Serdica J. Computing **4** (2010), 293–300

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

SEARCH FOR WIEFERICH PRIMES THROUGH THE USE OF PERIODIC BINARY STRINGS

Jan Dobeš, Miroslav Kureš

Abstract. The result of the distributed computing project Wieferich@Home is presented: the binary periodic numbers of bit pseudo-length $j \leq 3500$ obtained by replication of a bit string of bit pseudo-length $k \leq 24$ and increased by one are Wieferich primes only for the cases of 1092 or 3510.

1. Introduction. Let p be a Wieferich prime. A main motivation for this research is the periodicity of the binary expression of $p-1$ (for known Wieferich primes). The question of whether or not this phenomenon necessarily follows from properties of Wieferich primes is open. If we scan and test such periodic numbers, a need of knowledge about their quantity emerges, especially for computer processing. We have answered the problem of a number of B-periodic numbers of given bit pseudo-length n in Proposition 1 and present two tables with some values.

ACM Computing Classification System (1998): I.1.4, J.2.
Key words: Wieferich prime, periodic bit string, distributed computing.

After a brief introduction to Wieferich primes, the main result is presented. Within the distributed computing project Wieferich@Home, the authors have proved (case-by-case, by computer) that the binary periodic numbers of bit pseudo-length $j \leq 3500$ obtained by replication of a bit string of bit pseudo-length $k \leq 24$ and increased by one are Wieferich primes only for the cases of 1092 or 3510; i.e., there is no new Wieferich prime with the described property in the scanned area.

2. Number of periodic strings. The numbers $c(n)$ of aperiodic binary strings of length n, $n \in \mathbb{N}$, are tabulated in the OEIS database as the sequence A0275375, see [4]. Nevertheless, the explicit formula is also known, cf. e.g. [3]:

$$c(n) = \sum_{d|n} \mu(d) 2^{\frac{n}{d}},$$

where μ is the Möbius function.

Let us consider a binary string $\mathbf{a}$ of the form

$$\mathbf{a} = a_k a_{k-1} \dots a_1,$$

$a_1, \dots, a_k \in \{0, 1\}$, in which $a_1 = 0$ and at least one value is non-zero. Hereafter a number $x \in \mathbb{N}$ will be called a *B-periodic number*, if its binary representation $\mathbf{x}$ is a replication of such a string:

$$\mathbf{a} \dots \mathbf{a} = \mathbf{x} = x_j x_{j-1} \dots x_1,$$

$x_1, \dots, x_j \in \{0, 1\}$. Left zeros can occur in $\mathbf{x}$ and j is a proper multiple of k, $j > k$. The number j will be called the *bit pseudo-length* of x (as the true bit length can be lower just because of possible left zeros).

Example 1. The smallest B-periodic number is 10, because its binary representation is

$$10|10.$$

Further examples of B-periodic numbers are e.g. 1092 with binary representation

$$0100|0100|0100$$

and 3510 with binary representation

$$110|110|110|110.$$

Let us denote by $\tau(n)$ the number of B-periodic numbers of bit pseudo-length n. It is evident that $\tau(n) = 0$ if n is a prime (and, of course, if $n = 1$); hence the first non-zero value for $\tau(n)$ arises with $n = 4$. Further, let us denote $T(n)$ as a "cumulative $\tau(n)$", i.e.

$$T(n) = \sum_{i=4}^{n} \tau(i).$$

Proposition 1. *The number of B-periodic numbers of bit pseudo-length n equals*

$$\tau(n) = \frac{1}{2}\left(2^n - \sum_{d|n} \mu(d) 2^{\frac{n}{d}} - 2\right).$$

P r o o f. Very easy: the number of all periodic strings of bit pseudo-length n must be $2^n - c(n)$. Then we exclude two periodic strings obtained by replication of one digit strings: the string $111\ldots1$ (its last digit is not 0) and the string $000\ldots0$ (it does not contain any 1). Exactly half of remaining periodic strings have 0 as their last digit. Hence $\tau(n) = \dfrac{2^n - c(n) - 2}{2}$. $\square$

So we can present the values for small n.

n	$\tau(n)$	$T(n)$
4	1	1
5	0	1
6	4	5
7	0	5
8	7	12
9	3	15
10	16	31
11	0	31
12	37	68

And now, some higher (approximate) values:

n	$\tau(n)$	$T(n)$
500	$9.0463 \cdot 10^{74}$	$1.8093 \cdot 10^{75}$
1000	$1.6367 \cdot 10^{150}$	$3.2734 \cdot 10^{150}$
1500	$2.9612 \cdot 10^{225}$	$5.9224 \cdot 10^{225}$
2000	$5.3576 \cdot 10^{300}$	$1.0715 \cdot 10^{301}$
2500	$9.6931 \cdot 10^{375}$	$1.9386 \cdot 10^{376}$
3000	$1.7537 \cdot 10^{451}$	$3.5075 \cdot 10^{451}$
3500	$3.1729 \cdot 10^{526}$	$6.3459 \cdot 10^{526}$

3. Wieferich primes. A *Wieferich prime* is a prime p which is a solution to the congruence equation

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

Arthur Wieferich has demonstrated a relation between the described primes and the most famous mathematical question (answered by Andrew Wiles on June 23, 1993), Fermat's Last Theorem.

Theorem 1 (Wieferich 1909)**.** *Let p be an odd prime, and let a, b, c be non-zero integers such that $a^p + b^p + c^p = 0$. Furthermore, assume that p does not divide the product abc. Then p is a Wieferich prime.*

There are only two known Wieferich primes, $p_1 = 1093$ and $p_2 = 3511$; as we have seen, the numbers $p_1 - 1$ and $p_2 - 1$ are both B-periodic. This interesting property has been observed by Wells Johnson [2]. Furthermore, it is not known as yet if there exist infinitely or finitely many Wieferich primes (or even only these two). So a conjecture that all Wieferich primes have this "periodic" property is reasoned and dramatic.

Let us observe:

Example 2. It is not true that a B-periodic number increment by one is always a prime number. We have

$$110|110 = 54$$

as the fifth smallest B-periodic number and $54 + 1$ is not a prime.

Near-Wieferich primes are defined as primes having the form $Z + Ap \pmod{p^2}$ with both Z and A reduced modulo p values $Z = \pm 1$ and $|A| \leq 100$. (128 instead of 100 appears in the Wieferich@Home application.)

4. Search for Wieferich primes: the periodic test in Wieferich@Home. The Wieferich prime 1093 was discovered by Waldemar Meissner in 1913 and the Wieferich prime 3511 was discovered by Nicolaas G. W. H. Beeger in 1922. There are projects searching for new Wieferich primes. The newest result is:

Theorem 2 (Dorais and Klyve 2009, [1])**.** *Up to* $6.7 \cdot 10^{15}$*, only* 1093 *and* 3511 *are Wieferich primes.*

The authors have produced their own original project Wieferich@Home, [5], as a distributed computing project publicly launched on December 29, 2007. The application contains two search algorithms: the complete test and the periodic test. While the complete test tests linearly each successive prime, the periodic test takes B-periodic numbers and checks if these numbers satisfy the congruence condition. The algorithm for the periodic test works with numbers of bit pseudo-lengths up to 3500. It follows that there are $T(3500) \approx 6.3459 \cdot 10^{526}$ B-periodic numbers to scan. The non-primality mentioned in Example 2 suggests a sieving of these numbers.

5. Quick Division Test (QDT). Testing B-periodic numbers without pre-test filters of non-prime numbers could slow down the computing and decrease the count of tested B-periodic numbers. These cases can improve by the following algorithm. The Quick Division Test (QDT) algorithm with a bit parser prepares numbers (j-bit pseudo-length of B-periodic numbers) for the congruence equation (CEq in algorithm). The array M_n contains the first 9 Mersenne primes. Finally, B-periodic numbers are increased by 1 and these potential prime numbers are tested by the congruence equation.

Require: B-periodic number
Ensure: *true*, if input is not divisible by $3, 5, 7, 31, 127, ..., 2305843009213693951$
  if B is not divisible by 5 **then**
    for $i = 1$ to 9 **do**
      $e \Leftarrow M_n[i]$

```
      c ⇐ n[i]
      s ⇐ 1
      u ⇐ 0
      d ⇐ 0
      for j = 1 to the bit pseudo-length(B) do
        t ⇐ bit(B, j)
        if s ≤ c then
          d ⇐ d + t · 2^(s−1)
          s ⇐ s + 1
        else
          s ⇐ 2
          u ⇐ u + d
          d ⇐ t
        end if
      end for
      if (u + d) mod e ≡ 0 then
        return false
      end if
    end for
  else
    return false
  end if
  return true
```

6. Periodic Test (PT). As to the pseudo-code of the algorithm, B-periodic numbers of bit pseudo-length $50 \leq n \leq 3500$ are tested. B-periodic numbers of bit pseudo-length $n < 50$ are ignored, because these primes were tested already by usual linear tests. The congruence equation (CEq) for our purposes returns attributes: 1 — Wieferich prime, 2 — near Wieferich prime. For processing big integers of bit pseudo-length $i > 64$ we can use multiple-precision arithmetic.

```
Require: B — period, m — period count
  {big integer}
  {built-up B-period number from m-period B}
  p ⇐ Bnumber(B, m)
```

```
n ⇐ bitlength(P)
while n ≤ 3500 do
  p ⇐ Bnumber(B, m)
  {make odd number}
  p ⇐ p + 1
  n ⇐ bitlength(p)
  {numbers with pseudo-length n ≤ 50 were already tested}
  if 50 ≤ n ≤ 3500 then
    {Quick Division Test}
    if QDT(p) then
      {C: 1 — Wieferich prime, 2 — near Wieferich prime}
      C ⇐ CEq(p)
    end if
  end if
  {next B-period}
  m ⇐ m + 1
end while
```

We repeat that numbers of a bit pseudo-length up to 50 were scanned by several authors, see e.g. [1] and references mentioned there. With the aid of the periodic test, the first findings for a publishing present an improvement summarized in the following theorem.

Theorem 3. *Let n be a B-periodic number of a bit pseudo-length $j \leq 3500$ obtained by a replication of a bit string of bit pseudo-length $k \leq 24$. If $n+1$ is a Wieferich prime, then $n = 1092$ or $n = 3510$.*

REFERENCES

[1] Dorais F. G., D. W. Klyve. Near Wieferich Primes up to $6.7 \cdot 10^{15}$. `http://www-personal.umich.edu/~dorais/docs/wieferich.pdf`

[2] Johnson W. On the non-vanishing Fermat quotients. *Journal für die reine und angewandte Mathematik*, **292** (1977), 196–200.

[3] Lothaire M. Combinatorics on words. Addison-Wesley, Reading MA, 1983.

[4] The On-Line Encyclopedia of Integer Sequences.
http://www.research.att.com/~njas/sequences/

[5] Wieferich@Home.
http://www.elmath.org

Jan Dobeš
Software Development
Jiráskova 222/V
38001 Dačice, Czech Republic
e-mail: info@dobesoft.cz

Miroslav Kureš
Institute of Mathematics
Brno University of Technology
Technická 2
61669 Brno, Czech Republic
e-mail: kures@fme.vutbr.cz

Received October 10, 2009
Final Accepted March 11, 2010