WIEFERICH PRIMES

KEITH CONRAD

1. Introduction

Fermat's little theorem says that for prime p and a not divisible by p, $a^{p-1} \equiv 1 \bmod p$. We are going to consider the strengthened congruence

$$a^{p-1} \equiv 1 \bmod p^2. \tag{1.1}$$

Unlike the congruence in Fermat's little theorem, (1.1) usually does *not* hold. When (1.1) holds, p is called a *Wieferich prime to base a.*

In Section 2 we'll present examples and heuristics related to Wieferich primes. The next three sections give different settings where Wieferich primes appear: Fermat's last theorem in Section 3 (this is how Wieferich's name got associated to (1.1)), Catalan's conjecture in Section 4, and Fermat and Mersenne numbers in Section 5.[1]

2. Numerical data

The only known Wieferich primes to base 2 and 1093 and 3511: they are prime and

$$2^{1092} \equiv 1 \bmod 1093^2, \quad 2^{3510} \equiv 1 \bmod 3511^2.$$

These were found by Meissner [5] in 1913 and Beegner [1] in 1922. The known Wieferich primes to a squarefree base $a \leq 10$ are in Table 1. Searches for Wieferich primes have been carried out for $p < 1.25 \cdot 10^{15}$ when $a = 2$ [4] and for $p < 2^{32} \approx 10^{9.63}$ when $3 \leq a < 100$ [7]. Wieferich primes to a fixed base appear to be quite rare numerically, and for some bases none are known, *e.g.*, no Wieferich primes to base 21 or 29 have been found.

a	Known Wieferich primes to base a
2	1093, 3511
3	11, 1006003
5	2, 20771, 40487, 53471161, 1645333507, 6692367337, 188748146801
6	66161, 534851, 3152573
7	5, 491531
10	3, 487, 56598313

Table 1. Known Wieferich primes for squarefree bases up to 10

The difficulty in (1.1) is finding p when we fix a, not finding a when we fix p: for each prime p, there are $p-1$ values of a mod p^2 making $a^{p-1} \equiv 1 \bmod p^2$ (explicitly, the solutions are $a = b^p \bmod p^2$ for $1 \leq b \leq p-1$). Table 2 lists squarefree Wieferich bases for small primes.

[1] Another setting for Wieferich primes, accessible to those who know algebraic number theory, is in the calculation of the ring of integers of $\mathbf{Q}(\sqrt[n]{a})$ when $x^n - a$ is irreducible: see Theorem 5.3 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf.

p	Squarefree bases a with Wieferich prime p	As congruence mod p^2
2	5, 13, 17, 21, 29, 33, 37, 41, 53, 57, 61, 65	$a \equiv 1 \bmod 4$
3	10, 17, 19, 26, 35, 37, 46, 53, 55, 62, 71, 73	$a \equiv \pm 1 \bmod 9$
5	7, 26, 43, 51, 57, 74, 82, 93, 101, 107, 118	$a \equiv \pm 1, \pm 7 \bmod 25$
7	19, 30, 31, 67, 79, 97, 129, 146, 165, 166	$a \equiv \pm 1, \pm 18, \pm 19 \bmod 49$

Table 2. Squarefree bases a having small Wieferich primes p

There is a probabilistic heuristic that both (i) supports the infrequent appearance of Wieferich primes to a fixed base and (ii) suggests there are infinitely many Wieferich primes to each base. When $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$, so $a^{p-1} \equiv 1 + pb \bmod p^2$, where $0 \leq b \leq p-1$. Here is the heuristic: *assume b takes each of the p values $0, 1, \ldots, p-1$ with equal probability.* Since $b = 0$ corresponds to p being a Wieferich prime to base a, the "probability" some p not dividing a is a Wieferich prime to base a is $1/p$. Therefore the expected number of primes $p \leq x$ that are Wieferich primes to base a is found by adding up the "probabilities". This is $\sum_{p \leq x} 1/p$, which grows *very* slowly: it is asymptotic to $\log\log x$. Since $\log\log(2^{32}) \approx 3.1$, it is no surprise so few Wieferich primes for $p < 2^{32}$ are known to any particular base. (Strictly speaking, $\sum_{p \leq x} 1/p$ from the heuristic should not include p dividing a, making the sum even smaller. The effect is negligible.)

3. Case I of Fermat's last theorem

Fermat's last theorem says that $x^n + y^n = z^n$ has no solution in positive integers x, y, and z when $n \geq 3$. It was proposed by Fermat in the 1600s and proved by Wiles in the 1990s. Before its proof in general, Fermat's last theorem had been settled for many individual exponents.

Each $n \geq 3$ is divisible by an odd prime or 4. If there is no solution (x, y, z) in $\mathbf{Z}^+$ when the exponent is n then there is also no solution when the exponent is a multiple of n. So to prove Fermat's last theorem, it suffices to assume n is 4 or an odd prime. Fermat handled the case $n = 4$. Before the work of Wiles, progress on Fermat's last theorem for odd prime exponents[2] p was divided into two cases:

- Case I: show no solutions where $p \nmid xyz$,
- Case II: show no solutions where $p \mid xyz$.

Wieferich [12] proved the following result about Case I in 1909.

Theorem 3.1. *If Case I for exponent p has a counterexample, then $2^{p-1} \equiv 1 \bmod p^2$.*

That is, if $x^p + y^p = z^p$ in $\mathbf{Z}^+$ where $p \nmid xyz$ then $2^{p-1} \equiv 1 \bmod p^2$. Note this says nothing about counterexamples to Fermat's last theorem in Case II.

The following year, it probably came as a surprise when Mirimanoff [6] proved the same theorem with another base.

Theorem 3.2. *If Case I for exponent p has a counterexample, then $3^{p-1} \equiv 1 \bmod p^2$.*

Wieferich primes to a single base already seem to be quite rare, so a prime being Wieferich to bases 2 and 3 together looks extraordinarily unlikely, and heuristics like those in Section

[2] The proof by Wiles has $p \geq 5$ for technical reasons: see https://math.stackexchange.com/questions/4464666/. The case $p = 3$ was handled by Euler in the 1700s.

2 suggest it should happen only finitely many times.[3] By the time Wiles announced a proof of Fermat's last theorem in 1993, an analogue of Theorem 3.1 had been proved with 2 replaced by each prime up through 89. Nowadays this use of Wieferich primes is only of historical interest, since the proof of Fermat's last theorem makes no use of Wieferich primes or the Case I/Case II distinction.

4. Catalan's conjecture

A perfect power in $\mathbf{Z}^+$ is a number of the form a^m where $a \in \mathbf{Z}^+$ and $m \geq 2$. The sequence of perfect powers starts out as

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, \dots$$

and Catalan [2] conjectured in 1844 that the only consecutive perfect powers are $8 = 2^3$ and $9 = 3^2$. That is, the only solution to $x^m - y^n = 1$ in $\mathbf{Z}^+$ with $m, n \geq 2$ are $(x, y, m, n) = (3, 2, 2, 3)$. This was proved by Mihailescu in 2004.

As with Fermat's last theorem, to prove Catalan's conjecture it suffices to assume m and n are prime, and they are necessarily distinct. We'll write the equation as $x^p - y^q = 1$. The cases where p or q is 2 were completely settled by the 1960s. (Euler had treated the exponent pair with a solution, $p = 2$ and $q = 3$, in 1738.) Therefore p and q can be taken as odd primes, which allows us to regard the equation as being symmetric in p and q by aiming to prove there is no solution in *nonzero* integers rather than only in positive integers: if $x^q - y^p = 1$ then $(-y)^p - (-x)^q = 1$.

A breakthrough in work on Catalan's conjecture was Mihailescu's proof that if $x^p - y^q = 1$ for nonzero integers x and y and odd primes p and q, then $q^{p-1} \equiv 1 \bmod p^2$, so by symmetry $p^{q-1} \equiv 1 \bmod q^2$. Such primes are called a *Wieferich pair*. (This constraint on p and q had been proved earlier under additional assumptions, which Mihailescu removed.) Two examples of Wieferich pairs of odd primes are $(p, q) = (3, 1006003)$ and $(p, q) = (5, 1645333507)$. An overview of the proof of Catalan's conjecture in Schoof's book [10, pp. 3–5] describes how the Wieferich pair property is used in the proof.

5. Squarefree Fermat and Mersenne numbers and a generalization

A *Fermat number* is an integer of the form $F_n = 2^{2^n} + 1$, where $n \geq 0$. The first six Fermat numbers are

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \quad F_5 = 4294967297.$$

Fermat checked that F_n is prime for $n = 0, 1, 2, 3, 4$ and he conjectured F_n is prime for all n. This was disproved when Euler [?] showed $F_5 = 641 \cdot 6700417$, and in fact no further prime Fermat numbers have ever been found. We don't expect any Fermat number F_n with $n \geq 5$ to be prime, but we do expect them all to be squarefree. Every Fermat number that has been factored completely is squarefree, and the following theorem puts a Wieferich restriction on repeated prime factors of a Fermat number.

Theorem 5.1. *If F_n is divisible by p^2 where p is prime then $2^{p-1} \equiv 1 \bmod p^2$.*

Proof. This argument is a simplification of of the original proof by Warren and Bray [?].

If p is a prime factor of F_n then $p \neq 2$ and we will show $F_n \mid (2^{p-1} - 1)$.

The condition $p \mid F_n$, written as $p \mid (2^{2^n} + 1)$, is the same as $2^{2^n} \equiv -1 \bmod p$, and squaring both sides of the congruence gives us $2^{2^{n+1}} \equiv 1 \bmod p$. This implies the order of

[3] See https://math.stackexchange.com/questions/2893111.

2 mod p is a factor of 2^{n+1} but not a factor of 2^n, so the order of 2 mod p is exactly 2^{n+1}. Therefore $2^{n+1} \mid (p-1)$. Since $a \mid b \Rightarrow (2^a-1) \mid (2^b-1)$ we have

$$2^{n+1} \mid (p-1) \Longrightarrow 2^{2^{n+1}}-1 \mid 2^{p-1}-1.$$

Then the factorization $2^{2^{n+1}}-1 = (2^{2^n})^2-1 = (2^{2^n}-1)(2^{2^n}+1)$ shows $F_n \mid (2^{p-1}-1)$. Writing that as $2^{p-1} \equiv 1 \bmod F_n$, when $p^2 \mid F_n$ we get $2^{p-1} \equiv 1 \bmod p^2$. □

The only known Wieferich primes to base 2 are 1093 and 3511, and neither is a prime factor of an F_n even once: if F_n is divisible by a prime p greater than 1000 than $n \geq 4$, and $p \mid F_n$ implies $2^{n+1} \mid (p-1)$, so $p \equiv 1 \bmod 2^{n+1}$, and thus $p \equiv 1 \bmod 8$, but $1093 \equiv 5 \bmod 8$ and $3511 \equiv 7 \bmod 8$.

A *Mersenne number* is a number of the form 2^n-1. These numbers can have square factors bigger than 1, such as

$$2^6-1 = 63 = 3^2\cdot 7, \quad 2^{20}-1 = 5^2\cdot 3\cdot 11\cdot 31\cdot 41, \quad 2^{21}-1 = 7^2\cdot 127\cdot 337.$$

It is conjectured that 2^q-1 is squarefree for all primes q. The next theorem suggests counterexamples are rare: a repeated prime factor of 2^q-1 is a Wieferich prime to base 2.

Theorem 5.2. *For prime numbers p and q, the following conditions are equivalent and each implies $q \mid (p-1)$:*

(i) $p^2 \mid (2^q-1)$,

(ii) $p \mid (2^q-1)$ *and* $2^{p-1} \equiv 1 \bmod p^2$.

Proof. Neither condition holds when $q = 2$. Now let q be an odd prime.

(i) ⇒ (ii): This argument is a simplification of of the original proof by Warren and Bray [11].[4] Trivially $\boxed{p \mid (2^q-1)}$. Since 2^q-1 is odd, p is odd.

Write $p \mid (2^q-1)$ as $2^q \equiv 1 \bmod p$, so the order of 2 mod p is q since q is prime and $2 \not\equiv 1 \bmod q$. Every nonzero number mod p has order dividing $p-1$, so $q \mid (p-1)$. In $\mathbf{Z}^+$, if $a \mid b$ then $(m^a-1) \mid (m^b-1)$ for $m \geq 2$, so $(2^q-1) \mid (2^{p-1}-1)$. Since p^2 is a factor 2^q-1, $\boxed{p^2 \mid (2^{p-1}-1)}$.

(ii) ⇒ (i): This argument is from [8, p. 342]. As in (i), from $2^q \equiv 1 \bmod p$ we get $q \mid (p-1)$. Write $2^q = 1+bp$ and $p-1 = qr$ for $b, r \in \mathbf{Z}^+$. Then $2^{p-1} = (1+bp)^r \equiv 1+rbp \bmod p^2$, so $p \mid rb$. Since $r < p$, $p \mid b$. Thus $\boxed{2^q \equiv 1 \bmod p^2}$. □

Remark 5.3. Neither 1093 nor 3511, the only known Wieferich primes to base 2, divide 2^q-1 for a prime q even once: when proving (i) ⇒ (ii) we showed that if $p \mid (2^q-1)$ for an odd prime p then $q \mid (p-1)$, and that limits the choices for q. The prime factors of $1093-1$ are 2, 3, 7, and 13, and the prime factors of $3511-1$ are 2, 3, 5, and 13, and for no such prime q is 2^q-1 divisible by 1093 or 3511.

Corollary 5.4. *If 2^q-1 is not squarefree for infinitely many primes q then there are infinitely many Wieferich primes to base* 2.

Proof. For $a \geq 2$ and positive integers m and n, $(a^m-1, a^n-1) = a^{(m,n)}-1$, so the numbers 2^q-1 for different primes q are all pairwise relatively prime. Therefore different numbers 2^q-1 have no common prime factors. The previous theorem tell us each 2^q-1 that is not squarefree has a prime factor that is Wieferich to base 2, so if 2^q-1 is not squarefree for

[4] The paper [11] is a rare case of a published paper in pure math where the author names are not listed alphabetically.

infinitely many q then their repeated prime factors will be a list of infinitely many Wieferich primes to base 2.[5] □

We'll now extend the reasoning in the proof of Theorem 5.2 to numbers of the form

$$\frac{a^q - 1}{a - 1} = 1 + a + a^2 + \cdots + a^{q-1}$$

for $a \geq 2$ and prime q. When $a = 2$ this number is $2^q - 1$. For many $a > 2$, $(a^q - 1)/(a - 1)$ can have a repeated prime factor. See Table 3. For instance, $(3^5 - 1)/(3 - 1)$ and $(9^5 - 1)/(9 - 1)$ are both divisible by 11^2, while $(51^5 - 1)/(51 - 1)$ is divisible by 41^2.

a	3	9	18	22	27	30	44	51	53	53	56	58
q	5	5	3	3	5	3	19	5	23	29	19	5
p	11	11	7	13	11	7	229	41	47	59	647	131

Table 3. Repeated prime factor p of $(a^q - 1)/(a - 1)$.

First we'll determine when $(a^q - 1)/(a - 1)$ can have q as a repeated prime factor.

Theorem 5.5. *If $a \geq 2$ and q is a prime, then $q^2 \nmid (a^q - 1)/(a - 1)$ unless $q = 2$ and $a \equiv 3 \bmod 4$.*

Proof. If $q = 2$ then $(a^q - 1)/(a - 1) = a + 1$, which is divisible by 4 if and only if $a \equiv 3 \bmod 4$.

Now take $q \neq 2$. We will show that q divides $(a^q - 1)/(a - 1)$ at most once.

Assume $q \mid (a^q - 1)/(a - 1)$, so $q \mid (a^q - 1)$. Then $a^q \equiv 1 \bmod q$, so $a \equiv 1 \bmod q$. Let q^e be the highest power of q dividing $a - 1$, so $a - 1 = q^e b$ where $e \geq 1$ and $q \nmid b$. Then $a = 1 + q^e b$. Raising both sides to the qth power,

$$a^q = (1 + q^e b)^q = 1 + \sum_{i=1}^{q} \binom{q}{i} (q^e b)^i = 1 + q^{e+1} b + \sum_{i=2}^{q} \binom{q}{i} q^{ie} b^i,$$

so

$$a^q - 1 = q^{e+1} b + \sum_{i=2}^{q} \binom{q}{i} q^{ie} b^i.$$

All terms in the summation over i are more highly divisible by q then q^{e+1}:

- For $i \geq 3$, $ie \geq 3e > e + 1$ since $e \geq 1$.
- For $i = 2$, $\binom{q}{2} q^{2e} = q^{2e+1}(q - 1)/2$ and $2e + 1 > e + 1$ (the factor $(q - 1)/2$ is an integer since q is odd).

Therefore the highest power of q in $a^q - 1$ is q^{e+1}. Since the highest power of q in $a - 1$ is q^e, the highest power of q in the ratio $(a^q - 1)/(a - 1)$ is $q^{e+1-e} = q$. □

Lemma 5.6. *For $a \geq 2$ and a prime q, $\gcd(a - 1, (a^q - 1)/(a - 1))$ is 1 or q.*

Proof. Let d be a common divisor of $a - 1$ and $(a^q - 1)/(a - 1)$. From $d \mid (a - 1)$, we have $a \equiv 1 \bmod d$. Then $(a^q - 1)/(a - 1) = 1 + a + \cdots + a^{q-1} \equiv q \bmod d$, so $d \mid q$. By primality of q, d is 1 or q. □

Here is the generalization of Theorem 5.2 allowing bases other than 2. It is similar to [3, Theorem 18], which is about $a^q - 1$ rather than $(a^q - 1)/(a - 1)$.

[5] This corollary, in its contrapositive form, was first proved by Rotkiewicz [9, Théorème 2].

Theorem 5.7. *Let $a \geq 2$. For distinct primes p and q, the following conditions are equivalent*[6] *and each implies $q \mid (p-1)$:*

(*i*) $p^2 \mid (a^q - 1)/(a-1)$,

(*ii*) $p \mid (a^q - 1)/(a-1)$ *and* $a^{p-1} \equiv 1 \bmod p^2$.

This theorem is consistent with Table 3, *e.g.*, $11^2 \mid (3^5 - 1)/(3-1)$ and 11 is a Wieferich prime to base 3.

Proof. (i) ⇒ (ii): Trivially $\boxed{p \mid (a^q - 1)/(a-1)}$, so $a^q \equiv 1 \bmod p$. We have $p \nmid (a-1)$ since Lemma 5.6 tells us the only possible common factors of $a - 1$ and $(a^q - 1)/(a-1)$ are 1 and q. Therefore $a \not\equiv 1 \bmod p$, so $a \bmod p$ has order q. Thus $q \mid (p-1)$, so $(a^q - 1) \mid (a^{p-1} - 1)$. Since $p^2 \mid (a^q - 1)$ by condition (i), $p^2 \mid (a^{p-1} - 1)$. Thus $\boxed{a^{p-1} \equiv 1 \bmod p^2}$.

(ii) ⇒ (i): From $p \mid (a^q - 1)/(a-1)$, $a \bmod p$ has order q as in the proof of (i) ⇒ (ii), so $q \mid (p-1)$. Write $a^q = 1 + bp$ and $p - 1 = qr$ for $b, r \in \mathbf{Z}^+$. Then $a^{p-1} = (1+bp)^r \equiv 1 + rbp \bmod p^2$, so $p \mid rb$. Since $r < p$, $p \mid b$. Thus $a^q \equiv 1 \bmod p^2$, so $p^2 \mid (a^q - 1)$. Since $p \nmid (a-1)$ by Lemma 5.6, $p^2 \mid (a^q - 1)/(a-1)$. □

By Theorems 5.5 and 5.7, for $a \geq 2$ and an odd prime q, a repeated prime factor p of $(a^q - 1)/(a-1)$ has to be a Wieferich prime to base a and $p \equiv 1 \bmod q$.

References

[1] N. G. W. H. Beegner, "On a new case of the congruence $2^{p-1} = 1 \pmod{p^2}$," *Messenger of Mathematics* **51** (1922), 149–150. URL https://archive.org/details/messengerofmathe5051cambuoft/page/148/mode/2up

[2] E. Catalan, "Note extraite dune lettre adressée à l'éditeur, *J. Reine Angew. Mathematik* **27** (1844), 192. URL https://eudml.org/doc/147217.

[3] J. Klaška, "Jakóbczyk's Hypothesis on Mersenne Numbers and Generalizations of Skula's Theorem," *J. Integer Sequences* **26** (2023), Article 23.3.8 (21 pages). URL https://cs.uwaterloo.ca/journals/JIS/VOL26/Klaska/klaska6.pdf.

[4] J. Knauer and J. Richstein, "The Continuing Search for Wieferich Primes," *Math. Comp.* **74** (2005), 1559–1563.

[5] W. Meissner, "Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$," *Sitzungsber. der Königl. Preuss. Akad. der Wiss. Berlin* **35** (1913), 663–667. URL https://oeis.org/A001917/a001917.pdf.

[6] D. Mirimanoff, "Sur le dernier théorème de Fermat," *Comptes rendus hebdomadaires des séances de l'Académie des Sciences* **150** (1910), 204–206. URL https://gallica.bnf.fr/ark:/12148/bpt6k6294283c/f12.item.

[7] P. Montgomery, "New Solutions of $a^p - 1 \equiv 1 \bmod p^2$, *Math. Comp.* **61** (1993), 361–363.

[8] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, 1996.

[9] A. Rotkiewicz, "Sur les nombres de Mersenne depourves de diviseurs carres et sur les nombres naturels n, tels que $n^2 \mid (2^n - 2)$," *Matematički Vesnik* **2** (1965), 78–80. URL https://eudml.org/doc/259515.

[10] R. Schoof, *Catalan's Conjecture*, Springer-Verlag, 2009.

[11] L. J. Warren and H. G. Bray, "On the square-freeness of Fermat and Mersenne numbers," *Pacific J. Math.* **22** (1967), 563–564. URL https://msp.org/pjm/1967/22-3/pjm-v22-n3-p15-p.pdf.

[12] A. Wieferich, "Zum letzten Fermatschen Theorem," *J. Reine Angew. Mathematik* **136** (1909), 293–302. URL https://eudml.org/doc/149315.

[6] When $p = q > 2$, conditions (i) and (ii) in Theorem 5.7 are not equivalent: (i) doesn't happen by Theorem 5.5, while (ii) happens when $a \equiv 1 \bmod p^2$.