, ..., of powers of 2 (Proposition 10.1). By Proposition 11.31 (ii), at a prime $t \parallel b$ of an odd almost perfect number the part $m = b/t$ has defect $d_m = D(t + 1) + 1 \approx (2D)^{1/2}m$, that is, m is a near-solution with defect of the order of m . Each step of the descent ends at the condition that a discriminant be a square, for which no local obstruction is known (compare Remark 9.8A for even levels); an argument that excludes these conditions for every ω at once is what Section 14 calls the missing ingredient. [computed]

Remark 11.33 (spoof factorisations). Following [34], call a list of odd integers $x \geq 3$ (the bases), not necessarily prime or distinct, each with an exponent $2a$, an odd spoof almost perfect factorisation of $n = \prod x^{2a}$ if the product of the numbers $\tilde{\sigma}(x^{2a}) = 1 + x + \dots + x^{2a}$ over the list equals $2n - 1$. The proof of Lemma 11.18 uses only this equation, so every prime factor of every $\tilde{\sigma}(x^{2a})$ is $\equiv \pm 1 \pmod{8}$. When all exponents are 2, every base is moreover $\equiv 5$ or $23 \pmod{24}$: $\Phi(x) \equiv x + 2 \pmod{8}$ gives $x \equiv 5$ or $7 \pmod{8}$; a base $x \equiv 1 \pmod{3}$ would give $3 \mid \Phi(x)$; and a base $x \equiv 0 \pmod{3}$ would give $2n - 1 \equiv 2 \pmod{3}$, whereas every $\Phi(x)$ is $\equiv 0$ or $1 \pmod{3}$. An exhaustive search over the bases in nondecreasing order, with the bounds of Lemma 11.15 and the last base computed from a quadratic equation, finds no odd spoof almost perfect factorisation with all exponents equal to 2 and at most 7 bases, none with 8 bases whose first seven bases are at most 10^7 (12 branches need a larger base), none with 9 bases whose first eight bases are at most 10^7 (4,093,860 branches need a larger base; of the 693,239,045,103 candidates y for the eighth base, 677,371,739 give a discriminant $G^2 + 4d(G + 1)$ of the quadratic $dt^2 - Gt - (G + 1) = 0$ for the last base t , where $G = F\Phi(y)$, $d = 2My^2 - G$ and F, M are the products of $\Phi(x)$ and x^2 over the first seven bases, that is a square modulo ten primes near 2^{16} , and these are decided exactly), and none with at most 7 bases and exponents up to 4, or up to 6. Allowing bases of either sign, there is none with exponent 2 and two, three or four bases whose bases other than the last satisfy $|x| \leq 10^5$, $|x| \leq 2,000$ or $|x| \leq 60$, respectively; Computation 11.33F removes every bound on the bases for at most eight bases. With even bases admitted, the same search returns exactly the chain 2, 8, 512, 2^{27} . For perfect numbers the situation is different: Descartes's odd spoof factorisation $3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 22,021$ has five bases, and by [34] any proof that odd perfect numbers do not exist must use the primality of the bases. Whether the same holds for odd almost perfect numbers is open. [computed]

Remark 11.33A (the last two bases). Let all exponents be 2, let $F = \prod \Phi(x)$ and $M = \prod x^2$ over all bases but the last two, y and t , and put $u = yt$ and $W = (y + 2)(t + 2) - 3$. Then $FW^2 - ((8M - 3F)u^2 + 6Fu - 3F - 4) = -4(2Mu^2 - 1 - F\Phi(y)\Phi(t))$ identically [proved: polynomial identity; checked at 50,000 random points]. So the last two bases of a solution, whether the bases are prime or not, give an integral point (u, W) on the conic $FW^2 = (8M - 3F)u^2 + 6Fu - 3F - 4$, which in $X = (8M - 3F)u + 3F$ is the Pell-type equation $X^2 - F(8M - 3F)W^2 = 4(6FM + 8M - 3F)$; and y, t are integers only if $s^2 - 4u$ is a square, where $s = (W - u - 1)/2 = y + t$, since $s^2 - 4u = (t - y)^2$. The two conditions define a curve of genus one: it is the curve $L(yz)^2 - K\Phi(y)\Phi(z) = 1$ of Section 10 with $K = F$ and $L = 2M$. For the chain 2, 8, 512, 2^{27} of even bases the point lies on the conic with $F = 511$ and $M = 256$. Since the identity does not use primality, an argument that excludes the integral points of these curves for every admissible list of bases would also exclude the odd spoof factorisations with exponent 2, and the searches of Remark 11.33 find none. Neither local conditions (Section 11.4) nor the approximation of $\sqrt{((8M - 3F)/F)}$ by W/u , whose error is only of order $1/u$, give an obstruction; what remains is the integral points of a family of curves of genus one, as in the first route of Section 14.1.

Remark 11.33B (where the curve of the last two bases is locally insoluble). In the notation of Remark 11.33A let the bases be odd and admissible with $\gcd(F, M) = 1$, and put $Q = F(8M - 3F)$ and $N_1 = 6FM + 8M - 3F$, so that the Pell form reads $X^2 - QW^2 = 4N_1$. Then $Q \equiv 5 \pmod{8}$, N_1 is odd and $\gcd(N_1, Q) = 1$, and the Hilbert symbol $(4N_1, Q)_v$ equals 1 at $v = \infty$ ($N_1 > 0$), at $v = 2$ ($Q \equiv 1 \pmod{4}$), at every prime $p \mid F$ (there $N_1 \equiv 8M \pmod{p}$ and $p \equiv \pm 1 \pmod{8}$) and at every prime $p \mid 8M - 3F$ (there $8M \equiv 3F$, so $N_1 \equiv 6FM \equiv (3F/2)^2$); at a prime $p \mid N_1$ it equals $(Q/p)^e$, where $p^e \parallel N_1$. Hence the conic, and with it the curve of the last two bases, has no rational point as soon as $(Q/p) = -1$ for some prime p that divides N_1 to an odd power [proved]. For the single base 5, $N_1 = 67 \cdot 71$ and $(Q/67) = (Q/71) = -1$, and the curve has no point modulo 71 or modulo 67^2 . Among the lists of odd admissible bases with $\gcd(F, M) = 1$, bases repeated or not, no prime of N_1 obstructs, so that the conic has rational points, for 38 of the 95 single bases up to 2,000, for 71 of the 241 pairs up to 500 and for 46 of the 156 triples up to 150 [computed]; for most lists the curve of the last two bases is locally insoluble. For the twelve admissible single bases up to 200 the Pell form also yields the integral points: for eight of them the curve has no rational point, for 119 the conic has rational points but the class group, of order 112, leaves no integral point on the conic, and for 101, 167 and 173 the conic has integral points of which none gives integers y, t with $|yt| \leq 10^{100}$ [computed; the class-group computations assume the generalised Riemann hypothesis]; for the 78 pairs of admissible bases up to 200 the same computation finds no integral point with $|yt| \leq 10^{100}$ for 67 of the 78 pairs, and for the other 11 it does not finish within 20 minutes, in agreement with Remark 11.33. Since the equation is symmetric in the bases, a solution with ω bases passes this test for each of the $\omega(\omega - 1)/2$ choices of the last two bases. If the tests were independent this would be very unlikely already for small ω ; but they are consequences of the equation, a solution would pass all of them, and they do not give a proof. They explain why the searches of Remark 11.33 find nothing, and they can prune such searches.

Remark 11.33C (the last step: its defect, and coverings of the Pell orbits). (i) Put $G = F\Phi(y)$ and $d = 2My^2 - G$, so that t is the positive root of $dt^2 - Gt - (G + 1) = 0$. If $d = 1$ the quadratic is $(t - G - 1)(t + 1) = 0$, so $t = G + 1 = 2My^2$ is even: this is the chain step of Remark 11.34. Hence, for every choice of the last two bases of a solution with odd bases, $d \geq 2$, and since $\sqrt{(G^2 + 4d(G + 1))} \leq G + 2d$, $t \leq G/d + 1 \leq F\Phi(y)/2 + 1$ [proved]. (ii) The integral points of the conic of Remark 11.33A form finitely many orbits $\pm a_0 \varepsilon^n$, $n \in \mathbb{Z}$, with ε a unit of norm 1, and modulo a prime ℓ each orbit is periodic in n . A class of n modulo the period is excluded when $\ell \mid 8M - 3F$ and $X \not\equiv 3F \pmod{\ell}$, so that u is not an integer, or when $s^2 - 4u$ is a non-residue modulo ℓ . For all 28 admissible single bases up to 600 the last two bases cannot be completed: 21 have no orbit (Remark 11.33B, or the class group), and each of the 60 orbits of the other 7 bases is covered, every n being excluded by some prime $\ell \leq 3,000$ whose period divides 55,440; so these curves have no admissible integral point of any size. For 101 and 551 the admissible residues of y and t modulo $192 = 3 \cdot 2^6$ alone exclude every orbit. For the 78 pairs of admissible bases up to 200, 53 have no orbit, the orbits of 10 are covered, and for 15 the computation of the class group does not finish within 15

minutes [computed; the lists of orbits assume the generalised Riemann hypothesis; the coverings of the single bases are checked independently]. The covering primes vary from orbit to orbit. For many orbits a single prime suffices, such as 7, 11, 13, 17, 19 or 23 (for 7, 17 and 23 often with $\varepsilon \equiv 1$ modulo the prime, so that the orbit is constant there and $s^2 - 4u$ is a fixed non-residue); others need two primes, often 3 together with 5 or 11 (3 is inert in the field, since the bases are $\equiv 2 \pmod{3}$, so its period divides 4); some need four or more. No fixed set of primes covers every orbit; an argument that produced a covering for every list of bases would settle the last step, and this is the missing uniform statement.

Proposition 11.33D (almost every single base is obstructed locally). For an integer x put $N_1(x) = 6\Phi(x)x^2 + 8x^2 - 3\Phi(x) = 6x^4 + 6x^3 + 11x^2 - 3x - 3$ and $Q(x) = \Phi(x)(5x^2 - 3x - 3)$, the numbers N_1 and Q of Remark 11.33B for the list consisting of the single base x . The number of integers $1 \leq x \leq X$ for which the curve of the last two bases with this list has a rational point is $O(X \cdot (\log \log X / \log X)^{1/2})$; in particular it has no rational point for all x outside a set of density zero. [proved, using the Chebotarev density theorem and Selberg's upper-bound sieve [37]]

Proof. N_1 is irreducible with Galois group S_4 , $\text{Res}(N_1, Q) = 2^{14} \cdot 3^4$, and for a root r of N_1 the polynomial $T^2 - Q(r)$ is irreducible over $K = \mathbb{Q}(r)$ [computed], so $L = K(\sqrt{Q(r)})$ is a quadratic extension of K . For a prime $p \geq 5$ not dividing the discriminant of N_1 , call a root r of N_1 modulo p bad if $(Q(r)/p) = -1$, and let $\rho(p) \leq 4$ be the number of bad roots. By the Chebotarev density theorem in the Galois closure of L , half of the primes of K of degree one are inert in L , so $\sum_{p \leq z} \rho(p)/p = (1/2) \cdot \log \log z + O(1)$. If $x \equiv r \pmod{p}$ for a bad root r , then $p \mid N_1(x)$, $p \nmid Q(x)$ and $(Q(x)/p) = -1$, so by Remark 11.33B the curve has no rational point unless $p^2 \mid N_1(x)$. Put $w = \log X$ and $z = X^{1/3}$. The $x \leq X$ with $p^2 \mid N_1(x)$ for some prime p with $w < p \leq z$ number at most $\sum_{w < p \leq z} 4(X/p^2 + 1) \ll X/w + z$. Every other $x \leq X$ whose curve has a rational point avoids the bad classes modulo every prime p with $w < p \leq z$; this is a sieve of dimension 1/2 with remainders $O(\rho(d))$, and Selberg's upper-bound sieve with level z^2 bounds these x by $\ll X \prod_{w < p \leq z} (1 - \rho(p)/p) \ll X(\log w / \log z)^{1/2}$ ■ Among the admissible x the proportion that passes the test of Remark 11.33B is 0.400 for $x \leq 2,000$ and 0.337, 0.321, 0.279 and 0.247 in the windows of length 20,000 starting at 10^4 , 10^5 , 10^6 and 10^7 , and $\sum_{p \leq P} \rho(p)/p$ is 0.636, 0.769 and 0.878 at $P = 10^3$, 10^4 , 10^5 , increasing by about half the increase of $\log \log P$, in agreement with the dimension 1/2 [computed].

Remark 11.33E (Brauer–Manin and Skolem readings). (i) Lemma 11.18 and Proposition 4.5 are Brauer–Manin conditions. On the surface (E3) with $N = 2M^2$ (k odd), the quaternion algebra $(2, \Phi(x))$ is unramified, since on the curve $\Phi(x) = 0$ the equation gives $2(Mxyz)^2 = 1$, so 2 is a square there. At an integral point its local invariant vanishes at ∞ and at every odd prime: an odd prime dividing $\Phi(x)$ divides $q\Phi(x)\Phi(y)\Phi(z) = 2(Mxyz)^2 - 1$, so 2 is a square modulo it. The vanishing of the invariant at 2 is $\Phi(x) \equiv \pm 1 \pmod{8}$ [proved]. The class $(-3, M \cdot xyz - 1)$ of Remark 10.25C plays the same role for even k . (ii) Remark 11.33B evaluates, fibre by fibre, the Hilbert symbol $(4N_1, Q)$ of a single fibre; some fibres pass this test (for example $x = 101$ at $N = 2$), so conditions that depend only on the fibre cannot by themselves exclude points of the whole surface. (iii) The coverings of Remark 11.33C are instances of the Hasse-type principle for exponential Diophantine equations in the form of Bertók and Hajdu [35], who choose moduli whose periods divide a common smooth number, as in Remark 11.33C, and prove that the principle holds for almost all right-hand sides. Harari and Voloch [26] relate such a principle to the Brauer–Manin obstruction for integral points on affine curves, and the surfaces (E3), of tridegree $(2, 2, 2)$ in $(\mathbb{P}^1)^3$, are Wehler K3 surfaces, for which families with an integral Brauer–Manin obstruction have been constructed by Dao [36]. Proposition 11.33D is a statement of the same “almost all” kind for the last step; a statement for every list of bases would settle the last step. Its lists, like the single bases of Remarks 11.33B and 11.33C, have three bases in all, and three bases are already excluded by the abundance (Computation 11.33F); these results describe the family of curves, while for a solution the list of the other bases has at least two elements, so that a version of Proposition 11.33D for lists of every length is what is needed.

Computation 11.33F (bases of either sign). There is no list of at most eight odd integers x_i with $|x_i| \geq 3$, of either sign and not necessarily prime or distinct, such that $\prod \Phi(x_i) = 2\prod x_i^2 - 1$; no bound is placed on any base. In particular there is no odd spoof almost perfect factorisation with all exponents equal to 2 and eight bases, which removes the bound 10^7 of Remark 11.33. [computed] The congruences of Remark 11.33 use only the equation and hold for bases of either sign, so every base is $\equiv 5$ or $23 \pmod{24}$ and $\Phi(x)$ has no prime factor $\equiv \pm 3 \pmod{8}$. With $g(x) = \Phi(x)/x^2$, the bases are ordered by $|x|$; if r is the value of $\prod g$ over a prefix and the j remaining bases satisfy $|x| \geq a$, the final value $2 - 1/\prod x_i^2$ lies between $r \cdot g(-a)^j$ and $r \cdot g(a)^j$, since for $|x| \geq 2$ the value $g(x)$ decreases as $|x|$ grows when $x > 0$ and increases as $|x|$ grows when $x < 0$. Both ends are monotone in a , so the search stops once $r \cdot g(a)^j < 2 - 1/(M \cdot a^{2j})$, M being the product of x^2 over the prefix, or $r \cdot g(-a)^j \geq 2$, and the last base is a root of the quadratic $dt^2 - Gt - (G + 1) = 0$ of Remark 11.33 with d of either sign, decided exactly. A base $x < 0$ has $g(x) < 1$, so if a solution has a negative base, its positive bases have $\prod g > 2$; and since every admissible x satisfies $x = 5$ or $|x| \geq 19$, $g(x) \leq g(5) = 31/25$, so at most three bases are excluded by the abundancy alone: $(31/25)^3 = 1.9066 < 2$. For at most seven bases the search with every base other than the last bounded by 10^6 ends with no prefix needing a larger base. For eight bases the search with the bound $6 \cdot 10^7$ (142,520,023 nodes) leaves exactly two prefixes of six bases, 5, 5, 5, 23, 287, -21313 and 5, 5, 5, 23, 293, 40463, whose last two bases would have to exceed $6 \cdot 10^7$; for each of them a prime p (4,219 and 1,175,969 respectively) divides N_1 exactly once, does not divide Q , and Q is a non-residue modulo p , so by Remark 11.33B the conic of the last two bases has no rational point. A second program treats the last two bases together: for each prefix of six bases it applies this test with the primes up to 10^4 and otherwise runs through the whole window of the second-to-last base y , the admissible y with $|y| \leq 10^6$ from a sieve and every $y \equiv 5, 23 \pmod{24}$ beyond, keeping y only if the discriminant of the quadratic for the last base is a square modulo ten primes near 2^{16} . With the bound 10^6 it closes all 19,190 prefixes of six bases (1,203 by the conic, the others by their windows, which contain $1.4 \cdot 10^8$ values of y beyond 10^6), with no prefix left and no solution. Both programs return exactly the chain 2, 8, 512, 2^{27} when even bases are admitted, and a search without any filter over all integers $2 \leq |x| \leq 2,000$ for two bases and $2 \leq |x| \leq 60$ for three bases finds only 2, 8 and 2, 8, 512. Whether some odd integer solution with $|x_i| \geq 3$ exists for more bases is open; if none exists, a proof of the case of exponent 2 could avoid both the primality and the positivity of the bases.

Remark 11.33G (nine bases, repeated bases and the admissible sum). For nine bases of either sign the second program finds no solution when the seven bases of smallest absolute value satisfy $|x| \leq 3 \cdot 10^4$, the last two being unbounded (5,193,546 prefixes of seven bases, and $6.8 \cdot 10^{10}$ values of the eighth base beyond $3 \cdot 10^4$); 3,008 prefixes of five or six bases would need a seventh base beyond $3 \cdot 10^4$, against 1,996 with the bound 10^4 , so this search does not close. [computed] All 3,008 prefixes begin with 5, 5, 5, 23, for which $\prod g = 1.993125$, and so repeat a base. Without repetitions such prefixes do not occur: six distinct bases have $\prod g \leq 1.3721$, the value for the six smallest admissible bases 5, 23, 53, 71, 77, 95, and $\prod g$ over all 3,651 admissible $x \leq 10^5$ is 1.8404 and over the 1,013 admissible primes $p \leq 10^5$ it is 1.5037 [computed]. For odd almost perfect numbers the bases are distinct primes, and the corresponding quantity is the admissible sum of Remark 11.27, expected to converge to $S_\infty \approx 0.6146 < \log 2$. Remark 11.29B asks for an upper bound for the admissible primes beyond $8 \cdot 10^9$ within a factor of about 1.5 of their true number. For the primes themselves, upper bounds of Brun–Titchmarsh type have the factor 2 in place of 1 (Montgomery and Vaughan [38]), and sieve methods alone do not give a smaller factor (the parity phenomenon, [37]); Lemma 11.29C and Remark 11.29D express the requirement as a level of distribution. With the factor 2, the fit $S(X) = S_\infty - 0.70(\log X)^{-1/2}$ of Remark 11.27 would require the admissible sum to be computed up to X with $(\log X)^{1/2} \geq 0.70/(\log 2 - S_\infty) \approx 8.9$, that is $X \approx 3 \cdot 10^{34}$. [heuristic] The obstruction met by the searches with repeated bases and the one met by the admissible sum are therefore different, and for odd almost perfect numbers with squarefree root it is the second that matters.

Remark 11.34 (Descartes's number and the chain step). If $d = 2m^2 - \sigma(m^2)$ divides $2m^2$ and $x = 2m^2/d$, then $\sigma(m^2) \cdot x = 2m^2(x - 1)$. So $m^2 \cdot (x - 1)$, with $x - 1$ treated as a prime to the first power, is a spoof

perfect factorisation, while m^2x^2 has the same defect d as m (Remark 11.32). For $m = 3003$ this gives $x = 22,022$ and Descartes's spoof $3^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 22,021$: $\sigma(3003^2) \cdot 22,022 = 2 \cdot 3003^2 \cdot 22,021 = 397,171,152,378$. With $d = 1$ it is Euclid's construction: if n is almost perfect and $2n - 1$ is prime, then $n(2n - 1)$ is perfect, since $\sigma(n(2n - 1)) = (2n - 1) \cdot 2n$. For $n = 2^{k-1}$ this gives the even perfect numbers $2^{k-1}(2^k - 1)$; an odd almost perfect number n with $2n - 1$ prime would give an odd perfect number. [proved]

Remark 11.35 (near-solutions at other levels). For $f_N(b) = N \cdot b^2 - (N - 1)\sigma(b^2)$ and odd $b \leq 3 \cdot 10^7$, the only b with $1 \leq f_N(b) \leq b$ are $7055 = 5 \cdot 17 \cdot 83$ for $N = 4$ ($f = 5,977$), $247 = 13 \cdot 19$ for $N = 8$ ($f = 11$) together with four numbers $247 \cdot t$ with t prime near $8 \cdot 247^2/11 = 44,370.2$, and none for $N = 16$ and $N = 32$. The computation of Proposition 11.31 (ii) at level N gives $N \cdot m^2 = D \cdot \Phi(t) + t$ and $f_N(m) = D(t + 1) + 1$ at a prime $t \parallel b$ of a counterexample, so $f_N(m) \approx (ND)^{1/2}m$: a near-solution with defect much smaller than m cannot be the part $m = b/t$. For $m = 247$ and $N = 8$, $D(t + 1) = 10$ forces $t + 1 \mid 10$, so $t \in \{1, 4, 9\}$, and none of these is prime. The weaker condition $n \mid \sigma(n) + 1$ holds for $n \leq 2 \cdot 10^8$ only for the powers of 2. [computed]

12. Computations

All computations use exact integer arithmetic for every accept/reject decision (GMP, 128-bit integers or Python integers); floating point is used only to set enumeration windows, always enlarged by a margin. None of them is used in a formally verified proof; they delimit where counterexamples are excluded and support the conjectures. The source of every program and its logs are contained in the supplementary archive deposited with this report at <https://doi.org/10.5281/zenodo.23674490>, together with the Lean development.

12.1 Summary

Computation	Range	Result
Three primes, all exponents (Theorem 7.8)	every $k \leq 16$	no counterexample
Three primes, squarefree	every $k \leq 20$ ($k = 20$: $6.56 \cdot 10^{10}$ prime pairs)	no counterexample
Uniform sieve (Section 9)	every k ; $D_s \leq 500,000$	no counterexample (Theorem 9.6)
Integer equation (E3), any N	$N \leq 1,000$ and $N = 2^k$, $k \leq 15$	only the trivial chain
Four primes $p \cdot r \cdot s \cdot t^y$	every $k \leq 10$	no counterexample
Any exponents, three to five primes (Computation 11.8B)	$\omega = 3$: every $k \leq 15$; $\omega = 4$: every $k \leq 7$; $\omega = 5$: $k \leq 2$	no counterexample
A059046 sieve	$m \leq 2 \cdot 10^{10}$	2,741 non-prime-power terms, all squarefree, odd N
Two primes, pattern (2, 1), odd N	$\delta \leq 3,000$	3,019 integer points, none with both primes
Genus of $C_{N,D}$ (Proposition 11.10)	$k \leq 300$	certified
Odd squares, all quotients (Computation 11.6)	$3 \leq b \leq 10^{10}$	$s(b^2) \mid b^2 - 1$ only for prime powers
Two-variable deficit equation (Remark 10.11)	$L < 4,000$	2,158 solutions, 1,761 in the renormalisation family
Odd almost perfect numbers, all exponents (Computation 11.16)	$\omega(b) \leq 6$	no solution (Theorem 11.11)
Odd almost perfect numbers, all exponents (Computation 11.20)	$\omega(b) = 7$, 577 states	no solution (Theorem 11.19)
Odd almost perfect numbers, squarefree root (Computation 11.25)	admissible primes $p \leq 2 \cdot 10^9$; sieve on $(2 \cdot 10^9, 8 \cdot 10^9]$	largest prime $> 1.6 \cdot 10^{30}$, $\omega > 4.3 \cdot 10^{27}$ (Theorem 11.24)
Quasiperfect numbers, squarefree root (Computation 11.25)	the same ranges	largest prime $> 8 \cdot 10^{14}$, $\omega > 6.5 \cdot 10^{12}$

11.25 (c)		(Theorem 11.26)
Exponent families $d \mid e + 1$, $d = 3, 5, 7$ (Computation 11.29)	d-admissible primes up to $8 \cdot 10^9$ (supersets)	largest prime $> 8 \cdot 10^{28}, 2 \cdot 10^{21}, 3 \cdot 10^{19}$ (Theorem 11.28)
Admissible proportions (Computation 11.29A)	samples of consecutive primes to 10^{18} ($d = 3$), 10^{14} ($d = 5$) and 10^{10} ($d = 7$); exact sums to 10^7	proportion $B_d(\log x)^{-1/2}$; limits 0.613 (squarefree root), 0.621, 0.624, 0.527, all below $\log 2$ (Remarks 11.27, 11.29B)
Near-solutions (Remark 11.32)	odd $b \leq 10^8$	only $b = 3003$ with $1 \leq 2b^2 - \sigma(b^2) \leq b$; 1,547 with defect $\leq b^{3/2}$
Odd spoof almost perfect factorisations (Remark 11.33)	exponents 2: at most 7 bases, 8 bases with the first seven $\leq 10^7$, and 9 bases with the first eight $\leq 10^7$; exponents up to 6: at most 7 bases	none (the even-base search returns the chain 2, 8, 512, 2^{27})
Odd integer solutions of either sign, $x \geq 3$ (Computation 11.33F, Remark 11.33G)	at most 8 bases, no bound; 9 bases with the seven of smallest $ x \leq 3 \cdot 10^4$	none (2 prefixes for 8 bases closed by the conic; 3,008 prefixes for 9 bases left, all with a repeated base)
Near-solutions at levels $N = 4, \dots, 32$ (Remark 11.35)	odd $b \leq 3 \cdot 10^7$	7055 ($N = 4$); 247 and four multiples ($N = 8$); none for $N = 16, 32$

12.2 Dependency table: on what each elimination rests

Every elimination performed by a program rests on a condition proved to be necessary for every solution. The table lists, for each program, the conditions it uses to discard candidates and their status.

Program	Conditions used to discard candidates	Status of each condition
Three primes, all exponents (hx)	window for p and r from Lemma 3.5 (i)–(ii) with $s > r$; regimes (Theorem 7.2); $\alpha = 1$ in (P) (Theorem 7.3); $Q < 0$ and the bound on s in (P) (Theorem 7.7); $s \leq (N \cdot L_2 - 1)/g$ in (M); exponent caps (Theorem 7.6, enlarged); $s = \lfloor N \cdot m^2 / \Delta \rfloor$ and both identities of Theorem 4.1 checked exactly	Lemma 3.5: proved; Theorems 7.2, 7.3, 7.6, 7.7 and 4.1: formally verified; (M) bound: immediate from formally verified identities
Three primes, squarefree (sf3 family)	same window; s from Theorem 4.1; exact test of (2.1)	as above
Uniform sieve	Proposition 9.1 (window and valuation); Proposition 4.3 ($D \neq 1$); Lemma 8.3 (square d); Theorems 9.2–9.4; Nagell / continued-fraction completeness of fundamental solutions	Pell forms formally verified; bounds and Theorems 9.2–9.3 proved; Theorem 9.4 uses the cited estimate [13, 14] with a safety factor 10^4 ; completeness of step (1) classical [15, 16] and cross-validated
Integer equation (E3)	$x \leq 3N$ (Lemma 3.6 for integer variables); $y \in [LK/M], 2K/M + 5]$ with $K = (N - 1)\Phi(x)$ and $M = f_N(x)$, from $y > K/M$ and $z \geq y$ (Remark 10.17); z within two units of the real root of $f_N(xy)z^2 - K \cdot \Phi(y)(z + 1) = 1$; exact test $(z + 1) \mid f_N(xy) - 1$ and $D \cdot z^2 + z - 1 = K \cdot \Phi(y)$ with $D = (f_N(xy) - 1)/(z + 1)$	proved in Section 10, Remark 10.17 and Lemma 3.6; a solution with $x > N$ has $D \geq 1$ ($D = 0$ would give $f_N(xy) = 1$ with $N < x \leq y$, excluded by Proposition 10.1 (i); this covers odd N, where the parity argument of Theorem 4.1 is not available), hence $z < \sqrt{(K \cdot \Phi(y))} + 2$, which fits in 64 bits
Four primes	deficit windows for r and s; $p \leq 4N - 1$ (Lemma 3.6); t and γ from Theorem 4.1	proved; Theorem 4.1 formally verified
Effective procedure (Computation 11.8B)	the prime bound of step A and the exponent bound of step B of Theorem 11.8A, with $h(v) - 1 > 1/t'$; for the last prime, $1/t' < h(v) - 1 < 1/(t' - 1)$ in exponent boxes, and Theorem 4.1 for the exponent	proved (Theorem 11.8A); parity of g formally verified
Odd almost perfect numbers (oap.py, oapc.c)	Lemmas 11.12–11.15; the window for the last prime and the splitting of exponents; every solution returned is checked by evaluating σ	Identities and inequalities formally verified (module OddSearch); Lemma 11.14 (iv) is Theorem 4.1, formally verified
Odd almost perfect numbers, ω	Lemmas 11.12–11.15 as in oapc.c; Lemma 11.18 (Jacobi symbol and prime factors up to 3,000 of s'); every solution	Identities, inequalities and the quadratic-residue condition

= 7 (oap7.c)	returned is checked by evaluating σ	formally verified (modules OddSearch and OddQR); the Miller–Rabin bases are deterministic below 2^{64}
Squarefree roots (admS.c, seg.c, bound.py; admQ.c, segQ.c, boundQ.py)	Lemma 11.23 (for quasiperfect numbers Cattaneo’s condition): $p \equiv 5, 23 \pmod{24}$ and no prime factor of $\Phi(p) \equiv \pm 3 \pmod{8}$; beyond $8 \cdot 10^9$ the residue classes modulo 5,928 (728) and the estimate of [32]	Lemma 11.23 and the residue condition of Theorem 11.26 formally verified (module OddSquarefree); [32] cited; sums increased by 10^{-7}
Exponent families (sameexp.c, boundD.py)	$(p^d - 1)/(p - 1)$ divides $\sigma(p^e)$ when $d \mid e + 1$, so all its prime factors are $\equiv \pm 1 \pmod{8}$; classes modulo 8 and no prime $\ell \equiv \pm 3 \pmod{8}$, $\ell \leq 10^6$, dividing it; beyond $8 \cdot 10^9$ the classes modulo 5,928, 440 and 232 and the estimate of [32]	Divisibility and residue conditions formally verified (module OddFamilies); [32] cited
Admissible proportions (adm.gp, fit.py)	The prime factors of $(p^d - 1)/(p - 1)$, by complete factorisation or, for a composite cofactor C with $(2/C) = -1$, by the factor $\equiv \pm 3 \pmod{8}$ that C must have	Lemma 11.18 and the divisibility of Theorem 11.28 formally verified; the limits are heuristic and no statement depends on them
Near-solutions (near.c, parents.py)	none (the defect $2b^2 - \sigma(b^2)$ is computed exactly for every odd $b \leq 10^8$ from a sieve of smallest prime factors)	Exact 128-bit arithmetic
Spoof factorisations (spoof2.c, spoofG.c, negspoof.py; spoofW.c, spoofW3.c for 8 and 9 bases)	the abundancy bounds of Lemma 11.15 for every base but the last; for exponent 2, the bases $\equiv 5, 23 \pmod{24}$ with $\Phi(x)$ free of prime factors $\equiv \pm 3 \pmod{8}$; for other exponents, $\sigma \equiv \pm 1 \pmod{8}$ and free of such primes up to 2,000; for 8 and 9 bases the second-to-last base is kept only if the discriminant of the quadratic for the last base is a square modulo ten primes	Lemmas 11.15 and 11.18 formally verified; the argument modulo 3 proved in Remark 11.33; every solution checked exactly; validated on the chain with even bases; the discriminant of the quadratic is a square whenever the last base is an integer
Bases of either sign (signW.c, signW9.c, conic8.gp)	the congruences of Remark 11.33, which hold for either sign; the two-sided abundancy bound $r \cdot g(-a)^j \leq \text{value} \leq r \cdot g(a)^j$; the conic of the last two bases without rational point (Remark 11.33B); for the second-to-last base the discriminant modulo ten primes	every solution checked exactly; the even-base chain recovered by both programs; a search without filter on small ranges; 8 bases closed by two independent treatments of the last two bases (verify28.py, verify29.py)

12.3 Certificates

For each computation the table separates three claims: the mathematical statement that the search space is finite, the completeness of the execution, and its correctness. Every accept/reject decision is made with exact integers; floating point is used only to set enumeration windows, always enlarged by a margin.

Computation	Finiteness	Completeness of execution	Correctness of execution
Three primes, all exponents, $k \leq 16$ (Computation 7.9)	Theorem 7.8: (p, r) in the window of Lemma 3.5; regime (M): $s \leq (N \cdot L_2 - 1)/g$; regime (P): $\alpha = 1$ and Theorem 7.7; caps of Theorem 7.6; γ from Theorem 4.1	Every prime pair of the window by a segmented sieve. $k = 12$: 1,799,273 pairs, 63,413,029 exponent combinations; $k = 13$: 5,288,295 and 185,845,213; $k = 14$: 18,540,258 and 647,558,215; $k = 15$: 104,197,284 and 3,677,744,747; $k = 16$: 696,695,221 and 22,980,024,954 (24 resumable ranges). The pair counts for $k = 15, 16$ equal those of the independent squarefree program	$\Delta, s = \lfloor N \cdot m^2 / \Delta \rfloor$, D and both identities of Theorem 4.1 in exact GMP integers; a guard reports $s \geq 2^{63}$ and never fired
Three primes, squarefree, $k \leq 20$	Window of Lemma 3.5; s is the exact quotient of Theorem 4.1, so each pair is decided by one exact test	$k = 16$: 696,695,221 pairs; $k = 17$: 968,869,803; $k = 18$: 5,588,881,991; $k = 19$: 14,119,174,649; $k = 20$: 65,582,921,961 in 40 ranges, all completed (nine of them run twice, with identical counts).	128-bit exact tests ($k \leq 17$), or Δ from the exact formula of Theorem 8.4 and the identity checked modulo two 61-bit primes ($k = 18-20$); overflow counter zero in all final runs

		Validated on all known three-prime solutions of $s(n) \mid n - 1$	
Uniform sieve, $D \leq 100,000$ (Computation 9.5)	Theorems 9.2–9.4 and the coverage argument after Remark 9.9	199,998 pairs (D, d) , in five categories; the window of Proposition 9.1 met 1,284,588 times	Exact integer arithmetic; fundamental solutions cross-validated by brute force ($D \leq 200$, and 60 random $D \leq 20,000$); K enlarged by 10^4
Uniform sieve, $100,000 < D \leq 500,000$ (Computation 9.5A)	As Computation 9.5	800,000 pairs (D, d) ; window met 1,253,360 times	Faster implementation, identical output to the original on two test ranges; no cap warning
Integer equation (E3) (Computation 10.2)	$x \leq 3N$, the y -window of Remark 10.17, z within two units of a root (Section 12.2)	$N \leq 1,000$: $3.02 \cdot 10^9$ pairs (x, y) ; $N = 2^k$, $k \leq 15$: $1.81 \cdot 10^{10}$ pairs	Exact 128-bit tests; controls: the trivial chain for $x = N$, and 114 solutions of the exponent-one analogue
Four primes, $k \leq 10$ (Computation 11.9)	Deficit windows of Computation 11.9; $p \leq 4N - 1$; t and γ from Theorem 4.1	$k = 8$: $3.8 \cdot 10^8$ triples; $k = 9$: $1.7 \cdot 10^8$; $k = 10$: $4.09 \cdot 10^9$ triples from 328,633 pairs	Exact GMP tests; the triple with $t > 2^{63}$ rechecked with exact integers; validated on the known four-prime terms of A059047
Any exponents, $\omega = 3$ ($k \leq 15$), $\omega = 4$ ($k \leq 7$), $\omega = 5$ ($k \leq 2$) (Computation 11.8B)	Theorem 11.8A: exactly 2ω steps, each with finitely many explicit choices	Every branch of the procedure; $\omega = 3$, $k = 15$: $1.5 \cdot 10^8$ nodes; $\omega = 4$, $k = 7$: $1.4 \cdot 10^9$ nodes; $\omega = 5$, $k = 2$: $3.0 \cdot 10^8$ nodes	Exact multiprecision arithmetic; validated on the exponent-one equation (six known solutions for $N = 5, 17, 41, 97$); source and logs distributed
Sieve for $s(n) \mid n - 1$, $n \leq 2 \cdot 10^{10}$ (Computation 11.3)	Bounded range	Every n ; 2,741 non-prime-power solutions	Exact 64-bit sums ($\sigma(n) < 10^{11}$); reproduces the first 34 OEIS terms
Odd squares, $b \leq 10^{10}$ (Computation 11.6)	Bounded range	Every odd $b \leq 10^{10}$	Segmented factorisation sieve, 128-bit arithmetic; the number of b found equals the number of odd prime powers up to 10^{10}
Genus of $C_{N,D}$, $k \leq 300$ (Proposition 11.10)	Not a search: a certified sign condition	Sturm sequence for $R(2^k, D)$ for every $k = 2, \dots, 300$	Exact rational arithmetic; $R(N, D)$ by exact interpolation, checked at 40 points
Odd almost perfect numbers, $\omega(b) \leq 6$ (Computation 11.16)	Lemmas 11.13–11.15 bound every branch; splitting ends by Lemma 11.12	Exhaustive tree; identical counts in two implementations; three further window widths give no solution	Exact integer arithmetic (Python integers and GMP); validation (a)–(c) of Computation 11.16
Odd almost perfect numbers, $\omega(b) = 7$ (Computation 11.20)	Lemmas 11.13–11.15 bound every branch; splitting ends by Lemma 11.12	577 states, each run to completion ($rc = 0$) and recorded once; parts of a state checked to add up to the state	GMP arithmetic; validation (a)–(c) of Computation 11.20; 575 states also completed without Lemma 11.18
Squarefree roots (Computation 11.25)	the primes up to $8 \cdot 10^9$; beyond, [32, Thm. 1.2]	every prime up to $2 \cdot 10^9$ by a segmented factorisation sieve, every prime of $(2 \cdot 10^9, 8 \cdot 10^9]$ by a segmented sieve	independent complete factorisation up to 10^7 ; the sieve of (b) against trial division on $(10^5, 10^7]$; agreement with Yamada's product at 2^{29}
Exponent families (Computation 11.29)	the primes up to $8 \cdot 10^9$; beyond, [32, Thm. 1.2]	every prime up to $8 \cdot 10^9$ by a segmented sieve	agreement with direct evaluation for $d = 3, 5, 7, 9, 11$ and $p \leq 3 \cdot 10^5$
Admissible proportions (Computation 11.29A)	finite samples and ranges	every prime of each sample and of each exact range	Python factorisation against adm.gp on every prime up to 10^6 , 10^5 , 10^4 ($d = 3, 5, 7$) and on samples (verify22.py); the count for $d = 3$ equals that of Computation 11.25 (a)

Spoof factorisations, 9 bases (Remark 11.33)	bases other than the last $\leq 10^7$; the branches that need a larger base are counted	all 256 parts, each recorded once	two programs with identical counters on a slice; parts 3 and 200 re-executed; the even-base chain recovered (verify23.py)
Bases of either sign, at most 8 bases (Computation 11.33F)	two-sided abundancy bound in $ x $; the last base from a quadratic; prefixes beyond the bound are counted and printed	$k \leq 7$ with the bound 10^6 : no prefix left; $k = 8$ with $6 \cdot 10^7$: two prefixes, closed by the conic test	two programs with different treatments of the last two bases agree; the even-base chain recovered; a search without filter on small ranges (verify28.py, verify29.py)

13. Formal verification

The Lean 4 development (Lean v4.35.0-rc4, Mathlib [9], tag v4.35.0-rc4) consists of 26 modules and a root file. It contains 212 public theorems and lemmas, all checked with `#print axioms`: 173 depend on `propext`, `Classical.choice` and `Quot.sound`, 35 on `propext` and `Quot.sound`, 3 on `propext` alone and 1 on none; there is no `sorry` and no further axiom. In addition there are six definitions and three private auxiliary lemmas used inside one proof. The classification theorem (Theorem 6.3) and Theorems 7.2–7.3 are stated for Mathlib’s divisor function σ_1 ; the other modules are integer statements whose hypotheses are the component equations, linked to σ by the bridge lemmas. The companion document “Almost Perfect Numbers in Lean 4: Technical Reference to the Formalisation”, deposited at the same DOI, lists every module, theorem and hypothesis and reproduces the complete source.

What is not formalised: Lemma 3.5 and the window bounds used by the programs, Theorem 7.8 as a whole (its ingredients are), Section 9 beyond the Pell forms and the lemmas named in Proposition 9.10 and Theorem 9.14, the cited estimate of Bugeaud and Laurent, Baker’s theorem, the Hasse–Minkowski theorem, Kishore’s theorem, and all computations, including the searches of Computations 11.16 and 11.20 (their lemmas are formalised) and Computations 11.25 and 11.29, and the estimate of [32] used in Theorems 11.24, 11.26 and 11.28 (their residue conditions are formalised).

14. Status and the remaining gap

The almost perfect number conjecture is not proved. Established: (1) the odd part of a non-trivial almost perfect number has at least three prime factors (Theorem 6.3); (2) for three primes, the problem is reduced to explicit finite searches for each k , carried out for $k \leq 16$ (all exponents) and $k \leq 20$ (squarefree); (3) for squarefree b with three primes, every k is excluded when $D_s \leq 500,000$ (Theorem 9.6), and in the positive regime also when $(p - N) \cdot C_2(p, r) \leq (N/100)^{1/4}$ (Theorem 8.7); (4) the squarefree three-prime case is a statement about integral points of a $K3$ surface, independent of primality, and fibres over its smallest variable into curves of genus one, many of which are excluded by local conditions (Theorem 10.13, Computation 10.14); (5) every solution at an even level factors into primitive solutions (Theorem 3.10), so the conjecture for even levels is equivalent to the absence of primitive solutions; (6) a counterexample is exactly an odd $b > 1$ whose potential satisfies $E \equiv 1 \pmod{bNq}$ and $1 \leq E \leq bNq$ (Proposition 10.19); (7) every counterexample has odd part $b > 10^{10}$ (Computation 11.6); (8) every odd almost perfect number has at least eight distinct prime factors (Theorem 11.19), and every prime factor of its $\sigma(n)$ is $\equiv \pm 1 \pmod{8}$ (Lemma 11.18); (9) if its root is squarefree, it has a prime factor greater than $1.6 \cdot 10^{30}$ and more than $4.3 \cdot 10^{27}$ prime factors (Theorem 11.24), and bounds of the same kind hold when one of 3, 5, 7 divides $e + 1$ for every exponent e (Theorem 11.28); in each of these cases the sum over all admissible primes is expected to be below $\log 2$, so that no such number is expected to exist (Remarks 11.27 and 11.29B), and for squarefree roots a level of distribution $\theta > 0.87$ for the primes in arithmetic progressions would, with explicit error terms, make this a proof (Lemma 11.29C, Remark 11.29D); (10) there is no odd spoof almost perfect factorisation with exponent 2 and at most 8 bases, and no odd integer

solution of $\prod \Phi(x_i) = 2 \prod x_i^2 - 1$ with $|x_i| \geq 3$ and at most 8 bases of either sign, without any bound on the bases (Computation 11.33F), nor one with 9 bases whose bases other than the last are at most 10^7 , and the last two bases of any solution give an integral point on a curve of genus one which, for most lists of the other bases, has no rational point (Remarks 11.33, 11.33A and 11.33B); for the single bases up to 600 every orbit of that curve is excluded by covering congruences (Remark 11.33C), and for all single bases outside a set of density zero the curve has no rational point (Proposition 11.33D), a statement about the family of curves, since lists of three bases are already excluded by the abundance.

The precise gap for three primes. A squarefree three-prime counterexample has $D_s > 500,000$, hence $s < \text{pr} \cdot \sqrt{(N/500,001)}$, and lies in regime (M) or in regime (P) with $p - N < \sqrt{(N/500,001)}$. The missing ingredient has two formulations. (a) Pell form, equivalent: for $c_D = (3D + 1)(D - 1)$ and $d \in \{D, 2D\}$, show, uniformly in D , that no solution of $X^2 - dY^2 = -c_D$ with $v_2(Y) = t \geq 3$ and $2^{5t-4} < Y < 2^{7t}$ gives, with $P = Y/2^t$ and $2\Delta = X + D + 1$, a factorisation $P = \text{pr}$ into integers $N < p < r$ satisfying Proposition 8.1 (i), where $N = 2^{2t-2}$ if $d = D$ and $N = 2^{2t-1}$ if $d = 2D$. For almost all large D only the fundamental solution of each orbit meets this window (Remark 9.8), and the last condition to fail is the squareness of one discriminant, with no local cause (Remark 9.8A). (b) Slice form, sufficient: the genus-one curves $L(yz)^2 - K\Phi(y)\Phi(z) = 1$ with $K = (N - 1)\Phi(x)$, $L = Nx^2$ and $N < x \leq 3N$ have no integral point with $x \leq y \leq z$, uniformly in N and x . For each N this is a finite computation (Computation 10.2). The family shows no special structure (Remark 10.23); some of its everywhere locally soluble prime slices have no rational point, but others have rational points if III is finite (Remark 10.25B), so integrality must be used. Every route tested ends at the same place: joint control of e_1 and C_3 (Remark 10.6A), that is, the second-order behaviour of Φ at the corner $(\infty, \infty, \infty, \infty)$ of the threefold of all (x, y, z, N) , which the trivial chain populates (Remark 11.10A). Higher exponents with three primes are reduced to the same finite procedure for each k but have no uniform argument either.

Beyond three primes. A proof for every $\omega(b)$ requires an induction on the number of prime factors. Renormalisation (Section 3.1) makes the induction exact: it remains to exclude primitive solutions at every even level (the descent problem, Remark 3.13). Conjecture 10.3 is the natural squarefree statement.

14.1 Research programme, ranked

The routes below are ranked by how directly they address the gap.

- The slice family (Section 10). Show that the curves $L(yz)^2 - K\Phi(y)\Phi(z) = 1$ with $K = (N - 1)\Phi(x)$, $L = Nx^2$ have no integral point with $x \leq y \leq z$ for $N < x \leq 3N$, using the link $L - K = f_N(x)$ between the coefficients, which Remarks 10.12 and 10.17 show must be used. By Remark 11.33A the same curves, with $K = F$ and $L = 2M$ taken from any list of bases, govern the last two bases of every solution and of every spoof factorisation with exponent 2.
- Uniformity in D (Section 9). Bound, for all D , the 2-adic valuation of fundamental solutions of $X^2 - dY^2 = -(3D + 1)(D - 1)$ relative to their size, or show that solutions with $v_2(Y) > (\log_2 Y)/7$ have a special shape that contradicts Proposition 8.1 (i). By Theorem 9.14 and Remark 9.15, 2-adic conditions leave a set of D of density $1/48$ and cannot bound D , and sizes alone cannot bound D either.
- The size half of Proposition 10.19. For b satisfying $E \equiv 1 \pmod{bNq}$, show that $E > bNq$ unless $E = 1$. By Remark 10.21 such a statement must use the congruences.
- The reduced pair (Section 8.2). Control the single term $(B - 1)G$ with $B - 1 = (p - N)(p + 1)$; for $B = 1$ the two-prime proof closes.
- Induction on ω (Section 3.1, Remark 3.13, Conjecture 10.3). Along the primes in increasing order the partial potentials rise and must fall back to exactly 1 at the last step; for $\omega = 3$ it would suffice to show that this last descent cannot be exact after two ascents, and Theorem 7.2 is a first statement of this type. For odd almost perfect numbers Proposition 11.31 gives the exact form of these steps: the defects d_i start at 1, return to 1, and $\sum D_i s_i = 0$.

- A bound independent of k for fixed ω . Since $b > N$, a bound on b that does not grow with N would reduce each ω to a finite computation; the obstacle is the multi-scale structure described after Theorem 11.8A.
- Integral Brauer–Manin over $\mathbb{Q}(\omega)$ (Remark 10.25C). Decide whether the 3-primary Brauer group of the affine surface, or of one slice such as (64, 73), gives an obstruction to integral points with odd coordinates. Every reciprocity argument has this form; cubic-symbol sieves alone are excluded by explicit witnesses, and the natural quaternion class gives no obstruction.
- Squarefree roots (Section 11.7). An upper bound for the admissible primes beyond $8 \cdot 10^9$ within a factor of about 1.5 of their true number would exclude odd almost perfect numbers with squarefree root (Remark 11.27); the explicit sieves of dimension $3/2$ in the literature lose a much larger factor, and even for the primes alone upper-bound sieves give the factor 2 (Remark 11.33G). By Lemma 11.29C the sifting range is only p , and the factor becomes $(2/\theta)^{1/2}$ for primes of level of distribution θ ; $\theta > 0.87$, or $\theta > 0.67$ with an exact computation up to 10^{18} , would suffice, and the Elliott–Halberstam conjecture gives $\theta = 1$ (Remark 11.29D). The same type of bound would exclude the exponent families of Theorem 11.28, whose admissible sums are expected to converge below $\log 2$ (Remark 11.29B). For other exponents, such as all exponents equal to 16, the abundance gives no contradiction (Remark 11.30), and the search of Section 11.6 is the available tool.

14.2 Relation to the literature

No almost perfect number other than a power of 2 is known. For even almost perfect numbers $2^{k-1}b^2$ with $b > 1$ the literature records that b is an odd composite (Antalan and Tagle [3]) and that $2^k < b$ (Antalan and Dris [4]); the latter paper also quotes a search finding no odd square $u^2 < 10^{22}$ with at least two distinct prime factors in OEIS A059046, that is, with $s(u^2) \mid u^2 - 1$. The present report adds $\omega(b) \geq 3$ (Theorem 6.3, formally verified), hence $b > N^3$ by Lemma 3.4, and the exclusions of Sections 8–10 for three primes. Computation 11.6 ($b \leq 10^{10}$) is an independent check over a smaller range than the search quoted in [4]. No case with $\omega(b) \geq 3$ is settled for all k ; to our knowledge that question is open. [literature search, 22 October 2026]

For odd almost perfect numbers the bound $\omega \geq 6$ of Kishore [1, 2] had not been improved; Theorems 11.11 and 11.19 give $\omega \geq 7$ and $\omega \geq 8$. Independently, Alekseyev [30] shows by a search over all n that there is no odd almost perfect number n with $1 < n < 10^{47}$. The corresponding bounds for quasiperfect numbers are $\omega \geq 7$ (Hagis and Cohen [7]) and $\omega \geq 8$ (Toyohara, Yao and Tao [29], whose lemmas are also formalised in Lean). For quasiperfect numbers with squarefree root Yamada [33] proved $\omega \geq 406,550,054$; Theorem 11.26 raises this to $\omega > 6.5 \cdot 10^{12}$, and Theorem 11.24 is the corresponding statement for odd almost perfect numbers, for which we found no earlier result. Odd spoof perfect factorisations exist [34]; for odd almost perfect numbers none was found (Remark 11.33).

An additive analogue. The equation $\sum 1/x_i + 1/\prod x_i = 1$ (Znám’s problem and Sylvester’s sequence) has a similar structure: the greedy choice gives Sylvester’s numbers 2, 3, 7, 43, ..., which Curtiss [18] proved to be the unique best under-approximation of 1 by n unit fractions, and Brenton and Hill [19] related its solutions to a class of complex surface singularities. Non-greedy solutions exist, for example $1/2 + 1/3 + 1/11 + 1/23 + 1/31 + 1/47058 = 1$ with $47058 = 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31$. The trivial chain $(N, N^3, N^9, \dots)$ of (E3) is the greedy chain for $N/(N-1)$ with factors $1 + 1/x + 1/x^2$: after the choice $x = N$ the remaining target is $N^3/(N^3 - 1)$, of the same form. The existence of non-greedy solutions in the additive problem shows that minimal defect alone does not force uniqueness; consistently with Remark 10.4, a proof for (E3) must use the specific form of Φ .

Appendix A. Explicit coefficients for Section 8.6

Notation: $a = p - N$, $j = C_2(p, r) = qN - (p - N)(r - N)$, so that $a \cdot r = aN + qN - j$; $A = a^2\Delta$; $a^2N(pr)^2 = QA + R$. All identities are checked by the Lean theorem regimeP_division (ring normalisation).

$$A = N^4 + (-2 + a - aj)N^3 + (1 - 2j - 2a^2j)N^2 + (2j - a + a^3 - a^3j - a^2j + aj^2)N + A_0, A_0 = -aj + aj^2 + a^2 - a^2j + a^2j^2 + a^3 - a^3j + a^4 + j^2.$$

$$Q = N^3 + (3a + aj)N^2 + (2aj + 3a^2 + 4a^2j + a^2j^2)N + Q_0, Q_0 = 3aj + aj^2 + 7a^2j + 4a^2j^2 + 6a^3j + 5a^3j^2 + a^3j^3.$$

$$R = R_3N^3 + R_2N^2 + R_1N + R_0, \text{ with } R_3 = 3aj + 3aj^2 + 9a^2j + 13a^2j^2 + 2a^2j^3 - 3a^3 + 9a^3j + 18a^3j^2 + 6a^3j^3 - 3a^4 + 2a^4j + 10a^4j^2 + 6a^4j^3 + a^4j^4.$$

$$R_2 = -3aj + aj^3 - 6a^2j + 3a^2j^3 - 2a^3j + 11a^3j^2 + 6a^3j^3 + a^3j^4 - 3a^4 + 3a^4j + 21a^4j^2 + 9a^4j^3 - 6a^5 - 2a^5j + 15a^5j^2 + 11a^5j^3 + 2a^5j^4.$$

$$R_1 = -6aj^2 - 4aj^3 + 3a^2j - 13a^2j^2 - 17a^2j^3 - 2a^2j^4 + 8a^3j - 2a^3j^2 - 21a^3j^3 - 7a^3j^4 - 3a^4 + 16a^4j^2 - 3a^4j^3 - 6a^4j^4 - a^4j^5 - 3a^5 - 10a^5j + 12a^5j^2 + 10a^5j^3 + a^5j^4 - 3a^6 - 10a^6j + 4a^6j^3 + a^6j^4.$$

$$R_0 = -3aj^3 - aj^4 + 3a^2j^2 - 9a^2j^3 - 5a^2j^4 - 3a^3j + 9a^3j^2 - 11a^3j^3 - 10a^3j^4 - a^3j^5 - 10a^4j + 11a^4j^2 - 3a^4j^3 - 8a^4j^4 - a^4j^5 - 16a^5j + 3a^5j^2 + 2a^5j^3 - 4a^5j^4 - a^5j^5 - 13a^6j - 3a^6j^2 + 4a^6j^3 + a^6j^4 - 6a^7j - 5a^7j^2 - a^7j^3.$$

Appendix B. Verification record

The report, the companion document and the supplementary archive were checked from the ninety-four angles below. Identities were re-checked independently of Lean by exact integer or rational evaluation, at 2,000 random points unless stated. Computations were re-executed with the programs of the supplementary archive on the ranges stated; ranges that were not re-executed are recorded by the logs in the archive. The column Outcome states the result of each check.

#	Check	Method	Outcome
1	Lean: clean rebuild	All 27 files compiled from an empty build directory against Mathlib v4.35.0-rc4, in the order of the README	BUILD OK in 32 min 14 s; two linter warnings (unused hypotheses), no errors
2	Lean: rebuild from the archive	The lean/ folder of the supplementary archive copied to a fresh directory and compiled from scratch	BUILD OK in 31 min 28 s; the axiom output is identical to lean/axioms_output.txt
3	Lean: axioms	#print axioms on all 212 public theorems (CheckAll.lean)	173 use propext, Classical.choice, Quot.sound; 35 use propext, Quot.sound; 3 use propext; 1 uses none; no sorryAx
4	Lean: completeness of the axiom check	Declarations in the sources compared with CheckAll.lean	Every public theorem listed exactly once; not listed: six definitions and three private lemmas
5	Lean: forbidden constructs	Source scan for sorry, admit, axiom, unsafe, implemented_by, native_decide	None
6	Lean: build order	The order in the README compared with the import graph	Every module is compiled after the modules it imports; the root file imports all 26
7	Lean: names cited in the report	Every identifier after “formally verified” matched against the sources	All 139 names present; no private lemma cited
8	Lean: statement fidelity, σ level	almostPerfect_classification, three_prime_one_positive_sigma, three_prime_pair_negative_sigma, three_prime_exponent_sigma read against Theorems 6.3, 7.2, 7.3	Match (in Lean the exponent $e = 2$ of $n = 2^ap^e \dots$ is $\alpha = 1$ for b , and $a \geq 1$ is $N \geq 4$)
9	Lean: statement fidelity, integer level	component, component_quotient_odd, renormalise, two_var_integer, chain_first_eq_N, regimeP_top_exclusion, no_double_root, pell_D_three_mod_four, congruences_combine,	Match; hypotheses as listed in Section 6 of the companion document

		local_archimedean_split, gap_odd, closed_pos, closed_neg, last_upper, last_lower read against Theorems 3.10, 4.1, 8.7, 9.14, 11.8A, Lemmas 11.13–11.14 and Propositions 9.10, 10.1, 10.19	
10	Lean: trusted definitions	IsAlmostPerfect and pot read against $\sigma(n) = 2n - 1$ and f_N	IsAlmostPerfect $n := 0 < n \wedge \sigma 1 n + 1 = 2n$ and pot $N v := N \cdot v^2 - (N - 1) \sigma 1 (v^2)$, as in the report
11	Lean: statement numbers in comments	Every “Theorem/Lemma/Proposition/Remark x.y” in the Lean sources and in the programs resolved against the labels of the report	All resolve to a statement of the same kind
12	Lean: versions	lean-toolchain, lakefile.toml and the companion document compared with the installed toolchain and the Mathlib checkout	Lean 4.35.0-rc4 (commit c29b6dda4f7c) and Mathlib tag v4.35.0-rc4 (commit 1f414401f690) throughout
13	Lean: one source everywhere	Lean files of the archive, the compiled tree and the code blocks of the companion document compared byte by byte	Identical
14	Companion: source listing	Every code block compared line by line with the compiled files	All 31 files identical
15	Companion: module table	Line counts and theorem counts recomputed from the sources	All correct; theorem counts sum to 212
16	Companion: declaration table	Axiom class of each theorem against the #print axioms output	All 212 correct
17	Companion: correspondence table	Generated from the text of this report; checked to contain every cited name; entries for statements printed in blue here are printed in blue there	Complete (66 report entries) and consistent
18	Companion: hypothesis map	Each row compared with the Lean statement it describes	Correct
19	Companion: title page and register	Brand, title, author, e-mail and date; search for historical or conversational material	Present and identical to the report; none
20	Identities: Sections 2–5	Lemma 2.2 with true σ ; Theorem 4.1; Proposition 3.9 (800 coprime pairs, true σ); Remark 3.15; Propositions 4.4, 4.5, 4.8; Remarks 4.7, 4.10; Theorem 5.1 (one to four primes); Proposition 5.2; the selection rule modulo 8	Hold
21	Identities: Sections 6–8	Theorem 6.2 (the equation is $w(A - w) = c_0$); Proposition 7.1; Section 8.1 and Proposition 8.1; Proposition 8.6 with the coefficients parsed from the printed Appendix A; Theorem 8.7 ($N \leq R < A$); Proposition 8.11; Lemma 8.13	Hold
22	Identities: Section 9	Proposition 9.1; Proposition 9.10 (elimination identity, $D^*(e)$ for $e \leq 8$, $(2e + 1)(16/25)^e \leq 2.048$); Theorem 9.14 (modulo 64, the congruences for s , the parity of D , density of the admissible D $0.020833 = 1/48$); the constant $K = 9,981.2$ of Theorem 9.4	Hold
23	Identities: Section 10	Proposition 10.5 (norm form, content criterion on 3,000 triples); Remarks 10.6, 10.6A (20,000 points) and 10.8; Theorem 10.13, Remarks 10.16 and 10.17; Lemma 10.18 (33,000 triples); Proposition 10.19; Remarks 10.21 and 10.22	Hold
24	Identities: Sections 10.5 and 11	The blocks of Remark 10.25A; the rational point of Remark 10.25B on (16, 46), exactly; the cubic conditions of Remark 10.25C for (197, 2399, 4877) and (2, 8, 512); cubes modulo inert primes; the chain for $\omega \leq 4$; the boundary and second-order expansions of Remark 11.10A	Hold
25	Identities: totals	The eighteen independent check programs of the archive	38 of 38, 28 of 28, 10 of 10, 18 of 18, 18 of 18, 17 of 17, 11 of 11, 13 of 13, 3

			of 3, 12 of 12, 9 of 9, 6 of 6, 5 of 5, 5 of 5, 6 of 6, 10 of 10, 14 of 14 and 8 of 8 checks pass
26	Proofs: Sections 2–6	Every step of Lemmas 2.1–3.7, Theorem 3.8, Proposition 3.9, Theorem 3.10, Corollary 3.11, Theorem 4.1 (including the parity of D), Propositions 4.2–4.8 and Theorems 6.1–6.4 re-derived by hand	Correct; the inequalities in Lemma 3.6 and Theorem 6.2 are justified in the text
27	Proofs: Sections 7–9	Every step of Theorems 7.2–7.8, Theorem 8.4 (the comparison $a\Delta < N\text{-pr}$ also tested in 10,639,391 cases), Theorem 8.7, Lemma 8.13, Proposition 9.1, Theorems 9.2–9.4, Remark 9.9, Proposition 9.10, Theorems 9.11 and 9.14	Correct
28	Proofs: Sections 10–11	Every step of Propositions 10.1, 10.5, 10.19, Theorem 10.13 (Hilbert-symbol cases), Lemma 10.18, Propositions 11.2 and 11.8, Theorems 11.7 and 11.8A, Proposition 11.10, Lemmas 11.12–11.15, 11.18 and 11.23, Remark 11.22, Theorems 11.24, 11.26 and 11.28, Proposition 11.31 and the completeness argument of the searches in Section 11.6	Correct
29	Scope of hypotheses	Theorem 8.7 ($N \geq 2^{21}$), Theorem 9.14 ($k \geq 21$), Lemma 8.13 ($k \geq 5$), Lemma 8.5A ($a = 1$ by parity), uniqueness in Theorem 8.4 (regime (P) only), Lemma 3.6 ($N \geq 2$)	All stated in the text
30	Abstract and Section 14 against the body	Each claim of the abstract and of Section 14 traced to a labelled statement with its status	Every claim is a stated result; no claim exceeds its source
31	Cited results	Use of the estimate of Bugeaud and Laurent (Theorem H of [14]), Baker’s theorem, Siegel’s theorem, the Hasse–Minkowski theorem, Theorem 4 (a) of [22], Theorem 1.8 of [24], the 2-parity theorem and cubic reciprocity [28] compared with their hypotheses	Hypotheses verified in each application
32	Bibliography	Authors, titles, journals, volumes and years of the references checked against publisher and arXiv records where available	Correct; references [27], [29], [30], [32], [33] and [34] are given with their arXiv numbers
33	Status labels	Every theorem, lemma, proposition, corollary and computation carries a status label; every remark that calls a route closed exhibits a witness or a reformulation	Complete (for Lemma 2.2 and Theorem 4.1 the label follows the displayed equation)
34	Computation 7.9	hx re-executed for every $k \leq 10$; the 24 range logs of $k = 16$ summed	No counterexample; at $k = 10$: 123,199 pairs and 4,361,306 combinations; $k = 16$: 696,695,221 pairs and 22,980,024,954 combinations, as stated
35	Squarefree three primes	The range logs of $k = 20$ summed and checked for completeness and overflow	40 ranges, 65,582,921,961 pairs, no candidate, overflow counter zero
36	Computation 9.5	The Pell pipeline re-executed for every $2 \leq D \leq 100,000$	Exactly the stated figures: 156,188 / 11,299 / 3,429 / 28,544 / 538 pairs and 1,284,588 window points, no survivor
37	Computation 9.5A	Category sums of the four range logs recomputed	800,000 pairs and 1,253,360 window points, no survivor, no warning
38	Computation 10.2	isol3 re-executed for every $N \leq 1,000$; the exponent-one control for $N \leq 60$	No solution with $x > N$ (3,015,332,488 pairs); $113 + 1 = 114$ control solutions
39	Computation 10.14	Hilbert-symbol and $\mathbb{Z}_\ell$ tests re-executed for every $N \leq 120$	No surviving slice exactly for the fourteen listed N ; 0, 8, 3, 40 survivors for $N = 8, 16, 32, 64$
40	Remark 10.25B	The descent script of the archive re-executed on the controls $x = N$ ($N = 16, 32, 64$) and on (16, 37), (32, 71)	Controls recognised; no rational point proved on (16, 37) and (32, 71), ranks 3 and 1, witness primes above 10^6
41	Remark 10.25C	The cubic-condition program for $k = 7, 9, 11$,	107, 111 and 115 of 3,000 triples; both

		and the quaternion invariants at 2 and 3 with PARI/GP	values ± 1 at 3 on all seven slices, value 1 at 2
42	Computations 11.3 and 11.6	The sieve for $s(n) \mid n - 1$ re-executed for $n \leq 4 \cdot 10^8$; the sieve for odd squares for $b \leq 10^8$	532 non-prime-power solutions (520, 10, 2), all squarefree with odd N; only the 5,762,833 odd prime powers $b \leq 10^8$
43	Computation 11.8B	The procedure re-executed for $\omega = 3, k \leq 8$ and $\omega = 4, k \leq 4$, and on the exponent-one equation ($\omega = 4, N = 5$)	No solution; the validation finds $54,375,629 = 7 \cdot 11 \cdot 547 \cdot 1291$
44	Programs compile	Every C program of the archive compiled with gcc -O2 -Wall against GMP; every Python script byte-compiled	All 50 C programs and all Python scripts compile; warnings concern indentation style only
45	Programs are self-contained	Search for absolute paths and for files read by the scripts	No absolute path; every file a script reads is in the archive
46	Archive integrity	SHA256SUMS.txt regenerated and verified; README checked against the report (one entry per statement labelled [computed])	All checksums verify; every computation has its program and log
47	Cross-references	Every cited statement, section, equation and appendix resolved, with the kind of statement checked	All resolve
48	Labels	Uniqueness and increasing order of the 143 statement labels	Unique and increasing
49	Proofs closed	Every proof ends with ■	61 proofs, all closed
50	Order of dependence	Proofs scanned for references to later results	Four forward references, none circular: Theorem 3.8 $\rightarrow$ 4.1, Corollary 3.11 $\rightarrow$ 6.4, Lemma 8.3 $\rightarrow$ 8.4, Theorem 9.2 (c) $\rightarrow$ 9.4
51	Displayed equations	Labels (2.1), (4.1), (8.1), (9.1) and (E3) defined once and cited consistently	Correct
52	Citations	Every reference [1]–[34] cited in the text, none duplicated, consistent format	Correct
53	Notation	Every symbol of the notation table used with the stated meaning; levels N other than 2^k flagged where used	Consistent
54	Headings	Numbering of sections and subsections, and the organisation paragraph of Section 1.2	Continuous and consistent
55	Spelling	Dictionary check of both documents (hunspell en_US list), British spelling throughout	No misspelling; one spelling of each word (titles of cited works as published)
56	Typesetting	Unbalanced brackets (half-open intervals excepted), nested sub/superscripts, repeated words, double spaces, unrendered markup	None
57	Register and redundancy	Formal English addressed to the reader; search for conversational, historical and duplicated material	None
58	Consistency of repeated numbers	Every figure quoted more than once: ranges of k, $D \leq 500,000$ and $\sqrt{N/500,001}$, counts and bounds; numbers in Section 12 against the logs	Consistent
59	Blue statements	Statements printed in blue checked against the criterion of Section 1.3	43 statements: principal results without counterpart in the literature and the statements of the gap
60	Files	Both .docx files validated against the Office Open XML schema and rendered to PDF; title pages, dates and counts compared across the three files	Valid; rendered without error; consistent
61	Computation 11.16: two implementations	oap.py and oapc.c run for $(J, K, d) = (1, 2, 1)$ and $\omega = 1, \dots, 6$	No solution; identical counts at every ω ($\omega = 6$: 144,512 selection states, 5,568,577 last-prime states, 4,534,707 closed systems, 2,446,710 splittings)
62	Computation 11.16:	oapc for $\omega = 6$ with window widths 5, 100 and	No solution; the trees differ (7,403,895,

	other window widths	1,000	4,443,733 and 2,816,417 last-prime states)
63	Computation 11.16: validation, $\omega \leq 4$	Both programs against direct factorisation for $(J, K) \in \{(1, 2), (3, 4), (5, 6), (7, 8), (15, 16)\}$, $b \leq 3 \cdot 10^6$, $d \leq 10^7$: 6,349 cases	No mismatch in either program
64	Computation 11.16: validation, $\omega = 5, 6$	Both programs on the 359 tabulated pairs with $\omega = 5$ ($d \leq 10^{10}$) and the 8 with $\omega = 6$ ($d \leq 10^{13}$)	Every tabulated solution found, no other with $n \leq 9 \cdot 10^{12}$
65	Computation 11.16: planted solutions	Random b with three or four primes, largest prime up to $3 \cdot 10^4$, exponents up to 3; J and K chosen so that d is small	40 of 40 and 30 of 30 recovered among the runs that finished
66	Lemmas 11.12–11.15: independent checks	verify15.py: parity, identities and bounds on random data in exact rationals; the window of Lemma 11.14 on 2,027 tabulated solutions; re-run of the C program	10 of 10 checks pass
67	Lemma 11.18: formal proof	Module OddQR (qr_general, qr_two, oap_sigma_prime_mod8) compiled; statements read against Lemma 11.18	Match; the step modulo 8 is Mathlib's ZMod.exists_sq_eq_two_iff
68	Lemma 11.18: tabulated solutions	Every prime factor of $\sigma(n)$ over all tabulated solutions of $J \cdot \sigma(n) = K \cdot n - d$ tested for $(K \cdot d/q) = 1$ (lemma_qr_check.py)	18,334 prime factors, no exception
69	Computation 11.20: validation of the program	The final program and the version with Lemma 11.18 at selection and last-prime states against the tables (cval7.py; parameters as used)	6,414 cases each, no mismatch
70	Computation 11.20: the partition	The 577 states listed (states.txt) and compared; parts of a state compared with a single run on two states	577 distinct sets of four smallest primes; sums of the parts equal the single run
71	Computation 11.20: completeness of the record	results/final_states.txt and results/final_parts_163.txt read: one line per state or part, return code, solutions	577 states, each once, all $rc = 0$, no solution; the state 3, 5, 17, 257 in 32 parts, all $rc = 0$
72	Computation 11.20: independent runs	verify16.py: re-run of states with the final program and comparison of every count with the record; the earlier computation without Lemma 11.18	18 of 18 checks pass; 575 states also closed without Lemma 11.18, no solution
73	Lemma 11.23 and Theorem 11.26: formal proofs	Module OddSquarefree (oap_squarefree_residue, residue24, mod8_of_prime_factors, sigma_prime_sq, qp_squarefree_residue, qp_prime_mod8, mod8_13_of_prime_factors) compiled; statements read against Lemma 11.23 and the residue condition of Theorem 11.26	Match; $\sigma(p^2) = p^2 + p + 1$ is derived from Mathlib's σ , and the condition modulo 8 for -2 is Mathlib's ZMod.exists_sq_eq_neg_two_iff
74	Computation 11.25: factorisation sieves	admS.c and admQ.c against complete factorisation of every $\Phi(p)$, $p \leq 10^6$ (verify17.py), and against the Pollard-rho programs up to 10^7	Identical counts and sums
75	Computation 11.25: class sieves	seg.c and segQ.c against trial division on $(10^5, 3 \cdot 10^6]$; the logs of the runs to $2 \cdot 10^9$ and $8 \cdot 10^9$ read	Identical; the logs give the figures of Computation 11.25
76	Theorems 11.24 and 11.26: the bounds	The residue classes modulo 5,928 and 728 recounted; admissible primes below $2 \cdot 10^5$ checked to lie in them; bound.py and boundQ.py re-run from the logged values; $U(P) < \log 2$ checked along the range; Theorem 1.2 of [32] compared with the published statement	320 of 1,728 and 80 of 288 classes; $P_0 > 1.6 \cdot 10^{30}$, $\omega > 4.3 \cdot 10^{27}$; $P_0 > 8 \cdot 10^{14}$, $\omega > 6.5 \cdot 10^{12}$
77	Remark 11.27 and the comparison with [33]	Product of $\Phi(p)/p^2$ over the quasiperfect-admissible primes below 2^{29} against [33, (30)]; the fit of the five values of $S(X)$; verify17.py in total	1.7501432 against 1.75014319434; c between 0.701 and 0.703, S_∞ between 0.6145 and 0.6147; 18 of 18 checks pass
78	Theorem 11.28: formal part	Module OddFamilies (geom_dvd, oap_family_dvd, oap_family_mod8, oap_family3_residue, oap_family5_residue,	Match; the divisibility $(p^d - 1)/(p - 1) \mid \sigma(p^e)$ for $d \mid e + 1$ is proved for Mathlib's σ

		oap_family7_residue) compiled; statements read against Theorem 11.28	
79	Computation 11.29 and the bounds	sameexp.c against direct evaluation for $d = 3, 5, 7$, $p \leq 10^5$; d -admissible primes below 10^4 by complete factorisation checked to lie in the classes modulo 5,928, 440 and 232; boundD.py re-run from the logged sums	Identical; 320/1,728, 36/160, 44/112 classes; the bounds of Theorem 11.28 reproduced
80	Remark 11.30	Complete factorisations of $\sigma(p^{16})$ for $p = 3, 5, 7, 11$ and primality of $\sigma(5^{10})$, $\sigma(3^{12})$, $\sigma(7^{12})$; verify18.py in total	As stated; product 2.406; 17 of 17 checks pass
81	Computation 11.29A and Remarks 11.27, 11.29B	verify22.py: d -admissible primes recounted by an independent Python factorisation up to 10^6 ($d = 3$), 10^5 ($d = 5$) and 10^4 ($d = 7$) and on samples after 10^8 , 10^6 and 10^5 , against adm.gp; the fit re-run from the logs; the limits printed in the report compared with it	Identical counts and sums; every limit below $\log 2$; 12 of 12 checks pass
82	Proposition 11.31: formal part	Module OddDescent (descent_step, last_prime_quotient, last_prime_D_mod8, last_prime_D_mod3) compiled; statements read against Proposition 11.31	Match; the congruences are decided in ZMod 8 and ZMod 3
83	Proposition 11.31 and Remark 11.32: independent checks	verify19.py: the descent identity with the true σ on 3,000 odd b in random orders; the congruences on all integer solutions of $D \cdot \Phi(t) = 2m^2 - t$ in a box; the scan of near-solutions re-run to 10^7 and compared with the record to 10^8	11 of 11 checks pass
84	Remark 11.33: spoof searches	spoof2.c and spoofG.c re-run (exponent 2, $k \leq 7$; exponents up to 4 and 6, $k \leq 6$) and compared with the logs; the even-base validation; an independent brute force without bounds or admissibility for up to 4 bases	No odd spoof; the chain 2, 8, 512, 2^{27} recovered; the brute force finds only the even base 2
85	Remark 11.33: 8 and 9 bases	verify23.py: spoofW.c and spoofW3.c compared on 8 bases up to 10^6 and on a slice of 9 bases; the even-base chain; 8 bases up to 10^7 against spoof2.c; the log of the 256 parts for 9 bases read, and parts 3 and 200 re-executed	Identical counters; no solution; 9 of 9 checks pass
86	Remark 11.33A	verify24.py: the identity for the last two bases and its Pell form at 50,000 random points; $s = y + t$ and $s^2 - 4u = (t - y)^2$; the even-base chain on the conic; the curve of Section 10 with $K = F$, $L = 2M$	Hold; 6 of 6 checks pass
87	Remark 11.33B	verify25.py in plain Python: $Q \equiv 5 \pmod{8}$, $\gcd(N_1, Q) = 1$ and the Hilbert symbols at 2, at the primes of Q and at the primes of N_1 on 300 lists of bases; the example 5 modulo 71 and 67^2 ; the counts recomputed by an independent factorisation and compared with locex.gp	Hold; 5 of 5 checks pass
88	Remark 11.33C	verify26.py in plain Python: the 60 orbits of the seven single bases with orbits re-covered from the exported data (norms checked, periods and residues recomputed); the defect lemma on 20,000 random cases; the logs of the single bases and of the pairs read	Every orbit covered; the counts as stated; 5 of 5 checks pass
89	Proposition 11.33D and Remark 11.33E	verify27.py: the polynomials N_1 and Q ; the log of galois.gp (group S_4 , the resultant, the quadratic extension); the sums of $\rho(p)/p$ recomputed by brute force up to 10^4 ; the proportions in the log of dens.gp; the quadratic-residue step of Remark 11.33E (i)	Hold; 6 of 6 checks pass
90	Lemma 11.29C and Remark 11.29D	verify30.py: the lemma by complete factorisation of $\Phi(p)$ for every prime $p \equiv 5, 23 \pmod{24}$ below 10^5 (even number of bad prime factors, the smallest $\leq p$; 1,013 admissible primes); the logs of parity.py (to $3 \cdot 10^5$) and	Hold; 8 of 8 checks pass

		sifted.py (to $2 \cdot 10^6$); the ratios $F(0)/F(2)$ of the half-dimensional sieve; the factors 1.52 and 1.72 and the levels 0.87 and 0.67	
91	Computation 11.33F and Remark 11.33G	verify28.py: the residues 5, 23 (mod 24) for either sign; a search without filter for $2 \leq x \leq 2,000$ (two bases) and ≤ 60 (three bases); the two conic obstructions recomputed (p prime, $v_p(N_1) = 1$, $(Q/p) = -1$); the log of signW.c. verify29.py: signW9.c compiled and run (the even-base chain; 8 bases with $L = 10^6$ closed with counters equal to the log; 9 bases with $L = 1,500$); the log for 9 bases with $L = 3 \cdot 10^4$; the 3,008 prefixes; the products over distinct bases	Hold; 10 of 10 and 14 of 14 checks pass
92	Remarks 11.34 and 11.35	Descartes's identity and the general identity $\sigma(m^2)x = 2m^2(x - 1)$; the near-solutions at $N = 4, \dots, 32$ re-run to $3 \cdot 10^6$; $n \mid \sigma(n) + 1$ re-run to 10^7 ; verify20.py in total	As stated; 13 of 13 checks pass
93	Remark 11.10A and the proof of Theorem 11.24	The coefficients and the discriminant of the boundary curve as a quadratic in z , and their values at a root of Φ , checked for $N \leq 2,000$; the bound $n > 10^{16}$; verify21.py	Hold; 3 of 3 checks pass
94	Register and provenance	Both documents and every file of the archive searched for first- and second-person forms, conversational, historical and promotional wording, non-English script, absolute paths and tool or generator names; the document properties (author, dates, comments) of both documents inspected	None found; the document properties name the author and the date of the report

References

- [1] M. Kishore, Odd integers N with five distinct prime factors for which $2 - 10^{-12} < \sigma(N)/N < 2 + 10^{-12}$, Math. Comp. 32 (1978), 303–309.
- [2] M. Kishore, On odd perfect, quasiperfect, and odd almost perfect numbers, Math. Comp. 36 (1981), 583–586.
- [3] J. R. M. Antalan and R. P. Tagle, Revisiting forms of almost perfect numbers, preprint (2014), as cited in [4].
- [4] J. R. M. Antalan and J. A. B. Dris, Some new results on even almost perfect numbers which are not powers of two, arXiv:1602.04248.
- [5] M. Tang, X. Ren and M. Li, On near-perfect and deficient-perfect numbers, Colloq. Math. 133 (2013); see also Bull. Austral. Math. Soc. (2014).
- [6] M. Tang and M. Feng, On odd deficient-perfect numbers with three distinct prime factors, as cited in arXiv:1906.09947.
- [7] P. Hagis Jr. and G. L. Cohen, Some results concerning quasiperfect numbers, J. Austral. Math. Soc. 33 (1982), 275–286.
- [8] J. H. Silverman, Rational points on K3 surfaces: a new canonical height, Invent. Math. 105 (1991), 347–373.
- [9] The Mathlib Community, The Lean mathematical library, CPP 2020.
- [10] S. Aursukaree and P. Pongsriam, On exactly 3-deficient-perfect numbers, Fibonacci Quart. 59 (2021); arXiv:2001.06953.
- [11] J.-P. Serre, A Course in Arithmetic, GTM 7, Springer, 1973.
- [12] H. J. J. te Riele, Rules for constructing hyperperfect numbers, Fibonacci Quart. 22 (1984), 50–60; OEIS A059046 and A059047 (J. McCranie; b-file by D. Johnson).
- [13] Y. Bugeaud and M. Laurent, Minoration effective de la distance p -adique entre puissances de nombres algébriques, J. Number Theory 61 (1996), 311–342.

- [14] Y. Bugeaud, Estimates for linear forms in logarithms, survey lectures (BIRS, 2012), Theorem H.
- [15] K. R. Matthews, The Diophantine equation $x^2 - Dy^2 = N$, $D > 0$, *Expo. Math.* 18 (2000); J. P. Robertson, Solving the generalized Pell equation $x^2 - Dy^2 = N$ (2004).
- [16] T. Nagell, *Introduction to Number Theory*, Wiley, 1951 (bounds for fundamental solutions of $x^2 - Dy^2 = N$).
- [17] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* 65 (1969), 439–444.
- [18] D. R. Curtiss, On Kellogg’s Diophantine problem, *Amer. Math. Monthly* 29 (1922), 380–387.
- [19] L. Brenton and R. Hill, On the Diophantine equation $1 = \sum 1/n_i + 1/\prod n_i$ and a class of homologically trivial complex surface singularities, *Pacific J. Math.* 133 (1988), 41–67.
- [20] C. Pomerance, Multiply perfect numbers, Mersenne primes, and effective computability, *Math. Ann.* 226 (1977), 195–206.
- [21] D. R. Heath-Brown, Odd perfect numbers, *Math. Proc. Cambridge Philos. Soc.* 115 (1994), 191–196.
- [22] A. Levin, Variations on a theme of Runge: effective determination of integral points on certain varieties, *J. Théor. Nombres Bordeaux* 20 (2008), 385–417.
- [23] P. Corvaja and U. Zannier, On integral points on surfaces, *Ann. of Math.* 160 (2004), 705–726.
- [24] G. Heier and A. Levin, On the degeneracy of integral points and entire curves in the complement of nef effective divisors, *arXiv:1907.00896*.
- [25] J.-L. Colliot-Thélène and F. Xu, Brauer–Manin obstruction for integral points of homogeneous spaces and representation by integral quadratic forms, *Compos. Math.* 145 (2009), 309–363.
- [26] D. Harari and J. F. Voloch, The Brauer–Manin obstruction for integral points on curves, *Math. Proc. Cambridge Philos. Soc.* 149 (2010), 413–421.
- [27] A. Kresch and Yu. Tschinkel, Effectivity of Brauer–Manin obstructions on surfaces, *Adv. Math.* 226 (2011); *arXiv:1005.4331*.
- [28] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., GTM 84, Springer, 1990, Chapter 9.
- [29] A. Toyohara, S. Yao and Y. Tao, Every quasiperfect number has at least eight distinct prime factors, *arXiv:2608.02066* (2026).
- [30] M. A. Alekseyev, Computing bounded solutions to linear Diophantine equations with the sum of divisors, *arXiv:2601.17832* (2026).
- [31] P. Cattaneo, Sui numeri quasiperfetti, *Boll. Un. Mat. Ital.* (3) 6 (1951), 59–62.
- [32] M. A. Bennett, G. Martin, K. O’Bryant and A. Rechnitzer, Explicit bounds for primes in arithmetic progressions, *Illinois J. Math.* 62 (2018), 427–532; *arXiv:1802.00085*.
- [33] T. Yamada, Quasiperfect numbers with the same exponent, *arXiv:1610.01063*.
- [34] BYU Computational Number Theory Group (N. Andersen, S. Durham, M. J. Griffin, J. Hales, P. Jenkins, R. Keck, H. Ko, G. Molnar, E. Moss, P. P. Nielsen, K. Niendorf, V. Tombs, M. Warnick, D. Wu), Odd, spoof perfect factorizations, *J. Number Theory* 234 (2022), 31–47; *arXiv:2006.10697*.
- [35] C. Bertók and L. Hajdu, A Hasse-type principle for exponential Diophantine equations and its applications, *Math. Comp.* 85 (2016), 849–860; *arXiv:1407.6499*.
- [36] Q.-D. Dao, Brauer–Manin obstruction for Wehler K3 surfaces of Markoff type, *arXiv:2302.11515*.
- [37] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
- [38] H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* 20 (1973), 119–134.
- [39] E. Bombieri, On the large sieve, *Mathematika* 12 (1965), 201–225.
- [40] P. D. T. A. Elliott and H. Halberstam, A conjecture in prime number theory, *Symposia Mathematica* 4 (1970), 59–72.
- [41] H. Iwaniec, The half dimensional sieve, *Acta Arith.* 29 (1976), 69–95.