Estimates for Wieferich Numbers

William D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

January 30, 2005

Abstract

We define Wieferich numbers to be those odd integers $w \geq 3$ that satisfy the congruence $2^{\varphi(w)} \equiv 1 \pmod{w^2}$. It is clear that the distribution of Wieferich numbers is closely related to the distribution of Wieferich primes, and we give some quantitative forms of this statement. We establish several unconditional asymptotic results about Wieferich numbers; analogous results for the set of Wieferich primes remain out of reach. Finally, we consider several modifications of the above definition and demonstrate that our methods apply to such sets of integers as well.

1 Introduction

Let $\varphi(n)$ be the Euler function and $\lambda(n)$ be the Carmichael function. We recall that these functions give the order and exponent of the group of invertible elements modulo n, respectively.

Throughout this paper, for any real number $x > 0$ and any integer $\ell \geq 1$, we write $\log_\ell x$ for the function defined inductively by $\log_1 x = \max\{\log x,\, 1\}$ (where $\log x$ is the natural logarithm of x) and $\log_\ell x = \log_1(\log_{\ell-1} x)$ for $\ell > 1$. When $\ell = 1$, we omit the subscript in order to simplify the notation; however, we continue to assume that $\log x \geq 1$ for any $x > 0$.

In what follows, we use the Landau symbol O and the Vinogradov symbols $\ll$ and $\gg$ with their usual meanings, with the understanding that any implied constants are *absolute*. We recall that the notations $A \ll B$, $B \gg A$ and $A = O(B)$ are equivalent. We always use the letters p and q to denote prime numbers, while m and n always denote positive integers.

An odd integer $w \geq 3$ is called a *Wieferich number* if the congruence

$$2^{\varphi(w)} \equiv 1 \pmod{w^2} \tag{1}$$

holds. Note that if $w = q$ is prime, this agrees with the classical definition of a *Wieferich prime*. If (1) does not hold, we call $w \geq 3$ a *non-Wieferich number*. Accordingly, we denote by $\mathcal{W}$, $\mathcal{U}$, and $\mathcal{Q}$ the sets of Wieferich numbers, non-Wieferich numbers, and Wieferich primes, respectively.

Wieferich primes were first introduced in [21] in relation to the first case of *Fermat's Last Theorem*. In that historical work, Wieferich showed that if q is an odd prime, and $x^q + y^q + z^q = 0$ has a solution in integers x, y, z with $q \nmid xyz$, then necessarily $q \in \mathcal{Q}$. Many other surprising links have been discovered between Wieferich primes and other (sometimes seemingly unrelated) number theoretic problems; see [10, 17, 19] for some examples, problems and further references.

Despite the many efforts that were made to study Wieferich primes, very few theoretical or numerical results emerged. To this day, only two Wieferich primes have been discovered ($q_1 = 1093$ was found by Meissner in 1913, and $q_2 = 3511$ was found by Beeger in 1922; see, for example, [18] and also [4, 7, 15]); it is not known whether $\#\mathcal{Q} > 2$ or $\#\mathcal{Q} = 2$, and it is unknown whether or not there exist infinitely many "non-Wieferich" primes.

Building on results of Agoh, Dilcher and Skula [1], it is easy to show that if $\mathcal{Q}$ is a finite set, then $\mathcal{W}$ is also finite; see Theorem 9 below. In particular, if $\mathcal{Q} = \{1093, 3511\}$, then the set $\mathcal{W}$ contains exactly 104 numbers; these can be determined precisely, the largest one being 16547533489305, and they are the only currently known examples of Wieferich numbers; see [1].

If $\mathcal{S} = \mathcal{W}$, $\mathcal{U}$, or $\mathcal{Q}$, or any other set of odd integers that we consider in the sequel, and $x \ge 3$ is a real number, we then let $\mathcal{S}(x) \subset \mathcal{S}$ be the set of positive odd integers $n \le x$ such that $n \in \mathcal{S}$. In this paper, we give estimates for $\#\mathcal{W}(x)$ and $\#\mathcal{U}(x)$ as $x \to \infty$.

In Section 3, we show that $\#\mathcal{U}(x) \gg x/(\log x)^{o(1)}$ (see Theorem 5 for a more precise statement). Since $\#\mathcal{U}(x) = x/2 - \#\mathcal{W}(x) + O(1)$, this yields a nontrivial upper bound on $\#\mathcal{W}(x)$ as $x \to \infty$.

Rough heuristic arguments imply that the number $\#\mathcal{Q}(x)$ of Wieferich primes $q \le x$ should be about $\log_2 x$. Indeed, assuming that the quotient $(2^{q-1} - 1)/q$ is equally likely to fall into any one of the congruence classes modulo q, the "probability" that

$$(2^{q-1} - 1)/q \equiv 0 \pmod q$$

is about $1/q$, which leads to the expected number

$$\#\mathcal{Q}(x) \sim \sum_{q \le x} \frac{1}{q} \sim \log_2 x \tag{2}$$

of Wieferich primes $q \le x$. The same arguments, applied naively, lead to the conclusion that the number $\#\mathcal{W}(x)$ of Wieferich numbers $w \le x$ should be roughly

$$\#\mathcal{W}(x) \sim \sum_{n \le x} \frac{1}{n} \sim \log x. \tag{3}$$

In Section 4, we derive conditional upper and lower bounds for $\#\mathcal{W}(x)$ under various assumptions about the growth rate of $\#\mathcal{Q}(x)$, including (2).

Finally, in Section 5 we discuss some alternative ways to extend the notion of Wieferich primes to arbitrary odd integers. We also give some arguments which suggest that the conjecture (3) might be false and that, in fact, it is likely that

$$\#\mathcal{W}(x) \gg \frac{\log x \log_2 x}{(\log_3 x)^2}. \tag{4}$$

Acknowledgements. The authors wish to thank Glyn Harman and Filip Saidak for some useful conversations. The authors are also grateful to the anonymous referee for many valuable suggestions. In particular, these suggestions lead to the heuristic estimate (4), sharpening our original estimate, and also to Theorem 6. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459.

2 General Results on Wieferich Numbers

For a prime p, we denote by $\nu_p(n)$ the *p-adic valuation* of an integer $n \geq 1$; in other words, $p^{\nu_p(n)}$ is the largest power of p dividing n.

For an integer $n \geq 2$, we denote by n^* the *squarefree kernel* of n; that is, n^* is the product of the distinct primes dividing n.

The following characterization of Wieferich numbers is elementary (see, for example, Theorem 5.5 in [1] for a more general version of this result).

Lemma 1. *An odd integer $w \geq 3$ is a Wieferich number if and only if the inequality*

$$\nu_p(w) \leq \nu_p(2^{p-1} - 1) - 1 + \nu_p(\varphi(w^*))$$

holds for every prime divisor p of w.

Let $P(n)$ denote the largest prime divisor of an integer $n \geq 2$.

Lemma 2. *If w is a Wieferich number, then $P(w)$ is a Wieferich prime.*

Proof. Clearly, if $w \geq 2$ and $q = P(w)$, then q cannot divide $\varphi(w^*)$; hence, $\nu_q(\varphi(w^*)) = 0$. If $w \in \mathcal{W}$, by Lemma 1, we have $\nu_q(2^{q-1} - 1) \geq 2$; thus, $q \in \mathcal{Q}$. □

On page 154 of [18], it is shown that Mersenne or Fermat primes cannot be Wieferich primes. Here, we show that this result can be extended to Wieferich numbers.

Theorem 3. *If $m > 1$ is of the form $m = 2^n \pm 1$ for some positive integer n, then m is non-Wieferich.*

Proof. Assume that $m = 2^n - 1$. Clearly, n is the multiplicative order of 2 modulo m, that is, the smallest positive integer k with $2^k \equiv 1 \pmod{m}$.

Therefore, $n \mid \varphi(m)$. Now write $\varphi(m) = n\lambda$. If $m \in \mathcal{W}$, then $m^2 \mid 2^{n\lambda} - 1$, therefore

$$0 \equiv \frac{2^{n\lambda} - 1}{2^n - 1} = 1 + 2^n + 2^{2n} + \cdots + 2^{\lambda n} \equiv \lambda \pmod{2^n - 1}.$$

Hence $2^n - 1 \mid \lambda$, and therefore $\lambda \geq 2^n - 1$. This leads to $\varphi(2^n - 1) \geq n(2^n - 1)$, which is impossible since $n \geq 2$.

The case in which $m = 2^n + 1$ can be handled similarly. □

3 Non-Wieferich Numbers

In this section, we derive an unconditional lower bound for the number of odd non-Wieferich numbers $w \leq x$. Our principal tool is the following simplified and uniform version of a well-known theorem of Wirsing [22].

Lemma 4. *For any positive real number x and any odd prime $p \leq \log_2 x$, let $\mathcal{T}_p(x)$ be the set of those odd positive integers $n \leq x$ such that every prime factor q of n satisfies $q \not\equiv 1 \pmod{p}$. Then*

$$\#\mathcal{T}_p(x) \geq x \exp\left(-\frac{\log_2 x}{(p-1)} + O(\log_3 x)\right).$$

Proof. Define parameters w, z, k as follows:

$$w = \log x, \qquad z = \exp\left(\frac{\log x}{\log_2^2 x}\right), \qquad \text{and} \quad k = \left\lfloor \left(\frac{p-1}{p-2}\right) \log_2 x \right\rfloor.$$

Let $\mathcal{M}$ be the set of those squarefree integers m having precisely k prime factors q, all from the open interval (w, z) and satisfying $q \not\equiv 1 \pmod{p}$. Note that for every $m \in \mathcal{M}$ the inequality $m < z^k \leq x^{1/3}$ holds (since $\log_2 x \geq p \geq 3$), and therefore $x/m \geq x^{2/3}$.

Let n be any integer of the form $n = m\ell$, where $m \in \mathcal{M}$, and ℓ is a prime in the interval $(x^{1/2}, x/m]$ with $\ell \not\equiv 1 \pmod{p}$. Clearly, $n \in \mathcal{T}_p(x)$, and the integers n constructed in this way are distinct for different values of m. By the classical Page bound (see Chapter 20 of [6]), for each $m \in \mathcal{M}$ the number of possibilities for ℓ is at least

$$\pi(x/m) - \pi\big(x^{1/2}\big) - \pi(x/m; 1, p) \gg \left(\frac{p-2}{p-1}\right) \frac{x}{m \log(x/m)} \gg \frac{x}{m \log x}.$$

Consequently,

$$\#\mathcal{T}_p(x) \gg \frac{x}{\log x} \sum_{m \in \mathcal{M}} \frac{1}{m}. \tag{5}$$

We now show that the estimate

$$\sum_{m \in \mathcal{M}} \frac{1}{m} = \frac{S^k}{k!}\,(1+o(1)) \tag{6}$$

holds, where

$$S = \sum_{\substack{w<q<z \\ q \not\equiv 1 \pmod p}} \frac{1}{q}.$$

For this, we begin with the estimate

$$\frac{S^k}{k!} \le \sum_{m \in \mathcal{M}} \frac{1}{m} + \sum_{r>w} \frac{1}{r^2} \frac{1}{(k-2)!} \left(\sum_{\substack{w<q<z \\ q \not\equiv 1 \pmod p}} \sum_{j \ge 1} \frac{1}{q^j} \right)^{k-2}. \tag{7}$$

Observe that

$$\begin{aligned} \frac{1}{(k-2)!} \left(\sum_{\substack{w<q<z \\ q \not\equiv 1 \pmod p}} \sum_{j \ge 1} \frac{1}{q^j} \right)^{k-2} &\le \frac{1}{(k-2)!}\,(S+O(w^{-1}))^{k-2} \\ &= \frac{S^{k-2}}{(k-2)!}\,\exp\left(O\left(\frac{k}{wS}\right)\right). \end{aligned}$$

Using the Page bound again and partial summation, we derive that

$$S = \left(\frac{p-2}{p-1}\right)(\log_2 z - \log_2 w) + o(1) = \left(\frac{p-2}{p-1}\right)\log_2 x + O(\log_3 x);$$

in particular, $k \ll S$. Therefore,

$$\frac{S^{k-2}}{(k-2)!} \ll \frac{S^k}{k!} \cdot \frac{k^2}{S^2} \ll \frac{S^k}{k!},$$

and from inequality (7) we obtain that

$$\frac{S^k}{k!} \le \sum_{m\in\mathcal{M}} \frac{1}{m} + O\left(\frac{S^k}{k!}\sum_{r>w}\frac{1}{r^2}\right) \le \sum_{m\in\mathcal{M}}\frac{1}{m} + o\left(\frac{S^k}{k!}\right),$$

since

$$\sum_{r>w}\frac{1}{r^2} \ll \frac{1}{w\log w} = \frac{1}{\log x \log_2 x} = o(1).$$

This proves the lower bound of (6), while the upper bound is trivial.

Returning to the inequality (5), we now see that

$$\#\mathcal{T}_p(x) \gg \frac{x}{\log x}\cdot\frac{S^k}{k!} \gg \frac{x}{\log x\,\log_2^{1/2} x}\left(\frac{eS}{k}\right)^k.$$

Since

$$\frac{eS}{k} = e\left(1 + O\left(\frac{\log_3 x}{\log_2 x}\right)\right),$$

we get that

$$\begin{aligned}\#\mathcal{T}_p(x) &\gg x\exp\left(-\log_2 x + \left(\frac{p-2}{p-1}\right)\log_2 x + O(\log_3 x)\right)\\ &= x\exp\left(-\frac{\log_2 x}{(p-1)} + O(\log_3 x)\right),\end{aligned}$$

and the proof is complete. □

Theorem 5. *Let* $\beta = \log^{1/2} 2 = 0.8325\ldots$. *Then*

$$\#\mathcal{U}(x) \ge x\exp\left(-2\beta\log_2^{1/2} x + O\left(\log_2^{1/3} x\right)\right).$$

Proof. Let x be a large positive real number, put $y = \beta^{-1}\log_2^{1/2} x$, and let p be any prime in the interval $[y, y+y^{2/3}]$; the existence of such a prime (for sufficiently large x) is guaranteed by the known results about primes in short intervals (see, for example, [14]).

Let $h = \nu_p(2^{p-1}-1)$; note that $p^h \le 2^{p-1}-1 < 2^{p-1}$. If $n = p^h m$, where $m \in \mathcal{T}_p(x/p^h)$, then Lemma 1 immediately shows that n is a non-Wieferich number. Since

$$\log_2(x/p^h) = \log_2 x + O\left(\frac{p}{\log x}\right) = \log_2 x + O\left(\frac{\log_2^{1/2} x}{\log x}\right),$$

and $p \le \log_2 x$ if x is sufficiently large, by Lemma 4, we conclude that

$$\begin{aligned} \#\mathcal{U}(x) \ge \mathcal{T}_p(x/p^h) \quad & \ge \quad \frac{x}{p^h} \exp\left(-\frac{\log_2(x/p^h)}{(p-1)} + O(\log_3(x/p^h))\right) \\ & \ge \quad x \exp\left(-(p-1)\log 2 - \frac{\log_2 x}{p-1} + O(\log_3 x)\right) \\ & = \quad x \exp\left(-2\beta \log_2^{1/2} x + O(\log_2^{1/3} x)\right), \end{aligned}$$

where the last estimate follows from our choice of p. □

4 Conditional Results

As mentioned in the introduction, heuristic arguments lead to a conjectural asymptotic formula

$$\#\mathcal{Q}(x) \sim \log_2 x \tag{8}$$

for the number of Wieferich primes $q \le x$. In this section, we consider the problem of estimating $\#\mathcal{W}(x)$, the number of Wieferich numbers $w \le x$, under various assumptions about the rate of growth of $\#\mathcal{Q}(x)$. We also note that [10, 17, 19] contain several results of a very different spirit which are also based on various assumptions about the size of $\#\mathcal{Q}(x)$ (and similar sets).

We begin with an observation that if the sum of the reciprocals of the Wieferich primes converges:

$$\sum_{q \in \mathcal{Q}} \frac{1}{q} < \infty, \tag{9}$$

then $\#\mathcal{W}(x) = o(x)$. Roughly speaking, the underlying argument runs as follows. If (9) holds, then most integers are not divisible by a large Wieferich prime. On the other hand, most integers *are* divisible by *some* large prime. Thus, for most integers n, the largest prime factor $P(n)$ is non-Wieferich, and by Lemma 2, it follows that $n \notin \mathcal{W}$.

To make the preceding argument precise, we begin by defining (as usual):

$$\Psi(x, y) = \#\{n \le x : P(n) \le y\}.$$

Since $P(w) \in \mathcal{Q}$ for each $w \in \mathcal{W}$ by Lemma 2, it follows that

$$\#\mathcal{W}(x) \le \Psi(x,y) + \sum_{\substack{q \ge y \\ q \in \mathcal{Q}}} \sum_{\substack{w \le x \\ w \in \mathcal{W} \\ P(w)=q}} 1 \le \Psi(x,y) + \sum_{\substack{q \ge y \\ q \in \mathcal{Q}}} \sum_{\substack{w \le x \\ q \mid w}} 1.$$

Therefore

$$\#\mathcal{W}(x) \le \Psi(x,y) + xR(y), \tag{10}$$

where

$$R(y) = \sum_{\substack{q \ge y \\ q \in \mathcal{Q}}} \frac{1}{q}.$$

According to Corollary 1.3 of [13] (see also [5] and Chapter III.5 of [20]), the bound

$$\Psi(x,y) \le x u^{-u+o(u)}$$

holds as $u \to \infty$, where $u = (\log x)/(\log y)$, provided that $u \le y^{1/2}$. If we choose (for example):

$$y = \exp(\log^{1/2} x) \qquad \text{and} \qquad u = \frac{\log x}{\log y} = \log^{1/2} x,$$

it follows that $\Psi(x,y) = o(x)$, and by (9), we also have $R(y) = o(1)$; thus, $\#\mathcal{W}(x) = o(x)$.

We remark that, by partial summation,

$$R(y) \ll \int_y^\infty \frac{1}{z^2} \#\mathcal{Q}(z)\, dz, \tag{11}$$

and therefore

$$\#\mathcal{W}(x) \ll \Psi(x,y) + x \int_y^\infty \frac{1}{z^2} \#\mathcal{Q}(z)\, dz.$$

Clearly, under various assumptions about the growth rate $\#\mathcal{Q}(z)$, one can obtain different explicit versions of the above statement by optimizing the choice of y in order to balance upper bounds on $\Psi(x,y)$ and $xR(y)$. For example:

- If $\#\mathcal{Q}(z) \ll z/\log^2 z$, then from (11) we derive $R(y) \ll 1/\log y$; hence, taking
$$u = \frac{\log_2 x}{\log_3 x} \qquad \text{and} \qquad y = x^{1/u},$$
and using (10), we obtain that
$$\#\mathcal{W}(x) \ll x\frac{\log_2 x}{\log x \log_3 x}.$$

- If $\#\mathcal{Q}(z) \ll z^\alpha$ for some constant $\alpha < 1$, then from (11) it follows that $R(y) \ll y^{-1+\alpha}$; thus, taking
$$y = \exp\left(\left(\frac{1}{2(1-\alpha)}\log x \log_2 x\right)^{1/2}\right),$$
and using (10), we obtain that
$$\#\mathcal{W}(x) \ll x \exp\left(-\left((2-2\alpha+o(1))\log x \log_2 x\right)^{1/2}\right).$$

Theorem 6. *Suppose that*
$$\sum_{\substack{\log_2 x \le q \le x \\ q \notin \mathcal{Q}}} \frac{1}{q} \to \infty$$
as $x \to \infty$. Then
$$\#\mathcal{W}(x) = o(x).$$

Proof. We have:
$$\sum_{\substack{n \le x \\ P(\gcd(n,\varphi(n))) \ge z}} 1 \le \sum_{p \ge z} \sum_{\substack{m \le x/p \\ p \mid \varphi(m)}} 1 + \sum_{p \ge z} \sum_{\substack{m \le x \\ p^2 \mid m}} 1 \ll x \log_2 x \sum_{p \ge z} \frac{1}{p^2},$$
where the last inequality follows from Theorem 3.5 of [8], which gives the bound
$$\sum_{\substack{m \le y \\ p \mid \varphi(m)}} 1 \ll \frac{y \log_2 y}{p}$$

for any real $y > 0$. Therefore,

$$\sum_{\substack{n \le x \\ P(\gcd(n,\varphi(n))) \ge z}} 1 \ll \frac{x \log_2 x}{z \log z}. \qquad (12)$$

By the Brun sieve, we see that the assumption of the theorem implies that $x + o(x)$ positive integers $n \le x$ are divisible by a non-Wieferich prime $q > \log_2 x$. By (12), we see that for all but $o(x)$ of such n, we can also assume that $q \nmid \varphi(n)$. Thus, by Lemma 1, we conclude that every such n is non-Wieferich. □

Assuming that $\#\mathcal{Q}(x)$ grows sufficiently slowly, the following result improves the preceding upper bounds.

Let $\exp_r x$ denote the r-th iterate of $\exp x$; that is, $\exp_1 x = \exp x$, and $\exp_r x = \exp(\exp_{r-1} x)$ for $r \ge 2$. Note that $\exp_r a \cdot \exp_r b \le \exp_r ab$ for all positive real numbers $a, b > 1$, a fact that is easily proved by induction on r.

Theorem 7. *Suppose that for some constant $A > 0$ and some integer $r \ge 1$,*

$$\#\mathcal{Q}(x) \le \exp_r\left(\log_{r+1}^A x\right)$$

as $x \to \infty$. Then there exists a constant $B > 0$ depending only on A and r, such that

$$\#\mathcal{W}(x) \le \exp\left(B \frac{\log x \log_3 x}{\log_2 x}\right).$$

Proof. For every $w \in \mathcal{W}(x)$, we write

$$w = m\ell,$$

where every prime factor of m lies in $\mathcal{Q}$, and no prime factor of ℓ lies in $\mathcal{Q}$. It is clear that the above decomposition of n is unique, and that m and ℓ are coprime.

We first fix m and bound the number of admissible values of ℓ.

Since w is Wieferich, and no prime factor of ℓ is Wieferich, Lemma 1 implies that $\ell \mid \varphi(\ell^*)\varphi(m^*)$. In particular, $\ell^* \mid \varphi(\ell^*)\varphi(m^*)$. If $\ell^* > 1$, we then consider the following filtration of the squarefree number ℓ^*.

Let $\ell_1 = \gcd(\ell^*, \varphi(m))$. Note that $\ell_1 > 1$ for otherwise $\ell^* \mid \varphi(\ell^*)$, which is clearly impossible for $\ell^* > 1$. It then follows that ℓ^*/ℓ_1 divides $\varphi(\ell^*/\ell_1)\varphi(\ell_1)$. If $\ell^* = \ell_1$, we stop.

Otherwise, let $\ell_2 = \gcd(\ell^*/\ell_1, \varphi(\ell_1))$. By the same argument as before, it follows that $\ell_2 > 1$ and that $\ell^*/(\ell_1\ell_2)$ divides $\varphi(\ell^*/\ell_1\ell_2)\varphi(\ell_2)$. If $\ell^* = \ell_1\ell_2$, we stop; otherwise, we continue this process.

In general, given $\ell_j > 1$, and assuming that $\ell^* \neq \ell_1 \ldots \ell_j$, we define the next integer $\ell_{j+1} = \gcd(\ell^*/(\ell_1 \ldots \ell_j), \varphi(\ell_j))$. Arguing as before, we see that $\ell_{j+1} > 1$, and that $\ell^*/(\ell_1 \ldots \ell_{j+1})$ divides $\varphi(\ell^*/(\ell_1 \ldots \ell_{j+1}))\varphi(\ell_{j+1})$.

We stop at the first k such that $\ell^* = \ell_1 \ldots \ell_k$.

For a given m, we now determine an upper bound for the number of admissible values of ℓ. First, observe that $\ell_1 \mid \varphi(m)$. Since $\ell_2 \mid \varphi(\ell_1)$, it follows that $\ell_2 \mid \varphi(\varphi(m))$. By induction, $\ell_j \mid \varphi^{(j)}(m)$, where we use $\varphi^{(j)}$ to denote the j-th iterate of φ. Let n be the first index such that $\varphi^{(n)}(m) = 1$. Then ℓ^* is an odd squarefree divisor of

$$\prod_{j=1}^{n} \varphi^{(j)}(m), \tag{13}$$

and, in particular, the number of admissible prime factors of any such number ℓ is at most $\widehat{\omega_\varphi}(m)$, where $\widehat{\omega_\varphi}(m)$ denotes the number of odd prime factors of the number shown in (13) above. We now use induction on m to show that

$$2^{\widehat{\omega_\varphi}(m)} \leq m \tag{14}$$

holds for all positive integers $m \geq 2$. This is clearly so for $m = 2$ and 3. Assume now that m is given, and that the above inequality (14) is true for all positive integers smaller than m. We may assume that m is squarefree and odd, for otherwise we can replace m by its largest odd squarefree divisor and use the induction hypothesis. Now clearly the odd squarefree part of $\varphi(m)$ is at most $\varphi(m)/2^{\omega(m)}$. Since

$$\widehat{\omega_\varphi}(m) = \omega(m) + \widehat{\omega_\varphi}(\varphi(m)) = \omega(m) + \widehat{\omega_\varphi}\left(\frac{\varphi(m)}{2^{\omega(m)}}\right),$$

it follows from the induction hypothesis that

$$2^{\widehat{\omega_\varphi}(m)} = 2^{\omega(m)} 2^{\widehat{\omega_\varphi}(\varphi(m)/2^{\omega(m)})} \leq 2^{\omega(m)} \frac{\varphi(m)}{2^{\omega(m)}} \leq m,$$

which completes the induction and establishes (14) for all $m \geq 2$.

The above argument shows that

$$\widehat{\omega_\varphi}(m) \leq \frac{\log m}{\log 2} \leq 2\log m \leq 2\log x$$

for each m. Since $\omega(\ell)! \le \ell \le x$, the inequality $\omega(\ell) \le K$ also holds with $K = \lfloor 2\log x/\log_2 x\rfloor$, for sufficiently large x. Thus, the number of admissible choices for ℓ^*, is, by Stirling's formula, at most

$$\sum_{k\le K} \binom{\widehat{\omega_\varphi}(m)}{k} \le K \left(\frac{2e\log x}{K}\right)^{K+o(K)} = \exp\left(O\left(\frac{\log x \log_3 x}{\log_2 x}\right)\right). \tag{15}$$

Now suppose that both m and ℓ^* are fixed; we estimate the number of admissible choices for ℓ. Writing

$$\ell^* = \prod_{j=1}^{\nu} p_j,$$

it suffices to count the number of ν-tuples $(\delta_1, \ldots, \delta_\nu)$ of positive integers such that

$$\prod_{j=1}^{\nu} p_j^{\delta_j} \le x.$$

This inequality implies that

$$\sum_{j=1}^{\nu} \delta_j \le 2\log x,$$

and it is clear that, by the Stirling formula, the number of ν-tuples $(\delta_1, \ldots, \delta_\nu)$ satisfying this latter inequality is at most

$$\begin{aligned} \binom{\lfloor 2\log x\rfloor}{\nu-1} \le \binom{\lfloor 2\log x\rfloor}{K} &\le \left(\frac{2e\log x}{K}\right)^{K+o(K)} \\ &= \exp\left(O\left(\frac{\log x \log_3 x}{\log_2 x}\right)\right). \end{aligned} \tag{16}$$

By the estimates (15) and (16), we see that if m is given, then the number of choices for ℓ such that $m\ell \in \mathcal{W}(x)$ is at most $\exp(O(\log x \log_3 x/\log_2 x))$. It now remains to count the number of possible values for m.

As before we assume that the elements of $\mathcal{Q} = \{q_j\}$ are indexed in the ascending order (for example, $q_1 = 1093$, $q_2 = 3511$).

From the inequality

$$j = \#\mathcal{Q}(q_j) \le \exp_r\left(\log_{r+1}^A q_j\right),$$

we derive that

$$\log q_j \geq \exp_r \left(\log_r^{1/A} j \right) \tag{17}$$

for some constant $c > 0$. Let s be the largest integer such that

$$\sum_{j=1}^{s} \log q_j \leq \log x.$$

From the bound (17), we deduce that

$$s \ll \frac{\log x}{\exp_r \left(0.5 \log_{r+1}^{1/A} x \right)}.$$

Since

$$\log x \geq \log m \geq \sum_{q \,|\, m} \log q \geq \sum_{j=1}^{\omega(m)} \log q_j,$$

we have $\omega(m) \leq s$ for each such m. Therefore, m^* can take at most

$$\begin{aligned}
\#\mathcal{Q}(x)^s &= \exp\left(O\left(\frac{\exp_{r-1}\left(\log_{r+1}^{A} x\right) \log x}{\exp_r \left(0.5 \log_{r+1}^{1/A} x \right)} \right)\right) \\
&= \exp\left(O\left(\frac{\log x}{\exp_r \left(\frac{0.5 \log_{r+1}^{1/A} x}{A \log_{r+2} x} \right)} \right)\right) \\
&= \exp\left(O\left(\frac{\log x}{\exp_r \left(\log_{r+1}^{1/2A} x \right)} \right)\right) = \exp\left(O\left(\frac{\log x}{\log_2 x} \right)\right)
\end{aligned}$$

values, once x is sufficiently large. For each fixed value of m^* there are no more than

$$\begin{aligned}
(2 \log x)^s &= \exp\left(O\left(s \log_2 x \right)\right) \\
&= \exp\left(O\left(\frac{\log x \log_2 x}{\exp_r \left(0.5 \log_{r+1}^{1/A} x \right)} \right)\right) = \exp\left(O\left(\frac{\log x \log_3 x}{\log_2 x} \right)\right)
\end{aligned}$$

corresponding values of m, which completes the proof. □

Theorem 8. *If the inequality*

$$\#\mathcal{Q}(x) \geq \alpha \log_2 x$$

holds for some positive absolute constant α and all sufficiently large x, then

$$\#\mathcal{W}(x) \geq (\log x)^{\alpha \log 2 + o(1)}.$$

Proof. Let x be large, and put $t = \#\mathcal{Q}(x)$, $y = x^{1/t}$ and $s = \#\mathcal{Q}(y)$. Then,

$$s = \#\mathcal{Q}(y) \geq \alpha \log_2 y = \alpha(\log_2 x - \log \#\mathcal{Q}(x)) = (\alpha + o(1)) \log_2 x.$$

Using Lemma 1, it is clear that each of the $2^s - 1$ squarefree numbers $w \geq 3$ whose prime factors lie in $\mathcal{Q}(y)$ is a Wieferich number, and each one satisfies $w \leq y^s \leq y^t = x$. □

In particular, assuming (8), Theorem 7 and Theorem 8 yield the bounds

$$(\log x)^{\log 2 + o(1)} \leq \#\mathcal{W}(x) \leq \exp\left(O\left(\frac{\log x \log_3 x}{\log_2 x}\right)\right)$$

for the number of Wieferich numbers $w \leq x$.

We now show that if $\mathcal{Q}$ is finite, then $\mathcal{W}$ is finite as well and can be effectively evaluated.

Theorem 9. *Assume that $\mathcal{Q}$ is a finite set. Then $\mathcal{W}$ is a finite set too, and*

$$W \leq 2^{Q\#\mathcal{Q}} \exp\left((1 + o(1))Q\right),$$

where $W = \max_{w \in \mathcal{W}} w$ and $Q = \max_{q \in \mathcal{Q}} q$.

Proof. By Lemma 2, we see that $P(w) \leq Q$. Let

$$M = \prod_{q \leq Q} (q - 1),$$

where the product is taken over all primes $q \leq Q$. Now, by Lemma 1, we conclude that for every prime p,

$$\nu_p(w) \leq \nu_p\left(2^{p-1} - 1\right) - 1 + \nu_p(M).$$

Therefore

$$W \le \prod_{p \in \mathcal{Q}} 2^{p-1} p^{\nu_p(M)} \prod_{\substack{p \le Q \\ p \notin \mathcal{Q}}} p^{\nu_p(M)} = \prod_{p \in \mathcal{Q}} 2^{p-1} \prod_{p \le Q} p^{\nu_p(M)} \le 2^{Q \# \mathcal{Q}} M.$$

Using the well-known bound

$$\log M \le \sum_{p \le Q} \log p = (1 + o(1))Q,$$

we finish the proof. □

5 Some Alternative Definitions of Wieferich Numbers

By definition, a Wieferich number is an odd integer $w \ge 3$ satisfying (1). As we have already mentioned, in the special case that $w = q$ is prime, this definition is consistent with the usual definition of a Wieferich prime. In this section, we consider some other sets of positive odd integers, similar to $\mathcal{W}$, whose intersection with the set of primes is precisely $\mathcal{Q}$.

One of the possible ways to extend the definition of Wieferich primes is to request that

$$\gcd\left(\frac{2^{\varphi(w)} - 1}{w}, w\right) > 1.$$

Let $\widetilde{\mathcal{W}}$ be the set of odd integers $w \ge 3$ satisfying this condition, and let $\widetilde{\mathcal{U}}$ be the complimentary set consisting of all odd integers $w \ge 3$ with $w \notin \widetilde{\mathcal{W}}$. Surprisingly enough, it has been shown that $\widetilde{\mathcal{W}}$ is a set of relative density 1 in the set of all odd positive integers; that is, $\#\widetilde{\mathcal{W}}(x) = x/2 + o(x)$ (see [9]).

Next, let $\overline{\mathcal{W}}$ be the set of odd integers $w \ge 3$ satisfying the congruence

$$2^{\lambda(w)} \equiv 1 \pmod{w^2},$$

and let $\overline{\mathcal{U}}$ be the complimentary set of odd integers.

Combining the first two approaches, one can also consider the set $\widehat{\mathcal{W}}$ of all odd integers $w \ge 3$ for which the inequality

$$\gcd\left(\frac{2^{\lambda(w)} - 1}{w}, w\right) > 1$$

holds. We also denote by $\widehat{\mathcal{U}}$ the complimentary set.

Finally, let $\mathcal{W}^\dagger$ be the set of odd integers $w \ge 3$ such that w is a product of Wieferich primes, and let $\mathcal{U}^\dagger$ be the complimentary set of odd integers.

We observe that:

$$\mathcal{Q} \subsetneqq \mathcal{W}^\dagger \subsetneqq \overline{\mathcal{W}} \subsetneqq \mathcal{W} \subsetneqq \widehat{\mathcal{W}} \subsetneqq \widetilde{\mathcal{W}}. \tag{18}$$

Here, the various inclusions follow immediately from the definitions (although the inclusion $\mathcal{W} \subset \widehat{\mathcal{W}}$ is less obvious; for this, the idea is to show that if $w \in \mathcal{W}$, then for $q = P(w) \in \mathcal{Q}$ one has $qw \mid 2^{\lambda(w)} - 1$); the fact that these are all *proper* inclusions follows from the examples:

$$3837523 \in \mathcal{W}^\dagger \setminus \mathcal{Q}, \qquad 3279 \in \overline{\mathcal{W}} \setminus \mathcal{W}^\dagger, \qquad 68859 \in \mathcal{W} \setminus \overline{\mathcal{W}},$$
$$21 \in \widehat{\mathcal{W}} \setminus \mathcal{W}, \qquad \text{and} \qquad 63 \in \widetilde{\mathcal{W}} \setminus \widehat{\mathcal{W}}.$$

We remark that $\gcd(\varphi(w), \lambda(w^2)) = \lambda(w)$ if $w \ge 3$ is odd and squarefree; thus, if $w \in \mathcal{W}$ is squarefree, then $w \in \overline{\mathcal{W}}$ since

$$2^{\varphi(w)} \equiv 1 \equiv 2^{\lambda(w^2)} \pmod{w^2}.$$

We also note that if $w \in \mathcal{W}$ and $\gcd(w, \varphi(w)) = 1$, then $w \in \mathcal{W}^\dagger$; this follows immediately from Lemma 1.

We believe that our methods from the preceding sections can be applied to derive upper and lower bounds on $\#\mathcal{W}^\dagger(x)$, $\#\overline{\mathcal{W}}(x)$, $\#\widehat{\mathcal{W}}(x)$ and $\#\widetilde{\mathcal{W}}(x)$ (and thus, on the complementary sets as well), which in some cases are sharper than those that follow directly from the inclusions (18). In particular, we remark that the statement and proof of Theorem 8, without any changes, applies to $\#\overline{\mathcal{W}}(x)$ as well. Moreover, proceeding as in the proof of Theorem 5, we can take integers $n = p^h m$, where

$$h = \left\lceil \frac{p \log 2}{\log p} \right\rceil \ge \nu_p(2^{p-1} - 1),$$

and $m \le x/p^h$ is such that each prime factor q of m satisfies $q \not\equiv 1 \pmod{p^h}$. Lemma 4, with obvious minor adjustments, yields a lower bound on the number of such m, and choosing p as the smallest prime p such that $2^p \ge \log_2 x$, one derives the estimate

$$\begin{aligned} \#\overline{\mathcal{U}}(x) &\ge \frac{x}{p^h} \exp\left(-\frac{\log_2(x/p^h)}{p^{h-1}(p-1)} + O(\log_3(x/p^h)) \right) \\ &\ge x \exp\left(-p \log 2 - \frac{\log_2 x}{2^{p-1}} + O(\log_3 x) \right) \gg x (\log_2 x)^{-C}, \end{aligned}$$

for some absolute constant $C > 0$. In fact, taking $n = 3p^h m$ with $p \equiv 1 \pmod 3$ in the construction of Theorem 5 and in the above construction, we have

$$\begin{array}{rcl}\nu_3(2^{\varphi(n)} - 1) & = & \nu_3(2^{\varphi(3p^h m)} - 1) \geq \nu_3(2^{\varphi(3^{\nu_3(m)+1}p)} - 1)\\ & \geq & \nu_3(p-1) + \nu_3(m) + 1 > \nu_3(n),\end{array}$$

which in turn shows that

$$\#\widetilde{\mathcal{W}}(x) - \#\mathcal{W}(x) \gg x \exp\left(-2\beta \log_2^{1/2} x + O\left(\log_2^{1/3} x\right)\right),$$

where $\beta = \log^{1/2} 2$ as in Theorem 5; and

$$\#\widetilde{\mathcal{W}}(x) - \#\overline{\mathcal{W}}(x) \gg x(\log_2 x)^{-C}.$$

On the other hand, proving that $\#\mathcal{W}(x) - \#\overline{\mathcal{W}}(x) \to \infty$ still appears to be out of reach.

As we have remarked, it is shown in [9] that $\#\widetilde{\mathcal{U}}(x) = o(x)$. Here, we show that in fact one can obtain an explicit upper bound on the larger quantity $\#\widehat{\mathcal{U}}(x) \geq \#\widetilde{\mathcal{U}}(x)$.

Theorem 10. *The following bounds hold:*

$$\#\widetilde{\mathcal{U}}(x) \leq \#\widehat{\mathcal{U}}(x) \ll \frac{x}{\log_3 x}.$$

Proof. We assume that x is large enough and put

$$y = \frac{\log_2 x}{3 \log_3 x}.$$

Let $\mathcal{E}_1$ be the set of positive integers $n \leq x$ which do not have a prime divisor $p \leq y$. By the Brun sieve (see Theorem 2.2 in [11]), and the Mertens formula,

$$\#\mathcal{E}_1 \ll x \prod_{2 \leq p \leq y} \left(1 - \frac{1}{p}\right) \ll \frac{x}{\log y}.$$

Let $\mathcal{E}_2$ be the set of positive integers $n \leq x$ such that there exists a prime $p < y$ with $p^{\nu_p(n)} > y$. Clearly,

$$\nu_p(n) \geq \left\lceil \frac{\log y}{\log p} \right\rceil \geq 2.$$

Hence, putting

$$K = \left\lceil \frac{\log y}{\log 2} \right\rceil ,$$

we obtain

$$\#\mathcal{E}_2 \ll \sum_{k=2}^{K} \sum_{y^{1/k} < p \le y^{1/(k-1)}} \frac{x}{p^k} \ll x \sum_{k=2}^{K} \frac{k}{y^{(k-1)/k}} \ll xy^{-1/2} + xK^2 y^{-2/3} \le xy^{-1/2}.$$

Therefore, the set $\mathcal{I}$ of odd positive integers $n \le x$ such that for some prime p we have $p^{\nu_p(n)} \le y$ is of cardinality $\mathcal{I} = x/2 + O(x/\log y)$.

Let $\mathcal{E}_3$ be the set of odd positive integers $n \in \mathcal{I}$ such that there exists a prime p with $p^{\nu_p(n)} \le y$ and such that $\lambda(n) \not\equiv 0 \pmod{p^{\nu_p(n)}}$. Again by the Brun sieve, we obtain

$$\#\mathcal{E}_3 \ll x \sum_{k=2}^{\infty} \sum_{p^k \le y} \exp\left(- \sum_{\substack{\ell \le x \\ \ell \equiv 1 \pmod{p^k}}} \frac{1}{\ell} \right),$$

where ℓ and p run through odd prime numbers (see the proof of Theorem 3.4 in [8], or that of Lemma 2 in [16]). For $p^k \le y \le (\log x)^{1/3}$, one easily derives from the classical results on the distribution of primes in an arithmetic progression, that

$$\sum_{\substack{\ell \le x \\ \ell \equiv 1 \pmod{p^k}}} \frac{1}{\ell} = (1 + o(1)) \frac{\log_2 x}{p^{k-1}(p-1)} \ge (1 + o(1)) \frac{\log_2 x}{y}.$$

Hence,

$$\#\mathcal{E}_3 \ll xy \exp(-(1 + o(1)) y^{-1} \log_2 x).$$

Thus, the set $\mathcal{J} = \mathcal{I} \backslash \mathcal{E}_3$ is of cardinality

$$\#\mathcal{J} = x/2 + O(x/\log y + xy \exp(-(1 + o(1)) y^{-1} \log_2 x)).$$

For every $n \in \mathcal{J}$, there exists a prime $p \le y$ such that $\nu_p(n) \le \nu_p(\lambda(n))$. Therefore, $p^{\nu_p(n)}(p-1) \mid \lambda(n)$; thus, $p^{\nu_p(n)+1} \mid 2^{\lambda(n)} - 1$. This implies that $p \mid \gcd\big((2^{\lambda(n)} - 1)/n, n\big)$. Hence, $\#\widehat{\mathcal{W}}(x) \ge \#\mathcal{J}$. Recalling the value of y, we finish the proof. □

6 Some Heuristics and Further Questions

Let again

$$y = \frac{\log_2 x}{3 \log_3 x}.$$

The proof of of Theorem 10 (the bounds on $\#\mathcal{E}_2$ and $\#\mathcal{E}_3$), shows that for

$$t \ge \exp(y^3),$$

all odd positive integers $n \le t$, except for a set $\mathcal{F}(t)$ of cardinality $\#\mathcal{F}(t) = O(ty^{-1/2} + ty \exp(-(1 + o(1))y^{-1} \log_2 t)))$, we have

$$\prod_{\substack{p|n \\ p \le y}} p \mid \gcd\left((2^{\varphi(n)} - 1)/n, n\right) .$$

Thus, it is natural to assume that for each odd n with $\exp(y^3) \le n \le x$ and $n \notin \mathcal{F}(x)$, the "probability" that n is Wieferich is at least $f(n)/n$, where

$$f(n) = \prod_{\substack{p|n \\ p \le y}} p,$$

which suggests that

$$\#\mathcal{W}(x) \gg \sum_{n \le x} \frac{f(n)}{n}.$$

We now consider the set $\mathcal{V}(t)$ of integers of the form $n = ab$, where a is an odd squarefree integer in the interval $[y/2, y]$, and $b \le t/y$ is an positive integer whose all prime divisors are greater than y (that is, b is a so-called y-rough number). It is well-known (see Theorems 3 and 4 in Section 3.6 of [20]), that b takes at least $(e^{-\gamma} + o(1))\, t/y \log y$ possible values in any interval $b \le t$ with $y = o(t)$, where $\gamma = 0.5772\ldots$ is the Euler-Mascheroni constant. In particular, $\#\mathcal{V}(t) \gg t/\log y$; thus, for the above value of y we have $\#\mathcal{F}(t) = o(\#\mathcal{V}(t))$. Since $f(n) \ge y/2$ for every $n \in \mathcal{V}(x)\backslash\mathcal{F}(x)$, we derive

$$\#\mathcal{W}(x) \ge \sum_{\substack{\exp(y^3) \le n \le x \\ n \in \mathcal{V}(x)\backslash\mathcal{F}(x)}} \frac{f(n)}{n} \gg y \sum_{\substack{\exp(y^3) \le n \le x \\ n \in \mathcal{V}(x)\backslash\mathcal{F}(x)}} \frac{1}{n} \gg y \sum_{\substack{\exp(2y^3) \le n \le x \\ n \in \mathcal{V}(x)\backslash\mathcal{F}(x)}} \frac{1}{n}.$$

Using the fact that $\#\left(\mathcal{V}(t)\backslash\mathcal{F}(t)\right) \gg t/\log y$ for $t \geq \exp(y^3)$ together with partial summation, we derive

$$\begin{aligned}\sum_{\substack{\exp(2y^3)\leq n\leq x\\ n\in\mathcal{V}(x)\backslash\mathcal{F}(x)}} \frac{1}{n} &\gg \sum_{\exp(2y^3)\leq n\leq x} \big(\#\left(\mathcal{V}(n)\backslash\mathcal{F}(n)\right) - \exp(y^3)\big)\frac{1}{n^2}\\ &\gg \frac{1}{\log y}\sum_{\exp(2y^3)\leq n\leq x}\frac{1}{n} \gg \frac{\log x}{\log y}.\end{aligned}$$

Recalling the value of y, leads us to the conjectured inequality (4).

As in [9], we also remark that the set $\widetilde{\mathcal{W}}$ is contained in the set of the so-called *Crandall numbers*; thus, Theorem 10 gives an upper bound on the cardinality of the set of non-Crandall numbers $n \leq x$.

Let us consider the limit

$$\vartheta = \limsup_{n\to\infty}\frac{\log\gcd\big((2^{\varphi(n)}-1)/n, n\big)}{\log n}.$$

Certainly, if $\mathcal{Q}$ is infinite then $\vartheta = 1$. We now show that this also follows from a variant of the *Dickson prime s-tuplets conjecture*, which has somewhat more support (see [3]). Indeed, assume that for every s there exists a constant $A_s \geq 2$ such that there are infinitely many chains of primes $p_1, \ldots, p_s$ with $p_{i+1} = a_i p_i + 1$, for some positive integers $a_i \leq A_s$, $i = 1, \ldots, s-1$. Putting $n = p_1 \ldots p_s$, we see that

$$p_s \leq (A_s+1)^s p_1 \leq (A_s+1)^s n^{1/s},$$

and that $p_i(p_i-1)|\varphi(n)$, for $i = 1, \ldots, s-1$. Thus,

$$\gcd\left(\frac{2^{\varphi(n)}-1}{n}, n\right) \geq p_1\ldots p_{s-1} = n/p_s \geq (A_s+1)^{-s}n^{1-1/s},$$

which implies that $\vartheta = 1$. It is also easy to see that in fact one can allow the a_i to grow together with p_i as $a_i = p_i^{o(1)}$, for $i = 1, \ldots, s-1$.

We now present an unconditional lower bound on ϑ. By [2] (and some simple counting arguments), there are infinitely many primes p with $q = P(p-1) \geq p^{0.677}$ and $\nu_2(p-1) + \nu_2(q-1) \leq \log^{1/2} p$. Write $p - 1 = 2^{\alpha}\ell_1^{\alpha_1}\ldots\ell_s^{\alpha_s}m$, where $q - 1 = 2^{\beta}\ell_1^{\beta_1}\ldots\ell_s^{\beta_s}$ is the prime number factorization of $q-1$ and the integers $\alpha_1, \ldots, \alpha_s, m$ are such that $\gcd(m, q-1) = 1$. Put $n = 2^{-\alpha-\beta}(q-1)(p-1)p$. We see that

$$m^2 \ell_1^{2(\alpha_1+\beta_1)} \ldots \ell_s^{2(\alpha_s+\beta_s)} \mid 2^{\varphi(n)} - 1.$$

Hence, $\gcd\left((2^{\varphi(n)} - 1)/n, n\right) \geq (q-1)(p-1)2^{-\alpha-\beta} \gg n^{0.6264+o(1)}$. Therefore,

$$\vartheta \geq 0.6264\ldots,$$

which naturally leads to a question about getting a better unconditional bound on the above upper limit (and on the similar upper limit with $\varphi(n)$ replaced by $\lambda(n)$).

References

[1] T. Agoh, K. Dilcher and L. Skula, ‘Fermat quotients for composite moduli’, *J. Number Theory*, **66** (1997), 29–50.

[2] R. C. Baker and G. Harman, ‘Shifted primes without large prime factors’, *Acta Arith.*, **83** (1998), 331–361.

[3] A. Balog, ‘The prime k-tuplets conjecture on average’, *Analytic Number Theory*, Progress in Mathematics **85**, Birkhäuser, Boston, 1990, 47–75.

[4] R. Crandall, K. Dilcher and C. Pomerance, ‘A search for Wieferich and Wilson primes’, *Math. Comp.*, **66** (1997), 433–449.

[5] E. R. Canfield, P. Erdős and C. Pomerance, ‘On a problem of Oppenheim concerning “Factorisatio Numerorum”’, *J. Number Theory*, **17** (1983), 1–28.

[6] H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York 1980.

[7] K. Dilcher, ‘Fermat numbers, Wieferich and Wilson primes: Computations and generalizations’, *Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw, 2000*, Walter de Gruyter, 2001, 29–48.

[8] P. Erdős, A. Granville, C. Pomerance and C. Spiro, 'On the normal behavior of the iterates of some arithmetic functions', *Analytic Number Theory*, Birkhäuser, Boston, 1990, 165–204.

[9] Z. Franco and C. Pomerance, 'On a conjecture of Crandall concerning the $qn+1$ problem', *Math. Comp.*, **64** (1995), 1333–1336.

[10] A. Granville and K. Soundararajan, 'A binary additive problem of Erdős and the order of $2 \mod p^2$', *The Ramanujan Journal*, **2** (1998), 283–298.

[11] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[12] D. R. Heath-Brown, 'Artin's conjecture for primitive roots', *Quart. J. Math.*, **37** (1986), 27–38.

[13] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. de Théorie des Nombres de Bordeaux*, **5** (1993), 411–484.

[14] H. Iwaniec and J. Pintz, 'Primes in short intervals', *Monatsh. Math.*, **98** (1984), 115–143.

[15] J. Knauer and J. Richstein, 'The continuing search for Wieferich primes', *Math. Comp.*, (to appear).

[16] F. Luca and C. Pomerance, 'On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ', *Colloq. Math.*, **92** (2002), 111–130.

[17] S. Mohit and M. R. Murty, 'Wieferich primes and Hall's conjecture', *C. R. Math. Acad. Sci., Soc. R. Can.*, **20** (1998), 29–32.

[18] P. Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, New York-Heidelberg 1979.

[19] J. H. Silverman, 'Wieferich's criterion and the abc-conjecture', *J. Number Theory*, **30** (1988), 226–237.

[20] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.

[21] A. Wieferich, ‘Zum letzten Fermat’schen Theorem’, *J. Reine Angew. Math.*, **136** (1909), 293–302.

[22] E. Wirsing, ‘Über die Zahlen, deren Primteiler einer gegebenen Menge angehören’, *Arch. Math.*, **7** (1956), 263–272.