hexagon:2611.00366v1

DIVISORS OF MERSENNE NUMBERS UNDER DOUBLING, AND PRIME FACTORS OF $2^p - 1$ BESIDE NEAR-WAGSTAFF NUMBERS: SHARP ELEMENTARY BOUNDS, EXACT REDUCTIONS, AND BARRIERS

SUNAY VENKAT

ABSTRACT. Let $f(n) = \sum_{k \le n} \tau(2^k - 1)$. Erdős asked whether $f(2n)/f(n)$ tends to a limit (Problem #893). Kovač and Luca proved $\limsup f(2n)/f(n) = \infty$. Whether the limit is $+\infty$ is open. We prove that $f(2n) \ge 3f(n)$ for every n, with equality exactly for $n \in \{1, 2, 4\}$. If the Fermat number F_a is composite, then $f(2n) \ge \big(4 - \frac{16}{3 \cdot 2^{a-2}+4}\big) f(n)$ on $[2^a, 2^{a+1})$. Hence $f(2n) \ge \frac{24}{7} f(n)$ for $32 \le n < 2^{33}$, and $\liminf f(2n)/f(n) \ge 4$ if all large Fermat numbers are composite. For every C, the set $\{n : f(2n) > Cf(n)\}$ meets every chain $n, 2n, \dots, 2^{J(C)-1}n$ and has lower density at least $1/(2^{J(C)} - 1)$. We reduce $f(2n)/f(n) \to \infty$ exactly to a statement about indices whose odd part has few divisors. This gives a conditional theorem whose hypothesis is far weaker than that of Kovač and Luca. We also show that one natural route to a negative answer needs primes p for which $\tau(2^p + 1)$ is bounded and $\omega(2^p - 1) = \exp\big((\log 2 + o(1)) \log p / \log\log p\big)$.

This leads to the constant $\beta_K = \limsup_{p:\, \tau(2^p+1) \le K} \log \omega(2^p - 1)\ \log\log p / \log p$ and the conjecture $\beta_K = 0$. We do not settle it. We prove that a disproof would settle two open problems at once. We give barrier theorems, in sketch form: axioms that capture the bounded-depth properties of the factorizations are consistent with $\beta_K = 0$ and with $\beta_K = \infty$. We give an "honest ideal" family showing that exact divisibility at the level of ideals is still not enough. We prove the function-field analogue, which holds uniformly in p. All numerical claims were re-checked against independent factor tables.

CONTENTS

1. Introduction 2
1.1. Erdős Problem #893 2
1.2. Mersenne numbers beside near-Wagstaff numbers 3
1.3. What is new, and what is not 3
2. Preliminaries 3

Part I. The doubling ratio 4
3. An exact identity 4
4. The sharp constant 3 4
5. Growth along chains and the density of good n 5
6. Exact reduction to thin indices 6

Part II. Prime factors of $2^p - 1$ when $2^p + 1$ has few divisors 7
7. Elementary structure 7
8. What a disproof, or finiteness, would mean 8
9. Barriers for soft and bounded-depth arguments 9
9.1. Soft properties of $2^k - 1$ 9

Date: November 2026.

2020 *Mathematics Subject Classification.* Primary 11A51, 11N25; Secondary 11R18, 11B83.

Key words and phrases. Mersenne numbers, divisor function, Wagstaff primes, cyclotomic polynomials, Erdős problems.

9.2. Bounded-depth axioms for M_p and a_p 9
10. A genuine obstruction: honest ideals with many prime factors 10
11. The function-field analogue is true 11
12. Exact-divisibility tools, and the single open estimate 11
13. AI disclosure 12
References 13

1. Introduction

1.1. **Erdős Problem #893.** Write τ for the divisor function, ω for the number of distinct prime factors, and

$$T(k) = \tau(2^k - 1), \qquad f(n) = \sum_{k \le n} T(k).$$

Erdős [5] asked whether $f(2n)/f(n)$ tends to a limit; this is Problem #893 in [4]. He remarked that f probably has no simple asymptotic formula because it grows too fast. Kovač and Luca [9] proved $\limsup_n f(2n)/f(n) = \infty$, so no finite limit exists. They also proved that $f(2n)/f(n) \to \infty$ under either of two conjectures. One of them is

$$\omega(\Phi_d(2)) \le 10 \log d \qquad \text{for all sufficiently large } d. \tag{1}$$

Whether $f(2n)/f(n) \to \infty$ unconditionally, equivalently whether $\liminf f(2n)/f(n) = \infty$, is open. To our knowledge no lower bound for the lim inf beyond the trivial $f(2n) > 2f(n)$ has been recorded. That trivial bound, and a lim inf ≥ 4 conditional on a different hypothesis, appear in an informal online report [15]. Part I proves the following.

Theorem A (Sharp constant; Theorems 4.4, 4.6)**.** *$f(2n) \ge 3f(n)$ for all $n \ge 1$, with equality exactly for $n \in \{1, 2, 4\}$. If $a \ge 4$ and $F_a = 2^{2^a} + 1$ is composite, then $f(2n) \ge \big(4 - \frac{16}{3 \cdot 2^{a-2}+4}\big) f(n)$ for $2^a \le n < 2^{a+1}$. In particular $f(2n) \ge \frac{24}{7} f(n)$ for $32 \le n < 2^{33}$. If F_a is composite for all large a, then* $\liminf f(2n)/f(n) \ge 4$.

Theorem B (Good n are everywhere; Theorem 5.2)**.** *Let $D(M) = \max_{m \le M} \tau(m)$ and $J(C) = \min\{J : D(2^J) - 2 > J \log_2 C\}$. For every $C > 1$ and every n, some $0 \le j < J(C)$ has $f(2^{j+1}n) > Cf(2^j n)$. Hence $\{n : f(2n) > Cf(n)\}$ has lower natural density at least $1/(2^{J(C)} - 1)$. Here $J(C) = O(\log\log C \cdot \log\log\log C)$.*

Theorem B reproves the theorem of Kovač and Luca, since it gives $\limsup = \infty$.

Theorem C (Exact reduction; Theorem 6.2, Corollary 6.3)**.** *Call k K-*thin *if the odd part of k has fewer than K divisors. Then $f(2n)/f(n) \to \infty$ if and only if, for every fixed K, $\sum_{k \le n,\ k\ K\text{-thin}} T(k) = o\big(f(2n) - f(n)\big)$. Consequently $f(2n)/f(n) \to \infty$ provided that, for every K, $\omega(\Phi_d(2)) = o\big(\psi(d)/\log^2 d\big)$ as $d \to \infty$ through K-thin d, where $\psi(x) = \max_{m \le x} \tau(m) = 2^{(1+o(1))\log x/\log\log x}$.*

This hypothesis is much weaker than (1). It allows $\omega(\Phi_d(2))$ as large as $\psi(d)^{1-o(1)}$, and it says nothing at all about indices that are not thin.

Theorem D (What a negative answer needs; Propositions 6.4, 6.5)**.** *If $f(2n) \le Cf(n)$ for infinitely many n, then for a fixed $K = K(C)$ there are K-thin $d \le n$ with $\omega(\Phi_d(2)) \ge (1 - o(1))\psi(n)/(K \log_2^2 n)$ for each such n. If moreover a single prime index $p \le n$ carries a fixed fraction $1/\lambda$ of $f(n)$, then $\tau(2^p + 1) \le C\lambda$ and $\omega(2^p - 1) \ge \exp\big((\log 2 + o(1))\log p/\log\log p\big)$ for infinitely many such p.*

1.2. **Mersenne numbers beside near-Wagstaff numbers.** Theorem D isolates a concrete arithmetic scenario. Let p be prime, $M_p = 2^p - 1$, and for $K \geq 4$ let

$$P_K = \{p : \ \tau(2^p + 1) \leq K\}, \qquad \beta_K = \limsup_{p \to \infty,\ p \in P_K} \frac{\log \omega(M_p) \cdot \log\log p}{\log p},$$

with $\beta_K := 0$ if P_K is finite. For $p > 3$, $\tau(2^p + 1) = 4$ exactly when $(2^p + 1)/3$ is a Wagstaff prime. Theorem D shows that $\beta_K \geq \log 2$ for some K is necessary for the "prime spike" route to a negative answer to Problem #893.

Conjecture 1.1. *$\beta_K = 0$ for every $K \geq 4$.*

Gillies' heuristic [6] (see also Wagstaff [14]) predicts that $\omega(M_p)$ is typically of order $\log p$. This would make Conjecture 1.1 true with room to spare. Unconditionally, nothing better than $\omega(M_p) \leq (\frac{\log 2}{2} + o(1))\, p/\log p$ seems to be known pointwise. We do not resolve Conjecture 1.1. Part II proves:

- a disproof would give infinitely many composite M_p (p prime) on which $(2^p + 1)/3$ has at most $K/2 - 1$ prime factors (Theorem 8.1);
- barrier theorems: families of fake factorizations satisfy every bounded-depth property of the true ones, yet give $\beta_K = 0$ or $\beta_K = \infty$ as desired, and even saturate the trivial constant $\frac{\log 2}{2}$ (Section 9);
- an "honest ideal" obstruction: elements $2^k - \zeta_p$ share every algebraic feature of $2 - \zeta_p$ used by class-group, Stickelberger, Galois and lattice methods, but have $\omega \geq \tau(k)$ (Theorem 10.1);
- the function-field analogue: over $\mathbb{F}_\ell[T]$, $\tau(a^p + 1) \leq K$ implies $\omega(a^p - 1) \leq \deg a\,(1 + \log_2 K)$, uniformly in p (Theorem 11.1);
- a divisor-lattice inequality and an incidence lemma that isolate the one estimate every method we tried needs (Section 12).

1.3. **What is new, and what is not.** In short, *neither problem is resolved here.* The theorem $\limsup f(2n)/f(n) = \infty$ is due to Kovač and Luca. The trivial bounds, Zsigmondy-type facts and all factor data are classical or tabulated. To our knowledge, the following are not in the literature: Theorems A–D, the barrier theorems, the honest-ideal obstruction, the function-field theorem and the divisor-lattice lemma. All of them are elementary, or use only classical analytic input (Siegel–Walfisz, Bombieri–Vinogradov).

Remark 1.2 (Provenance). The results were first obtained in two working notes written with extensive help from AI research agents. For this paper every proof given in full was re-derived and checked line by line. Every numerical claim was re-verified against independent factor tables [12]. Results proved only in sketch form are labelled as such.

2. Preliminaries

For odd d let $o(d) = \operatorname{ord}_d 2$. We use the following standard facts.

(P1) *Cyclotomic factorization.* $2^k - 1 = \prod_{d \mid k} \Phi_d(2)$, and $2^m + 1 = \prod_{e \mid 2m,\ e \nmid m} \Phi_e(2)$.

(P2) *Bang–Zsigmondy* [1, 17]. For $n \notin \{1, 6\}$ there is a prime q with $\operatorname{ord}_q 2 = n$ (a *primitive* prime for n). Primitive primes for distinct n are distinct. A primitive prime for n divides $2^k - 1$ if and only if $n \mid k$.

(P3) *Lifting the exponent.* If q is an odd prime with $q \mid 2^m - 1$, then $v_q(2^{mt} - 1) = v_q(2^m - 1) + v_q(t)$.

(P4) *Coprimality.* $\gcd(2^m - 1, 2^m + 1) = 1$, so $T(2m) = T(m)\,\tau(2^m + 1)$.

(P5) *Wigert* [16]. $\psi(x) := \max_{m \leq x} \tau(m) = 2^{(1+o(1))\log x/\log\log x}$.

Lemma 2.1 (Divisor gain)**.** *Let $m \mid k$. Suppose $2^k - 1$ has s distinct prime factors that do not divide $2^m - 1$. Then $T(k) \geq 2^s T(m)$. In particular, if E is a set of divisors e of k with $e \nmid m$, then $T(k) \geq 2^{|E \setminus \{1,6\}|} T(m)$.*

Proof. $\tau(N) = \prod_{q|N}(v_q(N)+1)$. Every prime factor of $N' = 2^m - 1$ divides $N = 2^k - 1$ to at least the same power. Each of the s new primes contributes a factor ≥ 2. For the second claim apply (P2). □

Lemma 2.2. *$T(k) \leq (k+1)^{\omega(2^k-1)}$ and $\omega(2^k-1) \leq \tau(k)\max_{d|k}\omega(\Phi_d(2))$.*

Proof. Each exponent satisfies $v_q(2^k-1) \leq \log_3 2^k < k$. The second bound follows from (P1). □

Lemma 2.3. *(a) $\tau(2^m+1) \geq 4$ unless m is a power of 2 or $m = 3$; also $\tau(9) = 3$. (b) If u is the odd part of m, then $\omega(2^m+1) \geq \tau(u) - 1$.*

Proof. (a) Suppose m has an odd divisor $u > 1$. Then $2^{m/u}+1$ is a proper divisor of 2^m+1 greater than 1. If $\tau(2^m+1) = 3$, then $2^m+1 = q^2$, so $(q-1)(q+1) = 2^m$, which forces $q = 3$ and $m = 3$. (b) Write $m = 2^c u$. By (P1) the indices $e \mid 2m$ with $e \nmid m$ are $e = 2^{c+1}w$ with $w \mid u$. There are $\tau(u)$ of them, and each except possibly $e = 6$ has a primitive prime by (P2). □

Part I. The doubling ratio

3. An exact identity

Theorem 3.1. *$f(n) = \sum_{d \text{ odd}} \lfloor n/o(d) \rfloor$. Hence $f(2n) - 2f(n) = \#\{d \text{ odd} : \{n/o(d)\} \geq \frac{1}{2}\}$, where $\{\cdot\}$ is the fractional part.*

Proof. An odd d divides $2^k - 1$ if and only if $o(d) \mid k$. So $f(n) = \sum_d \#\{k \leq n : o(d) \mid k\} = \sum_d \lfloor n/o(d) \rfloor$, where only finitely many d contribute. For real x, $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ is 1 if $\{x\} \geq \frac{1}{2}$ and 0 otherwise. □

The identity is elementary and probably folklore. It shows that $f(2n) > 2f(n)$ always, since $d = 3$ gives $\{n/2\} = \frac{1}{2}$ for odd n, and $d = 2^{n+1} - 1$ gives $o(d) = n+1 > n$. It also recasts the problem: do the moduli d whose order puts n in the upper half of a period outnumber $\sum_d \lfloor n/o(d) \rfloor$ by an unbounded factor?

4. The sharp constant 3

Write $F_i = 2^{2^i} + 1$. By (P4), $T(2^{a+1}) = \tau(F_a)\,T(2^a)$ and $T(2^a) = \prod_{i<a}\tau(F_i)$.

Lemma 4.1. *Let $r = 2^b u$ with $u > 1$ odd, and $C(r) = \sum_{i=0}^{b} T(2^i u)$. Then $C(r) \leq T(2r)/3$.*

Proof. By (P4), $T(2^{i+1}u) = T(2^i u)\,\tau(2^{2^i u}+1)$. Since $u > 1$, the exponent $2^i u$ is never a power of 2. By Lemma 2.3(a), each factor $\tau(2^{2^i u}+1)$ is ≥ 4, except the factor $\tau(9) = 3$ when $i = 0$, $u = 3$. If all factors are ≥ 4, then $T(2^i u) \leq 4^{-(b+1-i)}T(2r)$, and $C(r) \leq T(2r)\sum_{j\geq 1} 4^{-j} = T(2r)/3$. If $u = 3$, the same bound holds for $i \geq 1$, and $T(3) = T(6)/3 \leq T(2r)/(3 \cdot 4^b)$. Then $C(r) \leq T(2r)\big(\sum_{j=1}^{b} 4^{-j} + \frac{1}{3\cdot 4^b}\big) = T(2r)/3$. □

Lemma 4.2. *For $c \geq 1$, $T(3 \cdot 2^c) \geq \frac{3}{2}\,2^c\,T(2^c)$.*

Proof. Let $N = 2^{3\cdot 2^c} - 1$ and $N' = 2^{2^c} - 1$. The indices $3 \cdot 2^i$, $0 \leq i \leq c$, $i \neq 1$, divide $3 \cdot 2^c$ but not 2^c. Their c primitive primes (P2) are distinct, do not divide N', and differ from 3, because $\mathrm{ord}_3\, 2 = 2$. By (P3), $v_3(N') = v_3(4^{2^{c-1}} - 1) = 1$ and $v_3(N) = 1 + v_3(3 \cdot 2^{c-1}) = 2$. So the prime 3 contributes 3 to $\tau(N)$ against 2 to $\tau(N')$, and $\tau(N) \geq \tau(N') \cdot \frac{3}{2} \cdot 2^c$. □

Lemma 4.3. *$T(2^{i+1}) \geq 2T(2^i)$. Hence $\sum_{i<a} T(2^i) < 2T(2^{a-1})$ for $a \geq 1$.*

Proof. $\tau(F_i) \geq 2$. Then $\sum_{i<a} T(2^i) \leq T(2^{a-1})\sum_{j=0}^{a-1} 2^{-j} < 2T(2^{a-1})$. □

The decomposition. Let $R = \mathbb{Z} \cap (n/2, n]$. Every $m \le n$ is uniquely $m = r/2^j$ with $r \in R$ and $0 \le j \le v_2(r)$. Hence

$$f(n) = \sum_{r \in R} C(r), \qquad C(r) = \sum_{j=0}^{v_2(r)} T(r/2^j), \tag{2}$$

which agrees with Lemma 4.1 for $r = 2^b u$. The numbers $2r$, $r \in R$, are distinct elements of $(n, 2n]$. So $f(2n) \ge f(n) + \sum_{r \in R} T(2r)$, and for every λ,

$$f(2n) - (\lambda + 1) f(n) \;\ge\; \sum_{r \in R} \big(T(2r) - \lambda\, C(r) \big). \tag{3}$$

Theorem 4.4. *$f(2n) \ge 3f(n)$ for every $n \ge 1$, with equality exactly for $n \in \{1, 2, 4\}$.*

Proof. For $n \le 15$ this is a direct computation from $T(1), \dots, T(30) = 1, 2, 2, 4, 2, 6, 2, 8, 4, 8, 4, 24, 2, 8, 8, 16, 2, 32, 2, 48, 12, 16, 4, 96, 8, 8, 8, 64, 8, 96$. The ratios $f(2n)/f(n)$ for $n = 1, \dots, 15$ are 3, 3, 3.4, 3, 3.545, 3.941, 4.053, 3.741, 4.355, 4.744, 4.953, 4.672, 4.768, 5.208, 5.941.

Let $n \ge 16$ and $2^a \le n < 2^{a+1}$, so $a \ge 4$. Apply (3) with $\lambda = 2$. For $r \in R$, $r \ne 2^a$, Lemma 4.1 gives $T(2r) - 2C(r) \ge T(2r)/3 \ge 0$. For $r = 2^a$, Lemma 4.3 gives

$$T(2^{a+1}) - 2 \sum_{i \le a} T(2^i) > (\tau(F_a) - 2) T(2^a) - 4T(2^{a-1}) \ge -4T(2^{a-1}).$$

To compensate, let $r_0 = 3 \cdot 2^{a-2}$ if $n < 3 \cdot 2^{a-1}$, and $r_0 = 3 \cdot 2^{a-1}$ otherwise. In both cases $r_0 \in R$ and $r_0 \ne 2^a$. Also $2^{3 \cdot 2^{a-1}} - 1$ divides $2^{2r_0} - 1$, so $T(2r_0) \ge T(3 \cdot 2^{a-1})$. By Lemma 4.2, $\frac{1}{3} T(2r_0) \ge \frac{1}{3} T(3 \cdot 2^{a-1}) \ge 2^{a-2} T(2^{a-1}) \ge 4T(2^{a-1})$. The sum in (3) is therefore strictly positive. □

Remark 4.5 (Sharpness for soft methods; heuristic). The constant 3 cannot be improved by any argument that uses only the soft properties listed in Section 9.1. Consider a model in which $\Phi_{2^a}(2) = F_{a-1}$ is replaced by a product of many primes, so that $T^*(2^a)$ dominates $f^*(2^a)$, and F_a is "prime". Then $T^*(2^{a+1}) = 2T^*(2^a)$, so $f^*(2^{a+1})/f^*(2^a) \to 3$.

Theorem 4.6. *If $a \ge 4$ and F_a is composite, then $f(2n) \ge \big(4 - \frac{16}{3 \cdot 2^{a-2} + 4}\big) f(n)$ for all $n \in [2^a, 2^{a+1})$.*

Proof. Apply (3) with $\lambda = 3$. The terms with $r \ne 2^a$ are ≥ 0 by Lemma 4.1. Since $F_a \equiv 2 \pmod 3$ is not a square, compositeness gives $\tau(F_a) \ge 4$. With Lemma 4.3, the $r = 2^a$ term is then $\ge T(2^a) - 6T(2^{a-1}) \ge -4T(2^{a-1})$. Put $t = T(2^{a-1})/f(n)$; this gives $f(2n)/f(n) \ge 4 - 4t$. On the other hand $3 \cdot 2^{a-1} \le 2n$, so by Lemma 4.2 $f(2n) \ge T(3 \cdot 2^{a-1}) \ge 3 \cdot 2^{a-2} T(2^{a-1})$, that is, $f(2n)/f(n) \ge 3 \cdot 2^{a-2} t$. The larger of the two bounds is smallest where they meet, at $t = 4/(3 \cdot 2^{a-2} + 4)$. □

Corollary 4.7. *(a) $F_5, \dots, F_{32}$ are composite, so $f(2n) \ge \frac{24}{7} f(n)$ for $32 \le n < 2^{33}$. (b) If F_a is composite for all sufficiently large a, then $\liminf_n f(2n)/f(n) \ge 4$.*

Proof. (a) Take $a = 5$ in Theorem 4.6; the bound increases with a. (b) Every large n lies in some $[2^a, 2^{a+1})$, and the bound tends to 4 as $a \to \infty$. □

The value 4 in (b) is the value predicted by the naive "random integer" model, which Kovač and Luca show to be misleading. Exact data give $\min_{32 \le n \le 606} f(2n)/f(n) = 14.26$, computed from the table of $\tau(2^n - 1)$, $n \le 1212$, in [12].

5. Growth along chains and the density of good n

Proposition 5.1. *For all $M, n \ge 1$, $f(Mn) \ge 2^{D(M)-2} f(n)$, where $D(M) = \max_{m \le M} \tau(m)$.*

Proof. Choose $h \le M$ with $\tau(h) = D(M)$, and fix $m \le n$. The indices me with $e \mid h$, $e > 1$, divide hm but not m. There are $\tau(h) - 1$ of them, and at most one equals 6. By Lemma 2.1, $T(hm) \ge 2^{\tau(h)-2}T(m)$. The numbers hm, $m \le n$, are distinct and at most Mn. Summing over m gives the claim. □

Theorem 5.2. *Let $J = J(C) = \min\{J : D(2^J) - 2 > J \log_2 C\}$. For every n some $0 \le j < J$ satisfies $f(2^{j+1}n) > Cf(2^j n)$. Consequently $\{n : f(2n) > Cf(n)\}$ has lower natural density at least $1/(2^J - 1)$. This bound is optimal for the chain property alone.*

Proof. By Proposition 5.1 with $M = 2^J$, $\prod_{j<J} f(2^{j+1}n)/f(2^j n) = f(2^J n)/f(n) \ge 2^{D(2^J)-2} > C^J$. So some factor exceeds C.

For the density, group $n \le x$ by odd part m. The chain $m, 2m, 4m, \dots$ has $\lfloor \log_2(x/m) \rfloor + 1$ terms up to x. Every J consecutive terms contain a good one, so at least $\lfloor (\lfloor \log_2(x/m) \rfloor + 1)/J \rfloor = \#\{i \ge 0 : m2^{iJ+J-1} \le x\}$ terms are good. Summing over odd m gives $\sum_{i \ge 0} \frac{x}{2^{iJ+J}} + O(J \log x) = \frac{x}{2^J - 1} + O(J \log x)$. The set $\{n : v_2(n) \equiv J - 1 \pmod J\}$ meets every chain of J consecutive terms and has density exactly $1/(2^J - 1)$. □

By direct computation, $D(2^J)$ for $J = 7, 8, 12, 13, 20, 21$ equals $16, 20, 48, 64, 240, 288$. Hence $J(4) = 8$, $J(16) = 13$ and $J(10^4) = 21$. By (P5), $\log_2 D(2^J) = (1 + o(1))J \log 2/\log J$, so $J(C) = O(\log\log C \cdot \log\log\log C)$.

Corollary 5.3 (Kovač–Luca [9])**.** $\limsup_n f(2n)/f(n) = \infty$. *More strongly, $f(M(n)n)/f(n) \to \infty$ for every integer sequence $M(n) \to \infty$.*

The argument of [9] also uses highly composite numbers, through $f'(n) = \sum_{k \le n} 2^{\tau(k)}$. Theorem 5.2 adds the chain and density statements.

6. Exact reduction to thin indices

Definition 6.1. Fix $K \ge 2$. An integer k is *K-thin* if its odd part has fewer than K divisors. Every divisor of a K-thin number is K-thin.

Theorem 6.2. *For all n and all $K \ge 2$,*

$$\sum_{\substack{k \le n \\ k \text{ not } K\text{-thin}}} T(k) \;\le\; \frac{f(2n) - f(n)}{2^{K-1} - 1}.$$

Hence $f(2n)/f(n) \to \infty$ if and only if, for every fixed K, the T-mass of the K-thin $k \le n$ is $o\big(f(2n) - f(n)\big)$.

Proof. For $k \le n$ there is a unique $b \ge 1$ with $N = 2^b k \in (n, 2n]$. The map $k \mapsto (N, b)$ is a bijection onto $\{(N, b) : N \in (n, 2n],\ 1 \le b \le v_2(N)\}$. If k is not K-thin, then every $2^i k$ has the same odd part u with $\tau(u) \ge K$. By (P4) and Lemma 2.3(b), each doubling multiplies T by at least 2^{K-1}, so $T(N) \ge 2^{b(K-1)}T(k)$. Therefore

$$\sum_{k \text{ not thin}} T(k) \le \sum_{N \in (n, 2n]} T(N) \sum_{b \ge 1} 2^{-b(K-1)} = \frac{f(2n) - f(n)}{2^{K-1} - 1}.$$

For the equivalence: if the thin mass is $o(f(2n) - f(n))$ for every K, then $\limsup f(n)/(f(2n) - f(n)) \le 1/(2^{K-1} - 1)$ for every K, so the ratio tends to infinity. The converse is trivial, since the thin mass is at most $f(n)$. □

Corollary 6.3 (Conditional divergence)**.** *Suppose that for every $K \ge 2$,*

$$\omega(\Phi_d(2)) = o\left(\frac{\psi(d)}{\log^2 d}\right) \qquad (d \to \infty,\ d \text{ } K\text{-thin}). \tag{4}$$

Then $f(2n)/f(n) \to \infty$. In particular this holds under (1), or under $\omega(\Phi_d(2)) \le \psi(d)^{1-\delta}$ for some $\delta > 0$ and all large d.

Proof. Fix K and a K-thin $k \le n$. Then $\tau(k) < K(\log_2 n + 1)$, and every divisor d of k is K-thin. We claim that $\max_{d|k} \omega(\Phi_d(2)) = o(\psi(n)/\log^2 n)$, uniformly in $k \le n$. Bounded d contribute $O_K(1)$. If $d \ge \sqrt{n}$, then $\log d \ge \frac{1}{2}\log n$ and $\psi(d) \le \psi(n)$, so (4) gives the claim, uniformly because $d \ge \sqrt{n} \to \infty$. If $d < \sqrt{n}$, then (4) gives $\omega(\Phi_d(2)) \le \psi(d) + O_K(1) \le \psi(\sqrt{n}) + O_K(1) = \psi(n)^{1/2+o(1)}$. This is $o(\psi(n)/\log^2 n)$ because $\psi(n)$ grows faster than any power of $\log n$. By Lemma 2.2,

$$\log_2 T(k) \le \log_2(n+1) \cdot K(\log_2 n + 1) \cdot o\big(\psi(n)/\log^2 n\big) = o(\psi(n)).$$

So the thin mass is at most $n\, 2^{o(\psi(n))} = 2^{o(\psi(n))}$. On the other hand, take $m^* \le n$ with $\tau(m^*) = \psi(n)$ and let N be the multiple $2^j m^*$ that lies in $(n, 2n]$. Since $2^{m^*} - 1 \mid 2^N - 1$, and by (P2), $f(2n) - f(n) \ge T(N) \ge T(m^*) \ge 2^{\psi(n)-2}$. Theorem 6.2 now applies. The two particular cases imply (4) because $\log d$ and $\psi(d)^{1-\delta}$ are both $o(\psi(d)/\log^2 d)$. □

Proposition 6.4 (What a negative answer needs)**.** *Suppose $f(2n) \le Cf(n)$ for infinitely many n, and fix K with $2^{K-1} - 1 > 2C$. Then for each such n there are a K-thin $k \le n$ with $\log_2 T(k) \ge \psi(n) - 3 - \log_2 n$, and a K-thin $d \mid k$ with*

$$\omega(\Phi_d(2)) \;\ge\; \frac{\psi(n) - 3 - \log_2 n}{K(\log_2 n + 1)\log_2(n+1)}.$$

Proof. By Theorem 6.2, the non-thin mass is at most $(f(2n) - f(n))/(2^{K-1} - 1) < f(n)/2$. So the thin mass is at least $f(n)/2 \ge 2^{\psi(n)-3}$, using $f(n) \ge T(m^*) \ge 2^{\psi(n)-2}$. There are at most n thin $k \le n$, which gives the first claim. The second follows from Lemma 2.2 and $\tau(k) < K(\log_2 n + 1)$. □

Proposition 6.5 (Prime spikes force near-Wagstaff Mersenne numbers)**.** *Let $C, \lambda \ge 1$. Suppose there are infinitely many n with $f(2n) \le Cf(n)$ for which some prime $p \le n$ satisfies $T(p) \ge f(n)/\lambda$. Then $P_{C\lambda}$ is infinite and $\beta_{C\lambda} \ge \log 2$.*

Proof. Since $2p \le 2n$, (P4) gives $\tau(2^p + 1) = T(2p)/T(p) \le f(2n)/T(p) \le C\lambda$, so $p \in P_{C\lambda}$. As $n \to \infty$ we have $T(p) \ge f(n)/\lambda \to \infty$, so infinitely many distinct p occur. Next, $\log_2 T(p) \ge \log_2 f(n) - \log_2 \lambda \ge \psi(n) - 2 - \log_2 \lambda \ge \psi(p) - 2 - \log_2 \lambda$. By Lemma 2.2, $\omega(M_p) \ge (\psi(p) - 2 - \log_2 \lambda)/\log_2(p+1)$. Hence $\log \omega(M_p) \ge (\log 2 + o(1)) \log p / \log\log p$ by (P5). □

So Conjecture 1.1 would rule out the simplest mechanism for a bounded ratio: a prime index carrying a fixed share of $f(n)$. The soft-property models of Theorem 9.1 realize exactly this mechanism.

Part II. Prime factors of $2^p - 1$ when $2^p + 1$ has few divisors

7. Elementary structure

Throughout, $p \ge 5$ is prime, $a_p = \Phi_{2p}(2) = (2^p + 1)/3$, $\zeta = \zeta_p$ and $\mathcal{O} = \mathbb{Z}[\zeta]$.

Lemma 7.1. *$3 \parallel 2^p + 1$, so $\tau(2^p + 1) = 2\tau(a_p)$.*

Proof. $\operatorname{ord}_9 2 = 6$ and p is odd and prime to 3, so $2^p + 1 \equiv 3$ or $6 \pmod 9$. □

Lemma 7.2. *(a) $a_p \equiv 3 \pmod 8$. (b) Every prime $Q \mid a_p$ has $\operatorname{ord}_Q 2 = 2p$, so $Q \equiv 1 \pmod{2p}$. (c) $Q \equiv 3 \pmod 8$ if $(Q-1)/2p$ is odd, and $Q \equiv 1 \pmod 8$ otherwise. (d) The number of prime factors $\equiv 3 \pmod 8$ of a_p, counted with multiplicity, is odd.*

Proof. $2^p \equiv 8 \pmod{24}$ gives (a). For (b): $2^p \equiv -1 \pmod Q$ and $Q \ne 3$ by Lemma 7.1. For (c), Euler's criterion gives $(\frac{2}{Q}) \equiv (2^p)^{(Q-1)/2p} \equiv (-1)^{(Q-1)/2p}$. Combine this with the parity of $(Q-1)/2 = p \cdot \frac{Q-1}{2p}$, which fixes $Q \bmod 4$. (d) follows from (a), since $3^k \equiv 3 \pmod 8$ if and only if k is odd. □

Corollary 7.3. *a_p is never a square. Hence $4 \mid \tau(2^p+1)$ and $P_K = P_{4\lfloor K/4 \rfloor}$. In particular $P_6 = P_7 = P_4$.*

Lemma 7.4 (Disjoint fibres)**.** *Prime factors q of M_p have $\operatorname{ord}_q 2 = p$, and prime factors Q of a_p have $\operatorname{ord}_Q 2 = 2p$. So no prime divides two members of $\{M_p\} \cup \{a_p\}$, and no covering-congruence argument can force a_p to be composite.*

Lemma 7.5 (Trivial bound)**.** $\omega(M_p) \le (\frac{\log 2}{2} + o(1))\, p/\log p$.

Proof. Let $q_1 < \cdots < q_k$ be the prime factors. They are $\equiv 1 \pmod{2p}$, so $q_j > 2pj$ and $(2p)^k k! < 2^p$. We may assume $k \ge p/\log^2 p$. Then $\log k \ge \log p - 2\log\log p$ and $k! \ge (k/e)^k$ give $k(2\log p - 2\log\log p + \log 2 - 1) < p\log 2$. □

Using that q lies in two classes modulo $8p$ and the Montgomery–Vaughan form of the Brun–Titchmarsh inequality [11], one gets the second-order form $\omega(M_p) \le \frac{\log 2}{2}\, p/(\log p - 1.0298 + o(1))$. The constant $\frac{\log 2}{2}$ is unchanged.

Remark 7.6 (Scale of the problem). The quantity in β_K lies in $[0, (1+o(1))\log\log p]$. So even $\beta_K < \infty$ requires $\omega(M_p) \le p^{O(1/\log\log p)}$ on P_K, far beyond Lemma 7.5. At most $p\log 2/\log X$ prime factors exceed X. So the range that must be controlled is $q \in [p^{1+o(1)}, 2^{p^{1-o(1)}}]$, not a range with a fixed ε.

8. What a disproof, or finiteness, would mean

Theorem 8.1. *Suppose $\beta_K > 0$ and $0 < c < \beta_K$. Then there are infinitely many primes p such that $\Omega(a_p) \le K/2 - 1$, $\omega(a_p) \le \log_2(K/2)$, and $\omega(M_p) \ge \exp(c\log p/\log\log p)$. In particular these M_p are composite.*

Proof. $\beta_K > 0$ forces P_K to be infinite. Apply $\tau(n) \ge \Omega(n)+1$ and $\tau(n) \ge 2^{\omega(n)}$ to $\tau(a_p) \le K/2$. □

The infinitude of composite M_p with p prime is open (Guy [7], A3). A disproof would settle it together with an almost-prime statement for $(2^p+1)/3$ on the same set of p.

Proposition 8.2. *P_K is finite for every K if and only if $\Omega(a_p) \to \infty$. In particular, finiteness of P_4 means that there are only finitely many Wagstaff primes.*

This is believed false. The Lenstra–Pomerance–Wagstaff-type heuristic (see [2]) predicts $\asymp \log x$ Wagstaff exponents $p \le x$.

Proposition 8.3 (No fixed-family certificate)**.** *Let $f_1, \ldots, f_r \in \mathbb{Z}[x]$ be nonconstant. There is a set of primes p of positive relative density on which no $f_j(p)$ is a divisor of a_p other than ± 1, and likewise for M_p.*

Proof. If $f_j = c\,x^k$, then $f_j(p) = cp^k$ is never such a divisor, because every prime factor of $a_p M_p$ is at least $2p+1$. Otherwise write $f_j = x^k g_j$ with $g_j(0) \ne 0$ and g_j nonconstant. By Schur's theorem infinitely many primes ℓ divide some value $g_j(r)$. Choose such odd primes ℓ_j, distinct and not dividing $g_j(0)$, with residues r_j. Then $r_j \not\equiv 0 \pmod{\ell_j}$. By the Chinese remainder theorem and Dirichlet's theorem, a positive proportion of primes satisfy $p \equiv r_j \pmod{\ell_j}$ for all j. For these p we have $\ell_j \mid f_j(p)$, while $\ell_j < 2p+1$ for large p. So $f_j(p)$ divides neither a_p nor M_p, unless $f_j(p) = 0$, which happens for finitely many p. □

The working note's proof of Proposition 8.3 omitted the case $f_j = cx^k$, in which no nonzero residue works; the repair is the first sentence above.

9. Barriers for soft and bounded-depth arguments

The results in this section are *meta-theorems*. Each lists properties of the true factorizations and builds fake factorizations with all of them but with opposite behaviour. Any argument that uses only the listed properties therefore proves nothing about the question. The constructions are explicit, but they rely on the Siegel–Walfisz or Bombieri–Vinogradov theorems and are ineffective. Full verifications are in the working notes. Here we give statements and the key steps; these results are *proved in sketch form only.*

9.1. Soft properties of $2^k - 1$.

The *soft properties* are the following:

- the cyclotomic factorization and $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)} - 1$;
- a primitive prime $\equiv 1 \pmod d$ for every index $d \neq 1, 6$;
- $T(2k) = T(k)\tau(2^k+1)$ and lifting-the-exponent multiplicities;
- the size $\log \Phi_d(2) \approx \varphi(d) \log 2$ and Aurifeuillian splitting;
- the rule $q \equiv \pm 1 \pmod 8$ if and only if $2 \mid (q-1)/\operatorname{ord}_q 2$, and power-residue rules of bounded depth;
- Stewart's lower bound for the largest prime factor [13];
- Brun–Titchmarsh and averaged sieve bounds.

Theorem 9.1 (Models for the doubling problem; sketch)**.** *There are "fake" factorizations, in which each $\Phi_d(2)$ is replaced by a product of genuine primes $\equiv 1 \pmod d$ satisfying all soft properties, of the following kind. They have one prime per generic index (two at Aurifeuillian indices). Along a sparse sequence of primes ℓ_j, index ℓ_j carries $W_j \geq D(3\ell_j) + O(\log \ell_j)$ primes and index $2\ell_j$ carries one. For these models $f^*(2\ell_j)/f^*(\ell_j) \to 5$, so $\liminf f^*(2n)/f^*(n) < \infty$. Other models, with every $\omega(\Phi_d^*(2)) \leq d^{o(1)}$, have $f^*(2n)/f^*(n) \to \infty$.*

Key steps. In $(\ell_j, 2\ell_j]$ the only multiples of ℓ_j are ℓ_j and $2\ell_j$, so $T^*(\ell_j) = 2^{W_j}$ and $T^*(2\ell_j) = 4T^*(\ell_j)$. Every other $k \leq 2\ell_j$ has $\log_2 T^*(k) \leq D(2\ell_j) + \sum_{i<j} W_i + O(\log \ell_j)$. When the ℓ_j grow fast, this is negligible against W_j. Then $f^*(\ell_j) \sim T^*(\ell_j)$ and $f^*(2\ell_j) \sim 5T^*(\ell_j)$. Size is compatible because $W_j \ll \ell_j/\log \ell_j$ primes $\equiv 1 \pmod{\ell_j}$ fit inside 2^{ℓ_j}. Primes in the required residue classes, of modulus $O(d)$, exist by Siegel–Walfisz. □

The model at index $2\ell_j$ has $\Phi^*_{2\ell_j}(2)$ "prime", that is, $\tau(2^{\ell_j}+1) = 4$, and $\omega(M^*_{\ell_j})$ is huge. This is exactly the near-Wagstaff scenario of Proposition 6.5. The one property such models cannot imitate is exact divisibility: $q \mid 2^p - 1$ if and only if 2 is a $\frac{q-1}{p}$-th power residue modulo q, a residue condition of unbounded depth.

9.2. Bounded-depth axioms for M_p and a_p.

Definition 9.2 (Axioms $\mathrm{Ax}_{D,J}$)**.** A family assigns to each prime $p \geq 5$ multisets of primes $F(p)$ (a fake M_p) and $G(p)$ (a fake a_p) such that:

- (A1) $\prod F(p)$ has p bits and $\prod G(p)$ has $p-1$ bits;
- (A2) every element is $\equiv 1 \pmod{2p}$;
- (A3) the mod-8 rules of Lemma 7.2 and $q \equiv \pm 1 \pmod 8$ for F-primes hold;
- (A4) $\prod F \equiv M_p$ and $\prod G \equiv a_p \pmod{8p^J}$; this includes the Fermat-quotient congruence;
- (A5) for $d \leq D$ with $d \mid q-1$: $2^{(q-1)/d} \equiv 1 \pmod q$ if and only if $d \mid (q-1)/p$ for F-primes, or $d \mid (q-1)/2p$ for G-primes;
- (A6) fibres are disjoint, and $3 \notin G(p)$;
- (A7) repeated primes are Wieferich-type;
- (A8) Brun–Titchmarsh holds, and (A9) Stewart's bound holds.

Theorem 9.3 (Barrier; sketch, modulo Siegel–Walfisz)**.** *The true factorizations satisfy every $\mathrm{Ax}_{D,J}$. For every D, J there are families satisfying $\mathrm{Ax}_{D,J}$ with $|G(p)| = 1$ for all large p, that*

is, with "$\tau(2^p+1)=4$", and with either (a) $|F(p)|=1$ for all large p, so $\beta_K=0$; or (b) $|F(p)|\geq p^{1-\delta}/4-1$ for all large p, so $\beta_K=\infty$. A diagonal family satisfies all $\mathrm{Ax}_{D,J}$ at once, eventually in p.

Construction. $F(p)$ consists of r primes (r even) with $q_i\equiv 1 \pmod{2p}$, $q_i\equiv 7 \pmod 8$, and $q_i\equiv 2 \pmod \ell$ for every odd prime $\ell\leq D$, chosen up to $\exp(p^\delta)$. A filler prime fixes (A1) and (A4); because r is even, the filler can be taken $\equiv 7 \pmod 8$. The condition $q\equiv 2 \pmod\ell$ means that the only $d\leq D$ dividing $q-1$ are $d\in\{1,2\}$, so (A5) reduces to the quadratic character of 2, which (A3) already fixes. $G(p)$ is a single prime in the right classes. The moduli are at most a fixed power of $\log x$, so Siegel–Walfisz applies uniformly. □

Proposition 9.4 (Sharpness)**.** *(A4) with $8p^J>2^{p-1}$ forces $\prod F(p)=M_p$, and adding exact divisibility $\prod F\mid M_p$ recovers the truth. So fake models die only at p-adic depth $J\gtrsim p\log 2/\log p$, or at residue depth $(q-1)/p$, which is unbounded.*

Lemma 9.5 (Mod-24 limit of the construction)**.** *No product of primes that are all $\equiv 7 \pmod 8$ and $\equiv 2 \pmod 3$ is $\equiv M_p \pmod{24}$.*

Proof. $M_p\equiv 7 \pmod 8$ needs an odd number of factors, and $M_p\equiv 1 \pmod 3$ needs an even number. □

So adding product congruences modulo 3 forces genuine Chebotarev conditions in non-abelian Kummer fields such as $\mathbb{Q}(\zeta_3,2^{1/3})$. The construction above does not handle these; that extension is *unproved*.

Theorem 9.6 (Barrier for the constant; sketch, using Bombieri–Vinogradov and Heath-Brown's Linnik bound [8])**.** *Fix $\varepsilon\in(0,\frac{1}{10})$ and $D\geq 3$. For all primes p outside a set of relative density zero, there are a set Q'_p of at least $(\frac{\log 2}{2}-\varepsilon)\,p/\log p$ primes in $[p^2,p^2(\log p)^{20}]$ and a prime r with the following properties. Each of them is $\equiv 1 \pmod{2p}$, $\equiv 7 \pmod 8$, and $\not\equiv 1 \pmod\ell$ for odd $\ell\leq D$. The product $N'=r\prod Q'_p$ satisfies $N'<M_p$ and $N'\equiv M_p \pmod{2^i p^j}$ for all $i\leq \varepsilon p/12$, $j\leq \varepsilon p/(12\log p)$. Brun–Titchmarsh and Stewart's bound hold for them. So no argument that uses only these properties can improve the constant in Lemma 7.5.*

Any improvement of $\frac{\log 2}{2}$ is equivalent to bounding the product of the $q\mid M_p$ in $[p^{2-\eta},p^{2+\eta}]$ by $2^{(1-\delta)p}$. This is a concentration lemma proved in the working notes. This window is Hooley's middle range in Artin's conjecture.

10. A genuine obstruction: honest ideals with many prime factors

The fake models violate exact divisibility. The next family does not: it consists of genuine elements of $\mathcal{O}$.

Theorem 10.1. *Let $p\geq 5$, $p\nmid k$, and $\alpha_k=2^k-\zeta$. Then:*

1. *$\mathrm{N}(\alpha_k)=\Phi_p(2^k)=\prod_{d\mid k}\Phi_{dp}(2)$ and $\mathcal{O}/(\alpha_k)\cong\mathbb{Z}/\Phi_p(2^k)$;*
2. *for every prime $q\neq p$ dividing $\mathrm{N}(\alpha_k)$, 2^k has order exactly p modulo q, and $(\alpha_k)=\prod_q(q,\zeta-2^k)^{v_q(\mathrm{N}\,\alpha_k)}$, a product of degree-one primes, one above each q;*
3. *$\omega(\alpha_k)\geq\tau(k)$. Choosing $k<p$ with $\tau(k)$ maximal gives $\log\omega(\alpha_k)\geq(\log 2+o(1))\log p/\log\log p$.*

Proof. (1) $\mathrm{N}(2^k-\zeta)=\prod_a(2^k-\zeta^a)=\Phi_p(2^k)$. Since $p\nmid k$, $\Phi_p(x^k)=\prod_{d\mid k}\Phi_{dp}(x)$. Also $\mathcal{O}/(2^k-\zeta)\cong\mathbb{Z}[x]/(\Phi_p(x),x-2^k)\cong\mathbb{Z}/\Phi_p(2^k)$. (2) If $q\mid\Phi_p(2^k)$ and $2^k\equiv 1 \pmod q$, then $\Phi_p(2^k)\equiv p \pmod q$, so $q=p$. Hence 2^k has order p. Because the quotient is cyclic, exactly one prime above q divides (α_k), namely $(q,\zeta-2^k)$, to the exponent $v_q(\mathrm{N}\,\alpha_k)$. (3) Each $\Phi_{dp}(2)$, $d\mid k$, has a primitive prime (P2), since $dp\notin\{1,6\}$. Distinct d give distinct primes. Finally, (P5) gives $\max_{k<p}\tau(k)=2^{(1+o(1))\log p/\log\log p}$. □

A direct computation for $p = 13$, $k = 12$ gives $\omega(\alpha_{12}) = 13 \geq \tau(12) = 6$.

Remark 10.2. The structural identities used by class-group, Stickelberger, Galois-orbit and successive-minima approaches hold for α_k exactly as for $\alpha_1 = 2 - \zeta$. Examples are the sub-ideal dictionary $\mathcal{O}/I \cong \mathbb{Z}/d_I$, free Galois orbits of the primes, and Stickelberger relations. The only datum separating $2 - \zeta$ from α_k is quantitative: the house is 3 against $2^k + 1$, and $\log \mathrm{N} \approx p \log 2$ against $kp \log 2$. So a proof of Conjecture 1.1 must use the *size* of the generator in a way stronger than the norm bound. One caveat: α_k does not satisfy the analogue of $p \in P_K$, since $\mathrm{N}(2^k + \zeta)$ has at least $\tau(\text{odd part of } k)$ prime factors. The coupling with $2 + \zeta$ enters the methods tested below only through the residue $2 + \zeta \equiv 4$, which needs no factorization.

11. The function-field analogue is true

For $g \in \mathbb{F}_\ell[T]$, $\tau(g)$ counts monic divisors and $\omega(g)$ counts distinct monic irreducible factors.

Theorem 11.1. *Let ℓ be an odd prime, $a \in \mathbb{F}_\ell[T]$ of degree $d \geq 1$, $p \neq \ell$ an odd prime, and $f = \mathrm{ord}_p\, \ell$. Then*

(1) $\omega(a^p - 1) \leq d\,(1 + (p-1)/f)$;
(2) $\omega(a^p + 1) \geq (p-1)/f$;
(3) *if $\tau(a^p + 1) \leq K$, then $\omega(a^p - 1) \leq d\,(1 + \log_2 K)$, uniformly in p.*

Proof. Let $\mu_p \subset \mathbb{F}_{\ell^f}$ be the p-th roots of unity. The Frobenius $x \mapsto x^\ell$ acts on $\mu_p \setminus \{1\}$ with $(p-1)/f$ orbits of size f. For $\eta \neq 1$ let $\mathrm{N}(a - \eta) = \prod_\sigma (a - \eta^\sigma) \in \mathbb{F}_\ell[T]$, the product over $\mathrm{Gal}(\mathbb{F}_{\ell^f}/\mathbb{F}_\ell)$.

(1) $a^p - 1 = (a-1) \prod_{\text{orbits}} \mathrm{N}(a - \eta)$. At most d primes divide $a - 1$. If an irreducible π divides $a^p - 1$ but not $a - 1$, then a has order p in $(\mathbb{F}_\ell[T]/\pi)^\times$, a cyclic group of order $\ell^{\deg \pi} - 1$. So $f \mid \deg \pi$. Each $\mathrm{N}(a - \eta)$ has degree df, so it has at most d distinct irreducible factors of degree $\geq f$.

(2) $a^p + 1 = \prod_{\eta \in \mu_p} (a + \eta)$, since p is odd. The norms $\mathrm{N}(a + \eta)$ over distinct orbits are nonconstant. They are pairwise coprime: a common prime factor in $\mathbb{F}_{\ell^f}[T]$ of $a + \eta^\sigma$ and $a + \eta'^{\sigma'}$ would divide the nonzero constant $\eta^\sigma - \eta'^{\sigma'}$.

(3) $2^{(p-1)/f} \leq 2^{\omega(a^p+1)} \leq \tau(a^p + 1) \leq K$, so $(p-1)/f \leq \log_2 K$; now apply (1). □

Remark 11.2 (Why it does not transfer). The constant-field Frobenius order f controls both $a^p - 1$ and $a^p + 1$. Over $\mathbb{Z}$, every prime above $q \mid M_p$ and above $Q \mid a_p$ has residue degree 1 in $\mathbb{Q}(\zeta_p)$, so no shared invariant exists. Over $\mathbb{Z}$, a uniform bound $\omega(M_p) \leq C(K)$ on P_K would be the literal analogue of (3). The data already strain it: $p = 43, 79, 191, 701$ have a_p prime and $\omega(M_p) = 3, 3, 5, 8$.

12. Exact-divisibility tools, and the single open estimate

Lemma 12.1 (Incidence/norm lemma)**.** *For $q \mid M_p$, the primes of $\mathcal{O}$ above q are $\mathfrak{q}_{q,j} = (q, \zeta - 2^j)$, $1 \leq j \leq p - 1$. They are distinct, of degree 1, and $v_{\mathfrak{q}_{q,j}}(\zeta - 2^j) = v_q(M_p)$. Consequently, for $P \in \mathbb{Z}[x]$ with $\Phi_p \nmid P$,*

$$\sum_{j=1}^{p-1} \log \gcd\big(P(2^j), M_p\big) \;\leq\; \log |\,\mathrm{N}(P(\zeta))| \;\leq\; (p-1) \log \|P\|_1.$$

Proof. 2 has order p modulo q, so the roots of Φ_p modulo q are 2^j, $1 \leq j \leq p - 1$, and q splits completely. For $1 \leq j \leq p - 1$, $\mathrm{N}(2^j - \zeta) = \Phi_p(2^j)$. By (P3), $v_q(\Phi_p(2^j)) = v_q(2^{jp} - 1) = v_q(M_p) + v_q(j) = v_q(M_p)$. The quotient $\mathcal{O}/(2^j - \zeta)$ is cyclic, so only $\mathfrak{q}_{q,j}$ above q divides $(2^j - \zeta)$, to exponent $v_q(M_p)$. Hence $P(\zeta) \equiv P(2^j) \pmod{\mathfrak{q}_{q,j}^{v_q(M_p)}}$, and $v_{\mathfrak{q}_{q,j}}(P(\zeta)) \geq \min(v_q(P(2^j)), v_q(M_p))$. The ideals $\mathfrak{q}_{q,j}$ are distinct of norm q, which gives the first inequality. The second is $|P(\zeta^a)| \leq \|P\|_1$. □

In the fake models this fails: for a fake q, $(q, \zeta - 2) = (1)$. It is the basic exact-divisibility input. Lattice-existence (Siegel, Minkowski) arguments cannot extract a bound on $|S|$ from it, because both sides agree up to factors independent of $|S|$.

Lemma 12.2 (Divisor lattices)**.** *Let $0 < \theta \le 1$ and $s > N^\theta$ with $\gcd(s, N) = 1$. Let a nonempty set D' of divisors of N meet R residue classes modulo s. Then $\theta\,\omega(N) < 1 + \log_2 R + \log_2(\tau(N)/|D'|)$.*

Proof. Let $t = \lfloor \theta\,\omega(N) \rfloor$ and let A be the product of the t smallest prime-power parts of N. Then $A \le N^{t/\omega(N)} \le N^\theta < s$. Write $N = AB$. Every divisor is ab with $a \mid A$, $b \mid B$. If $ab \equiv a'b \pmod s$, then $a \equiv a'$ because b is invertible modulo s, so $a = a'$ because $a, a' \le A < s$. Hence each class contains at most $\tau(B) = \tau(N)/\tau(A) \le \tau(N)/2^t$ divisors. So $|D'| \le R\,\tau(N)/2^t$, and $\theta\,\omega(N) < t + 1$. □

A hypothesis that all divisors of M_p lie in few classes modulo some $s \ge M_p^{1/4+\varepsilon}$ is what Lenstra's theorem [10] or Coppersmith–Howgrave-Graham–Nagaraj [3] would need. By Lemma 12.2, that hypothesis already gives the conclusion up to a factor 4 in ω. So the input is the problem itself.

Proposition 12.3 (p-adic constraints are void)**.** *Write the prime factors of M_p, with multiplicity $w = \Omega(M_p)$, as $q_i = 1 + 2pm_i$. Modulo p^J the full constraint is $\prod_i (1 + 2pm_i) \equiv M_p \pmod{p^{J+1}}$, one equation in the cyclic group $(1 + p\mathbb{Z})/(1 + p^{J+1}\mathbb{Z})$ of order p^J. Its solution set in $(\mathbb{Z}/p^J)^w$ has exactly $p^{J(w-1)}$ elements, a density of p^{-J} for every w. So no number of factors is ever excluded, and the elementary symmetric functions of the m_i are not individually determined.*

Proof. $m \mapsto 1 + 2pm$ is a bijection from $\mathbb{Z}/p^J$ onto that group, and $M_p \equiv 1 \pmod p$. □

Further tests. The working notes test four more families of methods, each with a stated point of failure.

- *Reciprocity.* Every power-reciprocity law between $2 - \zeta$ and $2 + \zeta$ reduces to local symbols needing neither factorization. For $q \mid M_p$ and $n \mid q - 1$ with $p \nmid n$, 2 is automatically an n-th power.
- *Subgroup bounds.* $\langle 2 \rangle \subset \mathbb{F}_q^\times$ is *the* subgroup of order p. So Stepanov, Heath-Brown–Konyagin and Bourgain–Glibichuk–Konyagin bounds are identical for every $q \equiv 1 \pmod{2p}$.
- *Sparse multiples.* Pigeonhole forces $d \mid \sum_{i \le 2T} \pm 2^{e_i}$ for every odd $d < \binom{p}{T}$. The needed uniform bound on $\gcd(u, M_p)$ for sparse u is false. For example, $\gcd(2 + 2^{30} - 2^{11} - 2^{12}, M_{43}) = 9719$ with $43 \in P_4$.
- *Kummer–Chebotarev.* $q \mid M_p$ if and only if q splits completely in $\mathbb{Q}(\zeta_m, 2^{1/m})$, $m = (q-1)/p$. The degree grows like $(q/p)^2$, and each m has one candidate q.

The single open estimate. Every route above stops at the following statement:

$$\#\{q \le 2^p : \ q \equiv 1 \ (2p),\ 2^p \equiv 1 \ (q)\} \le \exp\big(o(\log p/\log\log p)\big) \quad (p \in P_K \text{ or all } p). \tag{5}$$

The best known bound is $(\frac{\log 2}{2} + o(1))p/\log p$. We know of no pointwise bound that is even $o(p/\log p)$. By Section 9 and Theorem 10.1, a proof of (5) must use exact divisibility of unbounded depth *and* the archimedean smallness of $2 - \zeta_p$ beyond its norm.

13. AI disclosure

The author reports that the results collected here originated in two working documents, *Mersenne Doubling Barrier* and a research note on $\omega(2^p - 1)$, produced by an AI model (Anthropic's Claude), which was subsequently used to audit those documents: checking the proofs, correcting a numerical claim (now $\omega(2^{397} - 1) = 9$), comparing each result against the published literature, and re-verifying all numerical data with an accompanying script. The model also produced the exposition and the LaTeX manuscript. This disclosure describes the provenance of the work; it does not supersede the attribution of previously published results and methods cited in the paper, including those of Kovač and Luca, nor does it constitute independent human verification of the proofs. The human author retains responsibility for the correctness of the mathematical claims, the accuracy of this disclosure, and the decision to submit or disseminate the work.

References

[1] A. S. Bang, Taltheoretiske undersøgelser, *Tidsskrift Math.* 4 (1886), 70–80, 130–137.

[2] P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr., The new Mersenne conjecture, *Amer. Math. Monthly* 96 (1989), 125–128.

[3] D. Coppersmith, N. Howgrave-Graham and S. V. Nagaraj, Divisors in residue classes, constructively, *Math. Comp.* 77 (2008), 531–545.

[4] T. F. Bloom, Erdős Problems, Problem #893, `https://www.erdosproblems.com/893`.

[5] P. Erdős, Some of my new and almost new problems and results in combinatorial number theory, in *Number Theory (Eger, 1996)*, de Gruyter, 1998, 169–180.

[6] D. B. Gillies, Three new Mersenne primes and a statistical theory, *Math. Comp.* 18 (1964), 93–97.

[7] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, 2004.

[8] D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, *Proc. London Math. Soc.* 64 (1992), 265–338.

[9] V. Kovač and F. Luca, On the number of divisors of Mersenne numbers, arXiv:2506.04883 (2025); *Experimental Mathematics* (2026), doi:10.1080/10586458.2026.2636060.

[10] H. W. Lenstra, Jr., Divisors in residue classes, *Math. Comp.* 42 (1984), 331–340.

[11] H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* 20 (1973), 119–134.

[12] OEIS Foundation, The On-Line Encyclopedia of Integer Sequences, sequences A000978, A046798, A046800, A046801, A085021, `https://oeis.org`.

[13] C. L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Math.* 211 (2013), 291–314.

[14] S. S. Wagstaff, Jr., Divisors of Mersenne numbers, *Math. Comp.* 40 (1983), 385–397.

[15] P. White, Erdős #893 – working report (partial), Erdős Problem a Day, `https://erdosproblemaday.com/report/893`, checked 28 July 2026.

[16] S. Wigert, Sur l'ordre de grandeur du nombre des diviseurs d'un entier, *Ark. Mat. Astron. Fys.* 3 (1907), 1–9.

[17] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* 3 (1892), 265–284.