

# ON THE DIVISORS OF $x^n - 1$ IN $\mathbb{F}_p[x]$

LOLA THOMPSON

ABSTRACT. In a recent paper, we considered integers  $n$  for which the polynomial  $x^n - 1$  has a divisor in  $\mathbb{Z}[x]$  of every degree up to  $n$ , and we gave upper and lower bounds for their distribution. In this paper, we consider those  $n$  for which the polynomial  $x^n - 1$  has a divisor in  $\mathbb{F}_p[x]$  of every degree up to  $n$ , where  $p$  is a rational prime. Assuming the validity of the Generalized Riemann Hypothesis, we show that such integers  $n$  have asymptotic density 0.

## 1. INTRODUCTION AND STATEMENT OF RESULTS

In a recent paper [10], we examined the question “How often does  $x^n - 1$  have a divisor in  $\mathbb{Z}[x]$  of every degree between 1 and  $n$ ?” We called an integer  $n$  with this property  $\varphi$ -practical and showed that

$$\#\{n \leq X : n \text{ is } \varphi\text{-practical}\} \asymp \frac{X}{\log X}.$$

We examined variants of this question over other polynomial rings in [8] and [11]. In [8], Pollack and I extended the notion of  $\varphi$ -practical by defining an integer  $n$  to be  $F$ -practical if  $x^n - 1$  has a divisor of every degree between 1 and  $n$  over a number field  $F$ . We showed that, for any number field  $F$ ,

$$\#\{n \leq X : n \text{ is } F\text{-practical}\} \asymp_F \frac{X}{\log X}.$$

We shifted our focus to fields with positive characteristic in [11]. For each rational prime  $p$ , we defined an integer  $n$  to be  $\mathbb{F}_p$ -practical if  $x^n - 1$  has a divisor in  $\mathbb{F}_p[x]$  of every degree between 1 and  $n$ . Since every  $\varphi$ -practical number is  $p$ -practical for all  $p$ , our work from [10] immediately implies that  $\#\{n \leq X : n \text{ is } p\text{-practical}\}$  is at least a positive constant times  $\frac{X}{\log X}$ . Moreover, we showed in [11] that

$$\#\{n \leq X : n \text{ is } p\text{-practical for all } p\} \ll \frac{X}{\log X}$$

and that, for any fixed  $p$ ,

$$\#\{n \leq X : n \text{ is } p\text{-practical but not } \varphi\text{-practical}\} \gg \frac{X}{\log X}.$$

The difficulty lies in finding an upper bound for the count of integers up to  $X$  that are  $p$ -practical for an arbitrary but fixed prime  $p$ . This will be the subject of our present investigation.

For each fixed prime  $p$ , we define

$$F_p(X) := \#\{n \leq X : n \text{ is } p\text{-practical}\}.$$

Computational data seem to suggest an estimate for the order of magnitude of  $F_p(X)$ . For example, when  $p = 2$ , we can use Sage to compute a table of ratios of  $F_2(X)/\frac{X}{\log X}$ .

$X$	$F_2(X)$	$F_2(X)/(X/\log X)$
$10^2$	34	1.565758
$10^3$	243	1.678585
$10^4$	1790	1.648651
$10^5$	14703	1.692745
$10^6$	120276	1.661674
$10^7$	1030279	1.660614

TABLE 1. Ratios for 2-practicals

The table looks similar for other small values of  $p$ . For example, when  $p = 3, 5$  we have:

$X$	$F_3(X)$	$F_3(X)/(X/\log X)$
$10^2$	41	1.888120
$10^3$	258	1.782201
$10^4$	1881	1.732465
$10^5$	15069	1.734883
$10^6$	127350	1.759405
$10^7$	1080749	1.741962

TABLE 2. Ratios for 3-practicals

$X$	$F_5(X)$	$F_5(X)/(X/\log X)$
$10^2$	46	2.118378
$10^3$	286	1.975618
$10^4$	2179	2.006933
$10^5$	16847	1.939583
$10^6$	141446	1.954149
$10^7$	1223577	1.972173

TABLE 3. Ratios for 5-practicals

The fact that the sequences of ratios appear to vary slowly suggests the following conjecture:

**Conjecture 1.1.** *For each prime  $p$ ,  $\lim_{X \rightarrow \infty} F_p(X) / \frac{X}{\log X}$  exists.*

The strongest bound that we have been able to prove in this vein is as follows:

**Theorem 1.2.** *Let  $p$  be a prime number. Assuming that the Generalized Riemann Hypothesis holds, we have  $F_p(X) = O\left(X \sqrt{\frac{\log \log X}{\log X}}\right)$ .*

Here we use a version of the Generalized Riemann Hypothesis for Kummerian fields. The dependence on the GRH arises from a lemma of Li and Pomerance that we will use in Section 2.

For ease of reference, we compile a list of the common notation that will be used throughout this paper. Let  $n$  always represent a positive integer. Let  $p$  and  $q$ , as well as any subscripted variations, be primes. Let  $P(n)$  denote the largest prime factor of  $n$ , with  $P(1) = 1$ . We say that an integer  $n$  is  $B$ -smooth if  $P(n) \leq B$ . We will use  $P^-(n)$  to denote the smallest prime factor of  $n$ , with  $P^-(1) = +\infty$ .

We will use several common arithmetic functions in this body of work. Let  $\tau(n)$  denote the number of positive divisors of  $n$ . We use  $\Omega(n)$  to denote the number of prime factors of  $n$  counting multiplicity. Lastly, let  $\lambda(n)$  denote the Carmichael  $\lambda$ -function, which represents the exponent of the multiplicative group of integers modulo  $n$ .

## 2. PRELIMINARY LEMMAS

In this section, we provide some preliminary lemmas that will be used in the proof of Theorem 1.2. We begin by discussing multiplicative orders and their connection to the  $p$ -practical numbers. Let  $\ell_a(n)$  denote the multiplicative order of  $a$  modulo  $n$  for integers  $a$  with  $(a, n) = 1$ . If  $(a, n) > 1$ , let  $n_{(a)}$  represent the largest divisor of  $n$  that is coprime to  $a$ , and let  $\ell_a^*(n) = \ell_a(n_{(a)})$ . In particular, if  $(a, n) = 1$ , then  $\ell_a^*(n) = \ell_a(n)$ . In [11], we gave an alternative characterization of the  $p$ -practical numbers in terms of the function  $\ell_p^*(n)$ , which we state here as a lemma:

**Lemma 2.1.** *An integer  $n$  is  $p$ -practical if and only if every  $m$  with  $1 \leq m \leq n$  can be written as  $m = \sum_{d|n} \ell_p^*(d) n_d$ , where  $n_d$  is an integer with  $0 \leq n_d \leq \frac{\varphi(d)}{\ell_p^*(d)}$ .*

Throughout the remainder of this section, let  $a > 1$  be an integer and let  $A_q$  denote the set of primes  $p \equiv 1 \pmod{q}$  with  $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ . We will make use of several lemmas from [5], which we state here for the sake of completeness.

**Lemma 2.2** (Li, Pomerance). *Let  $\psi(X)$  be an arbitrary function for which  $\psi(X) = o(X)$  and  $\psi(X) \geq \log \log X$ . The number of integers  $n \leq X$  divisible by a prime  $p > \psi(X)$  with  $\ell_a^*(p) < \frac{p^{1/2}}{\log p}$  is  $O\left(\frac{X}{\log \psi(X)}\right)$ .*

**Lemma 2.3** (Li, Pomerance). *The number of integers  $n \leq X$  divisible by a prime  $p \equiv 1 \pmod{q}$  with*

$$\frac{q^2}{4 \log^2 q} < p \leq q^2 \log^4 q$$

is  $O\left(\frac{X \log \log q}{q \log q}\right)$ .

**Lemma 2.4** (Li, Pomerance). *(GRH) Suppose that  $q$  is an odd prime and that  $a$  is not a  $q^{\text{th}}$  power. The number of integers  $n \leq X$  divisible by a prime  $p \in A_q$  with  $p \geq q^2 \log^4 q$  is  $O\left(\frac{X}{q \log q} + \frac{X \log \log X}{q^2}\right)$ .*

Next, we present a version of Proposition 1 from Li and Pomerance's paper [5], which will play an important role in obtaining the bound stated in Theorem 1.2. As in [5], our lemma will make use of Lemma 2.4; thus, it will depend on the validity of the Generalized Riemann Hypothesis.

**Lemma 2.5.** *(GRH) Let  $a$  be a positive integer. Let  $\psi(X)$  be defined as in Lemma 2.2. The number of integers  $n \leq X$  with  $P\left(\frac{\lambda(n)}{\ell_a^*(n)}\right) \geq \psi(X)$  is  $O\left(\frac{X \log \log \psi(X)}{\log \psi(X)}\right)$ .*

*Proof.* Suppose that  $n \leq X$  and  $q = P(\lambda(n)/\ell_a^*(n)) \geq \psi(X)$ . We may assume that  $X$  is large, so  $a$  is not a  $q^{\text{th}}$  power and  $\psi(X) > a$ . Moreover, as we will now show, it must be the case that either  $q^2 \mid n$  or  $p \mid n$  for some  $p \in A_q$ . Observe that

$$q \mid \frac{\lambda(n)}{\ell_a^*(n)} \mid \frac{\text{lcm}_{p^e \mid n} [\lambda(p^e)]}{\text{lcm}_{p^e \mid n} [\ell_a^*(p^e)]} \mid \text{lcm}_{p^e \mid n} \left[ \frac{\lambda(p^e)}{\ell_a^*(p^e)} \right].$$

In particular,  $q$  must divide  $\frac{\lambda(p^e)}{\ell_a^*(p^e)}$  for some prime  $p$ . If  $q = p$ , then  $q \mid \lambda(p^e)$  implies that  $e \geq 2$ , so  $q^2 \mid n$ . If  $q \neq p$ , then  $q \mid \frac{\lambda(p)}{\ell_a^*(p)}$ , so  $p > q > \psi(X) > a$ . Thus,  $\ell_a^*(p) = \ell_a(p) \mid \frac{p-1}{q}$ , so  $p \mid a^{\frac{p-1}{q}} - 1$ , which implies that  $p \in A_q$ .

To handle the case where  $q^2 \mid n$ , we observe that

$$\begin{aligned} \#\{n \leq X : q^2 \mid n \text{ for some prime } q \geq \psi(X)\} &\leq \sum_{\substack{q \geq \psi(X) \\ q \text{ prime}}} \left\lfloor \frac{X}{q^2} \right\rfloor \\ &\leq X \sum_{\substack{q \geq \psi(X) \\ q \text{ prime}}} \frac{1}{q^2} \ll \frac{X}{\psi(X)}. \end{aligned}$$

Thus, we may assume that  $n$  is divisible by a prime  $p \in A_q$  with  $p > a$ .

By Lemma 2.2, we may assume that  $\ell_a^*(p) \geq p^{1/2}/\log p$ . However, since  $p \in A_q$  implies that  $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ , then  $\ell_a(p) \leq \frac{p-1}{q}$ , so  $p > \frac{q^2}{(4 \log^2 q)}$ . Thus, we can use Lemmas 2.3 and

2.4 to deal with the remaining values of  $n \leq X$ . In particular, we have

$$\begin{aligned}
& \#\{n \leq X : p \mid n \text{ for some } p \in A_q \text{ with } p > q^2/(4 \log^2 q)\} \\
& \leq \#\{n \leq X : p \mid n \text{ for some } p \equiv 1 \pmod{q} \text{ with } p \in (\frac{q^2}{4 \log^2 q}, q^2 \log^4 q]\} \\
& \quad + \#\{n \leq X : p \mid n \text{ for some } p \in A_q \text{ with } p \geq q^2 \log^4 q\} \\
(2.1) \quad & \ll \frac{X \log \log q}{q \log q} + \frac{X}{q \log q} + \frac{X \log \log X}{q^2},
\end{aligned}$$

where the final inequality follows from Lemmas 2.3 and 2.4. Since our hypotheses specify that  $q \geq \psi(X)$ , then the bound given in (2.1) implies

$$\begin{aligned}
& \#\{n \leq X : q \geq \psi(X) \text{ and } p \mid n \text{ for some } p \in A_q\} \\
& \ll X \sum_{q \geq \psi(X)} \left( \frac{\log \log q}{q \log q} + \frac{\log \log X}{q^2} \right) \\
& \ll \frac{X \log \log \psi(X)}{\log \psi(X)}.
\end{aligned}$$

□

### 3. KEY LEMMA

The key to proving Theorem 1.2 rests in showing that  $\ell_p^*(n)$  is usually not too small. We make this statement precise with the following lemma:

**Lemma 3.1.** (GRH) *Let  $\theta$  be a constant satisfying  $\frac{1}{10} \leq \theta \leq \frac{9}{10}$ . Let  $Y = e^{110(\log X)^\theta (\log \log X)^2}$ . For all  $a > 1$  and  $X$  sufficiently large, uniformly in  $\theta$ , we have*

$$(3.1) \quad \#\{n \leq X : \ell_a^*(n) \leq \frac{X}{Y e^{(\log X)^\theta}}\} \ll \frac{X}{(\log X)^\theta \log \log X}.$$

Before we prove Lemma 3.1, we will introduce three additional results, the first of which is due to Friedlander, Pomerance and Shparlinski [2] and the last of which is due to Luca and Pollack [6].

**Lemma 3.2.** *For sufficiently large numbers  $X$  and for  $\Delta \geq (\log \log X)^3$ , the number of positive integers  $n \leq X$  with*

$$\lambda(n) \leq n \exp(-\Delta)$$

*is at most  $X \exp(-0.69(\Delta \log \Delta)^{1/3})$ .*

**Corollary 3.3.** *Let  $\theta$  be as in Lemma 3.1. For sufficiently large  $X$ , the number of positive integers  $n \leq X$  with*

$$\lambda(n) \leq \frac{X}{e^{(\log X)^\theta}}$$

*is at most  $X/e^{(\log X)^\theta/3}$ .*

*Proof.* Trivially, there are at most  $X/\exp((\log X)^{\theta/2})$  values of  $n \leq X/\exp((\log X)^{\theta/2})$  with  $\lambda(n) \leq X/\exp((\log X)^{\theta})$ . On the other hand, if  $X/\exp((\log X)^{\theta/2}) < n \leq X$ , then  $X \leq n \exp((\log X)^{\theta/2})$ . Thus, for large  $X$ , we have

$$\begin{aligned} \#\left\{\frac{X}{e^{(\log X)^{\theta/2}}} < n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^{\theta}}}\right\} &\leq \#\left\{n \leq X : \lambda(n) \leq \frac{ne^{(\log X)^{\theta/2}}}{e^{(\log X)^{\theta}}}\right\} \\ &< \#\left\{n \leq X : \lambda(n) \leq \frac{n}{e^{\frac{1}{2}(\log X)^{\theta}}}\right\}. \end{aligned}$$

Applying Lemma 3.2 with  $\Delta = \frac{1}{2}(\log X)^{\theta}$ , we see that this is at most  $X/\exp(2(\log X)^{\theta/3})$ . Therefore,

$$\#\left\{n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^{\theta}}}\right\} \leq \frac{X}{e^{(\log X)^{\theta/2}}} + \frac{X}{e^{2(\log X)^{\theta/3}}} \leq \frac{X}{e^{(\log X)^{\theta/3}}}.$$

□

**Lemma 3.4.** *But for  $O(\frac{X}{(\log X)^3})$  choices of  $n \leq X$ , we have*

$$\Omega(\varphi(n)) < 110(\log \log X)^2.$$

We will use these results in the proof of Lemma 3.1, which we present below.

*Proof.* Let  $\theta$  be such that  $\frac{1}{10} \leq \theta \leq \frac{9}{10}$ , let  $B = e^{(\log X)^{\theta}}$  and let  $u(n)$  denote the  $B$ -smooth part of  $\lambda(n)$ . Let  $Y$  be defined as in the statement of Lemma 3.1. If  $\lambda(n)$  has a large  $B$ -smooth part, say  $u(n) > Y$ , then so does  $\varphi(n)$ , since  $u(n)$  must divide  $\varphi(n)$  as well. First, we will estimate the number of  $n \leq X$  for which  $u(n) > Y$ . Let  $\Omega(u(n)) = k$ . By definition, all prime factors of  $u(n)$  are at most  $e^{(\log X)^{\theta}}$ . Thus, we have

$$Y < u(n) \leq (e^{(\log X)^{\theta}})^k.$$

Solving for  $k$ , we obtain  $k \geq 110(\log \log X)^2$ . However, Lemma 3.4 implies that  $k < 110(\log \log X)^2$  except for  $O(\frac{X}{(\log X)^3})$  values of  $n \leq X$ . Hence, we can conclude that there are at most  $O(\frac{X}{(\log X)^3})$  values of  $n$  for which the  $B$ -smooth part of  $\lambda(n)$  is larger than  $Y$ . Thus, using Lemma 3.3, we have

$$\begin{aligned} \#\{n \leq X : \frac{\lambda(n)}{u(n)} \leq \frac{X}{Ye^{(\log X)^{\theta}}}\} &\leq \#\{n \leq X : \lambda(n) \leq \frac{X}{e^{(\log X)^{\theta}}}\} + \#\{n \leq X : u(n) > Y\} \\ &\ll \frac{X}{e^{(\log X)^{\theta/3}}} + \frac{X}{(\log X)^3}. \end{aligned}$$

However, if we take  $\psi(X) = Y \exp\{(\log X)^{\theta}\}$  then we can use Lemma 2.5 to show that, for all but  $O(\frac{X}{(\log X)^{\theta} \log \log X})$  choices of  $n \leq X$ , we have  $\frac{\lambda(n)}{u(n)} \mid \ell_a^*(n)$ . Therefore, we have

$$\ell_a^*(n) \geq \frac{\lambda(n)}{u(n)} > \frac{X}{Ye^{(\log X)^{\theta}}},$$

except for at most  $O\left(\frac{X}{(\log X)^\theta \log \log X}\right)$  values of  $n \leq X$ .  $\square$

#### 4. PROOF OF THEOREM 1.2

In this section, we present the proof of our main theorem. We begin by discussing the remaining lemmas that we will need in order to complete the argument. Let  $n$  be a positive integer, with  $d_1 < d_2 < \dots < d_{\tau(n)}$  its increasing sequence of divisors. Let  $Z \geq 2$ . We say that  $n$  is  $Z$ -dense if  $\max_{1 \leq i \leq \tau(n)} \frac{d_{i+1}}{d_i} \leq Z$  holds. The following lemma, due to Saias (cf. [9, Theorem 1]), describes the count of integers with  $Z$ -dense divisors.

**Lemma 4.1** (Saias). *For  $X \geq Z \geq 2$ , we have*

$$(4.1) \quad \#\{n \leq X : n \text{ is } Z\text{-dense}\} \ll \frac{X \log Z}{\log X}.$$

The next lemma is due essentially to Friedlander, Pomerance and Shparlinski (cf. [2, Lemma 2]).

**Lemma 4.2.** *Let  $n$  and  $d$  be positive integers with  $d \mid n$ . Then, for any rational prime  $p$ , we have  $\frac{d}{\ell_p^*(d)} \leq \frac{n}{\ell_p^*(n)}$ .*

*Proof.* The result is proven in [2] when  $(p, n) = 1$ . In the case where  $(p, n) > 1$ , let  $n_{(p)}$  and  $d_{(p)}$  represent the largest divisors of  $n$  and  $d$  that are coprime to  $p$ , respectively. Then

$$\frac{d}{d_{(p)}} \leq \frac{n}{n_{(p)}},$$

since the highest power of  $p$  dividing  $d$  is at most the highest power of  $p$  dividing  $n$ . After a rearrangement, we have

$$\frac{d}{n} \leq \frac{d_{(p)}}{n_{(p)}} \leq \frac{\ell_p^*(d)}{\ell_p^*(n)},$$

where the final inequality follows from the coprime case.  $\square$

We will also use the following elementary lemma:

**Lemma 4.3.** *Let  $X \geq 2$  and let  $\kappa \geq 1$ . Then, we have*

$$\#\{n \leq X : \tau(n) \geq \kappa\} \ll \frac{1}{\kappa} X \log X.$$

*Proof.* We observe that

$$\sum_{n \leq X} \tau(n) = \sum_{n \leq X} \sum_{d \mid n} 1 \leq X \sum_{d \leq X} \frac{1}{d} \ll X \log X.$$

The number of terms in the sum on the left-hand side of the equation that are  $\geq \kappa$  is  $\ll \frac{1}{\kappa} X \log X$ .  $\square$

Now we have all of the tools needed to prove Theorem 1.2. Below, we present its proof.

*Proof.* Let  $n$  be a positive integer with divisors  $d_1 < d_2 < \dots < d_{\tau(n)}$ . Let  $p$  be a rational prime with  $p \nmid n$ . Let  $\theta$  and  $Y$  be as in Lemma 3.1. In (4.1), set  $Z = Y^2$ . Assume that  $n$  is not in the set of size  $O(X \log Y^2 / \log X)$  of integers with  $Y^2$ -dense divisors. Then there exists an index  $j$  with

$$(4.2) \quad \frac{d_{j+1}}{d_j} > Y^2.$$

Moreover, we can use Lemma 4.3 to show that

$$(4.3) \quad \#\{n \leq X : \tau(n) > Y/e^{(\log X)^\theta}\} \ll \frac{X e^{(\log X)^\theta} \log X}{Y}.$$

As a result, we will assume hereafter that  $\tau(n) \leq Y/e^{(\log X)^\theta}$ . Examining the ratios  $\frac{d_{k+1}}{d_k}$ , we remark that it is always the case that  $d_1 = 1$  and  $d_2 = P^-(n)$ ; hence, we have

$$\#\{n \leq X : \frac{d_2}{d_1} > Y^2\} = \sum_{\substack{n \leq X \\ P^-(n) > Y^2}} 1 \ll X \prod_{q \leq Y^2} \left(1 - \frac{1}{q}\right),$$

where the final inequality follows from applying Brun's Sieve (cf. [3, Theorem 2.2]). By Mertens' Theorem (cf. [7, Theorem 3.15]), we have

$$(4.4) \quad X \prod_{q \leq Y^2} \left(1 - \frac{1}{q}\right) \ll \frac{X}{\log Y}.$$

Now, suppose that  $k > 1$ . On one hand, for all  $k > 1$ , we have

$$(4.5) \quad 1 + \sum_{l \leq k} \ell_p^*(d_l) \frac{\varphi(d_l)}{\ell_p^*(d_l)} = 1 + \sum_{l \leq k} \varphi(d_l) \leq k d_k \leq Y e^{-(\log X)^\theta} d_k.$$

On the other hand, Lemma 3.1 implies that  $\ell_p^*(n) > \frac{X}{Y e^{(\log X)^\theta}}$  but for

$$(4.6) \quad O\left(\frac{X}{(\log X)^\theta \log \log X}\right)$$

integers  $n \leq X$ . For such numbers  $n$ , for all  $i \geq 1$ , we have

$$(4.7) \quad \ell_p^*(d_{j+i}) \geq \frac{\ell_p^*(n) d_{j+i}}{n} > \frac{d_{j+i}}{Y e^{(\log X)^\theta}} > \frac{d_j Y^2}{Y e^{(\log X)^\theta}} = Y e^{-(\log X)^\theta} d_j$$

where the inequalities follow, respectively, from Lemma 4.2, Lemma 3.1 and the assumption that there exists an index  $j$  for which (4.2) holds. As a result, we can combine the inequality from (4.5) applied with  $k = j$  with (4.7) to show that

$$1 + \sum_{l \leq j} \ell_p^*(d_l) \frac{\varphi(d_l)}{\ell_p^*(d_l)} < \ell_p^*(d_{j+i})$$

holds for all  $i \geq 1$ . Thus,  $x^n - 1$  has no divisor of degree  $1 + \sum_{l \leq j} \varphi(d_l)$  in  $\mathbb{F}_p[x]$ , so  $n$  is not  $p$ -practical. Therefore, by (4.1), (4.3), (4.4) and (4.6), we have

$$(4.8) \quad F_p(X) \ll \frac{X \log Y}{\log X} + \frac{X e^{(\log X)^\theta} \log X}{Y} + \frac{X}{\log Y} + \frac{X}{(\log X)^\theta \log \log X}.$$

Now, the only significant terms in (4.8) are  $\frac{X}{(\log X)^\theta \log \log X}$  and  $\frac{X \log Y}{\log X}$ . Equating these expressions and using the fact that  $Y = e^{110(\log X)^\theta (\log \log X)^2}$ , we obtain  $\theta = \frac{1}{2} - \frac{3 \log_3 X}{2 \log_2 X}$  as a good choice for  $\theta$ . Plugging this value of  $\theta$  into the bound  $\frac{X}{(\log X)^\theta \log \log X}$  yields a bound of  $O\left(X \sqrt{\frac{\log \log X}{\log X}}\right)$  for the size of the set of  $p$ -practicals up to  $X$ .  $\square$

*Acknowledgements.* The work contained in this paper comprises a portion of my Ph.D. thesis [12]. I would like to thank my adviser, Carl Pomerance, for his guidance throughout the process of completing this work. I would also like to thank Paul Pollack for pointing out the relevant results in [6] and for his help with simplifying a few of my arguments.

#### REFERENCES

- [1] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith. **58** no. 4 (1991), 363 – 385.
- [2] J. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of the Carmichael function*, Math. Comp. **70** (2001), 1591 – 1605.
- [3] H. Halberstam and H.-E. Richert, *Sieve methods*. Academic Press, London, 1974.
- [4] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer*, Algebra Number Theory (to appear).
- [5] S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205 – 224.
- [6] F. Luca and P. Pollack, *An arithmetic function arising from Carmichael's conjecture*, J. Théorie des Nombres de Bordeaux **23** (2011), 697 – 714.
- [7] P. Pollack, *Not always buried deep: a second course in elementary number theory*. Amer. Math. Soc., Providence, 2009.
- [8] P. Pollack and L. Thompson, *On the degrees of divisors of  $T^n - 1$* , submitted, e-print available at <http://arxiv.org/abs/1206.2084>.
- [9] E. Saias, *Entiers à diviseurs denses. I.*, J. Number Theory **62** (1997), 163 – 191.
- [10] L. Thompson, *Polynomials with divisors of every degree*, J. Number Theory **132** (2012), p. 1038 - 1053.
- [11] ———, *Variations on a question concerning the degrees of divisors of  $x^n - 1$* , submitted, e-print available at <http://math.dartmouth.edu/~thompson/notes.html>.
- [12] ———, *Products of distinct cyclotomic polynomials*, Ph.D. thesis, Dartmouth College, 2012.

DEPARTMENT OF MATHEMATICS, 6188 KEMENY HALL, DARTMOUTH COLLEGE, HANOVER, NH 03755, USA

*E-mail address:* Lola.Thompson@Dartmouth.edu