Journal of Integer Sequences, Vol. 14 (2011),
Article 11.9.2

A Wieferich Prime Search up to 6.7×10^{15}

François G. Dorais
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109
USA
dorais@umich.edu

Dominic Klyve
Department of Mathematics
Central Washington University
400 E. University Way
Ellensburg, WA 98926
USA
klyved@cwu.EDU

Abstract

A *Wieferich prime* is a prime p such that $2^{p-1} \equiv 1 \pmod{p^2}$. Despite several intensive searches, only two Wieferich primes are known: $p = 1093$ and $p = 3511$. This paper describes a new search algorithm for Wieferich primes using double-precision Montgomery arithmetic and a memoryless sieve, which runs significantly faster than previously published algorithms, allowing us to report that there are no other Wieferich primes $p < 6.7 \times 10^{15}$. Furthermore, our method allowed for the efficent collection of statistical data on Fermat quotients, leading to a strong empirical confirmation of a conjecture of Crandall, Dilcher, and Pomerance. Our methods proved flexible enough to search for new solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ for other small values of a, and to extend the search for Fibonacci-Wieferich primes. We conclude, among other things, that there are no Fibonacci-Wieferich primes less than $p < 9.7 \times 10^{14}$.

1 Introduction

During the 19th and 20th centuries, several different classes of prime numbers were identified and studied because of their relationship to Fermat's Last Theorem (FLT). Most notable among these are Fibonacci-Wieferich primes, Wilson primes, and Wieferich primes. For example, if the first case of Fermat's Last Theorem holds for a prime p, then p must be a Fibonacci-Wieferich prime [22]. Similarly, any exponent p which permits a solution to the FLT equation $x^p + y^p = z^p$, while being coprime to x, y, and z, is a Wieferich prime. The relationship between Wilson primes and FLT is more complex; see [13]. Although it no longer makes sense to search for a solution to the equation in Fermat's Last Theorem, the questions inspired by these classes of primes still remain, and we can now turn our attention to the study of these primes for their own sake.

Of the three above-mentioned classes of primes, Wieferich primes are perhaps the simplest to define. Define the *Fermat quotient* of 2 mod p to be

$$q_2(p) = \frac{a^{p-1} - 1}{p}.$$

It is known from Fermat's little theorem that for any prime p, $2^{p-1} - 1$ is always divisible by p, and therefore $q_2(p)$ is always an integer. If $q_2(p)$ vanishes modulo p (that is, if $2^{p-1} - 1$ is divisible by p^2), p is said to be *Wieferich*. These primes were first studied by Arthur Wieferich, who in 1909 related them to Fermat's Last Theorem [23].

Although Wieferich himself found no example of such a prime, W. Meissner [15] in 1913 found that 1093 was Wieferich, and in 1922 N. G. W. H. Beeger [1] showed that 3511 was Wieferich, also. Since 1922, however, no new examples have been found.

2 Previous Searches

Exhaustive searches for new Wieferich primes began with Beeger, and continue today. The last eighty years have seen first computers, then new algorithmic techniques, and finally distributed computing applied to the search for Wieferich primes. Because we have been unable to find a comprehensive summary of the history of these searches in the literature, one has been compiled in Table 1.

The most recent of these searches, that of Knauer and Richstein, used a distributed approach, and incorporated more than 250 client computers during the course of their search, but in order to include as many computers as possible they were unable to use many of the standard optimizations sometimes used in a search for Wieferich primes. Notably, their code assumed only a 32-bit processor on client machines.

3 Improved Search Methods

Our search employed a number of new algorithmic enhancements not used in previous searches. For computations modulo p^2, we used a new "double-precision" variant Montgomery arithmetic. Finally, we used a new type of "memoryless" sieve to quickly eliminate composites.

Table 1: Previous Wieferich prime searches

Search bound	Author	Year
16000	Beeger [2]	1940
50000	Fröberg [7]	unknown
100000	Kravitz [11]	1960
200183	Pearson [18]	1964
500000	Riesel [20]	1964
3×10^7	Fröberg [8]	1968
3×10^9	Brillhart, Tonascia, and Weinberger [3]	1971
6×10^9	Lehmer [12]	1981
6.1×10^{10}	Clark	c. 1996
4×10^{12}	Crandall, Dilcher, and Pomerance [5]	1997
4.6×10^{13}	Brown and McIntosh [4]	2001
2×10^{14}	Crump [6]	2002
1.25×10^{15}	Knauer and Richstein [10]	2005

3.1 Faster Arithmetic

Our first task was to reduce the time for computing Fermat quotients to about 1μs (for the machines we had at hand). This was accomplished by using *double-precision Montgomery arithmetic*.

The idea behind (single-precision) Montgomery arithmetic modulo p is that instead of the ring $\mathbb{Z}/p\mathbb{Z}$, we can choose a parameter r coprime to p, and use the isomorphic ring

$$\mathbb{M}(p,r) = (\{0,1,\ldots,p-1\}, 0, e, \ominus, \oplus, \otimes)$$

with the usual negation $\ominus x = (-x) \bmod p$, addition $x \oplus y = (x+y) \bmod p$ and additive identity 0, but where multiplication is defined by $x \otimes y = xyr^{-1} \bmod p$ and, consequently, the multiplicative identity is defined by $e = r \bmod p$.

The advantage of this is that, by choosing r wisely, it is possible to arrange that the product $x \otimes y$ can always be computed without resorting to division by p. When the modulus p is odd, one such choice is $r = 2^n > p$, which corresponds to the original idea of P. L. Montgomery [16]. For double-precision Montgomery arithmetic, we use the same choice for r, but the modulus is now p^2. We also use a *double-precision representation* for the elements of $\mathbb{M}(p^2, 2^n)$, which consists in representing $x \in \{0,1,\ldots,p^2-1\}$ as an ordered pair (x_0, x_1) where $x = x_0 + px_1$ and $0 \le x_0, x_1 \le p-1$. Addition and subtraction of such pairs is straightforward. Multiplication is not so obvious, but it can still be done using without resorting to division.

The following result shows how to multiply two double-precision elements of $\mathbb{M}(p^2, 2^n)$ using only multiplication, addition, and subtraction of nonnegative n-bit integers.

Lemma 1. *Given two odd numbers p, q such that $0 < p, q < 2^n$ and $pq \equiv 1 \pmod{2^n}$ as parameters. The product of two double-precision elements of $\mathbb{M}(p^2, 2^n)$ can be computed using at most 7 multiplications and 8 additions/subtractions of nonnegative n-bit integers.*

The square of a double-precision element of $\mathbb{M}(p^2, 2^n)$ can be computed using at most 6 multiplications and 8 additions/subtractions of nonnegative n-bit integers.

Proof. Let $x_0 + x_1 p$ and $y_0 + y_1 p$ be double-precision elements of $\mathbb{M}(p^2, 2^n)$. Thus $0 \leq x_0, x_1, y_0, y_1 \leq p - 1$.

First compute:

$$\begin{aligned} t_0 + t_1 2^n &:= x_0 y_0, && \text{where } 0 \leq t_0 \leq 2^n - 1; \\ u_0 + u_1 2^n &:= q t_0, && \text{where } 0 \leq u_0 \leq 2^n - 1; \\ v_0 + v_1 2^n &:= p u_0, && \text{where } 0 \leq v_0 \leq 2^n - 1. \end{aligned}$$

This requires 3 multiplications. Note that $t_0 = v_0$ since $pq \equiv 1 \pmod{2^n}$, and so

$$x_0 y_0 - p u_0 = 2^n (t_1 - v_1). \tag{1}$$

Furthermore, note that $0 \leq t_1, v_1 \leq p - 1$.

Next compute:

$$\begin{aligned} t_0' + t_1' 2^n &:= x_0 y_1 + x_1 y_0 + u_0, && \text{where } 0 \leq t_0' \leq 2^n - 1; \\ u_0' + u_1' 2^n &:= q t_0', && \text{where } 0 \leq u_0' \leq 2^n - 1; \\ v_0' + v_1' 2^n &:= p u_0', && \text{where } 0 \leq v_0' \leq 2^n - 1. \end{aligned}$$

This requires 4 multiplications and 3 additions (with carry). Again, $t_0' = v_0'$ since $pq \equiv 1 \pmod{2^n}$, and so

$$(x_0 y_1 + x_1 y_0 + u_0) - p u_0' = 2^n (t_1' - v_1'). \tag{2}$$

Furthermore, note that $0 \leq t_1' \leq 2p - 1$ and $0 \leq v_1' \leq p - 1$.

Combining (1) and (2), we find that

$$\begin{aligned} (x_0 + x_1 p)(y_0 + y_1 p) &\equiv x_0 y_0 + (x_0 y_1 + x_1 y_0) p && \pmod{p^2} \\ &\equiv 2^n (t_1 - v_1) + 2^n (t_1' - v_1') p \end{aligned}$$

Since $-p < t_1 - v_1 < p$ and $-p < t_1' - v_1' < 2p$, with at most 5 more additions/subtractions, we can find z_0, z_1 such that

$$(x_0 + x_1 p)(y_0 + y_1 p) \equiv 2^n (z_0 + z_1 p) \pmod{p}$$

and $0 \leq z_0, z_1 \leq p - 1$.

In total, this process requires at most 7 multiplications and 8 additions (possibly with carry). For squaring, we have $x_0 y_1 = x_1 y_0$, so we can save 1 multiplication by computing this product only once. □

For comparison, single-precision Montgomery multiplication in $\mathbb{M}(p^2, 2^{2n})$ requires 3 multiplications and up to 2 additions/subtractions of nonnegative $2n$-bit integers. For small n, multiplication of $2n$-bit integers takes at least 3 times as long as multiplication of n-bit integers, and addition of $2n$-bit integers takes 2 times as long as addition of n-bit integers. Since

multiplication is usually much slower than addition, double-precision Montgomery squaring results in approximately 30% improvement over single-precision Montgomery squaring.

To test whether p is a Wieferich prime, we need to check whether $2^{p-1} \equiv 1 \pmod{p^2}$ or, equivalently, whether $2^{(p-1)/2} \equiv \pm 1 \pmod{p^2}$, as suggested by Crandall, et al. [5]. Our implementation used a standard binary powering ladder to accomplish this.

Theorem 2. *Given a n-bit prime number p ($n \geq 4$), we can test whether $2^{(p-1)/2} \equiv \pm 1 \pmod{p^2}$ using at most $6n + 2\lg(n) - 10$ multiplications and $12n + \lg(n) - 13$ additions/subtractions of nonnegative n-bit integers.*

Proof. We do the computations using double-precision Montgomery arithmetic in $\mathbb{M}(p^2, 2^n)$. To get started, we need to compute the auxiliary parameter q such that $pq \equiv 1 \pmod{2^n}$. This can be done in many ways; our implementation used a Newton iteration that requires $2\lg(n) - 4$ multiplications and $\lg(n) - 2$ subtractions (of $\leq n/2$-bit integers).

To get started with the binary powering ladder, we need to compute the double-precision representation of the multiplicative unit 2^n. Since p has n-bits, this can be done with only 1 subtraction.

Finally, the (left-to-right) binary powering ladder with the $(n-1)$-bit exponent $(p-1)/2$ requires $n-1$ squarings and at most $n-1$ doublings. Each squaring uses 6 multiplications and 8 additions/subtractions and each doubling uses up to 4 additions/subtractions. In total, this gives $6n-6$ multiplications and up to $12n-12$ additions/subtractions. □

3.2 Faster Sieving

Previous searches of Wieferich primes employed a segmented sieve of Eratosthenes to completely sieve an interval for primes before testing those primes for being Wieferich. Using the testing methods described above, we found that testing a single number for being Wieferich was quite fast (about 1μs), and that therefore much of our computing time would be spent sieving.

For traditional sieves, most of the sieving time is spent sieving small primes. Indeed, sieving an interval of length ℓ for the prime p requires about ℓ/p memory write operations. So, for example, it takes about as much time to sieve an interval for the six primes $2, 3, 5, 7, 11, 13$ as it takes to sieve the same interval for the primes $17, 19, 23, \ldots, 82139$. With this in mind, we began to look for better ways to sieve out multiples of very small primes. Since memory operations are usually much more costly than elementary arithmetic operations, we looked for sieves that require little or no memory.

3.2.1 The Magic Sieve

Sieving for a few small primes $p_1, \ldots, p_k$ amounts to enumerating the elements of the unit group modulo $M = p_1 \cdots p_k$. Our first idea was to make better use of the structure of the unit group $(\mathbb{Z}/M\mathbb{Z})^*$. After a few experiments, we found a special number that we ended up calling the *Magic Modulus*:

$$M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 47 \cdot 53 \cdot 59 \cdot 83 = 319514496269430.$$

This number was chosen because of the simple structure of the unit group mod M. Indeed, the group $(\mathbb{Z}/M\mathbb{Z})^*$ has a large cyclic factor of order 6569843280, generated by 31, and a second factor of order $8192 = 2^{13}$. The integers in the interval $[kM + 1, (k + 1)M]$ that are coprime to M can be listed in a rectangular array

$$x_{ij} = kM + (a_i \cdot 31^j \bmod M) \qquad (0 \le i < 8192, 0 \le j < 6569843280)$$

where the numbers a_i are chosen representatives of the cosets of the cyclic group $\langle 31 \rangle$ in $(\mathbb{Z}/M\mathbb{Z})^*$. Given a coset representative a_i, listing the integers x_{ij} $(0 \le j < 6569843280)$ only involves multiplying by 31, which can be accomplished by five doubling and one subtraction operation modulo M and essentially no memory access.

While the Magic Sieve is somewhat less efficient than the Spin Sieve (described below), it has the advantage that it is easy to implement and requires essentially no memory storage. In fact, our implementation used only 104 bytes of data to be stored in memory. The performance of the Magic Sieve was adequate for our purposes — we only had to compute Fermat quotients for 16.8% of the integers in an interval.

3.2.2 The Spin Sieve

For optimal results, a sieve should use the first few primes $2, 3, \ldots, p_k$. A weakness of the Magic Sieve is that it is sometimes preferable to omit a few small primes so that the unit group has a large cyclic factor. The Spin Sieve does away with the reliance on the structure of the unit group, while, like the Magic Sieve, requiring very little memory storage.

The Spin Sieve was inspired by Pritchard's Wheel Sieve [19]. A similar idea was independently discovered by Sorenson [21], from whom we borrowed some implementation ideas.

The idea behind the Spin Sieve is to find a simple bijection between the set of k-tuples

$$T_k = \{1\} \times \{1, 2\} \times \{1, 2, 3, 4\} \times \cdots \times \{1, \ldots, p_k - 1\}$$

and the set

$$A_k = \{x : 0 < x < M_k, (x, M_k) = 1\}$$

where $M_k = 2 \cdot 3 \cdot 5 \cdots p_k$. This bijection $s_k : T_k \to A_k$ is defined recursively by $s_1(1) = 1$, and

$$s_k(t_1, \ldots, t_k) = s_{k-1}(t_1, \ldots, t_{k-1}) + M_{k-1}((r_k(t_1, \ldots, t_{k-1}) + t_k) \bmod p_k)$$

where $r_k : T_{k-1} \to \{0, \ldots, p_k - 1\}$ satisfies

$$s_{k-1}(t_1, \ldots, t_{k-1}) + M_{k-1} r_k(t_1, \ldots, t_{k-1}) \equiv 0 \pmod{p_k}.$$

While the definition of s_k is somewhat unwieldy, it is rather simple to compute the values of s_k in succession with the lexicographic ordering of T_k. This "spinning" operation is the origin of the name of the sieve.

There are many ways to use the values of s_k. In our implementation, for each value of s_{10}, we further sieve (in the traditional way) the arithmetic progression $s_{10}(t_1, \ldots, t_{10}) \pmod{M_{10}}$ for the primes $31, \ldots, 65521$ and compute the Fermat quotients of the remaining values. On average, less than 15.8% of numbers survive the Spin Sieve, then about 32% of the remaining numbers survive the second sieve, so we only compute Fermat quotients for approximately 5% of the numbers in a given interval.

4 Other applications

4.1 Base-a Wieferich Primes

The definition of Wieferich prime uses base 2 for historical reasons, but mathematically there is no particular reason why we can't consider other bases as well. In an analogy to the base-2 case, define the *Fermat coefficient base-a* of p to be

$$q_a(p) = \frac{a^{p-1} - 1}{p}.$$

Primes for which $q_a(p)$ vanishes modulo p are sometimes called *base-a* Wieferich primes. Using the methods described above, we searched for solutions to this equation of $a = 3, 5$, and 7. For each of these bases, we looked for solutions up to about 9.7×10^{14} (or, more precisely, solutions not greater than $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29) \cdot 1.5 \times 10^5$). The previous record for searches with $a = 3$ and $a = 5$ was held by Keller and Richstein [9], who searched to 10^{11}. The previous record for $a = 7$ belonged to Montgomery [17], who searched to 2^{32}. We found no new base-a Wieferich primes for any of these bases, and therefore there are still only two known solutions for each base $2, 3$, and 7, and six solutions for base 5. We do not know whether there is any significance to larger number of base-5 solutions; this may be simply a statistical aberration. We also found 203 primes p with base-3 Fermat quotients less than 100, 179 with base-5, and 212 for base-7. These values, together with near-misses of larger Fermat quotient, are also available on the project web page, while primes with small relative Fermat coefficients base-a are reported in Tables 5–7.

4.2 Fibonacci-Wieferich primes

Another class of primes initially defined because of Fermat's Last Theorem are the *Fibonacci-Wieferich* primes, sometimes called *Wall-Sun-Sun* primes. Let F_u denotes the uth Fibonacci number, and $\left(\frac{p}{5}\right)$ denotes the Legendre symbol; that is,

$$\left(\frac{p}{5}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 5; \\ -1, & \text{if } p \equiv \pm 2 \pmod 5; \\ 0, & \text{if } p \equiv 0 \pmod 5. \end{cases}$$

Then although for any prime p,

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod p,$$

there are no known solutions to

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p^2}. \tag{3}$$

Any solution to (3) is a Fibonacci-Wieferich prime. Previous searches for Fibonacci-Wieferich primes these primes have extended as far as to 2.0×10^{14} [14] by McIntosh and Roettger. By modifying the methods described above, we were also able to use our code in the search for

these primes. We were able to search to about 9.7×10^{14} (or, more precisely, solutions not greater than $(2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29)\cdot1.5\times10^5$), in which space no Fibonacci-Wieferich primes were found. We did, however, find several new "near misses" – those primes for which $F_{p-\left(\frac{p}{5}\right)}$ is small $\pmod{p^2}$. These are reported in Table 8. A more extensive list of near-misses for Fibonacci-Wieferich primes, together with the near misses for Wieferich primes of each base we studied, will be available on the project web page. After we completed this work, we discovered that McIntosh and Roettger had extended the search described their search [14] to 10^{15}. Our values match theirs precisely. Because their new values have not yet been published, we include them here.

4.3 Computational considerations with Fibonacci-Wieferich primes

Searching for Fibonacci-Wieferich primes involves calculating $F_{p-\left(\frac{p}{5}\right)} \pmod{p^2}$, for (fairly) large p. Naturally space and memory considerations keep us from computing $F_{p-\left(\frac{p}{5}\right)}$ directly. Instead we do these calculations by recalling a well-known identity, namely that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

By doing all these computations modulo n^2 for some n, and the same type of binary ladder that we used above, we can compute our values quite quickly. In fact, we can save even more time by noting that all of our matrix calculations involve either squaring, or multiplying by $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Although naively multiplying two 2×2 matrices requires eight multiplications and four additions, squaring a symmetric matrix requires only three squares a^2, b^2, c^2, one product $(a + c) \cdot b$, and 3 additions:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}^2 = \begin{pmatrix} a^2 + b^2 & (a + c) \cdot b \\ (a + c) \cdot b & b^2 + c^2 \end{pmatrix}.$$

After implementing this algorithm, a test for a Fibonacci-Wieferich prime runs about four times slower than testing a Wieferich prime. In practice, since some of the multiplications can be done in parallel, the test takes a bit less than four times the time for Wieferich primes.

5 The Computation

The largest part of our computation was the search for Wieferich primes to 6.7×10^{15}. This was performed on DISCOVERY cluster at Dartmouth College, a cluster of (at the time) about 500 AMD Opteron nodes with 64-bit processors. We ran our code on 24 processors for a period of about 200 days. For short periods of low cluster load, we utilized more processors, once reaching a total of 96. At other times, our computation was tabled for higher priority tasks. Altogether, the search used approximately 12000 CPU days, a value that compares well with that of the previous record search, which used (based on the information provided by Knauer and Richstein) used roughly 50000 CPU days – although on slower computers.

The searches for base-3, 5, and 7 Wieferich primes, along with the search for Fibonacci-Wieferich primes, were performed on the Condor cluster in the Dartmouth College Mathematics Department during low-load times over a period of many months. We used between one and eighteen 64-bit Linux machines of various architectures. Computation times were carefully recorded for these runs. In the following table, the times are recorded: For (base-2) Wieferich primes, the total time taken for the computation $[N, 6.7 \times 10^{15}]$, and for all other primes, the time taken for computing the range $[N, 150000N]$, where $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = 6469693230$. (Computations of the range $[0, N]$ were very short, and were implemented with unsophisticated methods.)

Table 2: Time used in CPU days for calculations (Range values are approximate; see discussion above for precise values)

Search	Range	CPU Days
Wieferich primes	$[6.5 \times 10^9, 6.7 \times 10^{15}]$	12907.97
Base-3 Wieferich	$[6.5 \times 10^9, 9.7 \times 10^{14}]$	714.54
Base-5 Wieferich	$[6.5 \times 10^9, 9.7 \times 10^{14}]$	812.14
Base-7 Wieferich	$[6.5 \times 10^9, 9.7 \times 10^{14}]$	916.67
Fibonacci-Wieferich	$[6.5 \times 10^9, 9.7 \times 10^{14}]$	1978.49

6 Results

6.1 Wieferich and near-Wieferich primes

As we stated earlier, no new (base-2) Wieferich primes were found. It has become standard practice to report "near-Wieferich" primes; that is, those p for which $2^{(p-1)/2} \equiv \pm 1 + Ap \pmod{p^2}$, where $|A| \leq 100$. However, as the magnitude of the primes under consideration grows, the density of the near-Wieferich primes diminishes, and there are fewer to report. We propose, therefore, a new definition: a *near-Wieferich prime* is one for which the value of A/p is small; say less than 10^{-13}. Table 4 gives all such primes not greater than 6.7×10^{15}. For base-3 Wieferich primes, such a definition excludes some 200 previously unreported primes with $|A| < 100$, and simliar numbers are excluded for base-5 and base-7 primes. Rather than give a table of all these primes here, their values will be given on the project webpage.

We might well ask whether our results were to be expected: that is, should we expect to find any Wieferich primes in the region $[1.25 \times 10^{15}, 6.7 \times 10^{15}]$? Certainly $A = A(p)$ can take on any of p values (mod p). Assuming that A takes these values randomly, the "probability" that A takes any particular value (say, 0) is $1/p$. From this, a heuristic is given in [5] that the expected number of Wieferich primes in the interval $[x, y]$ is

$$\sum_{x \leq p \leq y} \frac{1}{p} \approx \log\left(\frac{\log y}{\log x}\right) = \log\log y - \log\log x. \tag{4}$$

From this we would conclude that the expected number of Wieferich primes in our interval is .0472, and therefore the lack of such primes there is not surprising.

Because our program recorded all p with "small" A (that is, all those for which $|A| < 2^{24}$), we compiled a large data set which can be used to give more rigorous (experimental) confirmation of this conjecture. Indeed, our program recorded more than 2.1 million primes p for which $A < 2^{24}$. Using this data, we checked the following conjecture, which follows from the same heuristic as does equation (4):

Conjecture 3 (Crandall, Dilcher, and Pomerance)**.** The number of prime $p \in [a, b]$ for which $A \in [K, L]$ is asymptotically

$$(L - K) \cdot (\log\log b - \log\log a).$$

The table below presents a small snapshot of our experimental results confirming this conjecture. Complete data will be available on our webpage. In Table 3, the values in row i, column k reflect the number of $p \in [i \times 10^{14}, (i+1) \times 10^{14}]$ with $A \in [4(k-1) \times 10^6, 4k \times 10^6)$. Overall, the conjecture holds up very well. Indeed, in the strip given by $k = 2$,

Table 3:

i	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$	Expected
15	7451	7473	7435	7315	7511	7356	7361	7423	7380.8
16	6779	6897	6999	6862	6858	6942	6879	6941	6920.8
17	6449	6448	6545	6480	6391	6497	6420	6622	6514.2
18	6000	6135	6099	6028	6071	6080	6256	6146	6152.1
19	6053	5887	5839	5866	5854	5752	5911	5831	5827.7

the relative error between the conjectured and experimental values is never greater than 5.5%. Furthermore, we can plot conjectured and actual numbers of near-Wieferich primes for different values of i. The result is a graph that looks remarkably like a straight line. Let x_i be the expected number primes p in the ith interval $[i \times 10^{14}, (i+1) \times 10^{14})$ for which $A < 4 \times 10^6$, and let y_i be the actual number of such p in the same interval (the values in column 1). We expect from Conjecture 3 that for any i, $y_i \approx x_i$. In fact, linear regression on the two data sets returns a best fit equation of

$$y = 0.999958129x + 9.7$$

(with $R^2 = .9992$), giving strong experimental agreement with the conjectured value. Similar tests using different parts of our data show no meaningful disagreement between the values of A and what is expected heuristically. A data set of all near misses with Fermat quotients less than 2^{24} (comprising roughly 2 million primes) is available on the project web page.

7 Acknowledgments

We would like to acknowledge the scientific support received from the Research Computing group at Dartmouth College and the generous amount of computational resources we were given on the DISCOVERY cluster. We thank Carl Pomerance, Giulio Genovese, and Chris Hall for valuable discussions which improved this work.

Table 4: Primes $p < 6.7 \times 10^{15}$ for which $2^{p-1} \equiv 1 + Ap \pmod{p^2}$, with $|A/p| < 10^{-13}$. (Values of $|A/p|$ are given in multiples of 10^{-14}.)

p	A	$\lvert A/p\rvert$	p	A	$\lvert A/p\rvert$
1093	0	0			
3511	0	0			
765760560131939	−76	9.925	3723113065138349	−36	0.967
993048728162299	+81	8.157	3925342714781797	−139	3.541
1302848719581529	+76	5.833	3948546628939699	−186	4.711
1515362530042687	+149	9.833	4032459967159163	−172	4.265
1680898792774051	−96	5.711	4143792274787999	+216	5.213
1865546314599557	+75	4.020	4150209531584437	+48	1.157
1885825033325021	+158	8.378	5109286219780877	−79	1.546
2276306935816523	+6	0.264	5131427559624857	−36	0.702
2576594157291871	−123	4.774	5294488110626977	−31	0.586
2718566561783551	+203	7.467	5367369195612269	+318	5.925
2849352392161111	+255	8.949	5464249230405811	+426	7.796
3167939147662997	−17	0.537	5539428831517831	+230	4.152
3383577137448533	+331	9.783	5592905052127597	+353	6.312
3411159925463651	+176	5.160	5625021395769599	−413	7.342
3544715971857451	+127	3.583	5683778474515027	+332	5.841
3660747680296367	−211	5.764	5755502459289463	+476	8.270
3690728733648797	−334	9.050	6227907715670981	−379	6.086
3692386431182551	+277	7.502	6517506365514181	+58	0.890
6521780305210439	−595	9.123			

Table 5: Primes $p < 9.7 \times 10^{14}$ for which $3^{p-1} \equiv 1 + Ap \pmod{p^2}$, with $|A/p| < 10^{-13}$. (Values of $|A/p|$ are given in multiples of 10^{-14}.)

p	A	$\lvert A/p\rvert$
1006003	0	0.0
39433103646379	−1	2.536
61629351935149	+2	3.245
191293826264479	+19	9.932
229887238986217	+11	4.785
431096201990017	+12	2.784
481589141680567	+13	2.699
566967768385507	+12	2.117
631564776981199	−59	9.342
638096726480497	+40	6.269

Table 6: Primes $p < 9.7 \times 10^{14}$ for which $5^{p-1} \equiv 1 + Ap \pmod{p^2}$, with $|A/p| < 10^{-13}$. (Values of $|A/p|$ are given in multiples of 10^{-14}.)

p	A	$\lvert A/p \rvert$
53471161	0	0.0
1645333507	0	0.0
6692367337	0	0.0
188748146801	0	0.0
319072335276077	+2	0.627
419207873154803	+26	6.202
817486743201059	−59	7.21724

Table 7: Primes $p < 9.7 \times 10^{14}$ for which $7^{p-1} \equiv 1 + Ap \pmod{p^2}$, with $|A/p| < 10^{-13}$. (Values of $|A/p|$ are given in multiples of 10^{-14}.)

p	A	$\lvert A/p \rvert$
87121568306639	+8	9.1826

Table 8: New primes for which $F_{p-\left(\frac{p}{5}\right)} \equiv Ap \pmod{p^2}$ satisfies $|A| < 100 \pmod{p^2}$ (for examples with $p < 2 \times 10^{14}$, see [14]).

p	A
267927950960309	−9
276225896955847	6
299920665662731	−49
321208072276457	−98
331961404795379	−98
399729951985657	−38
481154641312217	31
548865911671993	−92
549413206041731	62
585297174492313	11
635696842671829	52
732698387434649	−75

References

[1] N. Beeger, On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$, *Messenger of Mathematics* **51** (1922), 149–150.

[2] N. G. W. H. Beeger, On the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's last theorem, *Nieuw Arch. Wiskunde* **20** (1939), 51–54.

[3] J. Brillhart, J. Tonascia, and P. Weinberger, On the Fermat quotient, *Computers in Number Theory*, Proc. Sci. Res. Council Atlas Sympos., No. 2, Academic Press, 1971, pp. 213–222.

[4] R. Brown and R. McIntosh, http://www.loaria.fr/~zimmerma/records/Wieferich.status, 2001.

[5] Richard Crandall, Karl Dilcher, and Carl Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449.

[6] J. Crump, reported at http://www.spacefire.com/numbertheory/Wieferich.htm; website was not functioning at time of publication of this article, 2001.

[7] C. E. Fröberg, Some computations with Wilson and Fermat remainders, *Math. Tables Aids Comput.* **12** (1958), 281.

[8] C. E. Fröberg, On some number-theoretical problems treated with computers, in *Computers in Mathematical Research*, North-Holland, 1968, pp. 84–88.

[9] Wilfrid Keller and Jörg Richstein, Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$, *Math. Comp.* **74** (2005), 927–936.

[10] Joshua Knauer and Jörg Richstein, The continuing search for Wieferich primes, *Math. Comp.* **74** (2005), 1559–1563.

[11] Sidney Kravitz, The congruence $2^{p-1} \equiv 1 \pmod{p^2}$ for $p < 100,000$, *Math. Comp.* **14** (1960), 378.

[12] D. H. Lehmer, On Fermat's quotient, base two, *Math. Comp.* **36** (1981), 289–290.

[13] Emma Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* (2) **39** (1938), 350–360.

[14] R. J. McIntosh and E. L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.* **76** (2007), 2087–2094.

[15] W. Meissner, Über die Teilbarkeit von 2^{p-2} durch das Quadrat der Primzahl $p = 1093$, *Sitzungsberichte der Akademie der Wissenschaften, Berlin* **35** (1913), 663–667.

[16] Peter L. Montgomery, Modular multiplication without trial division, *Math. Comp.* **44** (1985), 519–521.

[17] Peter L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp.* **61** (1993), 361–363.

[18] Erna H. Pearson, On the congruences $(p-1)! \equiv -1$ and $2^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp.* **17** (1964), 194–195.

[19] Paul Pritchard, A sublinear additive sieve for finding prime numbers, *Comm. ACM* **24** (1981), 18–23.

[20] Hans Riesel, Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$, *Math. Comp.* **18** (1964), 149–150.

[21] Jonathan P. Sorenson, The pseudosquares prime sieve, in *Algorithmic Number Theory*, Lecture Notes in Comput. Sci., vol. 4076, Springer, 2006, pp. 193–207.

[22] Zhi Hong Sun and Zhi Wei Sun, Fibonacci numbers and Fermat's last theorem, *Acta Arith.* **60** (1992), 371–388.

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

2010 *Mathematics Subject Classification*: Primary 11A41; Secondary 11Y16, 11Y11.

Keywords: Wieferich prime, Fibonacci-Wieferich prime, Wall-Sun-Sun prime, wheel sieve, magic sieve, Montgomery arithmetic.
(Concerned with sequences A001220, A014127, A123692, and A123693.)

Received June 30 2011; revised version received September 12 2011. Published in *Journal of Integer Sequences*, October 16 2011.

Return to Journal of Integer Sequences home page.