On the degrees of divisors of $T^n - 1$

Paul Pollack and Lola Thompson

ABSTRACT. Fix a field F. In this paper, we study the sets $\mathscr{D}_F(n) \subset [0, n]$ defined by

$$\mathscr{D}_F(n) := \{0 \le m \le n : T^n - 1 \text{ has a divisor of degree } m \text{ in } F[T]\}.$$

When $\mathscr{D}_F(n)$ consists of all integers m with $0 \le m \le n$, so that $T^n - 1$ has a divisor of every degree, we call n an *F-practical number*. The terminology here is suggested by an analogy with the *practical numbers* of Srinivasan, which are numbers n for which every integer $0 \le m \le \sigma(n)$ can be written as a sum of distinct divisors of n. Our first theorem states that, for any number field F and any $x \ge 2$,

$$\#\{F\text{-practical } n \le x\} \asymp_F \frac{x}{\log x};$$

this extends work of the second author, who obtained this estimate when $F = \mathbf{Q}$.

Suppose now that $x \ge 3$, and let m be a natural number in $[3, x]$. We ask: For how many $n \le x$ does m belong to $\mathscr{D}_F(n)$? We prove upper bounds in this problem for both $F = \mathbf{Q}$ and $F = \mathbf{F}_p$ (with p prime), the latter conditional on the Generalized Riemann Hypothesis. In both cases, we find that the number of such $n \le x$ is $O_F(x/(\log m)^{2/35})$, uniformly in m.

CONTENTS

1. Introduction

Let F be a field. In this paper, we study the sets of nonnegative integers which appear as the set of degrees of divisors of $T^n - 1$ in $F[T]$, i.e., the sets

$$\mathscr{D}_F(n) := \{0 \le m \le n : T^n - 1 \text{ has a divisor of degree } m \text{ over } F\}.$$

2010 *Mathematics Subject Classification.* Primary: 11N25, Secondary: 11N37.

When this set consists of all integers $0 \le m \le n$, we call n an *F-practical number*. For example, 6 is a $\mathbf{Q}$-practical number, as shown by the following list of divisors of $T^6 - 1$:

$$1,\ \ T-1,\ \ T^2+T+1,\ \ T^3-1,\ \ T^4+T^3-T-1,\ \ T^5+T^4+T^3+T^2+T+1,\ \ T^6-1.$$

It is easy to see directly (for example, by applying Gauss's lemma) that if $T^n - 1$ has a divisor of a given degree over $\mathbf{Q}$, then it has a divisor of the same degree over $\mathbf{Z}$. As a consequence, for any field F, each $\mathbf{Q}$-practical number is also an F-practical number.

The distribution of $\mathbf{Q}$-practical numbers has been investigated by the second author [Tho12a]. Recall that with $\Phi_d(T)$ denoting the dth cyclotomic polynomial, we have

$$T^n - 1 = \prod_{d \mid n} \Phi_d(T). \tag{1.1}$$

Over $\mathbf{Q}$, each of the right-hand factors $\Phi_d(T)$ is irreducible of degree $\varphi(d)$. It follows that a natural number n is $\mathbf{Q}$-practical precisely when every integer $m \in [0, n]$ can be written as a sum of terms $\varphi(d)$, where d runs over a subset of the divisors of n.

The term "F-practical number" is suggested by an analogy between the $\mathbf{Q}$-practical numbers and *Srinivasan's practical numbers* [Sri48], which are numbers n for which every $m \in [0, \sigma(n)]$ can be written as a sum of distinct divisors of n. Such n have been studied by several authors, including Erdős [Erd50], Hausman & Shapiro [HS84], Tenenbaum [Ten86, Ten95], Margenstern [Mar91], and Saias [Sai97]. In the last of these papers, Saias shows that for all $x \ge 2$,

$$\#\{\text{practical } n \le x\} \asymp \frac{x}{\log x}. \tag{1.2}$$

Exploiting the analogy between practical numbers and $\mathbf{Q}$-practical numbers, the second author [Tho12a] proved the $\mathbf{Q}$-practical analogue of Saias's estimates:

$$\#\{\mathbf{Q}\text{-practical } n \le x\} \asymp \frac{x}{\log x}.$$

(In the above statements, the notation "$f \asymp g$" means that we have both $f \ll g$ and $g \ll f$.)

One of our goals in this paper is to gain some understanding of the F-practical numbers over more general fields F. We begin by observing that each cyclotomic polynomial $\Phi_d(T)$ always splits into (not necessarily distinct) irreducible factors of the same degree over F. This is easy to see in the case when the characteristic of F, say p, does not divide d (for example, in characteristic zero). In this case, the roots of $\Phi_d(T)$ are exactly the $\varphi(d)$ primitive dth roots of unity from the algebraic closure of F. Each primitive dth root of unity generates the same extension of F, and thus all irreducible

factors of $\Phi_d(T)$ have the same degree, as desired. The case when p divides d reduces to the previous one, since then $\Phi_d(T) = \Phi_{d_{(p)}}(T)^{\varphi(d/d_{(p)})}$, where $d_{(p)}$ denotes the largest divisor of d coprime to p.

From the last paragraph, it makes sense to define an arithmetic function φ_F by letting $\varphi_F(d)$ denote the common degree of each irreducible factor of $\Phi_d(T)$ over F. (For example, $\varphi_F = \varphi$ when $F = \mathbf{Q}$.) Then each $\Phi_d(T)$ is a product of $\varphi(d)/\varphi_F(d)$ (not necessarily distinct) irreducible polynomials of degree $\varphi_F(d)$. So from (1.1), m is the degree of a divisor of $T^n - 1$ precisely when there is a collection $\mathscr{S}$ of divisors of n for which m can be written in the form

$$m = \sum_{d \in \mathscr{S}} a_d \varphi_F(d), \quad \text{where each} \quad 0 \le a_d \le \frac{\varphi(d)}{\varphi_F(d)}. \tag{1.3}$$

In §2, we use this criterion and some easy algebraic number theory to extend Thompson's theorem on $\mathbf{Q}$-practical numbers to an arbitrary number field. Note that since each $\mathbf{Q}$-practical number is automatically F-practical, it is enough to prove the upper bound estimate.

Theorem 1.1. *Let F be a number field. Then for $x \ge 2$, the number of F-practical numbers in $[1, x]$ is $O_F(\frac{x}{\log x})$.*

In her thesis ([Tho12b]; see also [Tho12c], [Tho12d]), Thompson studies the F-practical numbers also in the case when $F = \mathbf{F}_p$ (with p prime). To discuss this case further, we need some notation. Write $\ell_p(d)$ for the multiplicative order of p modulo d, assuming that $\gcd(d, p) = 1$. In general, put $\ell_p^*(d) = \ell_p(d_{(p)})$, where $d_{(p)}$ denotes the largest divisor of d coprime to p. As shown in [Tho12d], we have $\varphi_{\mathbf{F}_p} = \ell_p^*$. Our limited understanding of the distribution of the numbers $\ell_p^*(d)$ is a significant obstacle to the study of $\mathbf{F}_p$-practical numbers. To work around this, Thompson assumes the *Generalized Riemann Hypothesis* (GRH). (Throughout this paper, GRH always means the Riemann Hypothesis for Dedekind zeta functions.) Under this assumption, she shows (ibid.) that for $x \ge 3$,

$$\frac{x}{\log x} \ll \#\{\mathbf{F}_p\text{-practical } n \le x\} \ll_p x\sqrt{\frac{\log\log x}{\log x}}.$$

The numerical data (see, for instance, [Tho12b, Tables 1.2–1.4]) suggests that for each fixed p, the true count of $\mathbf{F}_p$-practical numbers is $\sim C_p x/\log x$, as $x \to \infty$, where C_p is a positive constant depending on p.

Up to this point, we have been discussing integers n for which $\mathscr{D}_F(n)$ is the entire interval $[0, n]$. A weaker notion also suggests itself: Take an integer $m \le x$ and count how often, among those $n \le x$, one has $m \in \mathscr{D}_F(n)$. In other words, instead of requiring $T^n - 1$ to have divisors of every degree, we fix in advance a target degree m. Our next theorem gives an upper bound in the case when $F = \mathbf{Q}$. It is convenient to label once and for all the so-called

Erdős–Ford–Tenenbaum constant

$$\delta := 1 - \frac{1 + \log\log 2}{\log 2}. \tag{1.4}$$

Numerically, $\delta \approx 0.0860713$.

Theorem 1.2. *Fix a value δ' with $0 < \delta' < \delta$, where δ is defined in* (1.4)*. Then if $3 \le m \le x$, the number of $n \le x$ for which $T^n - 1$ has a divisor of degree m in $\mathbf{Q}[T]$ is $O(x/(\log m)^{\delta'})$.*

Theorem 1.2 should be viewed as analogous to a theorem of Erdős, who considered [Erd70, p. 130] how often a target natural number m could be written as a sum of distinct divisors of n. Indeed, our proof uses many of the same ideas. However, Erdős was content to work with fixed values of m, whereas we seek a result with complete uniformity in m.

It would be desirable to have a sharp lower bound to complement the upper bound in Theorem 1.2. An easy adaptation of the methods of [PT12] gives the following related estimate: *If $3 \le m \le \frac{1}{2}x$, then the number of $n \in [1, x]$ for which $T^n - 1$ has a divisor of each degree in $[0, m]$ is $\gg x/\log m$.*

Our last result is a GRH-conditional version of Theorem 1.2 with $F = \mathbf{F}_p$ rather than $F = \mathbf{Q}$.

Theorem 1.3 (assuming GRH)**.** *Fix a prime p. Suppose that $3 \le m \le x$.*

(i) *If $3 \le m \le x^{1-1/\log\log x}$, then the number of $n \le x$ for which $T^n - 1$ has a divisor of degree m in $\mathbf{F}_p[T]$ is*

$$\ll_p x/(\log m)^{1/13}.$$

(ii) *If $x^{1-1/\log\log x} < m \le x$, then the count of such n is*

$$\ll_p x/(\log m)^{2/35}.$$

The exponents $1/13$ and $2/35$ appearing above are close to the best our methods will yield. It would be interesting to know how close they are to being best possible.

The proof of Theorem 1.3 follows the same broad outline as that of Theorem 1.2. The extra difficulty stems from the fact that while $\varphi(d)$ is never much smaller than d (see Lemma 3.1 below), $\ell_p^*(d)$ can be considerably smaller. However, under GRH, one can show that $\ell_p^*(d)$ is typically fairly close to d. This is enough for our purposes.

One might compare Theorem 1.3 with the result of Car [Car84] that in a wide range of m and n, few polynomials of degree n over $\mathbf{F}_p$ (or a general finite field $\mathbf{F}_q$) have a divisor of degree m. One must be cautious about such comparisons, however. For example, a typical polynomial of degree n over $\mathbf{F}_p$ has about $n^{\log 2}$ divisors (compare with [KZ01, Theorem 3.3.7]). However, for each fixed $A > 0$, the polynomial $T^n - 1$ has more than $\exp((\log n)^A)$ divisors on a set of n of asymptotic density 1. One can prove this using the above results on the factorization of cyclotomic polynomials together

with the work of Erdős, Pomerance, and Schmutz on the normal order of Carmichael's function $\lambda(n)$ (see [EPS91, Theorem 2]).

A word about the organization of the paper: We prove Theorem 1.1 in §2. Theorem 1.2 is proved in §3, after recalling some helpful results from the anatomy of integers. In §4.1, we review the GRH-conditional results needed for the proof of Theorem 1.3, which we present in §4.3. We conclude the paper in §5 by discussing some natural variants of the $\mathbf{Q}$-practical numbers. For example, we show that $2^{2^5} - 1$ is the largest integer n for which $T^n - 1$ has exactly one monic divisor of each degree $0 \le m \le n$ in $\mathbf{Q}[T]$.

Notation. We write $\omega(n) := \sum_{p|n} 1$ for the number of distinct prime factors of n and $\Omega(n) := \sum_{p^k|n} 1$ for the number of prime factors of n counted with multiplicity; $\Omega(n; y) := \sum_{p^k|n,\ p\le y} 1$ denotes the number of prime divisors of n not exceeding y, again counted with multiplicity. The number of divisors of n is denoted $d(n)$; for the number of divisors not exceeding y, we write $d(n; y)$. We use $P^-(m)$ and $P^+(m)$ for the smallest and largest prime factors of m, respectively, with the conventions that $P^-(1) = \infty$ and $P^+(1) = 1$. An integer n for which $P^+(n) \le y$ is called *y-smooth* (or *y-friable*); the number of y-smooth $n \le x$ is denoted $\Psi(x, y)$.

We write $\lambda(n)$ for Carmichael's lambda-function, defined as the exponent of the finite abelian group $(\mathbf{Z}/n\mathbf{Z})^\times$. We also adopt the following notation, seen above when $a = p$: For each natural number n coprime to a, we write $\ell_a(n)$ for the multiplicative order of a mod n. For n not necessarily coprime to a, we let $n_{(a)}$ denote the largest divisor of n coprime to a, and we define $\ell_a^*(n) = \ell_a(n_{(a)})$. We call $\ell_a^*(n)$ the *generalized order* of a mod n. (Note that $\ell_a^*(n)$ always divides $\lambda(n)$.) When the intended value of a is clear, we omit the subscripts on ℓ and ℓ^*.

2. Proof of Theorem 1.1

The proof of Theorem 1.1 proceeds through a series of lemmas. The first of these, due to Stewart [Ste54] and Sierpiński [Sie55], characterizes Srinivasan's practical numbers in terms of their prime factorization.

Lemma 2.1. *Let n be a natural number, and write the prime factorization of n in the form $n = \prod_{i=1}^r p_i^{e_i}$, where each $e_i > 0$ and $p_1 < p_2 < \cdots < p_r$. Let j be the first index for which the inequality*

$$p_j \le 1 + \sigma\left(\prod_{1\le i<j} p_i^{e_i}\right) \tag{2.1}$$

fails, where we take $j = r + 1$ if no such index exists. Set

$$n' := \prod_{1\le i<j} p_i^{e_i}. \tag{2.2}$$

Then every natural number $1 \le m \le \sigma(n')$ can be written as a sum of distinct divisors of n, but $\sigma(n')+1$ cannot be written as a sum of distinct divisors of n. Consequently, n is practical precisely when (2.1) *holds for all indices $1 \le j \le r$.*

In what follows, we refer to n', as defined in (2.2), as the *practical component* of n. It can be shown (compare with [Mar91, Proposition 4]) that the practical component n' is the largest practical divisor of n.

For the remainder of the proof, we fix a number field F, viewed as a subfield of a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We use ζ_d for a primitive dth root of unity from $\overline{\mathbf{Q}}$. In the next several lemmas, we show that if n is F-practical, then there is a small multiple of n that is practical in the sense of Lemma 2.1. The desired upper bound then follows from Saias's upper bound (1.2) on the count of practical numbers.

Lemma 2.2. *Let d be a natural number coprime to the (absolute) discriminant of F. Then $\varphi_F(d) = \varphi(d)$.*

Proof. Since the discriminant of $\mathbf{Q}(\zeta_d)$ divides $d^{\varphi(d)}$ (see [Rib72, p. 269]), the number fields F and $\mathbf{Q}(\zeta_d)$ have relatively prime discriminants. Since $F(\zeta_d)$ is the compositum of F and $\mathbf{Q}(\zeta_d)$, we have (see [Rib72, p. 218])

$$[F(\zeta_d) : \mathbf{Q}] = [F : \mathbf{Q}] \cdot [\mathbf{Q}(\zeta_d) : \mathbf{Q}] = [F : \mathbf{Q}]\varphi(d).$$

It follows that $\varphi(d) = \frac{[F(\zeta_d):\mathbf{Q}]}{[F:\mathbf{Q}]} = [F(\zeta_d) : F] = \varphi_F(d)$, as claimed. □

Lemma 2.3. *Let p be a prime number. The product of the primes less than p is always at least $p-1$.*

Proof. This is easy to verify directly for primes $p < 5$. Now suppose that the claim has been shown for all primes smaller than p, where $p \ge 5$, and let p' be the prime directly preceding p. Note that $p < 2p'$, by Bertrand's postulate. By the induction hypothesis, the product of the primes smaller than p is at least

$$p'(p'-1) \ge 3(p'-1) = 3p' - 3 > \frac{3}{2}p - 3 \ge p - 1,$$

since $p \ge 5$. □

Lemma 2.4. *If n is F-practical and p is the first prime not dividing n, then pn is also F-practical.*

Proof. We need to show that $T^{pn} - 1$ has a divisor of degree m over F for all $0 \le m \le pn$. Since $\frac{T^{pn}-1}{T^n-1}$ has degree $(p-1)n$, and $T^n - 1$ has a divisor of each degree in $[0, n]$, we see that $T^{pn} - 1$ has a divisor of every degree m with $(p-1)n \le m \le pn$. So we can assume that $0 \le m < (p-1)n$.

Write $m = (p-1)q + r$, where $0 \le q < n$ and $0 \le r < p-1$. Since n is divisible by all primes $< p$, we have from Lemma 2.3 that $n \ge p-1 > r$. We

are assuming that n is F-practical, and so there is a divisor $f(T) \in F[T]$ of $T^n - 1$ of degree r. That is, there is an $f(T) \in F[T]$ of degree r for which

$$f(T) \mid \prod_{d|n} \Phi_d(T). \tag{2.3}$$

Similarly, since $q < n$, there is a divisor of $T^n - 1$ of degree q. Such a divisor implies the existence of a representation (as in 1.3)

$$q = \sum_{d|n} a_d \varphi_F(d), \quad \text{where} \quad 0 \le a_d \le \frac{\varphi(d)}{\varphi_F(d)}. \tag{2.4}$$

Multiplying (2.4) by $p-1$, we obtain a representation

$$\begin{aligned}(p-1)q &= \sum_{d|n} \left(a_d \frac{p-1}{\varphi_F(pd)/\varphi_F(d)} \right) \varphi_F(pd) \\ &= \sum_{d|n} b_d \varphi_F(pd), \quad \text{with each} \quad b_d := a_d \frac{p-1}{\varphi_F(pd)/\varphi_F(d)}. \end{aligned} \tag{2.5}$$

With $F_d := F(\zeta_d)$, we have (noting that $p \nmid d$, since $p \nmid n$)

$$\frac{\varphi_F(pd)}{\varphi_F(d)} = [F(\zeta_{pd}) : F(\zeta_d)] = [F_d(\zeta_p) : F_d] = \varphi_{F_d}(p) \mid p-1,$$

and so all the b_d are integers. Moreover, for each d dividing n,

$$0 \le b_d \le \frac{\varphi(d)}{\varphi_F(d)} \frac{p-1}{\varphi_F(pd)/\varphi_F(d)} = \frac{\varphi(pd)}{\varphi_F(pd)}.$$

We now deduce from (2.5) that there is a $g(T) \in F[T]$ of degree $(p-1)q$ for which

$$g(T) \mid \prod_{d|n} \Phi_{pd}(T). \tag{2.6}$$

Combining (2.3) and (2.6), we see that over F,

$$f(T)g(T) \mid \left(\prod_{d|n} \Phi_d(T)\Phi_{pd}(T) \right) = T^{pn} - 1,$$

and fg has degree $r + (p-1)q = m$. So fg is our sought-after divisor. □

Repeatedly applying Lemma 2.4, we arrive at the following result.

Lemma 2.5. *If n is F-practical, then $\operatorname{lcm}[n, \prod_{p \le z} p]$ is F-practical for every real number z.*

Lemma 2.6. *Set $M := \prod_{p \le 2|D|} p$, where D is the discriminant of F. If n is F-practical, then $\operatorname{lcm}[n, M]$ is practical (in the sense of Srinivasan).*

Proof. Put $N := \operatorname{lcm}[n, M]$. By Lemma 2.5, N is F-practical. We will show that N satisfies the Stewart–Sierpiński practicality criterion given in Lemma 2.1. Assuming N is not practical, let N' be the practical component of N. Then $N' < N$, and by Lemma 2.1, with p denoting the smallest prime dividing N/N', we have

$$p > \sigma(N') + 1. \tag{2.7}$$

We must also have that $p > 2|D|$. To see this, observe that by construction, N is divisible by all primes not exceeding $2|D|$. So if $p \le 2|D|$, then N' is divisible by all primes $< p$, and so by Lemma 2.3,

$$1 + \sigma(N') \ge 1 + \prod_{\substack{q<p \\ q \text{ prime}}} (q+1) \ge 1 + \prod_{\substack{q<p \\ q \text{ prime}}} q \ge 1 + (p-1) = p,$$

contradicting (2.7). Hence, $p > 2|D|$.

We claim that $T^N - 1$ has no divisor of degree $N' + 1$, contradicting that N is F-practical. Suppose contrariwise that

$$N' + 1 = \sum_{d|N} a_d \varphi_F(d), \quad \text{where} \quad 0 \le a_d \le \frac{\varphi(d)}{\varphi_F(d)}. \tag{2.8}$$

The contribution to the sum in (2.8) from divisors d of N' is bounded by $\sum_{d|N'} \varphi(d) = N'$; hence, there must be a d dividing N but not N' which contributes to the right-hand side of (2.8). Since all the summands on the right-hand side of (2.8) are nonnegative, clearly

$$\varphi_F(d) \le N' + 1. \tag{2.9}$$

Since d divides N but not N', we can choose a prime r dividing $\gcd(d, N/N')$. Clearly,

$$r \ge P^-(N/N') = p > \max\{2|D|, \sigma(N') + 1\}.$$

Since $r \mid d$ and $r \nmid D$, Lemma 2.2 shows that

$$\varphi_F(d) = [F(\zeta_d) : F] \ge [F(\zeta_r) : F] = \varphi_F(r) = \varphi(r) = r - 1 \ge \sigma(N') + 1.$$

Since $2 \mid N$, the practical component N' of N satisfies $N' \ge 2$, and so $\sigma(N') \ge N' + 1$. Thus, $\varphi_F(d) \ge N' + 2 > N' + 1$, contradicting (2.9). □

Proof of Theorem 1.1. Define M as in Lemma 2.6. If $n \le x$ is F-practical, then dn is practical for some d dividing M, namely $d = M/(M, n)$. Since $dn \le dx$, the upper-estimate of (1.2) shows that the number of F-practical $n \le x$ corresponding to this d is $O(dx/\log x)$. Summing over the $O_F(1)$ divisors d of M completes the proof. □

3. Proof of Theorem 1.2

The next few lemmas collect certain structural results about integers needed for the proof of Theorem 1.2. The first is a classical result of Landau (see [HW08, Theorem 328, p. 352]) giving the minimal order of the Euler φ-function.

Lemma 3.1. *We have* $\liminf_{n\to\infty} \frac{\varphi(n)}{n/\log\log n} = e^{-\gamma}$.

Recall that $d(n;y)$ denotes the number of divisors of n not exceeding y. The next lemma is implicit in [Erd70].

Lemma 3.2. *Let $x, y \geq 2$, and let $K \geq 1$. The number of integers $n \leq x$ with $d(n;y) \geq K$ is $O(\frac{1}{K} x \log y)$.*

Proof. This is immediate from the first-moment estimate

$$\sum_{n\leq x} d(n;y) = \sum_{d\leq y} \sum_{\substack{n\leq x\\ d\mid n}} 1 \leq x \sum_{d\leq y} \frac{1}{d} \ll x \log y. \qquad \square$$

The next result (easily deduced from [HT88, Theorems 08–09, pp. 5–6]; see also [HT88, Exercise 04, p. 12]) is an upper bound on the number of integers n with an abnormally large number of prime factors.

Lemma 3.3. *Let $x \geq 3$. Uniformly for $0 < \kappa \leq 1.9$, the number of $n \leq x$ with $\Omega(n) > \kappa \log\log x$ is*

$$\ll x/(\log x)^{Q(\kappa)}, \quad \textit{where} \quad Q(\kappa) = \kappa\log\kappa - \kappa + 1.$$

Remark. It is straightforward to check that the Erdős–Ford–Tenenbaum constant δ of (1.4) satisfies $\delta = Q(1/\log 2)$. This property of δ will be important in what follows.

Write $H(x,y,z)$ for the count of $n \in [1,x]$ possessing a divisor from the interval $(y,z]$. The proof of Theorem 1.2 requires fairly precise estimates for H. Conveniently, Ford [For08] has determined the order of magnitude of $H(x,y,z)$ in the complete space of parameters. His full result is somewhat complicated to state, but the next two lemmas isolate the special cases that are of interest to us (extracted from [For08, Theorem 1(v), (vi)]). For our purposes, earlier results of Tenenbaum would also suffice (see, e.g., [HT88, Theorem 21, pp. 29–30]).

Lemma 3.4. *Let $x > 10^5$. Suppose $y \geq 100$ and that $2y \leq z \leq y^2 \leq x$. Write $z = y^{1+u}$, so that $u = \log(z/y)/\log(y)$. Then*

$$H(x,y,z) \asymp x u^{\delta} \big(\log\frac{2}{u}\big)^{-3/2},$$

where $\delta \approx 0.08607$ is the constant defined in (1.4).

Lemma 3.5. *Let $x > 10^5$. Suppose that $\sqrt{x} < y < z \le x$. Suppose also that $z \ge y+1$ and $x/y \ge 1 + x/z$. Then*

$$H(x,y,z) \asymp H(x, x/z, x/y).$$

We also need some understanding of the distribution of smooth numbers. The following upper bound is contained in work of de Bruijn [dB66]. Recall that $\Psi(x,y)$ denotes the number of y-smooth numbers $n \le x$.

Lemma 3.6. *For $2 \le y \le x$, set $u := \frac{\log x}{\log y}$. Whenever $y \ge (\log x)^2$ and $u \to \infty$, we have*

$$\Psi(x,y) \le \exp(-(1+o(1))u \log u).$$

Proof of Theorem 1.2. We may suppose that m (and hence also x) is large, since the assertion of the theorem is trivial for bounded values of m. We take two cases.

Case 1: For the first half of the proof, we will assume that

$$m \le x \exp(-\log x/\log\log x). \tag{3.1}$$

Suppose that $T^n - 1$ has a divisor of degree m in $\mathbf{Q}[T]$. We can assume that n satisfies the inequality

$$d(n; 2m\log\log m) < (\log m)^2. \tag{3.2}$$

Indeed, by Lemma 3.2, the count of $n \le x$ not satisfying (3.2) is $O(x/\log m)$, which is negligible for us.

Since $T^n - 1$ has a divisor of degree m, we can choose (as in (1.3)) a subset $\mathscr{S}$ of the divisors of n with

$$m = \sum_{d \in \mathscr{S}} \varphi(d). \tag{3.3}$$

If $d \in \mathscr{S}$, then $\varphi(d) \le m$, and so Lemma 3.1 implies that $d \le 2m\log\log m$. (We use here that m is large and that $e^\gamma < 2$.) Thus, $\#\mathscr{S} < (\log m)^2$ by (3.2). But then some term on the right-hand side of (3.3) must exceed $m/(\log m)^2$. In particular, there must be some $d \in \mathscr{S}$ with

$$2m\log\log m \ge d \ge \varphi(d) > m/(\log m)^2.$$

Hence, n is counted by

$$\tilde{H} := H(x, m/(\log m)^2, 2m\log\log m).$$

We consider three cases:

- If $2m\log\log m \le \sqrt{x}$, we apply Lemma 3.4 with $y = m/(\log m)^2$, $z = 2m\log\log m$. In this case, $u \asymp \frac{\log\log m}{\log m}$, and we find that

$$\tilde{H} \ll x\left(\frac{\log\log m}{\log m}\right)^\delta (\log\log m)^{-3/2} \ll x/(\log m)^\delta,$$

  as desired.

- If $m/(\log m)^2 > \sqrt{x}$, then by Lemma 3.5,
$$\tilde{H} \asymp H\bigg(x, \frac{x}{2m \log\log m}, x\frac{(\log m)^2}{m}\bigg).$$
Recall we are assuming that m satisfies (3.1). Apply Lemma 3.4 with $y = \frac{x}{2m\log\log m}$ and $z = x\frac{(\log m)^2}{m}$, so that (using (3.1))
$$\begin{aligned} u &\asymp \frac{\log\log m}{\log(x/(2m\log\log m))} \\ &\ll \frac{(\log\log m)(\log\log x)}{\log x} \ll \frac{(\log\log m)^2}{\log m}. \end{aligned}$$
We obtain that
$$\tilde{H} \ll x\left(\frac{(\log\log m)^2}{\log m}\right)^{\delta} (\log\log m)^{-3/2} \ll x/(\log m)^{\delta}.$$
- Finally, suppose that $m/(\log m)^2 \le \sqrt{x} < 2m\log\log m$. Then $\sqrt{x}/(\log\sqrt{x})^3 \le m/(\log m)^2$ and $2m\log\log m < \sqrt{x}(\log x)^3$. Thus,
$$\begin{aligned} \tilde{H} &= H\left(x, \frac{m}{(\log m)^2}, \sqrt{x}\right) + H(x, \sqrt{x}, 2m\log\log m) \\ &\le H\left(x, \frac{\sqrt{x}}{(\log\sqrt{x})^3}, \sqrt{x}\right) + H(x, \sqrt{x}, \sqrt{x}(\log x)^3). \end{aligned}$$
Applying Lemmas 3.4 and 3.5 as above, we find that both terms on the right-hand side are $\ll x/(\log x)^{\delta} \ll x/(\log m)^{\delta}$.

This completes the proof of Theorem 1.2 in the case when m satisfies (3.1). In fact, in this case we obtain the upper bound claimed in the theorem with δ' replaced by the larger number δ.

Case 2: Now suppose (3.1) fails, i.e., that
$$x\exp(-\log x/\log\log x) < m \le x. \tag{3.4}$$

Let $n \le x$ be such that $T^n - 1$ has a divisor of degree m. We may assume that $p = P^+(n)$ satisfies
$$P^+(n) > \exp(2\log x/\log\log x). \tag{3.5}$$

Indeed, by Lemma 3.6 (with $u = \frac{1}{2}\log\log x$), the number of $n \le x$ not satisfying (3.5) is, for large x, at most
$$\frac{x}{\exp(\frac{1}{3}\log\log x\log\log\log x)} < \frac{x}{\log x} \le \frac{x}{\log m},$$
which is negligible.

We fix $\epsilon > 0$ (depending only on δ') so that all but $O(x/(\log x)^{\delta'})$ natural numbers $n \le x$ satisfy the inequality
$$\Omega(n) \le \left(\frac{1}{\log 2} - \epsilon\right)\log\log x. \tag{3.6}$$

Since $\delta = Q(1/\log 2)$ and $\delta' < \delta$, the possibility of choosing such an ϵ follows from Lemma 3.3 and the continuity of the function $Q(\kappa)$ appearing in the lemma statement. In what follows, we assume that (3.6) holds.

Since $T^n - 1$ has a divisor of degree m, we may take a representation of m in the form (3.3), where $\mathscr{S}$ is a set of divisors of n. For each $d \in \mathscr{S}$ divisible by p, the number $\varphi(d)$ is divisible by $p-1$. So reducing (3.3) modulo $p-1$, we find that

$$m \equiv \sum_{d \in \mathscr{T}} \varphi(d) \pmod{p-1}, \quad \text{where} \quad \mathscr{T} := \{d \in \mathscr{S} : p \nmid d\}. \tag{3.7}$$

Notice that $\mathscr{T}$ consists of divisors of $r := n/p$. Also, from (3.5), we have

$$r \le x/\exp(2\log x/\log\log x).$$

Moreover, recalling (3.4),

$$\begin{aligned} m - \sum_{d \in \mathscr{T}} \varphi(d) &\ge m - \sum_{d \mid r} \varphi(d) \ge m - r \\ &\ge x\exp(-\log x/\log\log x) - x\exp(-2\log x/\log\log x) > 0. \end{aligned} \tag{3.8}$$

We now count the possibilities for n by first fixing r and then using the relation (3.7) to count the number of possibilities for p given r. Since $\mathscr{T}$ consists entirely of divisors of r, the number of possibilities for $\mathscr{T}$, given r, is at most

$$2^{d(r)} < 2^{d(n)} \le 2^{2^{\Omega(n)}} < \exp((\log x)^{1-\frac{1}{2}\epsilon}).$$

(We use (3.6) in the last step.) Rewriting (3.7) in the form

$$p - 1 \mid \left(m - \sum_{d \in \mathscr{T}} \varphi(d) \right),$$

we see that given $\mathscr{T}$, the number of possibilities for p is bounded by

$$\max_{h \le x} d(h) < \exp(\log x/\log\log x).$$

(We use here the maximal order of the divisor function, as in [HW08, Theorem 317, p. 345].) Since p and r determine $n = pr$, the number of possibilities for n is

$$\begin{aligned} &< \frac{x}{\exp(2\log x/\log\log x)} \cdot \exp((\log x)^{1-\frac{1}{2}\epsilon}) \cdot \exp(\log x/\log\log x) \\ &< \frac{x}{\exp(\frac{1}{2}\log x/\log\log x)} < \frac{x}{\log x}, \end{aligned}$$

which is negligible. This completes the proof. □

4. Proof of Theorem 1.3

4.1. Preliminary estimates. Throughout §4, we assume that $a > 1$ is a fixed integer, and we write $\ell^*(n)$ for the generalized order of a modulo n. In §4.1, we collect some known results on the behavior of $\ell^*(n)$ and the closely associated function $\lambda(n)$. These estimates will eventually be applied to prove Lemma 4.7, which will be the key component of our demonstration of Theorem 1.3.

Remark. For the rest of §4, we suppress any dependence of implied constants on a.

The following lemma, due to Kurlberg and Pomerance [KP05, Theorem 23], shows that under GRH the numbers $\ell(p)$ are usually close to $p-1$.

Lemma 4.1 (assuming GRH)**.** *Uniformly for $1 \le y \le \log x$, the number of primes $p \le x$ (not dividing a) for which $\ell(p) \le p/y$ is*

$$\ll \frac{\pi(x)}{y} + \frac{x}{(\log x)^2} \log\log x.$$

Lemma 4.2 (assuming GRH)**.** *Let $x \ge 3$. The number of primes $p \le x$ coprime to a with $\ell(p) \le p/\log p$ is $O(\frac{x}{(\log x)^2} \log\log x)$.*

Proof. We can restrict our attention to $p > \sqrt{x}$. Then $\ell(p) \le p/\log p < 2p/\log x$, and the estimate follows from Lemma 4.1 with $y = \frac{1}{2}\log x$. □

The next lemma is a special case of a result of Gottschlich [Got12, Lemma 2.3].

Lemma 4.3. *Let $\mathscr{P}$ be a set of primes. Suppose that for certain constants $\theta_1 > 1$, $\theta_2 > 0$, the number of elements of $\mathscr{P}$ not exceeding x is*

$$\ll \frac{x}{(\log x)^{\theta_1}} (\log\log x)^{\theta_2},$$

for all $x \ge 3$. Then for $x \ge 3$, the number of integers $n \le x$ all of whose prime factors belong to $\mathscr{P}$ is also

$$\ll \frac{x}{(\log x)^{\theta_1}} (\log\log x)^{\theta_2},$$

where the implied constant depends at most on $\mathscr{P}$ and the θ_i.

Lemma 4.4 (assuming GRH)**.** *Let $x \ge 3$. The number of $n \le x$ all of whose prime factors p either*

(i) *divide a,* or
(ii) *satisfy $\ell(p) \le p/\log p$*

is $O(\frac{x}{(\log x)^2} \log\log x)$.

Proof. We let $\mathscr{P}$ be the set of primes p dividing a or satisfying $\ell(p) \le p/\log p$. Since there are only $O(1)$ primes dividing a, Lemma 4.2 shows that the hypotheses of Lemma 4.3 are satisfied with $\theta_1 = 2$ and $\theta_2 = 1$. □

Finally, we recall an estimate of Friedlander, Pomerance, and Shparlinski [FPS01] for the number of occurrences of small values of the Carmichael λ-function.

Lemma 4.5. *Suppose that x is sufficiently large and that $\Delta \geq (\log\log x)^3$. Then the number of $n \leq x$ with $\lambda(n) \leq n\exp(-\Delta)$ is at most*

$$x\exp(-0.69(\Delta\log\Delta)^{1/3}).$$

4.2. Key lemmas. In this section, we present several lemmas that play an important role in the proof of Theorem 1.3. The following lemma is a close cousin of Lemma 3.2, but the proof is somewhat more intricate. It should also be compared with Lemma 3.3, which gives a sharper result but only under more restrictive hypotheses.

Lemma 4.6. *Let $x, y \geq 2$, and let $k \geq 1$. The number of $n \leq x$ with $\Omega(n;y) \geq k$ is $O(\frac{k}{2^k}x\log y)$.*

Remark. Taking $y = x$, we see that the number of $n \leq x$ with $\Omega(n) \geq k$ is $O(\frac{k}{2^k}x\log x)$.

Proof. The proof is almost identical to that suggested in Exercise 05 of [HT88, p. 12], but we include it for the sake of completeness. Let $v := 2-1/k$. Let g be the arithmetic function determined through the convolution identity $v^{\Omega(n;y)} = \sum_{d|n} g(d)$. Then g is multiplicative. For $e \geq 1$, we have $g(p^e) = v^e - v^{e-1}$ if $p \leq y$, and $g(p^e) = 0$ if $p > y$. Hence,

$$\begin{aligned}\sum_{n\leq x} v^{\Omega(n;y)} &= \sum_{d\leq x} g(d)\left\lfloor \frac{x}{d}\right\rfloor \leq x\sum_{d\leq x}\frac{g(d)}{d}\\ &\leq x\prod_{p\leq y}\left(1+\frac{v-1}{p}+\frac{v^2-v}{p^2}+\dots\right)\\ &= \frac{x}{2-v}\prod_{3\leq p\leq y}\left(1+\frac{v-1}{p-v}\right).\end{aligned}$$

Now $2-v = 1/k$, and the rightmost product does not exceed

$$\exp\left(\sum_{3\leq p\leq y}\frac{v-1}{p-v}\right) \leq \exp\left(\sum_{3\leq p\leq y}\frac{1}{p-2}\right) \leq \exp\left(\sum_{p\leq y}\frac{1}{p}+O(1)\right) \ll \log y.$$

Collecting our estimates, we have shown that

$$\sum_{n\leq x} v^{\Omega(n;y)} \ll kx\log y.$$

But each term with $\Omega(n;y) \geq k$ makes a contribution to the left-hand side that is at least $v^k \geq (2-1/k)^k = 2^k(1-\frac{1}{2k})^k \gg 2^k$. Thus, the number of such terms is $O(\frac{k}{2^k}x\log y)$. □

We noted in the introduction that there is no direct analogue for ℓ^* of the minimal order result for φ expressed in Lemma 3.1. The following result is a partial workaround.

Lemma 4.7 (assuming GRH)**.** *Fix θ with $0 < \theta \le \frac{1}{2}$. Suppose that $3 \le y \le x$. The number of integers $n \le x$ which have a divisor $d > y$ satisfying*

$$\ell^*(d) \le d/\exp(4(\log d)^\theta)$$

is $O_\theta(x \log\log y/(\log y)^\theta)$.

Proof. Throughout the argument, we suppress the dependence of implied contants on θ. We may assume always that y is large, since the lemma is trivial for bounded values of y. For real $t \ge 1$, define the three sets

$$\begin{aligned}
\mathscr{E}_1(t) &:= \{e \le t : e \text{ squarefull}\},\\
\mathscr{E}_2(t) &:= \{e \le t : p \mid e \Rightarrow (p \mid a \text{ or } \ell(p) \le p/\log p)\},\\
\mathscr{E}_3(t) &:= \{e \le t : \lambda(e) \le e/\exp((\log e)^\theta)\}.
\end{aligned}$$

We set e_1, e_2, and e_3 equal to the largest divisors of n from the three sets $\mathscr{E}_1, \mathscr{E}_2, \mathscr{E}_3$, respectively. We start by showing that we can assume each of the following inequalities:

$$e_1 \le \log y, \tag{4.1}$$

$$e_2 \le \exp((\log y)^\theta), \tag{4.2}$$

$$e_3 \le y. \tag{4.3}$$

It is easy to dispense with (4.1). Indeed, by partial summation and the well-known estimate $\#\mathscr{E}_1(t) \ll \sqrt{t}$, the number of $n \le x$ with a squarefull divisor larger than $\log y$ is $O(x/(\log y)^{1/2})$. This is acceptable for us, since $\theta \le \frac{1}{2}$. To see that we can assume (4.2), note that the number of exceptional values of $n \le x$ is at most

$$\begin{aligned}
x \sum_{\substack{e > \exp((\log y)^\theta)\\ e \in \mathscr{E}_2(x)}} \frac{1}{e} &\le x\left(\frac{\#\mathscr{E}_2(x)}{x} + \int_{\exp((\log y)^\theta)}^{x} \frac{\#\mathscr{E}_2(t)}{t^2}\,dt\right)\\
&\ll \frac{x}{(\log x)^2}\log\log x + \frac{x}{(\log y)^\theta}\log\log y \ll \frac{x}{(\log y)^\theta}\log\log y,
\end{aligned}$$

where we have used the estimate of Lemma 4.4 for $\#\mathscr{E}_2$.

It remains to justify the assumption (4.3). We first estimate the counting function $\#\mathscr{E}_3(t)$. If e is counted by $\#\mathscr{E}_3(t)$, then either $e \le \sqrt{t}$ or $\lambda(e) \le e/\exp((\log\sqrt{t})^\theta)$. Lemma 4.5, with $x = t$ and $\Delta = (\log\sqrt{t})^\theta$, thus implies that for large t,

$$\#\mathscr{E}_3(t) \ll \sqrt{t} + t\exp(-(\log t)^{\theta/3}) \ll t/(\log t)^2.$$

Consequently, the number of $n \le x$ with a divisor $e > y$ belonging to $\mathscr{E}_3$ is

$$\ll x \sum_{\substack{e>y \\ e\in\mathscr{E}_3(x)}} \frac{1}{e} \le x\left(\frac{\#\mathscr{E}_3(x)}{x} + \int_y^x \frac{\#\mathscr{E}_3(t)}{t^2}\,dt\right) \ll \frac{x}{\log y},$$

which is negligible for us.

In addition to the conditions (4.1)–(4.3), we may also suppose that n does not have any divisor $d > y$ with $\Omega(d) \ge 10 \log\log d$. To see this, suppose for the sake of contradiction that d is such a divisor. In the case when $d > x^{1/2}$, this implies that

$$\Omega(n) \ge \Omega(d) \ge 10 \log\log d \ge 9 \log\log x.$$

But the number of $n \le x$ with $\Omega(n) \ge 9 \log\log x$ is $O(x/(\log x)^5)$ by Lemma 4.6, and this is negligible for us. If $d \le \sqrt{x}$, we can choose an integer $j \ge 0$ with

$$y^{2^j} < d \le y^{2^{j+1}} \le x.$$

Then with $z = y^{2^{j+1}}$, we have

$$\Omega(n; z) \ge \Omega(d) \ge 10 \log\log d \ge 10 \log\log(z^{1/2}) \ge 9 \log\log z,$$

and by Lemma 4.6 again, the number of such $n \le x$ is

$$\ll \frac{x}{(\log z)^5} \ll 2^{-5j} \frac{x}{(\log y)^5}.$$

Summing over j, we see that the number of possible values of x that can arise this way is $O(x/(\log y)^5)$, which is acceptable.

We will show that for all values of n that remain, every divisor $d > y$ of n satisfies

$$\ell^*(d) > d/\exp(4(\log d)^\theta). \tag{4.4}$$

From the last paragraph, we have

$$\Omega(d) < 10 \log\log d.$$

Put $d = d_1 d_2 q$, where d_1 is the largest divisor of n from $\mathscr{E}_1$ and d_2 is the largest divisor of d/d_1 from $\mathscr{E}_2$. Then q is squarefree and relatively prime to a, and $\ell(p) > p/\log p$ for every prime p dividing q. Moreover,

$$d_1 \le e_1 \le \log y \le \log d \tag{4.5}$$

and

$$d_2 \le e_2 \le \exp((\log y)^\theta) \le \exp((\log d)^\theta). \tag{4.6}$$

Since $d > y$ but $e_3 \le y$, it follows that $d \notin \mathscr{E}_3$, and so

$$\lambda(d) > d/\exp((\log d)^\theta). \tag{4.7}$$

Because $d = d_1 d_2 q$ with d_1, d_2, and q supported on disjoint sets of primes,

$$\lambda(d) = \operatorname{lcm}[\lambda(d_1), \lambda(d_2), \lambda(q)] \le \lambda(q) d_1 d_2.$$

Hence, estimates (4.5), (4.6), and (4.7) yield

(4.8)
$$\lambda(q) \geq \frac{\lambda(d)}{d_1 d_2} \geq \frac{d}{\exp((\log d)^\theta)} (\log d)^{-1} \exp(-(\log d)^\theta) > \frac{d}{\exp(3(\log d)^\theta)}.$$

For each prime p dividing q, write $p - 1 = \ell(p)\iota(p)$, so that $\iota(p)$ is the index of the subgroup of $\mathbf{F}_p^\times$ generated by a; from the definition of q,

$$\iota(p) < \frac{p}{\ell(p)} \leq \log p \leq \log d$$

for all p dividing q. Also,

$$\ell(q) = \operatorname*{lcm}_{p|q}[\ell(p)] = \operatorname*{lcm}_{p|q}\left[\frac{p-1}{\iota(p)}\right] \geq \frac{\operatorname{lcm}_{p|q}[p-1]}{\prod_{p|q} \iota(p)} = \frac{\lambda(q)}{\prod_{p|q} \iota(p)}.$$

Thus, from (4.8), the bound $\iota(p) \leq \log d$, and the inequality $\omega(q) \leq \Omega(d) < 10 \log\log d$,

$$\begin{aligned} \ell(q) &\geq \frac{d}{\exp(3(\log d)^\theta)} \Big(\prod_{p|q} \iota(p) \Big)^{-1} \\ &\geq \frac{d}{\exp(3(\log d)^\theta)} (\log d)^{-10 \log\log d} > \frac{d}{\exp(4(\log d)^\theta)}. \end{aligned}$$

Since q is a divisor of d that is coprime to a, we have that $\ell^*(d) \geq \ell(q)$, and so (4.4) holds. This completes the proof of the lemma. □

We also need a simple observation concerning the behavior of the function φ/ℓ^* along the divisor lattice (compare with [FPS01, Lemma 2]).

Lemma 4.8. *If d and e are natural numbers for which $d \mid e$, then $\frac{\varphi(d)}{\ell^*(d)} \mid \frac{\varphi(e)}{\ell^*(e)}$.*

Proof. By iteration, it suffices to treat the case when $e = qd$, where q is a prime. We will prove the equivalent result that, in this case,

$$\frac{\ell^*(qd)}{\ell^*(d)} \mid \frac{\varphi(qd)}{\varphi(d)}. \tag{4.9}$$

We can assume that $q \nmid a$, since otherwise the left-hand ratio is 1 and (4.9) holds trivially. We consider two cases, depending on whether or not q divides d. If $q \nmid d$, then

$$\ell^*(qd) = \operatorname{lcm}[\ell(q), \ell^*(d)] \mid \operatorname{lcm}[q-1, \ell^*(d)] \mid (q-1)\ell^*(d).$$

Hence,

$$\frac{\ell^*(qd)}{\ell^*(d)} \mid q - 1 = \frac{\varphi(qd)}{\varphi(d)},$$

i.e., (4.9) holds. Now suppose that $q \mid d$. Write $d = q^k d'$, where $q \nmid d'$. Then $\ell^*(qd) = \operatorname{lcm}[\ell(q^{k+1}), \ell^*(d')]$. Since $a^{\ell(q^k)} \equiv 1 \pmod{q^k}$, we have $a^{q\ell(q^k)} \equiv 1 \pmod{q^{k+1}}$, and so $\ell(q^{k+1}) \mid q\ell(q^k)$. Thus,

$$\ell^*(qd) = \operatorname{lcm}[\ell(q^{k+1}), \ell^*(d')] \mid \operatorname{lcm}[q\ell(q^k), \ell^*(d')] \mid q \operatorname{lcm}[\ell(q^k), \ell^*(d')].$$

Since $q \operatorname{lcm}[\ell(q^k), \ell^*(d')] = q\ell^*(d)$, we obtain (4.9) in this case upon noting that $\varphi(qd)/\varphi(d) = q$. □

4.3. Completion of the proof of Theorem 1.3. Throughout this section, we take $a = p$, where $\mathbf{F}_p$ is the field for which we are proving Theorem 1.3. Thus, $\ell^*(d)$ denotes the generalized order of p modulo d. We continue to suppress the dependence of implied constants on a.

Proof of Theorem 1.3. We may always assume that m is larger than any convenient constant (depending on p), since the theorem is trivial for bounded values of m.

Case 1: We suppose that

$$3 \le m \le x \exp(-\log x/\log\log x). \tag{4.10}$$

Suppose that $T^n - 1$ has a divisor of degree m in $\mathbf{F}_p[T]$. By Lemma 4.7, with $y = m$ and $\theta = 0.079$, we may assume that every divisor d of n with $d > m$ satisfies

$$\ell^*(d) > d/\exp(4(\log d)^{0.079});$$

indeed, the number of exceptional n is $O(x \log\log m/(\log m)^{0.079})$, which is small relative to our target upper bound. (Note that $\frac{1}{13} = 0.0769\ldots < 0.079$.) Since m appears as the degree of a divisor of $T^n - 1$, we can write

$$m = \sum_{d \mid n} \ell^*(d) a_d, \tag{4.11}$$

where each a_d satisfies $0 \le a_d \le \frac{\varphi(d)}{\ell^*(d)}$. For each d with $a_d > 0$, we have $\ell^*(d) \le m$. So, either $d \le m$ or

$$d/\exp(4(\log d)^{0.079}) < \ell^*(d) \le m. \tag{4.12}$$

The inequalities (4.12) force $d < M$, where

$$M := m \exp(5(\log m)^{0.079}).$$

Indeed, if we were to have $d > M$, then

$$\begin{aligned} m \ge d/\exp(4(\log d)^{0.079}) &> M/\exp(4(\log M)^{0.079}) \\ &\ge \frac{m \exp(5(\log m)^{0.079})}{\exp(5(\log m)^{0.079})} = m, \end{aligned}$$

contradicting (4.12). Of course, if $d \le m$, then it is also the case that $d \le M$. So $d \le M$ in any case.

Lemma 3.2 allows us to assume that $d(n; M) < (\log m)^2$, since the exceptional set has size $O(x/\log m)$. Referring back to (4.11), we see that there

is a divisor d of n with $\ell^*(d)a_d > m/(\log m)^2$. But $\ell^*(d)a_d \le \varphi(d) \le d$, so $d > m/(\log m)^2$. Therefore, n has a divisor in the interval $(m/(\log m)^2, M]$ and so is counted by $H(x, m/(\log m)^2, M)$. We estimate the number of such $n \le x$ using Lemmas 3.4 and 3.5. As in the proof of Theorem 1.2, there are three cases to consider:

- If $M \le \sqrt{x}$, we apply Lemma 3.4 directly, with $y = m/(\log m)^2$ and $z = M$. Then $\log(z/y) \asymp (\log m)^{0.079}$. On the other hand, $\log y \asymp \log m$. Thus, $u = \frac{\log(z/y)}{\log y} \asymp (\log m)^{-0.921}$. By Lemma 3.4,

$$H(x, y, z) \asymp xu^\delta \left(\log \frac{2}{u}\right)^{-3/2} \ll \frac{x}{(\log m)^{0.921\delta}} \ll \frac{x}{(\log m)^{0.079}}.$$

- If $\sqrt{x} < m/(\log m)^2$, Lemma 3.5 gives

$$H\left(x, \frac{m}{(\log m)^2}, M\right) \asymp H\left(x, \frac{x}{M}, \frac{x}{m/(\log m)^2}\right).$$

  Now set $y = x/M$ and $z = \frac{x}{m/(\log m)^2}$. We are assuming that $m \le x^{1-\frac{1}{\log\log x}}$, and so

$$\log y = \log \frac{x}{M} = \log\left(\frac{x/m}{e^{5(\log m)^{0.079}}}\right) \gg \frac{\log x}{\log\log x}.$$

  Since $z/y = M(\log m)^2/m < \exp(6(\log m)^{0.079})$, we see that

$$u = \frac{\log(z/y)}{\log y} \ll \frac{(\log m)^{0.079}}{\log x/\log\log x} \ll \frac{\log\log x}{(\log x)^{0.921}}.$$

  So by Lemma 3.4,

$$\begin{aligned} H(x, y, z) &\ll x\left(\frac{\log\log x}{(\log x)^{0.921}}\right)^\delta (\log\log x)^{-3/2} \\ &\ll \frac{x}{(\log m)^{0.079}}. \end{aligned}$$

- If $\frac{m}{(\log m)^2} \le \sqrt{x} < M$, then we certainly have $\frac{\sqrt{x}}{\exp(6(\log\sqrt{x})^{0.079})} \le \frac{m}{(\log m)^2}$ and $M \le \sqrt{x}\exp(6(\log x)^{0.079})$. Thus,

$$\begin{aligned} H\left(x, \frac{m}{(\log m)^2}, M\right) &= H\left(x, \frac{m}{(\log m)^2}, \sqrt{x}\right) + H\left(x, \sqrt{x}, M\right) \\ &\le H\left(x, \frac{\sqrt{x}}{\exp(6(\log\sqrt{x})^{0.079})}, \sqrt{x}\right) \\ &\quad + H\left(x, \sqrt{x}, \sqrt{x}\exp(6(\log x)^{0.079})\right). \end{aligned} \tag{4.13}$$

  We may now apply Lemmas 3.4 and 3.5 as in the previous two cases to show that each term on the right-hand side of (4.13) is $O(x/(\log x)^{0.079})$.

This completes the proof of the Theorem 1.3 in the case when m satisfies (4.10).

Case 2: We now suppose instead that

$$x \exp(-\log x/\log\log x) < m \le x.$$

Let $q = P^+(n)$. We will assume that $q > \exp(2\log x/\log\log x)$; by Lemma 3.6, this introduces an exceptional set of size $O(x/\log x)$, which is acceptable for us. Since m appears as the degree of a divisor of $T^n - 1$, we may write

$$m = \sum_{d|n} a_d \ell^*(d), \quad \text{where each} \quad 0 \le a_d \le \frac{\varphi(d)}{\ell^*(d)}. \tag{4.14}$$

Now consider (4.14) modulo $\ell^*(q)$. Whenever $q \mid d$, we have $\ell^*(q) \mid \ell^*(d)$. So mod $\ell^*(q)$, the only divisors that contribute to the sum in (4.14) are those d not divisible by q, and all of these d divide $r := n/q$. Consequently,

$$\ell^*(q) \mid \left(m - \sum_{d|r} a_d \ell^*(d) \right). \tag{4.15}$$

The right-hand side of relation (4.15) is (cf. (3.8)) at least

$$\begin{aligned} m - \sum_{d|r} \varphi(d) &= m - r \\ &\ge x \exp(-\log x/\log\log x) - x\exp(-2\log x/\log\log x) > 0. \end{aligned}$$

As in the proof of Case 2 of Theorem 1.2, our strategy will be to count, for each fixed r, the number of possibilities for q allowed by (4.15). Since q and r determine $n = qr$, this will lead to an upper bound on the number of possible values of n.

To carry this plan out, it is convenient to impose some restrictions on n additional to the lower bound on $q = P^+(n)$ assumed above, namely:

(i) $n > x/\log x$,
(ii) n satisfies the conditions of Lemma 4.7 with

$$\theta := 0.0579 \quad \text{and} \quad y := \exp(\log x/\log\log x).$$

(iii) $\Omega(n) \le 1.359 \log\log x$.

Clearly, (i) can be assumed excluding $O(x/\log x)$ values of n, which is acceptable. By Lemma 4.7, the number of $n \le x$ which are exceptions to (ii) is $O(x/(\log x)^{0.0578})$. Finally, by Lemma 3.3, the number of $n \le x$ which violate (iii) is $\ll x/(\log x)^{Q(1.359)} \ll x/(\log x)^{0.0578}$. (Note that the exponent $\frac{2}{35}$ claimed in this case of the theorem satisfies $\frac{2}{35} = 0.0571\ldots < 0.0578$.)

Since $r = n/q$ while $q > \exp(2\log x/\log\log x)$, the number of possible r is at most

$$x/\exp(2\log x/\log\log x).$$

Given r, the inequalities governing the a_d in (4.14) imply that the number of possibilities for the right-hand side of (4.15) is bounded by

$$\prod_{d|r} (1 + \varphi(d)/\ell^*(d)) . \tag{4.16}$$

By condition (ii) above, we have (using $n > x/\log x > y$)

$$\ell^*(n) > n/\exp(4(\log n)^\theta).$$

So by Lemma 4.8, the product (4.16) is bounded above by

$$\left(1 + \frac{\varphi(n)}{\ell^*(n)}\right)^{d(n)} \leq \left(1 + \exp(4(\log n)^\theta)\right)^{d(n)} \leq \exp(O((\log x)^\theta 2^{\Omega(n)})).$$

By condition (iii), $2^{\Omega(n)} \leq (\log x)^{1.359 \log 2}$, while $1.359 \log 2 + \theta < 0.9999$. So given r, the right-hand side of (4.15) is determined in at most

$$\exp((\log x)^{0.9999})$$

ways, for large x. Since the right-hand side of (4.15) is an integer in $[1, x]$, once it is fixed, the number of possibilities for its divisor $\ell^*(q)$ is at most

$$\exp(\log x/\log\log x).$$

(We are using again the maximal order of the divisor function.) Once more invoking condition (ii), we have (since $q > y^2 > y$)

$$\frac{q-1}{\ell^*(q)} < \frac{q}{\ell^*(q)} < \exp(4(\log q)^\theta) < \exp(4(\log x)^\theta);$$

since the ratio $(q-1)/\ell^*(q)$ is integral, we see that given $\ell^*(q)$, there are at most $\exp(4(\log x)^\theta)$ possibilities for q.

Piecing everything together (determining successively r, the right-hand side of (4.15), $\ell^*(q)$, and finally q), the number of possibilities for $n = rq$ is bounded above by

$$\frac{x}{\exp\left(2\frac{\log x}{\log\log x}\right)} \cdot \exp((\log x)^{0.9999}) \cdot \exp\left(\frac{\log x}{\log\log x}\right) \cdot \exp(4(\log x)^\theta) < \frac{x}{\exp\left(\frac{1}{2}\frac{\log x}{\log\log x}\right)} < \frac{x}{\log x},$$

which is negligible. This completes the proof of the second case of the theorem, with the exponent $\frac{2}{35} = 0.0571\ldots$ replaced by the larger number 0.0578. □

5. Concluding remarks: variations on the Q-practical numbers

Srinivasan's practical numbers have a natural dual, namely, those n for which each $m \in [0, \sigma(n)]$ has *at most one* representation as a sum of distinct divisors of n. Call these *efficient numbers*. Using the theory of sets of multiples, Erdős showed [Erd70, Theorem 2] that the set of efficient numbers possesses a positive asymptotic density.

On the polynomial side, we define n to be $\mathbf{Q}$-*efficient* if $T^n - 1$ has at most one monic divisor in $\mathbf{Q}[T]$ of each degree $m \in [0, n]$. Erdős's argument, based on the theory of sets of multiples, may be adapted to show that the $\mathbf{Q}$-efficient numbers also have positive density. Indeed, this is immediate from the methods of [Erd70] and the following lemma.

Lemma 5.1. *If $\mathscr{S}$ is the set of natural numbers n satisfying*

(i) *n is not $\mathbf{Q}$-efficient,*
(ii) *if $d \mid n$ and $d < n$, then d is $\mathbf{Q}$-efficient,*
(iii) *$\Omega(n) < 1.1 \log\log(3n)$,*

then the sum of the reciprocals of the members of $\mathscr{S}$ converges.

Proof. The proof is similar to Erdős's argument and to our own proof of Case 2 of Theorem 1.2, so we provide only a sketch. By partial summation, it suffices to show that the counting function of $\mathscr{S}$ is $O(x/(\log x)^2)$ for large x. Suppose that $n \in \mathscr{S} \cap [1, x]$. Since n is not $\mathbf{Q}$-efficient, there are two monic divisors of $T^n - 1$ of the same degree, and hence there is a nontrivial solution to the equation

$$\sum_{d \mid n} \epsilon_d \varphi(d) = 0, \quad \text{where each} \quad \epsilon_d \in \{-1, 0, 1\}. \tag{5.1}$$

(Here *nontrivial* means that not all $\epsilon_d = 0$.) Put $p := P^+(n)$. We can assume that

$$p > z^2, \quad \text{where} \quad z := \exp(\log x / \log\log x),$$

since the number of exceptional $n \le x$ is $O(x/(\log x)^2)$ by Lemma 3.6. We can also assume that p divides n only to the first power. Otherwise, n has squarefull part at least z^4, and the number of such $n \le x$ is $O(x/z^2)$, which is negligible.

Consider (5.1) modulo $p - 1$. Whenever $p \mid d$, one has that $p - 1 \mid \varphi(d)$. So putting $r := n/p$, it follows that

$$p - 1 \mid \sum_{d \mid r} \epsilon_d \varphi(d). \tag{5.2}$$

We claim that the right-hand side of (5.2) is a nonzero integer. If some ϵ_d appearing in (5.2) is nonzero, this is clear: In that case, the vanishing of the right-hand side of (5.2) implies that $T^r - 1$ has two monic divisors of the same degree, contradicting condition (ii) in the definition of $\mathscr{S}$. But if all

of the ϵ_d in (5.2) vanish, then the original sequence of ϵ_d appearing in (5.1) is supported on multiples of p. In that case, after dividing (5.1) through by $p-1$, we again obtain a contradiction to the $\mathbf{Q}$-efficiency of $r = n/p$.

Now we fix r and count the number of p allowed by (5.2). Mimicking the end of the proof of Case 2 of Theorem 1.2, we find that the number of possible n is at most

$$\frac{x}{\exp(2\log x/\log\log x)} \cdot 2^{2^{1.1\log\log(3x)}} \cdot \exp(\log x/\log\log x) < x/\exp(\frac{1}{2}\log x/\log\log x),$$

once x is large. (We use here that $1.1 < 1/\log 2$.) This last quantity is certainly $O(x/(\log x)^2)$. □

One might ask for both efficiency and practicality simultaneously, i.e., for numbers n where each $m \in [0, \sigma(n)]$ has *precisely one* representation as a sum of distinct divisors of n. The powers of 2 have this property, and it is not so hard to show that these are all such n. The answer to the analogous polynomial problem is perhaps more unexpected. Define a $\mathbf{Q}$-*optimal number* as an n for which $T^n - 1$ has precisely one monic divisor of each degree $m \in [0, n]$. In the remainder of this subsection, we classify the $\mathbf{Q}$-optimal numbers.

The following lemma is due to the second author [Tho12a, Lemma 4.1].

Lemma 5.2. *Suppose that n is $\mathbf{Q}$-practical. If p is a prime not dividing n, then pn is $\mathbf{Q}$-practical if and only if $p \le n+2$. Moreover, $p^k M$ is $\mathbf{Q}$-practical, where $k \ge 2$, if and only if $p \le n+1$.*

Let $F_m := 2^{2^m} + 1$ represent the mth *Fermat number*. Below, we use the well-known result that if p is an odd prime for which $p-1$ is a power of 2, then $p = F_m$ for some m (see [HW08, p. 18]); such a prime p is called a *Fermat prime*.

Proposition 5.3. *Let k be a nonnegative integer. Suppose that all of $F_0, F_1, \dots, F_{k-1}$ are prime. Then*

$$n := F_0 F_1 \cdots F_{k-1} \tag{5.3}$$

is a $\mathbf{Q}$-optimal number with k distinct prime factors. (We understand that $n = 1$ if $k = 0$.) Conversely, if there is any $\mathbf{Q}$-optimal number with k distinct prime factors, then $F_0, \dots, F_{k-1}$ are all prime, and n is given by (5.3).

Proof (sufficiency). Suppose that all of $F_0, \dots, F_{k-1}$ are prime, and define n by (5.3). The $\mathbf{Q}$-practicality of n follows immediately from Lemma 5.2 and the identity

$$\begin{aligned} F_0 F_1 \cdots F_{j-1} + 2 &= (2^{2^0} - 1)\left((2^{2^0}+1)(2^{2^1}+1)\cdots(2^{2^{j-1}}+1)\right) + 2 \\ &= (2^{2^j} - 1) + 2 = F_j, \end{aligned}$$

valid for all $j \geq 0$ (provided one interprets the empty product as 1). Moreover, the identity (1.1) and the irreducibility of the cyclotomic polynomials together imply that the number of monic divisors of $T^n - 1$ is $2^{d(n)} = 2^{2^k}$, while the number of integers in $[0, n]$ is precisely

$$n + 1 = F_0 \cdots F_{k-1} + 1 = F_k - 1 = 2^{2^k}.$$

As these two numbers agree, the $\mathbf{Q}$-practicality of n implies the $\mathbf{Q}$-efficiency of n (by the pigeonhole principle). Hence, n is $\mathbf{Q}$-optimal. □

Proof (necessity). This is clear if $k = 0$, so assume that $k \geq 1$. The key observation is that for each $\mathbf{Q}$-optimal number n, we have the formal identity

$$\prod_{d|n} (1 + T^{\varphi(d)}) = \sum_{m=0}^{n} T^m = \frac{1 - T^{n+1}}{1 - T}. \tag{5.4}$$

Evaluating (5.4) at $T = 1$, we find that $2^D = n + 1$, so that $n = 2^D - 1$. In particular, n is odd. Feeding the equality $n = 2^D - 1$ back into (5.4), we find that

$$\begin{aligned} \prod_{d|N} (1 + T^{\varphi(D)}) &= \frac{1 - T^{2^D}}{1 - T} \\ &= (1 + T)(1 + T^2)(1 + T^4) \cdots (1 + T^{2^{D-1}}). \end{aligned}$$

In both sides of this identity, we have a product of D nonconstant polynomials. Moreover, each of the D right-hand factors is irreducible over $\mathbf{Q}$ (in fact, $1 + T^{2^{j-1}} = \Phi_{2^j}(T)$). It follows from uniqueness of factorization in $\mathbf{Q}[T]$ that if one arranges the list of terms $\varphi(d)$, where $d \mid n$, in increasing order, one obtains the sequence $\langle 1, 2, 4, \ldots, 2^{D-1} \rangle$.

The number n must be squarefree. Otherwise, $p^2 \mid n$ for some $p \geq 3$ and so $\varphi(p^2) = p(p - 1)$ is divisible by p, contradicting that $\varphi(p^2)$ is a power of 2. So we may write

$$n = p_1 \cdots p_k, \quad \text{where} \quad p_1 < p_2 < \cdots < p_k.$$

Since each $\varphi(d)$ is a power of 2, we have in particular that each $p_i - 1 = \varphi(p_i)$ is a power of 2, and so p_i is a Fermat prime. Hence, the prime factorization of n can be rewritten in the form

$$n = F_{i_1} \cdots F_{i_k}, \quad \text{where} \quad 0 \leq i_1 < i_2 < \cdots < i_k.$$

To complete the proof, we have to show that the sequence $\langle i_1, i_2, \ldots, i_k \rangle$ coincides with the sequence $\langle 0, 1, \ldots, k - 1 \rangle$.

We claim that $T^n - 1$ has a divisor of degree $m := F_{i_1} F_{i_2} \cdots F_{i_{k-1}} + 1$. To see this, it is sufficient (since n is $\mathbf{Q}$-practical) to show that $m \leq n$. Clearly,

$$m + 1 \leq F_0 F_1 F_2 \cdots F_{i_{k-1}} + 2 = F_{i_{k-1}+1}. \tag{5.5}$$

Since $i_k \geq i_{k-1}+1$, we have $m+1 \leq F_{i_k} \leq n$. So $m < n$. Write m as a sum of distinct terms $\varphi(d)$, where $d \mid n$. If every d involved in this representation divides $F_{i_1} \cdots F_{i_{k-1}} = n/F_{i_k}$, then $m \leq \sum_{d \mid F_{i_1} \cdots F_{i_{k-1}}} \varphi(d) = F_{i_1} \cdots F_{i_{k-1}}$, which is not the case. So some d in the representation is divisible by F_{i_k}, and hence $F_{i_k} - 1 \leq \varphi(d) \leq m$. Hence,

$$F_{i_k} \leq m+1.$$

But from (5.5), we also have

$$m+1 \leq F_{i_{k-1}+1} \leq F_{i_k}.$$

It follows that $i_k = i_{k-1}+1$ and that equality holds throughout (5.5). The latter forces the $(k-1)$-tuple $\langle i_1, i_2, \ldots, i_{k-1}\rangle$ to coincide with the $(i_{k-1}+1)$-tuple $\langle 0, 1, 2, \ldots, i_{k-1}\rangle$, so that $\langle i_1, \ldots, i_{k-1}\rangle = \langle 0, 1, \ldots, k-2\rangle$. Since $i_k = i_{k-1}+1$, we conclude that $\langle i_1, i_2, \ldots, i_k\rangle = \langle 0, 1, \ldots, k-1\rangle$, as was to be shown. □

Corollary 5.4. *There are precisely six* **Q***-optimal numbers, namely* $2^{2^i}-1$ *for* $i = 0, 1, \ldots, 5$.

Proof. Since $F_0, F_1, \ldots, F_4$ are prime while $F_5 = 641 \cdot 6700417$, Proposition 5.3 shows that the **Q**-optimal numbers are precisely the numbers $F_0 F_1 \cdots F_{i-1} = 2^{2^i}-1$ for $i = 0, 1, \ldots, 5$. □

Acknowledgements

We thank Greg Martin and Carl Pomerance for helpful conversations. Some of the work on this paper was conducted while the first author was visiting Dartmouth College. He thanks the Dartmouth mathematics department for their hospitality.

References

[Car84] Car, M. Polynômes de $\mathbf{F}_q[X]$ ayant un diviseur de degré donné, *Acta Arith.* **43** (1984), no. 2, 131–154. MR0773783 (86j:11125), Zbl 0493.12022.

[dB66] de Bruijn, N. G. On the number of positive integers $\leq x$ and free prime factors $> y$. II, *Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math.* **28** (1966), 239–247. MR0205945 (34 #5770), Zbl 0139.27203.

[EPS91] Erdős, P.; Pomerance, C.; Schmutz, E. Carmichael's lambda function, *Acta Arith.* **58** (1991), no. 4, 363–385. MR1121092 (92g:11093), Zbl 0734.11047.

[Erd50] Erdős, P. On a Diophantine equation, *Mat. Lapok* **1** (1950), 192–210. MR0043117 (13,208b).

[Erd70] ———, Some extremal problems in combinatorial number theory, *Mathematical Essays Dedicated to A. J. Macintyre, Ohio Univ. Press, Athens, Ohio,* 1970, pp. 123–133. MR0276194 (43 #1942), Zbl 0214.30602.

[For08] Ford, K. The distribution of integers with a divisor in a given interval, *Ann. of Math.* (2) **168** (2008), no. 2, 367–433. MR2434882 (2009m:11152), Zbl 1181.11058.

[FPS01] Friedlander, J. B.; Pomerance, C.; Shparlinski, I. E. Period of the power generator and small values of Carmichael's function, *Math. Comp.* **70** (2001), no. 236, 1591–1605, errata in **71** (2002), 1803–1806. MR2434882 (2009m:11152), Zbl 1029.11043.

[Got12] Gottschlich, A. On positive integers n dividing the nth term of an elliptic divisibility sequence, *New York J. Math.* **18** (2012), 409–420. MR2928585, Zbl 06098855.

[HS84] Hausman, M.; Shapiro, H. N. On practical numbers, *Comm. Pure Appl. Math.* **37** (1984), no. 5, 705–713. MR0752596 (86a:11036), Zbl 0544.10005.

[HT88] Hall, R. R.; Tenenbaum, G. Divisors, Cambridge Tracts in Mathematics, vol. 90, *Cambridge University Press, Cambridge,* 1988. MR0964687 (90a:11107), Zbl 0653.10001.

[HW08] Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Sixth edition. *Oxford University Press, Oxford,* 2008. MR2445243 (2009i:11001), Zbl 1159.11001.

[KP05] Kurlberg, P.; Pomerance, C.; On the periods of the linear congruential and power generators, *Acta Arith.* **119** (2005), no. 2, 149–169. MR2167719 (2006k:11153), Zbl 1080.11059.

[KZ01] Knopfmacher, J.; Zhang, W.-B. Number theory arising from finite fields, Monographs and Textbooks in Pure and Applied Mathematics, vol. 241, *Marcel Dekker Inc., New York,* 2001. MR1835434 (2002h:11089), Zbl 0982.11054.

[Mar91] Margenstern, M. Les nombres pratiques: théorie, observations et conjectures, *J. Number Theory* **37** (1991), no. 1, 1–36. MR1089787, Zbl 0715.11001.

[PT12] Pollack, P.; Thompson, L. Practical pretenders, *Publ. Math. Debrecen* **82** (2013), to appear.

[Rib72] Ribenboim, P. Algebraic numbers, Pure and Applied Mathematics, vol. 27, *Wiley-Interscience, New York-London-Sydney,* 1972. MR0340212, Zbl 0247.12002.

[Sai97] Saias, E. Entiers à diviseurs denses. I, *J. Number Theory* **62** (1997), no. 1, 163–191. MR1430008 (98c:11096), Zbl 0872.11039.

[Sie55] Sierpiński, W. Sur une propriété des nombres naturels, *Ann. Mat. Pura Appl.* (4) **39** (1955), 69–74. MR0075219 (17,711d), Zbl 0066.29104.

[Sri48] Srinivasan, A. K. Practical numbers, *Current Science* **17** (1948), 179–180. MR0027799 (10,356e).

[Ste54] Stewart, B. M. Sums of distinct divisors, *Amer. J. Math.* **76** (1954), 779–785. MR0064800 (16,336d), Zbl 0056.27004.

[Ten86] Tenenbaum, G. Sur un problème de crible et ses applications, *Ann. Sci. École Norm. Sup.* (4) **19** (1986), no. 1, 1–30. MR0860809 (87m:11094), Zbl 0599.10037.

[Ten95] ———, Sur un problème de crible et ses applications. II. Corrigendum et étude du graphe divisoriel, *Ann. Sci. École Norm. Sup.* (4) **28** (1995), no. 2, 115–127. MR1318066 (96e:11119), Zbl 0852.11048.

[Tho12a] Thompson, L. Polynomials with divisors of every degree, *J. Number Theory* **132** (2012), 1038–1053. MR2890525, Zbl 06030257.

[Tho12b] ———, Products of distinct cyclotomic polynomials, *Ph.D. thesis, Dartmouth College,* 2012.

[Tho12c] ———, Variations on a question concerning the degrees of divisors of $x^n - 1$, submitted; e-print available at `arXiv:1206.4355 [math.NT]` (2012).

[Tho12d] ———, On the divisors of $x^n - 1$ in $\mathbf{F}_p[x]$, *Int. J. Number Theory* **9** (2013), no. 2, 421–430.

Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, Georgia 30602, USA
pollack@uga.edu

Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, Georgia 30602, USA
lola@math.uga.edu