MATHEMATICS OF COMPUTATION
Volume 74, Number 251, Pages 1559–1563
S 0025-5718(05)01723-0
Article electronically published on January 19, 2005

THE CONTINUING SEARCH FOR WIEFERICH PRIMES

JOSHUA KNAUER AND JÖRG RICHSTEIN

Abstract. A prime p satisfying the congruence

$$2^{p-1} \equiv 1 \pmod{p^2}$$

is called a *Wieferich prime*. Although the number of Wieferich primes is believed to be infinite, the only ones that have been discovered so far are 1093 and 3511. This paper describes a search for further solutions. The search was conducted via a large scale Internet based computation. The result that there are no new Wieferich primes less than $1.25 \cdot 10^{15}$ is reported.

1. Introduction

One year prior to his early death in 1829, Niels Henrik Abel [1] was the first to ask:

> "Kann $a^{\mu-1} - 1$, wenn μ eine Primzahl und a eine ganze Zahl und kleiner als μ und größer als 1 ist, durch μ^2 theilbar sein?"

In other words: Given a prime p not dividing an integer a, is it possible that the integer $(a^{p-1} - 1)/p$ is again divisible by p? Although one can immediately construct solutions to the corresponding congruence

$$a^{p-1} \equiv 1 \pmod{p^2} \tag{1}$$

when the exponent p is fixed and a is variable (see, e.g., [18]), it is not yet known how to locate a matching prime p for a fixed base a. Many connections between these solutions and other problems in number theory have been uncovered ([8], [25]). Probably the most famous one is due to Arthur Wieferich [29], connecting (1) with Fermat's last theorem:

Theorem 1.1 (Wieferich, 1909 [29]). *If for an odd prime p not dividing xyz it follows that*

$$x^p + y^p + z^p = 0,$$

then (1) *must be satisfied for $a = 2$.*

Today, Wieferich's theorem is known to be true for all prime bases a less than and including 103 ([13], [28]). Solutions to (1) where $a = 2$ are called *Wieferich primes*. Although there have been numerous searches for Wieferich primes (a believed to be complete list of references to published historical computations can be found in the bibliography), only two solutions have been discovered so far: 1093 [22], and 3511 [3].

Received by the editor June 18, 2003 and, in revised form, April 11, 2004.
2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 11-04.
The second author was supported in part by the Killam Trusts.

After a large scale Internet based search it turns out that there are no other Wieferich primes below $1.25 \cdot 10^{15}$.

In the following two sections the methodology used in the computation and a more in-depth examination of the results will be presented.

2. Searching for Wieferich primes

Due to a lack of algorithmic advances, there is currently no alternative to a brute force search. The use of computers has pushed the search limit from 16000 in 1940 [4] to $4.6 \cdot 10^{13}$ in 2001 [6], later extended to $2 \cdot 10^{14}$ [9]. Increasing this limit by a factor of 6 was achieved by distributing the computation over as many computers as possible through the Internet.

On each client machine an efficient implementation of a binary powering ladder was run. The implementation was based on the GNU multiple precision arithmetic library GMP [12]. Previous searches for Wieferich primes have made use of optimizations such as base-p arithmetic and steady-state division as described in [23], [8], and [7]. Neither of these optimizations was used in this search. In order to include as many computers as possible, only a 32-bit processor was presumed when constructing the client code. To realize the benefits of base-p arithmetic, intermediate values in the computation must be stored in registers on the client machine's processor. A standard 32-bit processor does not have large enough registers to contain the intermediate values encountered when dealing with primes in the range searched. A preliminary C language version of the client code that made use of steady-state division did see a performance enhancement. However, this version was out-performed by the highly optimized assembly language based GMP library. The GMP library made it possible to construct efficient versions of the client code for Linux-, Solaris-, and Windows-based platforms. The basic enhancement of only computing $2^{\frac{p-1}{2}} \mod p^2$ (as (1) is equivalent to $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p^2$) was employed. A segmented sieve of Eratosthenes as described in [26] was used to extract the prime numbers from a given range of integers (see also [8]).

The client and server machines used the hypertext transfer protocol (HTTP) to communicate with one another. The processes of distributing ranges of numbers to be checked and collecting results were implemented through common gateway interface (CGI) scripts. This made the construction of both client and server programs simpler. Pre-built HTTP library code was used for the client and a basic system of Perl scripts turned out to be sufficient for the server.

3. Results

As stated, the primary result of this search is that other than 1093 and 3511, there are no Wieferich primes smaller than $1.25 \cdot 10^{15}$.

In [7] a probabilistic argument for the existence of more Wieferich primes is presented. The result of computing $2^{\frac{p-1}{2}} \mod p^2$ can be written as $\pm 1 + Ap \mod p^2$, for some integer A. If we assume the event of A taking on some particular value ($A = 0$ indicates a Wieferich prime) as being random and independent with probability $\frac{1}{p}$, we can expect the number of Wieferich primes in an interval $[x, y]$ to be around

$$\ln(\ln y / \ln x). \tag{2}$$

TABLE 1. Near Wieferich primes in $[4 \cdot 10^{12}, 1.25 \cdot 10^{15}]$.

p	$2^{\frac{p-1}{2}} \mod p^2$	p	$2^{\frac{p-1}{2}} \mod p^2$
4006528141163	$-1+17p$	68132247624521	$+1-55p$
4169357937293	$-1-27p$	92226580839683	$-1-76p$
5216344035949	$-1+93p$	118485210646981	$-1-90p$
5240305919047	$+1-95p$	134257821895921	$+1+10p$
7355288787229	$-1-68p$	153332502585091	$-1+59p$
7876427903107	$-1-48p$	181841793213263	$+1+90p$
8851776421399	$+1-81p$	**205250817470827**	$-1-78p$
11344191252809	$+1-92p$	**259990715684839**	$+1-12p$
12456646902457	$+1+2p$	**339258218134349**	$-1+2p$
15056776355693	$-1-19p$	**342092449620191**	$+1+90p$
23639424831877	$-1-48p$	**346412396858131**	$-1-48p$
24990087401551	$+1+16p$	**362061154308767**	$+1-64p$
28506780213511	$+1-28p$	**694936752678643**	$-1+75p$
28785529445977	$+1+33p$	**696740841781447**	$+1+61p$
29230410915073	$+1+96p$	**734180764265903**	$+1+37p$
30189412701163	$-1-37p$	**739507312099561**	$+1-78p$
30309769394167	$+1+28p$	**765760560131939**	$-1+38p$
63735899194511	$+1-16p$	**1140417231387373**	$-1-82p$
63918629031731	$-1+38p$	**1170553064286511**	$+1-84p$
67961346537659	$-1-49p$		

Formula (2) predicts approximately 0.0998 Wieferich primes in our search range $[4.6 \cdot 10^{13}, 1.25 \cdot 10^{15}]$, putting the chance of finding one at approximately 1 in 10. So the result was not unexpected. As the probability of encountering a new Wieferich prime is relatively low, it has been the practice of the last few searches to report "near Wieferich" primes, defined as instances of

$$2^{\frac{p-1}{2}} \equiv \pm 1 + Ap \pmod{p^2}$$

where $|A| \leq 100$. Table 1 gives a listing of all such exponents greater than $4 \cdot 10^{12}$ encountered during the search. The last 13 entries in bold font are the new near Wieferich primes uncovered.

As in [7], formula (2) can be applied to predict the number of near Wieferich primes in an interval to be around

$$201 \cdot \ln(\ln y / \ln x).$$

From this we would expect approximately 10.88 near Wieferich primes in $[2 \cdot 10^{14}, 1.25 \cdot 10^{15}]$, a close correspondence to the 13 uncovered.

During the course of the search the system was able to incorporate more than 250 client computers of varying configurations. At peak speed the system was capable of running through approximately 1.6 million primes per second, with individual machines running through 1000 to 30000 primes per second. The largest interval covered in one day was approximately $3 \cdot 10^{12}$, but average performance was approximately $1.5 \cdot 10^{12}$ a day.

Acknowledgments

The results of this work are due to the generosity of many individuals from over thirteen countries who donated computer time to the Wieferich prime search. We want to thank everyone who helped to make this computation possible.

Most work for this paper was done at Dalhousie University in Halifax, Nova Scotia, Canada. The authors thank the Department of Mathematics and Statistics for the resources and hospitality.

References

1. Abel, N. H. (1828). *Journal für die reine und angewandte Mathematik*, 3:212.
2. Beeger, N. (1914). Quelques remarques sur les congruences $r^{p-1} \equiv 1 \pmod{p^2}$ et $(p-1)! \equiv -1 \pmod{p^2}$. *Messenger of Mathematics*, 43:72–84.
3. Beeger, N. (1922). On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. *Messenger of Mathematics*, 51:149–150.
4. Beeger, N. (1940). On the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's last theorem. *Nieuw Archief Voor Wiskunde*, pages 51–54. MR0000390 (1:65d)
5. Brillhart, J., Tonascia, J., and Weinberger, P. (1971). On the Fermat quotient. *Computers in Number Theory*, pages 213–222. MR0314736 (47:3288)
6. Brown, R. and McIntosh, R. (2001). `http://www.loria.fr/~zimmerma/records/Wieferich.status`.
7. Crandall, R., Dilcher, K., and Pomerance, C. (1997). A search for Wieferich and Wilson primes. *Mathematics of Computation*, 66(217):433–489. MR1372002 (97c:11004)
8. Crandall, R. and Pomerance, C. (2001). Prime Numbers – A Computational Perspective. *Springer-Verlag, New York*, 2001. MR1821158 (2002a:11007)
9. Crump, J. (2002). `http://www.spacefire.com/NumberTheory/Wieferich.htm`.
10. Cunningham, A. (1910). *Proceedings of the London Mathematical Society*, 2(8):xiii.
11. Fröberg, C.-E. (1958). Some computations of Wilson and Fermat remainders. *Mathematical Tables and other Aids to Computation*, page 281.
12. Granlund, T. (2000). *GNU MP: The GNU Multiple Precision Arithmetic Library*, 3.1.1 edition.
13. Granville, A. and Monagan, M. B. (1988). The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389. *Transactions of the American Mathematical Society*, (306):329–359. MR0927694 (89g:11025)
14. Grave, D. (1909). *An elementary text on the theory of numbers (in Russian)*. Kiev Izv. Univ., Kiev.
15. Haußner, M. and Sachs, D. (1963). On the congruence $2^p \equiv 2 \pmod{p^2}$. *American Mathematical Monthly*, 70:996.
16. Hertzer, H. (1908). Über die Zahlen der Form $a^{p-1} - 1$, wenn p eine Primzahl. *Archiv der Mathematik und Physik*, (13):107.
17. Jacobi, C. and Busch (1828). *Journal für die reine und angewandte Mathematik*, 3:301–302.
18. Keller, W. and Richstein, J. (2001). Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *To appear*.
19. Kloss, K. E. (1965). Some number-theoretic calculations. *Journal of Research of the National Bureau of Standards-B. Mathematics and Mathematical Physics*, 69B(4):335–336. MR0190057 (32:7473)
20. Kravitz, S. (1960). The congruence $2^{p-1} \equiv 1 \pmod{p^2}$ for $p < 100,000$. *Mathematics of Computation*, page 378. MR0121334 (22:12073)
21. Lehmer, D. (1981). On Fermat's quotient, base two. *Mathematics of Computation*, 36(153):289–290. MR0595064 (82e:10004)
22. Meissner, W. (1913). Über die Teilbarkeit von $2^{p-1} - 2$ durch das Quadrat der Primzahl $p = 1093$. *Sitzungsberichte*, pages 663–667.
23. Montgomery, P. L. (1993). New prime solutions of $a^{p-1} \equiv 1 \pmod{p^2}$. *Mathematics of Computation*, 203(61):361–363. MR1182246 (94d:11003)
24. Pearson, E. H. (1963). On the congruences $(p-1)! \equiv -1$ and $2^{p-1} \equiv 1 \pmod{p^2}$. *Mathematics of Computation*, pages 194–195. MR0159780 (28:2996)

25. Ribenboim, P. (1996). The New Book of Prime Number Records. *Springer-Verlag, New York*, 1996. MR1377060 (96k:11112)
26. Richstein, J. (2000). Verifying the Goldbach conjecture up to $4 \cdot 10^{14}$. *Mathematics of Computation*, 70(236):1745–1749. MR1836932 (2002c:11131)
27. Riesel, H. (1964). Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$. *Mathematics of Computation*, pages 149–150. MR0157928 (28:1156)
28. Suzuki, J. (1994). On the generalized Wieferich criteria. *Proc. Japan Acad. Ser. A Math. Sci.*, (70):230–234. MR1303569 (95j:11026)
29. Wieferich, A. (1909). Zum letzten Fermat'schen Theorem. *Journal für die reine und angewandte Mathematik*, 136:293–302.

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, V5A 1S6 Canada
E-mail address: jknauer@cecm.sfu.ca

Institut für Informatik, Justus-Liebig-Universität, Giessen, Germany
E-mail address: Joerg.Richstein@informatik.uni-giessen.de