THE LARGEST KNOWN WIEFERICH NUMBERS

Amir Akbary[1]
Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, AB, T1K 3M4, Canada
amir.akbary@uleth.ca

Sahar Siavashi[1]
Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive West, Lethbridge, AB, T1K 3M4, Canada
sahar.siavashi@uleth.ca

Received: , Revised: , Accepted: , Published:

Abstract

A prime p is called a Wieferich prime in base $a > 1$, if $(a, p) = 1$ and $a^{p-1} \equiv 1 \pmod{p^2}$. An integer $m > 1$ is called a Wieferich number in base $a > 1$, if $(a, m) = 1$ and $a^{\varphi(m)} \equiv 1 \pmod{m^2}$, where φ is the Euler function. In 2007, Banks, Luca, and Shparlinski proved that if the set of Wieferich primes in base 2 is finite, then the set of Wieferich numbers in base 2 is also finite. Moreover, they found an upper bound for the largest element of this set. Here we present a procedure in which the largest element can be constructed in any base.

A prime p is called a *Wieferich prime in base* $a > 1$, if $(a, p) = 1$ and $a^{p-1} \equiv 1 \pmod{p^2}$. For $a = 2$, these primes were first considered by Arthur Wieferich in 1909 in relation with Fermat's last theorem. In [5] Wieferich proved that if for a prime exponent p the first case of Fermat's last theorem is false, then p must satisfy the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. According to [4], the only Wieferich primes in base 2 below 6×10^{17} are 1903 and 3511. Information on the search for Wieferich primes in various bases can be found in [4].

Let $m, a > 1$ be integers with $(a, m) = 1$. Then m is called a *Wieferich number in base* a, if $a^{\varphi(m)} \equiv 1 \pmod{m^2}$, where φ is the Euler function. In [1], Agoh, Dilcher, and Skula studied Wieferich numbers and developed a criterion that determines Wieferich numbers (see Theorem 3). Also in [1, page 47], given the two known Wieferich primes in base 2, all the known Wieferich numbers are constructed. There are a total of 104 known Wieferich numbers in base 2.

[1]Research of the authors is partially supported by NSERC.

It is expected that the set of Wieferich primes (and thus Wieferich numbers) in any base to be infinite, although such primes (numbers) appear to be rare. In [2], by employing the criterion for Wieferich numbers, Banks, Luca, and Shparlinski found an upper bound for the number of Wieferich numbers in base 2, given that there are finitely many Wieferich primes. More precisely, let W_2 be the set of Wieferich primes in base 2 and N_2 be the set of Wieferich numbers in base 2. The following is given in Theorem 9 of [2].

Theorem 1 (**Banks-Luca-Shparlinski**). *If W_2 is a finite set, then N_2 is also finite. Moreover, let*

$$M = \prod_{p \le w_0} (p-1),$$

where w_0 is the largest Wieferich prime in base 2. Then

$$\max N_2 \le 2^{w_0 |W_2|} M,$$

where $\max N_2 := \max\{x;\ x \in N_2\}$.

We note that by [3, p. 167, Theorem 5], we have $M \le 4^{w_0}$. Thus,

$$\max N_2 \le 2^{w_0(|W_2|+2)}.$$

Theorem 1 can be generalized to any base a.

In this note, given the set of known Wieferich primes in base a, we find an exact expression for the maximum of the set of known Wieferich numbers in base a. In order to describe our main result, we consider the following notation.

From now on p and ℓ denote primes. We denote the set of Wieferich primes and Wieferich numbers in base a by W_a and N_a, respectively. For a prime p and positive integer n, we denote the largest power of p in n by $\nu_p(n)$. Let

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

be the *Fermat quotient*. We set

$$\overline{q}(a,p) = \begin{cases} q(a,p) & \text{if } p \neq 2, \text{ or } p = 2 \text{ and } a \equiv 1 \pmod 4, \\ (a+1)/2 & \text{if } p = 2 \text{ and } a \equiv 3 \pmod 4. \end{cases}$$

For $n \ge 0$ we define the sequence $S_a^{(n)}$ by the following procedure. Let

$$S_a^{(0)} = \begin{cases} W_a \cup \{2\} & \text{if } \nu_2(\overline{q}(a,2)) \ge 1, \\ W_a & \text{otherwise.} \end{cases}$$

For $n \ge 1$ let

$$S_a^{(n)} = \{p;\ p \nmid a \text{ and } p | \ell - 1 \text{ for } \ell \in S_a^{(n-1)}\}.$$

Lastly, we form

$$S_a = \bigcup_{n=0}^{\infty} S_a^{(n)}.$$

For example

$$S_2 = \{3, 5, 7, 13, 1093, 3511\}$$

and

$$S_3 = \{2, 5, 7, 11, 41, 83, 499, 55889, 1006003\}.$$

Our main result is the following.

Theorem 2. *If W_a is a finite set, then N_a is also finite. Moreover, let*

$$\widetilde{M} = \prod_{p \in S_a} (p-1).$$

Then

$$\max N_a = \prod_{\ell \in S_a} \ell^{\alpha_\ell},$$

where

$$\alpha_\ell = \nu_\ell(\widetilde{M}) + \nu_\ell(\overline{q}(a, \ell)).$$

The main tool in the proof is a criterion for Wieferich numbers. The following is Theorem 5 of [1].

Theorem 3 (**Agoh-Dilcher-Skula**). *Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and a be two relatively prime integers, with $m \geq 3$. Then $m \in N_a$ if and only if for every $1 \leq i \leq k$, we have*

$$\alpha_i \leq \nu_{p_i}(\prod_{j=1}^{k} (p_j - 1)) + \nu_{p_i}(\overline{q}(a, p_i)).$$

Note that for $m = 2$, by the definition of a Wieferich number, we have that 2 is a Wieferich number in base $a > 1$ if and only if $a \equiv 1 \pmod 4$.

Before presenting the proof of Theorem 2 we need to establish the connection of Wieferich numbers with the set S_a. Lemma 2 which is a consequence of Theorem 3 is for this purpose. We also need a lemma regarding the largest prime divisor of a Wieferich number. The following is basically Lemma 2 of [2] which is written for Wieferich numbers in a general base a (see also [1, Corollary 5.9]).

Lemma 1. *Let m be a Wieferich number in base a. Let $P(m)$ be the largest prime divisor of m. Then $P(m) \in S_a^{(0)}$.*

Proof. Let $m = 2$ be a Wieferich number in base a. Then $P(m) = 2$ is a Wieferich prime in base a and thus $P(m) \in S_a^{(0)}$. Now let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 2$ be a Wiefriech number in base a. Observe that

$$P(m) \nmid \prod_{j=1}^{k} (p_j - 1).$$

Hence,

$$\nu_{P(m)}(\prod_{i=1}^{k} (p_i - 1)) = 0.$$

Therefore by Theorem 3 we have

$$\nu_{P(m)}(\overline{q}(a, P(m))) \geq 1. \tag{1}$$

Now if $P(m) = 2$ and $a \equiv 1 \pmod 4$, or $P(m) \neq 2$, then (1) yields $\nu_{P(m)}(a^{P(m)-1} - 1) \geq 2$. Therefore $P(m) \in W_a = S_a^{(0)}$. If $P(m) = 2$ and $a \equiv 3 \pmod 4$, then by (1) and the definition of $S_a^{(0)}$ we have $P(m) = 2 \in S_a^{(0)}$. □

Lemma 2. *Let m be a Wieferich number in base a. Then for every prime divisor p of m we have $p \in S_a$.*

Proof. First of all note that if $m = 2$ is a Wieferich number in base a, then it is also a Wieferich prime. Thus $2 \in S_a$. Now let p_1 be a prime divisor of a Wieferich number $m > 2$. If $p_1 \in S_a^{(0)}$, then $p_1 \in S_a$. Otherwise, if $p_1 \notin S_a^{(0)}$, we have $\nu_{p_1}(\overline{q}(a, p_1)) = 0$. Hence, by the fact that $\nu_{p_1}(m) > 0$ and employing Theorem 3, we have

$$\nu_{p_1}(\prod_{p|m} (p - 1)) > 0.$$

Therefore there exists a prime divisor of m like p_2 such that p_1 divides $p_2 - 1$. Now we consider cases. If $p_2 \in S_a^{(0)}$, then we have $p_1 \in S_a^{(1)}$. Consequently we have $p_1 \in S_a$. If $p_2 \notin S_a^{(0)}$, by a similar argument, there exists a prime divisor of m like p_3 such that $p_2 | p_3 - 1$. If $p_3 \in S_a^{(0)}$, then $p_2 \in S_a^{(1)}$ and $p_1 \in S_a^{(2)}$ (Since $p_1 | p_2 - 1$). If $p_3 \notin S_a^{(0)}$ then we continue this process. However the process terminates with a prime in $S_a^{(0)}$. This is true since $p_1 < p_2 < \cdots$ is an increasing sequence. Thus, either at some point we hit a prime which is in $S_a^{(0)}$ or we reach to the largest prime divisor of m, which is, by Lemma 1, also in $S_a^{(0)}$. Thus, $p_1 \in S_a^{(j)} \subseteq S_a$, for some integer j, and therefore $p_1 \in S_a$. □

Corollary 1. *If $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is a Wieferich number in base a then for every $1 \leq i \leq k$ we have*

$$\alpha_i \leq \nu_{p_i}(\widetilde{M}) + \nu_{p_i}(\overline{q}(a, p_i)).$$

Proof. If $m = 2$, then $a \equiv 1 \pmod 4$ and $\nu_2(q(a,2)) \geq 1$. Thus the assertion is true. For $m \geq 3$ the result follows from Theorem 3 and Lemma 2. □

We are ready to prove our main result.

Proof of Theorem 2. Let

$$m_0 = \prod_{\ell \in S_a} \ell^{\nu_\ell(\widetilde{M}) + \nu_\ell(\overline{q}(a,\ell))}.$$

Let $m = \prod_\ell \ell^\alpha$ be a Wieferich number. Then by Lemma 2 we have $\ell \in S_a$. Thus by Corollary 1 we have $m \leq m_0$. Now let $m_0 = \prod_{\ell \in S_a} \ell^{\alpha_\ell}$, where

$$\alpha_\ell = \nu_\ell(\widetilde{M}) + \nu_\ell(\overline{q}(a,\ell)) = \nu_\ell(\prod_{\ell | m_0} (\ell - 1)) + \nu_\ell(\overline{q}(a,\ell)).$$

Thus from Theorem 3 we conclude that m_0 is a Wieferich number. Since m_0 is greater than any other Wieferich numbers, then m_0 is the largest Wieferich number. □

By employing Theorem 2, we calculated the largest known Wieferich numbers in different bases, using the known Wieferich primes given in [4]. We collected our results for $\max N_a$ for bases a from 2 to 25 in Table 1.

Acknowledgement The authors would like to thank the referee for her/his helpful comments and suggestions.

References

[1] T. Agoh, K. Dilcher, and L. Skula, Fermat quotients for composite moduli, *J. Number Theory* **66** (1999), 29–50.

[2] W. Banks, F. Luca, and I. Shparlinski, Estimates for Wieferich numbers, *Ramanujan J.* **14** (2007), 361–378.

[3] P. Erdös and J. Surányi, *Topics in the Theory of Numbers*, Springer-Verlag, New York, 2003. Translated from the second Hungarian edition by Barry Guiduli.

[4] http://www.fermatquotient.com/FermatQuotienten/FermQ_Sort.txt.

[5] A. Wieferich, Zum letzten Fermatschen Theorem, *J. Reine Angew. Math.* **136** (1909), 293–302.

a	Known Wieferich primes	Largest known Wieferich numbers
2, 4,16	1093, 3511	$3^6 \times 5 \times 7 \times 13^2 \times 1093 \times 3511$
3	11, 1006003	$2^{15} \times 5^2 \times 7 \times 11 \times 41 \times 83 \times 499 \times 55889 \times 1006003$
5	$2, 20771, 40487, 53471161,$ $1645333507, 6692367337,$ 188748146801	$2^{55} \times 3^{24} \times 7^6 \times 11^3 \times 13 \times 17^3 \times 19 \times 23^2 \times 31^2 \times 47 \times 67 \times 113 \times 163 \times 239 \times 283 \times 653 \times 761 \times 1429 \times 1523 \times 4951 \times 20771 \times 40487 \times 91127 \times 123397 \times 148531 \times 1974353 \times 15491591 \times 30469139 \times 53471161 \times 278848639 \times 1645333507 \times 6692367337 \times 188748146801$
6	66161, 534851, 3152573	$5^6 \times 7^3 \times 11 \times 17 \times 19 \times 23 \times 29 \times 41 \times 47 \times 59 \times 281 \times 409 \times 563 \times 827 \times 66161 \times 534851 \times 3152573$
7	5, 491531	$2^{11} \times 3^5 \times 5^3 \times 11 \times 13 \times 19 \times 199 \times 491531$
8	3, 1093, 3511	$3^7 \times 5 \times 7 \times 13^2 \times 1093 \times 3511$
9	2, 11, 1006003	$2^{16} \times 5^2 \times 7 \times 11 \times 41 \times 83 \times 499 \times 55889 \times 1006003$
10	3, 487, 56598313	$3^{12} \times 7 \times 11 \times 13 \times 23 \times 31 \times 127 \times 487 \times 599 \times 56598313$
11	71	$2^6 \times 3 \times 5 \times 7 \times 71$
12	2693, 123653	$5 \times 7 \times 19 \times 271 \times 673 \times 1627 \times 2693 \times 123653$
13	2, 863, 1747591	$2^{16} \times 3^3 \times 5^3 \times 7^2 \times 43 \times 431 \times 863 \times 4481 \times 1747591$
14	29, 353, 7596952219	$3^6 \times 5^4 \times 11^2 \times 29^2 \times 59 \times 353 \times 401 \times 991 \times 17839 \times 7596952219$
15	29131, 119327070011	$2^{29} \times 7^2 \times 11 \times 13 \times 17 \times 23 \times 29 \times 47 \times 97 \times 113 \times 137 \times 823 \times 971 \times 2246791 \times 119327070011$
17	$2, 3, 46021, 48947, 478225523351$	$2^{30} \times 3^9 \times 5^8 \times 7^3 \times 11 \times 13^2 \times 19 \times 23^2 \times 29 \times 31 \times 59 \times 79 \times 101 \times 1381 \times 24473 \times 48947 \times 494699 \times 9564510467 \times 478225523351$
18	5, 7, 37, 331, 33923, 1284043	$5^4 \times 7^4 \times 11 \times 13 \times 17 \times 37 \times 43 \times 137 \times 331 \times 823 \times 2423^2 \times 8231 \times 214007 \times 33923 \times 1284043$
19	3, 7, 13, 43, 137, 63061489	$2^{26} \times 3^8 \times 7^4 \times 13^2 \times 17 \times 43 \times 53 \times 73 \times 107 \times 137 \times 857 \times 63061489$
20	281, 46457, 9377747, 122959073	$3^9 \times 7^3 \times 11 \times 13^2 \times 17 \times 29^2 \times 281 \times 433 \times 1171 \times 1451 \times 2903 \times 5807 \times 25763 \times 46457 \times 132499 \times 669839 \times 122959073$
21	2	2
22	$13, 673, 1595813, 492366587,$ 9809862296159	$3^{21} \times 5^3 \times 7^3 \times 13^3 \times 19 \times 23 \times 29 \times 47 \times 73 \times 109 \times 181 \times 293 \times 541 \times 673^2 \times 2539 \times 2693 \times 13757 \times 198043 \times 1188259 \times 1595813 \times 61545823 \times 246183293 \times 492366587 \times 44999368331 \times 9809862296159$
23	$13, 2481757, 13703077, 15546404183,$ $2549536629329,$	$2^{60} \times 3^{15} \times 5^4 \times 7^2 \times 11 \times 13^3 \times 17^3 \times 37^2 \times 43^2 \times 61^2 \times 113 \times 137 \times 149 \times 173 \times 347 \times 1097 \times 1621 \times 2753 \times 5507 \times 38149 \times 206813 \times 380641 \times 2481757 \times 13703077 \times 15546404183 \times 2549536629329$
24	5, 25633	$5^2 \times 11 \times 89 \times 25633$
25	$2, 20771, 40487, 53471161,$ $1645333507, 6692367337,$ 188748146801	$2^{56} \times 3^{24} \times 7^6 \times 11^3 \times 13 \times 17^3 \times 19 \times 23^2 \times 31^2 \times 47 \times 67 \times 113 \times 163 \times 239 \times 283 \times 653 \times 761 \times 1429 \times 1523 \times 4951 \times 20771 \times 40487 \times 91127 \times 123397 \times 148531 \times 1974353 \times 15491591 \times 30469139 \times 53471161 \times 278848639 \times 1645333507 \times 6692367337 \times 188748146801$

Table 1: The largest known Wieferich numbers in bases $2 \leq a \leq 25$.