Spring 2019

Results for nonWieferich Primes

Nelson A. Carella
CUNY Bronx Community College

Results for nonWieferich Primes

N. A. Carella

***Abstract*:** Let $v \geq 2$ be a fixed integer, and let $x \geq 1$ be a large number. The exact asymptotic counting function for the number of nonWieferich primes $p \leq x$ such that $v^{p-1} - 1 \equiv 0 \bmod p^2$ in the interval $[1, x]$ is proposed in this note. The current results in the literature provide lower bounds, which are conditional on the *abc* conjecture or the Erdos binary additive conjecture.

1 Introduction

Let $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ be the set of prime numbers, and let $v \geq 2$ be a fixed integer. The subsets of Wieferich primes and nonWieferich primes are defined by

$$\mathcal{W}_v = \{p \in \mathbb{P} : v^{p-1} - 1 \equiv 0 \bmod p^2\} \tag{1}$$

and

$$\overline{\mathcal{W}}_v = \{p \in \mathbb{P} : v^{p-1} - 1 \not\equiv 0 \bmod p^2\}$$

respectively. The set of primes $\mathbb{P} = \mathcal{W}_v \cup \overline{\mathcal{W}}_v$ is a disjoint union of these subsets.

The subsets $\mathcal{W}_v$ and $\overline{\mathcal{W}}_v$ have other descriptions by means of the orders $\mathrm{ord}_p(v) = d \mid p - 1$ and $\mathrm{ord}_{p^2}(v) = pd \neq p$ of the base v in the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ respectively. The order is defined by $\mathrm{ord}_n(v) = \min\{m \geq 1 : v^{m-1} - 1 \equiv 0 \bmod n\}$. Specifically,

$$\mathcal{W}_v = \left\{p : \mathrm{ord}_{p^2}(v) \mid p - 1\right\} \tag{2}$$

and

$$\overline{\mathcal{W}}_v = \left\{p : \mathrm{ord}_{p^2}(v) \nmid p - 1\right\}.$$

For a large number $x \geq 1$, the corresponding counting functions for the number of such primes up to x are defined by

$$W_v(x) = \#\left\{p \leq x : \mathrm{ord}_{p^2}(v) \mid p - 1\right\} \tag{3}$$

and

$$\overline{W}_v(x) = \pi(x) - W_v(x),$$

where $\pi(x) = \#\{p \leq x\}$ is the primes counting function, respectively.

Assuming the *abc* conjecture, several authors have proved that there are infinitely many non-Wieferich primes, see [13], [4], et alii. These results have lower bounds of the form

$$\overline{W}_v(x) \gg \frac{\log x}{\log\log x} \tag{4}$$

or slightly better. In addition, assuming the Erdos binary additive conjecture, there is a proof that the subset of nonWieferich primes has nonzero density. More precisely,

$$\overline{W}_v(x) \geq c\frac{x}{\log x} \tag{5}$$

July 29, 2019
AMS MSC:Primary 11A41; Secondary 11B25.
Keywords: Distribution of primes; Wieferich Prime; nonWieferich Prime

where $c > 0$ is a constant, see [5, Theorem 1] for the details. Here, it is shown that the subset of nonWieferich primes has density 1 in the set of primes unconditionally.

Theorem 1.1. *Let $v \geq 2$ be a small base, and let $x \geq 1$ be a large number. Then, the number of nonWieferich primes has the asymptotic formula*

$$\overline{W}_v(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{6}$$

Proof. The upper bound $W_v(x) = O(\log\log x)$, confer Theorem 6.1, is used below to derive a lower bound for the counting function $\overline{W}_v(x)$. This is as follows:

$$\begin{aligned} \overline{W}_v(x) &= \#\left\{p \leq x : \operatorname{ord}_{p^2}(v) \nmid p-1\right\} \\ &= \pi(x) - W_v(x) \\ &\geq \pi(x) + O(\log\log x) \\ &= \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right), \end{aligned} \tag{7}$$

where $\pi(x) = \#\{p \leq x\} = x/\log x + O(x/\log^2 x)$. ∎

Corollary 1.1. *Almost every odd integer is a sum of a squarefree number and a power of two.*

Proof. Same as Theorem 1 in [5], but use the sharper upper bound $W_v(x) = O(\log\log x)$. ∎

2 Characteristic Functions Modulo Prime Powers

The standard method for constructing characteristic function for primitive elements are discussed in [11, Corollary 3.5], [9, p. 258], and some characteristic functions for finite rings are discussed in [6]. These type of characteristic functions detect the orders of the elements $v \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ by means of the divisors of $\varphi(p^2)$.

A new method for constructing characteristic functions in cyclic groups is developed here. These type of characteristic functions detect the orders of the elements $v \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ by means of the solutions of the equation $\tau^{pn} - v \equiv 0 \bmod p^2$, where v, τ are constants, and n is a variable such that $1 \leq n < p-1$, and $\gcd(n, p-1) = 1$. The formula $\varphi(n) = \prod_{p|n}(1-1/p)$ denotes the Euler totient function.

Lemma 2.1. *Let $p \geq 3$ be a prime, and let τ be a primitive root* $\bmod p^2$. *Let $v \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ be a nonzero element. Then*

$$\sum_{\substack{1\leq n<p-1\\ \gcd(n,p-1)=1}} \frac{1}{\varphi(p^2)} \sum_{0\leq m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{pn}-v)m}{\varphi(p^2)}} = \begin{cases} 1 & \text{if } \operatorname{ord}_{p^2}(v) = p-1, \\ 0 & \text{if } \operatorname{ord}_{p^2}(v) \neq p-1. \end{cases}$$

Proof. Let $\tau \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ be a fixed primitive root of order $p(p-1) = \varphi(p^2)$. As the index $n \geq 1$ ranges over the integers relatively prime to $p-1$, the element $\tau^{pn} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ ranges over the elements of order $\operatorname{ord}_{p^2}(\tau^{pn}) = p-1$. Hence, the equation

$$\tau^{pn} - v = 0 \tag{8}$$

has a solution if and only if the fixed element $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is an elements of order $\operatorname{ord}_{p^2}(v) = p-1$. Setting $w = e^{i2\pi(\tau^{pn}-v)/\varphi(p^2)}$ and summing the inner sum yield

$$\sum_{\gcd(n,p-1)=1} \frac{1}{\varphi(p^2)} \sum_{0\leq m<\varphi(p^2)} w^m = \begin{cases} 1 & \text{if } \operatorname{ord}_{p^2}(v) = p-1, \\ 0 & \text{if } \operatorname{ord}_{p^2}(v) \neq p-1. \end{cases} \tag{9}$$

This follows from the geometric series identity $\sum_{0\leq m\leq x-1} w^m = (w^x - 1)/(w-1), w \neq 1$ applied to the inner sum. ∎

The characteristic function for any element $v \geq 2$ of any order $\mathrm{ord}_{p^2}(v) = d \mid p-1$ in the cyclic group $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is a sum of characteristic functions.

Lemma 2.2. *Let Let $v \geq 2$ be a fixed base, let $p \geq 3$ be a prime, and let τ be a primitive root* $\bmod p^2$. *The indicator function for the subset of primes such that $v^{p-1} - 1 \equiv 0 \bmod p^2$ is given by*

$$\begin{aligned}\Psi_0(p^2) &= \sum_{d \mid p-1} \sum_{\substack{1 \leq n < p-1 \\ \gcd(n,(p-1)/d)=1}} \frac{1}{\varphi(p^2)} \sum_{0 \leq m < \varphi(p^2)} e^{\frac{i2\pi(\tau^{dpn} - v)m}{\varphi(p^2)}} \\ &= \begin{cases} 1 & \text{if } \mathrm{ord}_{p^2}(v) \mid p-1, \\ 0 & \text{if } \mathrm{ord}_{p^2}(v) \not| \, p-1. \end{cases}\end{aligned}$$

Proof. Suppose that $\mathrm{ord}_{p^2}(v) \mid p-1$. Then, the congruence $\tau^{dpn} - v \equiv 0 \bmod p^2$ has a unique solution pair $d \mid p-1$ and $n \geq 1$ with $\gcd(n,(p-1)/d) = 1$. Otherwise, $\tau^{dpn} - v \not\equiv 0 \bmod p^2$ for all pairs $d \mid p-1$ and $\gcd(n,(p-1)/d) = 1$. To complete the proof, proceed as in the proof of Lemma 2.1. ■

3 Equivalent Exponential Sums

For any fixed $0 \neq s \in \mathbb{Z}/p^2\mathbb{Z}$, an asymptotic relation for the exponential sums

$$\sum_{\gcd(n,\varphi(p^2))=1} e^{i2\pi s\tau^n/\varphi(p^2)} \quad \text{and} \quad \sum_{\gcd(n,\varphi(p^2))=1} e^{i2\pi\tau^n/\varphi(p^2)}, \tag{10}$$

is provided in Lemma 3.1. This result expresses the first exponential sum in (10) as a sum of simpler exponential sum and an error term. The proof is based on Lagrange resolvent in the finite ring $\mathbb{Z}/p^2\mathbb{Z}$. Specifically,

$$(\omega^t, \zeta^{s\tau^{dp}}) = \zeta^s + \omega^{-t}\zeta^{s\tau^{dp}} + \omega^{-2t}\zeta^{s\tau^{2dp}} + \cdots + \omega^{-(p-1)t}\zeta^{s\tau^{(p-1)dp}}, \tag{11}$$

where $\omega = e^{i2\pi/p}$, $\zeta = e^{i2\pi/\varphi(p^2)}$, and the variables $0 \neq s \in \mathbb{Z}/p^2\mathbb{Z}$, and $0 \neq t \in \mathbb{Z}/p\mathbb{Z}$.

Lemma 3.1. *Let $p \geq 2$ be a large prime. If τ be a primitive root modulo p^2, then,*

$$\sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi s\tau^{ndp}/\varphi(p^2)} = \sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi\tau^{ndp}/\varphi(p^2)} + O(p^{1/2}\log^3 p),$$

for any fixed $d \mid p-1$, and $0 \neq s \in \mathbb{Z}/p^2\mathbb{Z}$.

Proof. Summing (11) times ω^{tn} over the variable $t \in \mathbb{Z}/p\mathbb{Z}$ yields, (all the nontrivial complex pth root of unity),

$$p \cdot e^{i2\pi s\tau^{ndp}/\varphi(p^2)} = \sum_{0 \leq t \leq p-1} (\omega^t, \zeta^{s\tau^{ndp}})\omega^{tn}. \tag{12}$$

Summing (12) over the variable $n \geq 1$, for which $\gcd(n,(p-1)/d) = 1$, yields

$$\begin{aligned} p \cdot \sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi s\tau^{ndp}/\varphi(p^2)} &= \sum_{\gcd(n,(p-1)/d)=1,\ 0 \leq t \leq p-1} (\omega^t, \zeta^{s\tau^{dp}})\omega^{tn} \\ &= \sum_{1 \leq t \leq p-1} (\omega^t, \zeta^{s\tau^{dp}}) \sum_{\gcd(n,(p-1)/d)=1} \omega^{tn} - p. \end{aligned} \tag{13}$$

The first index $t = 0$ contributes p, see [10, Equation (5)] for similar calculations. Likewise, the basic exponential sum for $s = 1$ can be written as

$$p \cdot \sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi\tau^{ndp}/\varphi(p^2)} = \sum_{1 \leq t \leq p-1} (\omega^t, \zeta^{\tau^{dp}}) \sum_{\gcd(n,(p-1)/d)=1} \omega^{tn} - p, \tag{14}$$

Differencing (13) and (14) produces

$$\begin{aligned} S_1 &= p\cdot\left(\sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi s\tau^{ndp}/\varphi(p^2)} - \sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi \tau^{ndp}/\varphi(p^2)}\right) \\ &= \sum_{1\le t\le p-1}\Big((\omega^t,\zeta^{s\tau^{dp}}) - (\omega^t,\zeta^{\tau^{dp}})\Big)\sum_{\gcd(n,(p-1)/d)=1}\omega^{tn}. \end{aligned} \tag{15}$$

The right side sum S_1 can be rewritten as

$$\begin{aligned} S_1 &= \sum_{1\le t\le p-1}\Big((\omega^t,\zeta^{s\tau^{ndp}}) - (\omega^t,\zeta^{\tau^{ndp}})\Big)\sum_{\gcd(n,(p-1)/d)=1}\omega^{tn} \\ &= \sum_{1\le t\le p-1}\Big((\omega^t,\zeta^{s\tau^{ndp}}) - (\omega^t,\zeta^{\tau^{ndp}})\Big)\sum_{e\le(p-1)/d}\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}} \\ &= \sum_{1\le t\le p-1,\ e\le(p-1)/d}\Big((\omega^t,\zeta^{s\tau^{ndp}}) - (\omega^t,\zeta^{\tau^{ndp}})\Big)\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}}. \end{aligned} \tag{16}$$

The second line follows from Lemma 3.2-i. The upper bound

$$\begin{aligned} |S_1| &\le \sum_{1\le t\le p-1,\ e\le(p-1)/d}\left|\Big((\omega^t,\zeta^{s\tau^{ndp}}) - (\omega^t,\zeta^{\tau^{ndp}})\Big)\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}}\right| \\ &\le \sum_{1\le t\le p-1,\ e\le(p-1)/d}\Big|(\omega^t,\zeta^{s\tau^{ndp}}) - (\omega^t,\zeta^{\tau^{ndp}})\Big|\left|\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}}\right| \\ &\le \sum_{1\le t\le p-1,\ e\le(p-1)/d}\Big(2p^{1/2}\log p\Big)\cdot\left|\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}}\right| \\ &\le \sum_{1\le t\le p-1}\Big(2p^{1/2}\log p\Big)\cdot\left(\frac{2p\log p}{\pi t}\right) \\ &\le \Big(4p^{3/2}\log^2 p\Big)\sum_{1\le t\le p-1}\frac{1}{t} \\ &\le 8p^{3/2}\log^3 p. \end{aligned} \tag{17}$$

The third line follows the upper bound for Lagrange resolvents, and the fourth line follows from Lemma 3.2-ii. Here, the difference of two Lagrange resolvents, (Gauss sums), has the upper bound

$$\Big|(\omega^t,\zeta^{s\tau^{dp}}) - (\omega^t,\zeta^{\tau^{dp}})\Big| \le 2\left|\sum_{1\le t\le p-1}\chi(t)e^{i2\pi t/p}\right| \le 2p^{1/2}\log p, \tag{18}$$

where $|\chi(t)|=1$ is a root of unity. Taking absolute value in (15) and using (17) return

$$\begin{aligned} p\cdot\left|\sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi s\tau^{ndp}/p} - \sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi\tau^{ndp}/p}\right| &\le |S_1| \\ &\le 8p^{3/2}\log^3 p. \end{aligned} \tag{19}$$

The last inequality implies the claim. ■

Lemma 3.2. *Let $p\ge 2$ be a large prime, and let $\omega = e^{i2\pi/p}$ be a pth root of unity. Then,*

(i)

$$\sum_{\gcd(n,(p-1)/d)=1}\omega^{tn} = \sum_{e\le(p-1)/d}\mu(e)\frac{\omega^{et}-\omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}},$$

(ii)

$$\left| \sum_{\gcd(n,(p-1)/d)=1} \omega^{tn} \right| \leq \frac{2p\log p}{\pi t},$$

where $\mu(k)$ is the Mobius function, for any fixed pair $d \mid p-1$ and $t \in [1, p-1]$.

Proof. (i) Use the inclusion exclusion principle to rewrite the exponential sum as

$$\begin{aligned} \sum_{\gcd(n,(p-1)/d)=1} \omega^{tn} &= \sum_{n\leq(p-1)/d} \omega^{tn} \sum_{\substack{e|(p-1)/d \\ e|n}} \mu(e) \\ &= \sum_{e\leq(p-1)/d} \mu(e) \sum_{\substack{n\leq(p-1)/d \\ e|n}} \omega^{tn} \\ &= \sum_{e\leq(p-1)/d} \mu(e) \sum_{m\leq(p-1)/de} \omega^{etm} \qquad (20) \\ &= \sum_{e\leq(p-1)/d} \mu(e) \frac{\omega^{et} - \omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}}. \end{aligned}$$

(ii) Observe that the parameters $\omega = e^{i2\pi/p}$, the integers $t \in [1, p-1]$, and $e \leq (p-1)/d$ imply that $\pi et/p \neq k\pi$ with $k \in \mathbb{Z}$, so the sine function $\sin(\pi et/p) \neq 0$ is well defined. Using standard manipulations, and $z/2 \leq \sin(z) < z$ for $0 < |z| < \pi/2$, the last expression becomes

$$\left| \frac{\omega^{et} - \omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}} \right| \leq \left| \frac{2}{\sin(\pi et/p)} \right| \leq \frac{2p}{\pi et} \qquad (21)$$

for $1 \leq d \leq p-1$. Finally, the upper bound is

$$\begin{aligned} \left| \sum_{e\leq(p-1)/d} \mu(e) \frac{\omega^{et} - \omega^{et(\frac{p-1}{d}+1)}}{1-\omega^{et}} \right| &\leq \frac{2p}{\pi t} \sum_{e\leq(p-1)/d} \frac{1}{e} \qquad (22) \\ &\leq \frac{2p\log p}{\pi t}. \end{aligned}$$

■

4 Upper Bound For The Main Term

An estimate for the finite sum occurring in the evaluation of the main term is considered in this section.

Lemma 4.1. *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{p\leq x} \frac{1}{\varphi(p^2)} \sum_{d|p-1,\, \gcd(n,(p-1)/d)=1} \sum 1 \leq 2\log\log x.$$

Proof. Use the identity $\sum_{d|n} \varphi(d) = n$ to eliminate the inner double sum in the following way:

$$\sum_{d|p-1,\, \gcd(n,(p-1)/d)=1} \sum 1 = \sum_{d|p-1} \varphi((p-1)/d) = p-1. \qquad (23)$$

Substituting this returns

$$\sum_{p\leq x} \frac{1}{\varphi(p^2)} \sum_{d|p-1,\, \gcd(n,(p-1)/d)=1} \sum 1 = \sum_{p\leq x} \frac{1}{\varphi(p^2)} \cdot (p-1) = \sum_{p\leq x} \frac{1}{p}. \qquad (24)$$

Lastly, apply Mertens theorem to the prime harmonic sum. ■

5 Estimate For The Error Term

Upper bound for the error term occurring in the proof of Theorem 1.1 is determined here. This estimate is weak, but sufficient in many applications.

Lemma 5.1. *Let $x \geq 1$ be large number. Let $p \geq 2$ be a large prime, and let $\tau \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times}$ be a primitive root mod p^2. If the element $v \geq 2$ is a small fixed integer, then*

$$\sum_{p\leq x,\, d|p-1,\, \gcd(n,(p-1)/d)=1} \frac{1}{\varphi(p^2)} \sum_{1\leq m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{pdn}-v)m}{\varphi(p^2)}} = O\left(\log\log x\right),$$

for all sufficiently large numbers $x \geq 1$.

Proof. Rearrange the inner triple finite sum in the form

$$\begin{aligned} T &= \sum_{p\leq x} \sum_{d|p-1,\, \gcd(n,(p-1)/d)=1} \frac{1}{\varphi(p^2)} \sum_{1\leq m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{dpn}-v)m}{\varphi(p^2)}} \qquad (25)\\ &= \sum_{p\leq x} \frac{1}{\varphi(p^2)} \sum_{0<m<\varphi(p^2)} e^{-i2\pi\frac{vm}{\varphi(p^2)}} \sum_{d|p-1,\, \gcd(n,(p-1)/d)=1} e^{i2\pi\frac{m\tau^{dpn}}{\varphi(p^2)}}\\ &= \sum_{p\leq x} \frac{1}{\varphi(p^2)} \sum_{0<m<\varphi(p^2)} e^{-i2\pi\frac{vm}{\varphi(p^2)}} \sum_{d|p-1} \left(\sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi\frac{\tau^{dpn}}{\varphi(p^2)}} + O\left(p^{1/2}\log^3 p\right)\right)\\ &= \sum_{p\leq x} \frac{1}{\varphi(p^2)} T_1 \times T_2. \end{aligned}$$

The last line in (25) follows from Lemma 3.1. Taking absolute the value of the first term T_1 yields

$$|T_1| = \left| \sum_{0<m<\varphi(p^2)} e^{-i2\pi vm/\varphi(p^2)} \right| = w \leq v \qquad (26)$$

where $\gcd(v, p(p-1)) = w \leq v$. The second term T_2 has the trivial upper bound

$$\begin{aligned} |T_2| &\leq \left| \sum_{d|p-1} \left(\sum_{\gcd(n,(p-1)/d)=1} e^{i2\pi\frac{\tau^{dpn}}{\varphi(p^2)}} + O\left(p^{1/2}\log^3 p\right)\right)\right|\\ &\ll \sum_{d|p-1} \sum_{\gcd(n,(p-1)/d)=1} 1 + p^{1/2}\log^4 p\\ &\ll \sum_{d|p-1} \varphi\left(\frac{p-1}{d}\right) + p^{1/2}\log^4 p\\ &\ll p-1. \qquad (27) \end{aligned}$$

Replace the identity $\varphi(p^2) = p(p-1)$, and the estimates (26) and (27) back into (25). These lead to

$$\begin{aligned} |T| &\leq \sum_{p\leq x} \frac{1}{\varphi(p^2)} |T_1| \times |T_2| \qquad (28)\\ &\ll \sum_{p\leq x} \frac{1}{(p-1)p} \left(v \times (p-1)\right)\\ &\ll \sum_{p\leq x} \frac{1}{p}\\ &\ll \log\log x, \end{aligned}$$

where $v \geq 2$ is the base. ∎

6 Upper Bound For The Wieferich Primes

The subset of primes $\mathcal{W}_2 = \left\{p : \mathrm{ord}_{p^2}(2) \mid p-1\right\} = \{1093, 3511, \dots, \}$ associated with the base $v = 2$ is the best known case. But, many other bases have been computed too, see [2], [8]. The heuristic argument in [12, p. 413], [1], [7, Section 2], et alii, claims that

$$W_v(x) \approx \sum_{p \le x} \frac{1}{p} \ll \log\log x. \tag{29}$$

The basic foundation of this heuritic is correct. An unconditional upper bound is computed here.

Theorem 6.1. *The number of Wieferich primes on the interval* $[1, x]$ *has the upper bound*

$$W_v(x) = O\left(\log\log x\right).$$

Proof. Let $x \ge 1$ be a large number, and fix an integer $v \ge 2$. The sum of the characteristic function over the interval $[1, x]$ is
written as

$$W_v(x) = \sum_{p \le x} \Psi_0(p^2). \tag{30}$$

Replacing the characteristic function, see Lemma 2.2, and expanding yield

$$\begin{aligned}
\sum_{p\le x} \Psi_v(p^2) &= \sum_{p\le x,\, d\mid p-1,\, \gcd(n,(p-1)/d)=1} \frac{1}{\varphi(p^2)} \sum_{0\le m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{pn}-v)m}{\varphi(p^2)}} \\
&= \sum_{p\le x} \frac{1}{\varphi(p^2)} \sum_{d\mid p-1,\, \gcd(n,(p-1)/d)=1} 1 \\
&\quad + \sum_{p\le x,\, d\mid p-1,\, \gcd(n,(p-1)/d)=1} \frac{1}{\varphi(p^2)} \sum_{1\le m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{pn}-v)m}{\varphi(p^2)}} \\
&= M_v(x) \quad + \quad E_v(x).
\end{aligned} \tag{31}$$

The main term $M_v(x)$ is determined by the index $m = 0$, and the error term $E_v(x)$ is determined by the range $1 \le m < \varphi(p^2)$. Applying Lemma 4.1 to the main term and applying Lemma 5.1 to the error term yield

$$\begin{aligned}
W_v(x) &= M_v(x) \quad + \quad E_v(x) \\
&\le 2\log\log(x) + O\left(\log\log x\right) \\
&= O\left(\log\log x\right).
\end{aligned} \tag{32}$$

This verifies the upper bound. ∎

References

[1] RICHARD CRANDALL, KARL DILCHER, CARL POMERANCE. *A search for Wieferich and Wilson primes.* Math. Comp. **66** (1997), no. 217, 433–449.

[2] FRANCOIS GDORAIS, DOMINIC KLYVE. *A Wieferich prime search up to* 6.7×10^{15}. J. Integer Seq. **14** (2011), no. 9, Article 11.9.2, 14 pp.

[3] J.-M. DEKONINCK, N. DOYON . *On the set of Wieferich primes and of its complement.* Ann. Univ. Sci. Budapest. Sect. Comput. **27** (2007), 3- 13.

[4] H. GRAVES, M. RAM MURTY. *The abc conjecture and non-Wieferich primes in arithmetic progressions,* J. Number Theory **133** (2013) 1809-1813.

[5] ANDREW GRANVILLE, K SOUNDARARAJAN. *A binary additive problem of Erdos and the order of* 2 mod p^2. Ramanujan J. **2** (1998), no. 1-2,

283-298.

[6] JOHN JOHNSEN. *On the distribution of powers in finite fields.* J. Reine Angew. Math. **251** 1971 10-19.

[7] NICHOLAS M KATZ. *Wieferich past and future.* Topics in finite fields, 253-270, Contemp. Math., **632**, Amer. Math. Soc., Providence, RI, 2015.

[8] WILFRID KELLER, JORG RICHSTEIN. *Solutions of the congruence* $a^{p-1} \equiv 1 \bmod p^r$, Math. Comp. **74** (2005), 927-936.

[9] RUDOLF LIDL, HARALDNIEDERREITER. *Finite fields.* With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, **20**20. Cambridge University Press, Cambridge, 1997.

[10] L. J MORDELL. *On the exponential sum* $\sum_{1\leq x\leq X} exp(2\pi i(ax + bg^x)/p)$. *Mathematika* **19** (1972), 84-87.

[11] H. E.ROSE. *A course in number theory.* Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New

York, 1994.

[12] PAULORIBENBOIM. *The new book of prime number records* , Berlin, New York: Springer-Verlag, 1996.

[13] J. H. SILVERMAN. *Wieferich criterion and the abc-conjecture* , J. Number Theory **30** (1988) no. 2, 226-237.

ResultNonWieferichPrimes-07-21-19-11.tex.