



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



General Section

# Prime divisors of sparse values of cyclotomic polynomials and Wieferich primes <sup>☆</sup>

M. Ram Murty <sup>\*</sup>, François Séguin

Department of Mathematics, Queen's University, Kingston, Ontario K7L 3N6,  
Canada

ARTICLE INFO

ABSTRACT

*Article history:*

Received 17 September 2018

Received in revised form 31

December 2018

Accepted 25 February 2019

Available online 20 March 2019

Communicated by F. Pellarin

*MSC:*

11B39

11N69

11D45

11A41

*Keywords:*

Lucas sequences

Wieferich primes

Bang (1886), Zsigmondy (1892) and Birkhoff and Vandiver (1904) initiated the study of the largest prime divisors of sequences of the form  $a^n - b^n$ , denoted  $P(a^n - b^n)$ , by essentially proving that for integers  $a > b > 0$ ,  $P(a^n - b^n) \geq n + 1$  for every  $n > 2$ . Since then, the problem of finding bounds on the largest prime factor of Lehmer sequences, Lucas sequences or special cases thereof has been studied by many, most notably by Schinzel (1962), and Stewart (1975, 2013). In 2002, Murty and Wong proved, conditionally upon the *abc* conjecture, that  $P(a^n - b^n) \gg n^{2-\epsilon}$  for any  $\epsilon > 0$ . In this article, we improve this result for the specific case where  $b = 1$ . Specifically, we obtain a more precise result, and one that is dependent on a condition we believe to be weaker than the *abc* conjecture. Our result actually concerns the largest prime factor of the  $n$ th cyclotomic polynomial evaluated at a fixed integer  $a$ ,  $P(\Phi_n(a))$ , as we let  $n$  grow. We additionally prove some results related to the prime factorization of  $\Phi_n(a)$ . We also present a connection to Wieferich primes, as well as show that the finiteness of a particular subset of Wieferich primes is a sufficient condition for the infinitude of non-Wieferich primes. Finally, we use the technique used in the proof of the

<sup>☆</sup> Research of the first author partially supported by an NSERC Discovery grant. Research of the second author partially supported by a FRQNT B2 Research Scholarship.

<sup>\*</sup> Corresponding author.

E-mail addresses: [murty@mast.queensu.ca](mailto:murty@mast.queensu.ca) (M.R. Murty), [francois.seguin@queensu.ca](mailto:francois.seguin@queensu.ca) (F. Séguin).

aforementioned results to show an improvement on average of estimates due to Erdős for certain sums.

© 2019 Elsevier Inc. All rights reserved.

## 1. Introduction

In 1965, Erdős [2] conjectured that

$$\frac{P(2^n - 1)}{n} \rightarrow \infty \quad \text{as } n \rightarrow \infty,$$

where  $P(m)$  denotes the largest prime factor of  $m$ . This prompted the study of this special case of Lucas numbers. In 1975, Stewart showed [13] that given  $0 < \lambda < 1/\log 2$ ,

$$\frac{P(a^n - b^n)}{n} \rightarrow \infty$$

as  $n$  goes to infinity, provided that  $n$  only runs through integers with at most  $\lambda \log \log n$  prime factors. By a famous theorem of Hardy and Ramanujan [4], “almost all” numbers (in the sense of natural density) satisfy this condition. His approach relies heavily on Baker’s theory of linear forms in logarithms.

In 2002, Ram Murty and Wong [9] proved, conditionally to the *abc* conjecture, that for any  $\epsilon > 0$  and  $a > b > 0$  integers, then

$$P(a^n - b^n) > n^{2-\epsilon} \tag{1.1}$$

for  $n$  large enough, which in particular gives a conditional proof of Erdős’s conjecture. As remarked above, Theorem 1.1 gives an improvement on this result in the specific case of  $b = 1$ , mostly by weakening the hypothesis.

In 2004, Murata and Pomerance [5] proved conditionally to the generalized Riemann hypothesis that

$$P(2^n - 1) > \frac{n^{4/3}}{\log \log n}$$

for a set of positive integers  $n$  of asymptotic density 1.

Finally, in 2013, Stewart [12] proved Erdős’s conjecture unconditionally, specifically by showing that for suitable  $\alpha$  and  $\beta$  (for which the corresponding Lucas sequence is non-degenerate),

$$P(\Phi_n(\alpha, \beta)) > n \exp\left(\frac{\log n}{104 \log \log n}\right)$$

for  $n$  large enough, where,  $\Phi_n(\alpha, \beta)$  denotes the homogeneous cyclotomic polynomial. For  $\alpha = 2, \beta = 1$ , this proves Erdős’s conjecture (see Remark 1 below).

These last two results use heavily the method of linear forms in logarithms and methods of transcendental number theory.

Here, we give an improvement on the result of Murty and Wong in the specific case where  $b = 1$ . Specifically, we give an alternative hypothesis which we believe to be weaker than the *abc* conjecture, and obtain a more precise formulation of the lower bound.

**Theorem 1.1.** *Let  $P(m)$  denote the largest prime divisor of  $m$ . Let  $a > 1$  be an integer, and  $f_a(p)$  be the multiplicative order of  $a$  modulo  $p$ . Suppose that there exists a constant  $\kappa$  for which  $\text{ord}_p(a^{f_a(p)} - 1) \leq \kappa$  for all primes  $p$ . Then, there exists a positive constant  $C$  (depending on  $a$  and  $\kappa$ ) such that*

$$P(\Phi_n(a)) > C\phi(n)^2$$

for all  $n$ .

This is related to the study of  $P(a^n - 1)$  as explained in Remark 1.

This result is in line with a conjecture that Stewart formulated in [14], stating that for  $\alpha$  and  $\beta$  real numbers, it should be the case that

$$P(\Phi_n(\alpha, \beta)) > C\phi(n)^2$$

for any  $n > 2$  and where  $C$  is a positive constant. Stewart also states that the conjecture is true when  $\Phi_n(\alpha, \beta)$  is square free, and hints at part of the argument we use in the proof of Theorem 1.1.

We call the primes  $p$  such that  $a^{p-1} \equiv 1 \pmod{p^2}$  *Wieferich primes (for  $a$ )*. Classically, Wieferich primes usually refer to the specific case where  $a = 2$ . However, every argument goes through for arbitrary  $a \geq 2$ . We expect them to be sparse in all the primes. The only Wieferich primes  $p \leq 4 \times 10^{17}$  for  $a = 2$  are 1093 and 3511, and those are the only two we know of at the moment. Heuristically, if we think of  $(a^{p-1} - 1)/p$  as a random integer, the probability that  $p$  divides it is approximately  $1/p$ . As such, according to these heuristics, we could expect around

$$\sum_{p \leq x} \frac{1}{p} \ll \log \log x$$

Wieferich primes up to  $x$  (see [1] for more details). As they are expected to be sparse, it is difficult to determine whether there are finitely many or infinitely many of them.

We can then restrict our attention to the set of *super-Wieferich primes (for  $a$ )* which are the primes  $p$  such that  $a^{p-1} \equiv 1 \pmod{p^3}$ . Obviously, they form a subset of the Wieferich primes. However, the same heuristics suggest that the number of such primes is

$$\sum_p \frac{1}{p^2} \leq c',$$

that is, there are only finitely many of them. In turn, this suggests that there should be an integer  $k$ , independent of  $p$ , for which  $a^{p-1} \not\equiv 1 \pmod{p^k}$  for any prime  $p$ . Notice that this is an even weaker assumption to make than the finiteness of super-Wieferich primes.

The hypothesis appearing in the statement of Theorem 1.1 is even weaker. Let  $p^{\gamma_p}$  be the largest power of  $p$  dividing  $a^{p-1} - 1$ , and  $p^{\alpha_p}$  be the largest power  $p$  dividing  $a^{f(p)} - 1$ . Instead of looking at the  $\gamma_p$ , our hypothesis will concern  $\alpha_p$ . Since  $f(p)|p - 1$ , we can write  $f(p)r = p - 1$  so that

$$a^{p-1} = a^{f(p)r} \equiv 1^r \equiv 1 \pmod{p^{\alpha_p}}$$

and so

$$\alpha_p \leq \gamma_p \tag{1.2}$$

for all  $p$ . We will be assuming in Theorem 1.1 that  $\alpha_p$  is bounded. Again, this would follow from the finiteness of super-Wieferich primes.

**Remark 1.** Recall that

$$\prod_{d|n} \Phi_d(a) = a^n - 1, \tag{1.3}$$

and therefore,  $\Phi_n(a)$  divides  $a^n - 1$ . As such, the above Theorem 1.1 implies that  $P(a^n - 1) > C\phi(n)^2$  for  $n$  large enough granted that  $\alpha_p$  is bounded. Additionally, recall that we have the bound  $\phi(n) \gg \frac{n}{\log \log n}$  due to Ramanujan. As such, we get as a corollary that under the same hypothesis on  $\alpha_p$ ,

$$P(a^n - 1) > C' \frac{n^2}{(\log \log n)^2}.$$

For any integer  $n > 4$ ,  $n \neq 6, 12$ , we will see from Lemma 2.3 that there is at most one prime dividing both  $n$  and  $\Phi_n(a)$ , which we will call  $P_n$ . We define  $\delta_n$  as the largest power of  $P_n$  dividing  $\Phi_n(a)$ , i.e.

$$p^{\delta_p} || \Phi_n(a).$$

Actually, in Lemma 2.3 below, we will see that  $\delta_n$  is always 0 or 1.

We will be proving the following theorem about  $\delta_n$ .

**Theorem 1.2.** For some  $\theta < 1$ ,

$$\sum_{n \leq x} \delta_n \log P_n = O(x^\theta).$$

This also gives the following obvious corollary.

**Corollary 1.3.** *For some  $\theta < 1$ ,*

$$\sum_{n \leq x} \delta_n = O(x^\theta).$$

In particular, this shows that  $\delta_n$  is zero “most of the time”.

Using our analysis of Wieferich primes used to prove Theorem 1.1, we are also able to prove the following result.

**Theorem 1.4.** *Suppose that there are only finitely many super-Wieferich primes. Then, there are infinitely many non-Wieferich primes.*

Finally, applying the technique developed in Section 3 to different arithmetic functions, we are able to prove the following result

**Theorem 1.5.**

$$\sum_{n \leq x} \sum_{d|a^n-1} \frac{1}{d} = Rx + o(x)$$

where  $R$  is the “Romanoff” constant

$$R := \sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{1}{d f_a(d)}.$$

In particular, this gives an improvement on average to a result of Erdős [3] (see (5.1) below).

## 2. Proof of Theorem 1.1

Let  $f_a(p)$  be the order of  $a$  in the group  $(\mathbb{Z}/p\mathbb{Z})^\times$ . For the sake of readability, we will write  $f(p)$  instead of  $f_a(p)$  when  $a$  is clear from context. We start by stating a few facts about the cyclotomic polynomials  $\Phi_n(x)$ .

**Proposition 2.1.** *For any prime  $p$  not dividing  $m$  or  $a$ ,*

$$f_a(p) = m \quad \text{if and only if} \quad p | \Phi_m(a).$$

**Proof.** This is exercise 1.5.25 in [6].  $\square$

**Proposition 2.2.**

$$\Phi_n(a) \geq \frac{1}{2} a^{\phi(n)}.$$

See [15] for the proof.

We also need the following description of the primes dividing  $\Phi_n(a)$ , which is [14, Lemma 6].

**Lemma 2.3.** *If  $n > 4$  and  $n \neq 6, 12$ , then  $P(n/(3, n))$  divides  $\Phi_n(a)$  to at most the first power. All other primes factors of  $\Phi_n(a)$  are congruent to 1 (mod  $n$ ).*

Finally, we will need to use the Brun-Titchmarsh Theorem, which we recall here.

**Theorem 2.4** (Brun-Titchmarsh). *Let  $\theta < 1$  and  $d < x^\theta$ . For  $x$  sufficiently large,*

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{d}}} \log p \leq \frac{2x \log x}{\phi(d) \log(x/d)}$$

where  $\phi(d)$  is Euler’s totient function.

Recall that we define the integer  $\alpha_p$  as  $\text{ord}_p(a^{f(p)} - 1)$ , i.e.

$$p^{\alpha_p} \parallel a^{f(p)} - 1.$$

Clearly,  $\alpha_p \geq 1$  for every prime  $p$ .

**Proposition 2.5.** *For every prime  $p$  coprime to  $a$ ,  $\text{ord}_p(\Phi_{f(p)}(a)) = \alpha_p$ .*

**Proof.** Let  $p$  be any prime coprime to  $a$ . We can factor  $a^{f(p)} - 1$  above to get that

$$p^{\alpha_p} \parallel \prod_{d|f(p)} \Phi_d(a).$$

We claim that actually,  $p$  cannot divide any factor  $\Phi_d(a)$  other than  $\Phi_{f(p)}(a)$ . Indeed, suppose that  $p$  divides  $\Phi_d(a)$  for some  $d$  strictly dividing  $f(p)$ . Clearly,  $p$  does not divide  $d$  as  $d$  divides  $f(p)$  which divides  $p - 1$ . Therefore, by Proposition 2.1,  $f(p) = d$  which is a contradiction. We conclude that

$$p^{\alpha_p} \parallel \Phi_{f(p)}(a). \quad \square$$

Note that we essentially have the prime factorization for  $\Phi_n(a)$ . If we take any  $n$ , then every prime factor  $p$  of  $\Phi_n(a)$  other than those dividing  $n$  are such that  $f(p) = n$  by Proposition 2.1. Therefore, by the above, for those primes,  $p^{\alpha_p} \parallel \Phi_n(a)$ . The only

prime factors of  $\Phi_n(a)$  for which we don't know the order are those also dividing  $n$ . By Lemma 2.3, there is at most one such prime, namely  $P_n = P(n/(3, n))$  (when  $n > 4$  and not 6 or 12). Additionally, Lemma 2.3 tells us that

$$P_n^{\delta_n} \parallel \Phi_n(a)$$

where  $\delta_n$  is either 0 or 1. We just proved the following.

**Proposition 2.6.** For  $n > 4$ ,  $n \neq 6, 12$ ,

$$\Phi_n(a) = P_n^{\delta_n} \prod_{\substack{p \mid \Phi_n(a) \\ p \neq P_n}} p^{\alpha_p}.$$

With this description in hand, let us now prove Theorem 1.1.

**Proof of Theorem 1.1.** We will argue by contradiction. Suppose that  $P(\Phi_n(a)) \leq C\phi(n)^2$ . Then,

$$\Phi_n(a) \leq P_n^{\delta_n} \prod_{\substack{p \leq C\phi(n)^2 \\ p \neq P_n}} p^{\alpha_p}$$

and by the second part of Lemma 2.3,

$$\leq P_n^{\delta_n} \prod_{\substack{p \leq C\phi(n)^2 \\ p \equiv 1 \pmod n}} p^{\alpha_p}.$$

By taking the logarithm,

$$\log \Phi_n(a) \leq \log P_n^{\delta_n} + \sum_{\substack{p \leq C\phi(n)^2 \\ p \equiv 1 \pmod n}} \alpha_p \log p.$$

Since we assume that  $\alpha_p \leq \kappa$  for all  $p$ , we have

$$\leq \log P_n^{\delta_n} + \kappa \sum_{\substack{p \leq C\phi(n)^2 \\ p \equiv 1 \pmod n}} \log p$$

and by Theorem 2.4

$$\ll \delta_n \log P_n + \kappa \left( \frac{2C\phi(n)^2}{\phi(n)} \right) \tag{2.1}$$

for  $n$  large enough.

On the other hand, by Proposition 2.2 we have

$$\Phi_n(a) \geq \frac{1}{2} a^{\phi(n)}$$

and so

$$\log \Phi_n(a) \geq \phi(n) \log a - \log 2. \tag{2.2}$$

Putting (2.1) and (2.2) together, we get that

$$\phi(n) \log a - \log 2 \ll 2\kappa C \phi(n) + \delta_n \log P_n.$$

Note that  $\log P_n \leq \log n$ . Therefore, if  $C$  is sufficiently small, we obtain a contradiction for  $n$  large enough.  $\square$

As we pointed out, this result is close to (1.1) which Murty and Wong obtained assuming the *abc* conjecture. We remark here that assuming a weaker hypothesis, to which we will refer as the *quasi-abc*, we easily get a lower bound on  $P(a^n - b)$  for any  $a, b \in \mathbb{Z}$  with  $a \geq 2$ .

**Conjecture 2.7** (*The quasi-abc conjecture*). *There exists a constant  $k$  such that for any mutually coprime integers  $a, b$  and  $c$  such that  $a + b = c$ ,*

$$\max(|a|, |b|, |c|) \leq (\text{rad}(abc))^k.$$

**Proposition 2.8.** *Let  $a, b$  be integers,  $a \geq 2$ . Assuming the quasi-abc conjecture, there exists an effectively computable constant  $C$  depending on  $a$  and  $b$  such that*

$$P(a^n - b) \geq Cn.$$

**Proof.** We write  $a^n - b + b = a^n$  and apply the quasi-*abc* conjecture. There exists a constant  $k$  such that

$$a^n \leq \left( ab \prod_{p|a^n-b} p \right)^k$$

and so

$$n \log a \leq k \sum_{p \leq P(a^n-b)} \log p + C'.$$

We know that (see [6, 3.1.2])

$$\sum_{p \leq x} \log p \ll x,$$



by Chebycheff. Therefore, we conclude that

$$P(a^n - b) \geq Cn$$

as required.  $\square$

### 3. Proof of Theorem 1.2

We first need the following simple formula for the  $p$ -adic valuation of certain binomial coefficients.

**Lemma 3.1.** *For any prime  $p$  and any integer  $1 \leq k \leq p^n$ ,*

$$\text{ord}_p \left( \binom{p^n}{k} \right) = n - \text{ord}_p(k).$$

**Proof.** For  $k = p^n$ , this is clear. For any  $m$  in the range  $1 \leq m < p^n$ , by the ultrametric inequality, we have that  $\text{ord}_p(p^n - m) = \text{ord}_p(m)$ . By definition,

$$k! \binom{p^n}{k} = p^n(p^n - 1) \cdots (p^n - (k - 1)),$$

and by taking the valuation on both sides

$$\text{ord}_p(k!) + \text{ord}_p \left( \binom{p^n}{k} \right) = n + \text{ord}_p((k - 1)!),$$

from which the result follows directly.  $\square$

Next, we give a description of the multiplicative order of the element  $a$  modulo powers of the prime  $p$ . Here, we extend the definition of  $f_a(p)$  to powers of  $p$  in the obvious way, by defining  $f(p^n)$  to be the multiplicative order of  $a$  in the group  $(\mathbb{Z}/p^n\mathbb{Z})^\times$ .

**Proposition 3.2.** *Let  $p$  be any prime,  $a$  any non-zero integer and define  $\alpha_p$  as  $\text{ord}_p(a^{f(p)} - 1)$ . Then, for any  $r \geq 0$ ,*

$$f(p^{\alpha_p+r}) = p^r f(p).$$

**Proof.** In this proof we fix  $p$  and write  $\alpha = \alpha_p$  for simplicity of notation. To begin, notice the following three facts that are true for any  $r$ .

(1)  $f(p^{\alpha+r})$  divides  $p^r f(p^\alpha)$ .

Indeed,

$$a^{p^r f(p^\alpha)} = (1 + mp^\alpha)^{p^r}$$

for some integer  $m$ , and so by the binomial theorem

$$a^{p^r f(p^\alpha)} = \sum_{k=0}^{p^r} \binom{p^r}{k} m^k p^{k\alpha}.$$

We note in passing that for any integer  $k > 0$ ,

$$k \geq p^{\text{ord}_p(k)} \geq 2^{\text{ord}_p(k)} \geq \text{ord}_p(k) + 1.$$

For  $k > 0$ , the  $k$ th term in the sum is given by

$$T_k := \binom{p^r}{k} m^k p^{k\alpha}$$

and so

$$\text{ord}_p(T_k) \geq r - \text{ord}_p(k) + k\alpha,$$

and by Lemma 3.1,

$$\begin{aligned} &\geq r - (k - 1) + k\alpha \\ &\geq r + \alpha + (\alpha - 1)(k - 1) \\ &\geq r + \alpha, \end{aligned}$$

where the last inequality follows from  $\alpha \geq 1$ . Therefore, we conclude that

$$a^{p^r f(p^\alpha)} \equiv 1 \pmod{p^{\alpha+r}},$$

meaning that  $f(p^{\alpha+r})$  divides  $p^r f(p^\alpha)$ .

- (2) For any  $m$ ,  $f(p^m)$  divides  $f(p^{m+1})$ .

This is because

$$a^{f(p^{m+1})} \equiv 1 \pmod{p^{m+1}}$$

and so

$$a^{f(p^{m+1})} \equiv 1 \pmod{p^m}.$$

Note that this fact actually implies the following

- (3)  $f(p) = f(p^2) = \dots = f(p^\alpha)$ .

Indeed, for any  $1 \leq m \leq \alpha$ ,  $f(p)|f(p^m)$  by the above. On the other hand,  $a^{f(p)} - 1 \equiv 0 \pmod{p^m}$ , meaning that  $f(p^m)|f(p)$ .

Now, to show the statement of Proposition 3.2, we proceed by induction on  $r$ . From (3) above, we can instead show that  $f(p^{\alpha_p+r}) = p^r f(p^\alpha)$ .

When  $r = 1$ , we have from (1) above that  $f(p^{\alpha+1})|pf(p^\alpha)$ . However,  $f(p^{\alpha+1})$  must be a multiple of  $p$ , as otherwise

$$f(p^{\alpha+1})|f(p^\alpha) = f(p)$$

meaning that

$$a^{f(p)} - 1 \equiv 0 \pmod{p^{\alpha+1}}$$

which contradicts the definition of  $\alpha$ .

On the other hand, by (2) above,  $f(p^{\alpha+1})$  must be a multiple of  $f(p^\alpha)$ . We conclude that  $f(p^{\alpha+1}) = pf(p^\alpha)$  which is the base case.

Using induction, we show that  $f(p^{\alpha+r}) = p^r f(p^\alpha)$ .

As before, using (1) we get

$$f(p^{\alpha+r})|p^r f(p^\alpha).$$

On the other hand, by the induction hypothesis and (2),

$$p^{r-1} f(p^\alpha) = f(p^{\alpha+r-1})|f(p^{\alpha+r}).$$

We get from the above that  $f(p^{\alpha+r}) = p^q f(p^\alpha)$  where  $q$  is either  $r$  or  $r - 1$ . We are only left to show that  $q$  cannot be  $r - 1$ . Suppose it is. Then, on one hand, by definition,

$$a^{f(p^{\alpha+r})} \equiv 1 \pmod{p^{\alpha+r}}.$$

On the other hand, write  $a^{f(p)} = 1 + kp^\alpha$ . Then,

$$\begin{aligned} a^{f(p^{\alpha+r})} &= a^{f(p)p^{r-1}} \\ &= (1 + kp^\alpha)^{p^{r-1}} \\ &\equiv 1 + kp^{\alpha+r-1} \pmod{p^{\alpha+r}}. \end{aligned}$$

We can conclude that  $k$  must be divisible by  $p$ , meaning that  $a^{f(p)} = 1 + k'p^{\alpha+1}$ , which is a contradiction to the definition of  $\alpha$ .  $\square$

Now consider the Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{\log(a^n - 1)}{n^s}.$$

We need the following lemma about  $F(s)$ .

**Lemma 3.3.** *We can write the Dirichlet series  $F(s)$  as*

$$F(s) = \zeta(s) \left( \sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s) \right)$$

where  $D(s)$  is a Dirichlet series absolutely convergent for  $\Re(s) > \theta$  for some  $\theta < 1$ .

To prove this lemma, we will need the following two results which can be found in [7].

**Theorem 3.4.** *For any  $\epsilon > 0$ ,*

$$\sum_{m \geq 1} \frac{1}{mf_a(m)^\epsilon} \leq e^\gamma \log \log a + 2e^\gamma \epsilon^{-1} + C$$

for some constant  $C$ .

In the above theorem, the definition of  $f_a(p)$  is extended to any integer  $m$  as

$$f_a(m) = \inf \{r \in \mathbb{Z} : r \geq 1 \text{ and } a^r \equiv 1 \pmod{m}\}.$$

**Theorem 3.5.** *For any  $\epsilon > 0$ ,*

$$\sum_p \frac{\log p}{pf_a(p)^\epsilon} \leq \log \log a + 2\epsilon^{-1} + C$$

for some constant  $C$ .

We use this to prove Lemma 3.3.

**Proof.** First, notice that we can write  $\log m = \sum_{d|m} \Lambda(d)$  where  $\Lambda$  is the von Mangoldt function. Therefore, we have the alternative expression for  $F(s)$ :

$$\begin{aligned} F(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|a^n-1} \Lambda(d) \\ &= \sum_{d=1}^{\infty} \Lambda(d) \sum_{n: d|a^n-1} \frac{1}{n^s}. \end{aligned}$$

We know that  $d|a^n - 1$  if and only if  $a^n \equiv 1 \pmod{d}$  if and only if  $f(d)|n$ . Thus,

$$F(s) = \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \Lambda(d) \sum_{n: f(d)|n} \frac{1}{n^s}$$

$$\begin{aligned}
 &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \Lambda(d) \sum_{m=1}^{\infty} \frac{1}{(mf(d))^s} \\
 &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} \zeta(s).
 \end{aligned} \tag{3.1}$$

Now we show that

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} = \sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s)$$

with  $D(s)$  as in the statement of the lemma.

We first notice that the summand on the left-hand side is non-zero only when  $d$  is a prime power. As such, we have

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} = \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \sum_{r=1}^{\infty} \frac{\Lambda(p^r)}{f(p^r)^s}.$$

Note that for a fixed prime  $p$ , the summand for  $r$  between 1 and  $\alpha_p$  will be the same, namely  $\frac{\log p}{f(p)^s}$ . For  $r = \alpha_p + q$ , by Proposition 3.2, it will be  $\frac{\log p}{p^{qs} f(p)^s}$ . We get

$$\begin{aligned}
 \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{\Lambda(d)}{f(d)^s} &= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \left( \frac{\alpha_p \log p}{f(p)^s} + \sum_{q=1}^{\infty} \frac{\log p}{p^{qs} f(p)^s} \right) \\
 &= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s} \sum_{q=1}^{\infty} \frac{1}{p^{qs}} \\
 &= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s} \left( \frac{1}{1 - \frac{1}{p^s}} - 1 \right) \\
 &= \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\alpha_p \log p}{f(p)^s} + \sum_{\substack{p \text{ prime} \\ (p,a)=1}} \frac{\log p}{f(p)^s (p^s - 1)}.
 \end{aligned}$$

Consider the series

$$D(s) = \sum_{p:(p,a)=1} \frac{\log p}{f(p)^s (p^s - 1)}.$$

Trying to evaluate the series at  $s = 1$ , we obtain

$$D(1) = \sum_{p:(p,a)=1} \frac{\log p}{(p-1)f(p)} \leq C' \sum_p \frac{\log p}{pf(p)} \leq C''$$

for some constants  $C'$  and  $C''$ , where the last inequality is obtained from Theorem 3.5. Therefore  $D(s)$  is an absolutely convergent series for  $s = 1$ . However, Landau’s Theorem (see [6, 2.5.14]) tells us that a Dirichlet series with non-negative terms must have a singularity at  $s = \sigma_0$ , where  $\sigma_0$  is its abscissa of convergence. Since our series  $D(s)$  converges at  $s = 1$ , we conclude that 1 cannot be its abscissa of convergence, and so that  $D(s)$  must converge strictly to the left of 1.

Therefore, we have

$$F(s) = \zeta(s) \left( \sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s) \right)$$

with  $D(s)$  as required.  $\square$

We use this lemma to prove Theorem 1.2.

**Proof.** From Lemma 3.3,

$$\frac{1}{\zeta(s)} \sum_{n=1}^{\infty} \frac{\log(a^n - 1)}{n^s} = \sum_p \frac{\alpha_p \log p}{f(p)^s} + D(s).$$

On one hand,

$$\begin{aligned} \frac{1}{\zeta(s)} \sum_{n=1}^{\infty} \frac{\log(a^n - 1)}{n^s} &= \left( \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) \left( \sum_{n=1}^{\infty} \frac{\log(a^n - 1)}{n^s} \right) \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \left( \sum_{d|n} \mu(d) \log(a^{n/d} - 1) \right) \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \left( \log \prod_{d|n} (a^{n/d} - 1)^{\mu(d)} \right) \\ &= \sum_{n=1}^{\infty} \frac{\log \Phi_n(a)}{n^s}. \end{aligned}$$

On the other hand, we can write

$$\sum_p \frac{\alpha_p \log p}{f(p)^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

as a Dirichlet series where

$$a_n = \sum_{p:f(p)=n} \alpha_p \log p.$$

However, by Proposition 2.1, this is

$$\begin{aligned} &= \sum_{\substack{p|\Phi_n(a) \\ p \neq P_n}} \alpha_p \log p \\ &= \log \prod_{p|\Phi_n(a)} p^{\alpha_p} - \delta_n \log P_n \\ &= \log \Phi_n(a) - \delta_n \log P_n. \end{aligned}$$

Putting the two above statements together, we obtain the following expression for  $D(s)$ .

$$D(s) = \sum_{n=1}^{\infty} \frac{\delta_n \log P_n}{n^s}.$$

Call  $b_n = \delta_n \log P_n$  and notice that  $b_n$  are all non-negative. Recall that  $D(s)$  converges absolutely strictly to the left of 1. Therefore, for some  $\theta < 1$ , we have

$$\sum_{n \leq x} b_n \leq \sum_{n \leq x} b_n \left(\frac{x}{n}\right)^\theta \leq x^\theta \sum_{n=1}^{\infty} \frac{b_n}{n^\theta} = Cx^\theta$$

and we conclude that

$$\sum_{n \leq x} \delta_n \log P_n = O(x^\theta). \quad \square$$

Corollary 1.3 follows since  $\log P_n \geq \log 2$ .

#### 4. Connection to Wieferich primes

Here, we take a closer look at what it means to be a Wieferich prime in light of Proposition 2.5, and in doing so we prove the following result.

**Theorem 4.1.** *Suppose that there are only finitely many super-Wieferich primes. Then, there are infinitely many non-Wieferich primes.*

We start by proving the following lemma about the characterization of Wieferich primes.

**Lemma 4.2.** *The prime  $p$  is a Wieferich prime (for  $a$ ) if and only if*

$$p^2 \mid \Phi_n(a)$$

for some  $n$ .

Moreover, if  $p^2$  divides  $\Phi_n(a)$  for some  $n$ , then  $n = f(p)$ .

Finally,  $p$  does not divide  $\Phi_n(a)$  for  $n$  other than  $f(p)$  and multiples of  $p$ .

**Proof.** We start by proving the last two statements. Suppose that  $p$  divides  $\Phi_n(a)$  for some  $n$ . Then, by Proposition 2.1, either  $n = f(p)$  or  $p$  divides  $n$ .

Now suppose that  $p^2$  divides  $\Phi_n(a)$  for some  $n$ . Since the only prime dividing both  $n$  and  $\Phi_n(a)$  does so with order at most one, we know that  $p$  does not divide  $n$ . Therefore, by Proposition 2.1,  $n = f(p)$ .

For the first part of the lemma, suppose first that  $p^2$  divides  $\Phi_n(a)$  for some  $n$ . By the above,  $n = f(p)$ . By (1.3),  $p^2$  also divides  $a^{f(p)} - 1$ . Finally, by (1.2),  $p^2$  divides  $a^{p-1} - 1$ .

To show the other implication, suppose that  $p$  is a Wieferich prime. Then,  $p^2$  divides  $a^{p-1} - 1$  and by (1.3),

$$p^2 \mid \prod_{d|p-1} \Phi_d(a).$$

Following exactly the proof of Proposition 2.5, we obtain that  $p^2$  divides  $\Phi_{f(p)}(a)$ .  $\square$

**Remark 2.** Call a prime  $p$  a  $k$ -super-Wieferich prime if  $a^{p-1} \equiv 1 \pmod{p^k}$ . The same proof can be used to show the following more general lemma.

**Lemma 4.3.** *The prime  $p$  is a  $k$ -super-Wieferich prime ( $k \geq 2$ ) if and only if*

$$p^k \mid \Phi_n(a)$$

for some  $n$ .

Also, if  $p^k$  divides  $\Phi_n(a)$  for some  $n$ , then  $n = f(p)$ .

Moreover,  $p$  does not divide  $\Phi_n(a)$  for  $n$  other than  $f(p)$  and multiples of  $p$ .

We now prove Theorem 4.1.

**Proof.** We start by assuming that there are finitely many super-Wieferich primes. Suppose that  $p$  is a super-Wieferich prime. Clearly  $p$  is also a Wieferich prime. From Lemma 4.2,  $p$  only divides  $\Phi_n(a)$  for  $n = f(p)$  or when  $n$  is a multiple of  $p$ . Consider the set

$$\mathcal{W} := \left\{ q \text{ prime} : \begin{array}{l} q \text{ is not a super-Wieferich prime, and} \\ f(p) \neq q \text{ for any super-Wieferich prime } p \end{array} \right\}.$$



Then, for every  $q \in \mathcal{W}$ ,  $\Phi_q(a)$  is not divisible by any super-Wieferich prime. Also, since we assume that there are only finitely many super-Wieferich primes, we only remove a finite number of primes from the set of all primes, and so the set  $\mathcal{W}$  is infinite.

Let  $q$  be any prime number. Then,

$$\begin{aligned} q|\Phi_q(a) &\Rightarrow q|a^q - 1 \\ &\Rightarrow a^q - 1 \equiv 0 \pmod q \\ &\Rightarrow a - 1 \equiv 0 \pmod q \end{aligned}$$

since  $a^q \equiv a \pmod q$  by Fermat's little Theorem. Therefore, the only primes  $q$  for which  $q$  can divide  $\Phi_q(a)$  are the divisors of  $a - 1$ .

Now consider the set

$$\mathcal{P} = \mathcal{W} \cap \{p \text{ prime} : p \text{ does not divide } a - 1\}.$$

For this set, we also have that  $q$  does not divide  $\Phi_q(a)$  for all  $q \in \mathcal{P}$ . Since we again only remove finitely many primes from  $\mathcal{W}$ , we still have that  $\mathcal{P}$  is infinite.

We prove the statement of the theorem by the method of contradiction. In particular, we suppose that there are only finitely many non-Wieferich primes. Suppose that there are  $N$  of them, and call them  $p_1, \dots, p_N$ . Let  $q \in \mathcal{P}$ , and consider  $\Phi_q(a)$ . We ask which primes can divide  $\Phi_q(a)$ , and with what power.

Of course, any non-Wieferich primes can potentially divide  $\Phi_q(a)$ , but they must do so to at most the first power, as otherwise they would be Wieferich primes by Lemma 4.2. Also, as we remarked above, since  $q \in \mathcal{P}$ , no super-Wieferich prime can divide  $\Phi_q(a)$ . As for the Wieferich primes, they can certainly divide  $\Phi_q(a)$ , but if they do, they must do so with order exactly 2. Indeed, if  $p$  is such a Wieferich prime dividing  $\Phi_q(a)$ , then  $p^3$  dividing  $\Phi_q(a)$  would imply that  $p$  is a super-Wieferich prime. Also, if  $p$  were to divide  $\Phi_q(a)$  with order 1, by Lemma 4.2,  $q$  would be a multiple of  $p$ , that is  $p = q$ . However, since  $q \in \mathcal{P}$ , this cannot happen.

We therefore have the general form of  $\Phi_q(a)$  as

$$\Phi_q(a) = p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2$$

where each  $\epsilon_i$  is either 0 or 1, and  $W$  is a product of distinct Wieferich primes. Since  $q$  is prime, we can write

$$\Phi_q(a) = \frac{a^q - 1}{a - 1}$$

and so

$$a^q - 1 = (a - 1)p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2.$$

Writing  $q$  as  $3j + \delta$  for some integer  $j$  and  $\delta \in \{0, 1, 2\}$ , we get

$$a^\delta (a^j)^3 - 1 = (a - 1)p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} W^2.$$

The curves

$$a^\delta X^3 - 1 = (a - 1)p_1^{\epsilon_1} \cdots p_N^{\epsilon_N} Y^2$$

are elliptic curves. Moreover, there are  $3 \times 2^N$  of them. By Siegel’s Theorem [10, IX.3], there is a finite number of integral points  $(X, Y)$  on each of them. However, the above construction gives a distinct integral point on one of the curves for every  $q \in \mathcal{P}$ . This gives a contradiction, and we conclude that there are infinitely many non-Wieferich primes.  $\square$

**Remark 3.** It is not known unconditionally at the moment whether there are infinitely many non-Wieferich primes. From the heuristics presented in Section 1, along with numerical computations, we suspect that this is the case. In particular, we believe it is possible to get a quantitative lower bound on the number of non-Wieferich primes using this method. Following the argument presented in [8, Sec. 9] mutatis mutandis, it is possible to get a lower bound of  $\log \log x$  non-Wieferich primes up to  $x$ . This should be compared with [11], where Silverman shows that the *abc*-conjecture implies that there are at least  $\gg \log x$  non-Wieferich primes up to  $x$ . The bound we obtain is more modest but depends on an assumption much weaker than the *abc*-conjecture.

### 5. Generalizations

In [3], Erdős proved estimates of the form

$$\sum_{d|a^n-1} \frac{1}{d} \leq C(a) \log \log n. \tag{5.1}$$

In Section 3, we were considering a very similar sum, namely

$$\sum_{d|a^n-1} \Lambda(d).$$

It would be interesting to see the extent with which we can generalize the above discussion and if we can obtain a result similar to that of Erdős. We exploited the fact that we can write  $\log n$  as a sum of  $\Lambda(d)$  where  $d$  ranges over divisors of  $n$ . This is also true for  $\sigma(n)/n$  because

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}.$$

In general, let  $G(n)$  be an arithmetic function, and  $F(n)$  be defined as

$$F(n) = \sum_{d|n} G(d).$$

Then, consider the Dirichlet series given by

$$\sum_{n=1}^{\infty} \frac{F(a^n - 1)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|a^n - 1} G(d).$$

Under suitable convergence conditions, we can interchange the order of summation to get

$$= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} G(d) \sum_{n:d|a^n - 1} \frac{1}{n^s}.$$

Notice once again that the integers  $n$  for which  $d$  divides  $a^n - 1$  are specifically the multiples of  $f_a(d)$ . We get

$$\begin{aligned} &= \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} G(d) \sum_{r=1}^{\infty} \frac{1}{(rf(d))^s} \\ &= \zeta(s) \sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}. \end{aligned}$$

In Section 3, we used Theorem 3.5 to show the convergence of the series on the right. Suppose that the Dirichlet series

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}$$

converges absolutely for  $\Re(s) \geq 1$  and the function  $F(a^n - 1) \geq 0$  for every  $n$ . Then, we could apply the Tauberian Theorem, which we recall here. See [6, Thm 3.3.1] for the proof.

**Theorem 5.1.** *Let  $H(s) = \sum_{n=1}^{\infty} b_n/n^s$  be a Dirichlet series with non-negative coefficients and absolutely convergent for  $\Re(s) > 1$ . Suppose that  $H(s)$  can be extended to a meromorphic function in the region  $\Re(s) \geq 1$  having no poles except for a simple pole at  $s = 1$  with residue  $r \geq 0$ . Then,*

$$\sum_{n \leq x} b_n = Rx + o(x)$$

as  $x \rightarrow \infty$ .

We therefore have

$$\sum_{n \leq x} F(a^n - 1) = \sum_{n \leq x} \sum_{d|a^n-1} G(d) = Cx + o(x)$$

where

$$C = \sum_{d=1}^{\infty} \frac{G(d)}{f(d)}.$$

The above discussion essentially proves the following theorem:

**Theorem 5.2.** *Let  $G(n)$  be an arithmetic function, and  $F(n)$  be defined as*

$$F(n) = \sum_{d|n} G(d).$$

*Suppose that  $F(a^n - 1) \geq 0$  for every  $n$ ,*

$$\sum_{n=1}^{\infty} \frac{F(a^n - 1)}{n^s}$$

*converges for  $\Re(s) > 1$ , and*

$$\sum_{\substack{d=1 \\ (d,a)=1}}^{\infty} \frac{G(d)}{f(d)^s}$$

*converges absolutely for  $\Re(s) \geq 1$ , then*

$$\sum_{n \leq x} \sum_{d|a^n-1} G(d) = Cx + o(x)$$

where

$$C = \sum_{d=1}^{\infty} \frac{G(d)}{f(d)}.$$

Applying this to  $F(n) = \sigma(n)/n$  and  $G(d) = 1/d$ , we get that

$$\sum_{n=1}^{\infty} \frac{\sigma(a^n - 1)}{(a^n - 1)n^s} = \zeta(s) \sum_{\substack{d=1 \\ (d,a)=1}} \frac{1}{df(d)^s}.$$

From Theorem 3.4, we know that the series

$$\sum_{\substack{d=1 \\ (d,a)=1}} \frac{1}{d f(d)^s}$$

converges absolutely everywhere to the right of 0 (that is for every  $s$  with  $\Re(s) > 0$ ). Therefore, Theorem 5.2 above can be applied to obtain the following result.

**Corollary 5.3.**

$$\sum_{n \leq x} \sum_{d|a^n-1} \frac{1}{d} = Rx + o(x)$$

where  $R$  is the “Romanoff” constant

$$R := \sum_{\substack{d \geq 1 \\ (d,a)=1}} \frac{1}{d f_a(d)}.$$

It is interesting to see that Corollary 5.3 actually gives an improvement of (5.1) on average.

**6. Concluding remarks**

As noted earlier, the hypothesis of Theorem 1.1 is satisfied if there are only finitely many primes  $p$  such that

$$a^{p-1} \equiv 1 \pmod{p^3}.$$

This is substantially weaker than the *abc* conjecture and may be amenable to resolution. We can of course also replace  $p^3$  by  $p^d$  for any fixed  $d \geq 3$ .

**Acknowledgments**

We would like to thank Professors Cameron Stewart and Francesco Pappalardi, as well as the referee for helpful comments on a previous version of this paper.

**References**

- [1] Richard Crandall, Karl Dilcher, Carl Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* 66 (217) (1997) 433–449.
- [2] Paul Erdős, Some recent advances and current problems in number theory, in: *Lectures on Modern Mathematics*, vol. III, Wiley, New York, 1965, pp. 196–244.
- [3] Paul Erdős, On the sum  $\sum_{d|2^n-1} d^{-1}$ , *Israel J. Math.* 9 (1971) 43–48.

- [4] G.H. Hardy, S. Ramanujan, The normal number of prime factors of a number  $n$  [Quart. J. Math. 48 (1917) 76–92], in: *Collected Papers of Srinivasa Ramanujan*, AMS Chelsea Publ., Providence, RI, 2000, pp. 262–275.
- [5] Leo Murata, Carl Pomerance, On the largest prime factor of a Mersenne number, in: *Number Theory*, in: CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 209–218.
- [6] M. Ram Murty, *Problems in Analytic Number Theory*, second edition, Springer, 2008.
- [7] M. Ram Murty, Michael Rosen, Joseph H. Silverman, Variations on a theme of Romanoff, *Internat. J. Math.* 7 (3) (1996) 373–391.
- [8] Ram Murty, François Séguin, Cameron L. Stewart, A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences, *J. Number Theory* 194 (2019) 8–29.
- [9] Ram Murty, Siman Wong, The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences, in: *Number Theory for the Millennium, III*, Urbana, IL, 2000, A K Peters, Natick, MA, 2002, pp. 43–54.
- [10] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer-Verlag, New York, 1986.
- [11] J.H. Silverman, Wieferich’s criterion and the abc-conjecture, *J. Number Theory* 30 (1988) 226–237.
- [12] Cameron L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Math.* 211 (2) (2013) 291–314.
- [13] C.L. Stewart, The greatest prime factor of  $a^n - b^n$ , *Acta Arith.* 26 (1975) 427–433.
- [14] C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.* 35 (1977) 425–447.
- [15] R. Thangadurai, A. Vatswani, The least prime congruent of one modulo  $n$ , *Amer. Math. Monthly* 118 (8) (2011) 737–742.