Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 4, 705–712
DOI: 10.7546/nntdm.29.4.705-712

Perfect numbers, Wieferich primes and the solutions of $\binom{2n}{n} \equiv 2^n \bmod n$

Gabriel Guedes[1] and Ricardo Machado[2]

[1] Department of Mathematics, Rural Federal University of Pernambuco (UFRPE)
Recife-PE, Brazil
e-mail: gabriel.guedes@ufrpe.br

[2] Department of Mathematics, Rural Federal University of Pernambuco (UFRPE)
Recife-PE, Brazil
e-mail: ricardo.machadojunior@ufrpe.br

Received: 4 April 2023 **Revised:** 22 August 2023
Accepted: 25 October 2023 **Online First:** 16 November 2023

Abstract: In this article we focus on the solutions of a congruence equation: "$\binom{2n}{n} \equiv 2^n \bmod n$". Using the main result of this article and the SageMath software, we improve largely the number of known solutions. Furthermore, we prove that some famous numbers like even perfect numbers and Wieferich primes are connected to solutions of this equation.

Keywords: Perfect numbers, Wieferich primes, Binomial coefficient, Algorithmic number theory, Wolstenholme converse problem.
2020 Mathematics Subject Classification: 11A07, 11A41, 11B65, 11B75, 11-04.

1 Introduction

The search for properties that characterize prime numbers is intense, given their fundamental importance.

A classical theorem in number theory is the Wolstenholme's Theorem.

Theorem 1.1 (Wolstenholme)**.** *Let $p > 3$ be a prime number, then $p^3 \mid \binom{2p}{p} - 2$.*

A natural question is the reciprocal conclusion of the Theorem 1.1.

Conjecture 1. *If $n > 3$ and $n^3 \mid \binom{2n-1}{n-1} - 1$ then n is a prime number.*

The Conjecture 1 is known as Wolstenholme's converse problem which if true will characterize the prime numbers. This conjecture was proposed by J. P. Jones and remains open. See [8, p. 23] and [4, p. 84]. In [5], McIntosh verified that this holds for all $n < 10^9$.

We are interested in problems related to Conjecture 1. Using the Theorem 1.1 and Fermat's Little Theorem we arrive at the congruence equation: $\binom{2p}{p} \equiv 2^p \bmod p$, which is valid for primes. We can ask for solutions to the same congruence equation in the case of composite integers. That is, which are the composite integers n that satisfy the following equation?

$$\binom{2n}{n} \equiv 2^n \bmod n.$$

In [7] sequence id:A084699 shows that the known solutions of this equation are

$$12, 30, 56, 424, 992, 16256, 58288, 119984, 356992, 1194649,$$
$$9973504, 12327121, 13141696, 22891184, 67100672, 233850649.$$

In the next sections, we make use of Theorem 2.1 and computational effort to find some new solutions and we were able to relate the set of solutions with some famous numbers such as Mersenne primes, even perfect numbers, and Wieferich primes.

2 Solutions and perfect numbers

The relation of the Equation (1) and the very famous class of numbers as even perfect numbers, Mersenne primes, and Wieferich primes, appears to us in a very interesting way. Our initial aim with this article was to obtain new values to the sequence id:A084699 (see [7]). For this, we use the result proved in this article, Theorem 2.1. In particular, item *b)* enabled a more efficient implementation than the direct test on Equation (1).

In this article, we show an algorithm implemented in SageMath, in order to generate solutions to this equation. The algorithm is based on the following theorem:

Theorem 2.1. *Let $n = 2^k p$, where p is an odd prime and $k \in \mathbb{N}$, then n is solution of the equation*

$$\binom{2n}{n} \equiv 2^n \bmod n \tag{1}$$

if and only if p satisfies the following conditions:

a) p divides $\binom{2^{k+1}}{2^k} - 2^{2^k}$;

b) p has at least k digits 1's in its binary expansion.

Proof. Since $\gcd(2^k, p) = 1$, the Equation (1) is equivalent to the system:

$$\binom{2n}{n} \equiv 2^n \bmod p, \tag{2}$$
$$\binom{2n}{n} \equiv 2^n \bmod 2^k. \tag{3}$$

Using the left-hand side of Equation (2), by Babbage's Theorem (see page 68, Exercise 2.5.10 of [3]), we have

$$\binom{2n}{n} \equiv \binom{2 \cdot 2^k p}{2^k p} \equiv \binom{2^{k+1}}{2^k} \bmod p.$$

Using the right-hand side of Equation (2), by Fermat's Little Theorem,

$$2^n \equiv \left(2^{2^k}\right)^p \equiv 2^{2^k} \bmod p.$$

Consequently, the Equation (2) is equivalent to

$$\binom{2^{k+1}}{2^k} \equiv 2^{2^k} \bmod p,$$

which is equivalent to item *a)*. Now, using the right-hand side of Equation (3), since $n = 2^k p$, it is clear that $2^n \equiv 0 \bmod 2^k$. Let $v_p(n)$ the p-adic valuation of n. Since $v_2\left(\binom{2n}{n}\right) = v_2\left(\binom{2p}{p}\right)$, by Kummer's Theorem (see [3], p. 99, Theorem 3.7), $v_2\left(\binom{2n}{n}\right)$ is the number of 1's in binary expansion of p. Then the Equation (3) is satisfied if and only if item *b)* is satisfied, i.e., p has at least k digits 1's in binary expansion. □

In addition to the solutions available at [7] (sequence id:A084699), using Theorem 2.1 and some implementation on SageMath, we discovered two more numbers:

$$2^{17} \times 131071 = 17179738112 \quad \text{and} \quad 2^{19} \times 524287 = 274877382656.$$

The algorithm code follows:

Algorithm 2.1.

```
def algorithm_theo2(start, end):
    '''spbin is the sum of the digits of p in base 2'''
    p = start
    while (p<=end):
        p = next_prime(p)
        spbin = sum(p.digits(base=2))
        for k in range(1,spbin+1):
            if (binomial(2^(k+1),2^(k))-2^(2^k)).mod(p)==0:
                print('2^%d x %d = %d' %(k, p, (2^k)*p))
algorithm_theo2(2, 10^6)
```

The Algorithm 2.1 searches for primes p such that

$$\binom{2^{k+1}}{2^k} - 2^{2^k} \equiv 0 \bmod p,$$

in which k varies from 1 to the sum of the digits of p in base 2. In all computational tests, we used a PC with a Core i5 1135G7 processor and this routine took 55 seconds to compute.

Factoring the solutions found, we verify that the Mersenne primes are related to a solution in the way of the next theorem.

Theorem 2.2. *If m is an even perfect number, then $n = 2m$ satisfies the Equation* (1).

Proof. If m is an even perfect number, then $m = 2^{p-1} \cdot q$ with p and $q = 2^p - 1$ prime numbers. Like the proof of Theorem 2.1, Equation (1) is equivalent to the system

$$\binom{2^{p+1}}{2^p} \equiv 2^{2^p} \bmod q, \tag{4}$$

$$\binom{2q}{q} \equiv 2^q \bmod 2^p. \tag{5}$$

Now, we consider two cases.
Case 1: If $p = 2$, the congruence is immediate.
Case 2: If $p > 2$, the q-adic expansion of $2^p = 2^p - 1 + 1 = q + 1$ and $2^{p+1} = 2q + 2$ by Lucas's Theorem (see [1], page 95) the left-hand side of Equation (4)

$$\binom{2^{p+1}}{2^p} \equiv \binom{2q+2}{q+1} \equiv \binom{2}{1} \cdot \binom{2}{1} \equiv 4 \bmod q.$$

Now look to the right-hand side and applying Fermat's Little Theorem

$$2^{2^p} = 2 \cdot 2^{2^p - 1} = 2 \cdot 2^q \equiv 4 \bmod q$$

and this verifies the Equation (4).

In Equation (5), applying Kummer's Theorem for the left-hand side we have $v_2\left(\binom{2q}{q}\right) = p$, then $2^p \mid \binom{2q}{q}$. For the right-hand side, $p < q \Rightarrow 2^p \mid 2^q$. Hence 2^p divides both sides of the Equation (5). □

2.1 Using Pollard's Rho algorithm for prime factorization

Pollard's Rho (see [2]) algorithm for prime factorization is particularly fast for a large composite number with small prime factors. Algorithm 2.2 uses Pollard's Rho algorithm to search for some prime factors of $\binom{2^{k+1}}{2^k} - 2^{2^k}$ and proceeds like Algorithm 2.1 to verify the second condition of Theorem 2.1. Using Algorithm 2.2, we found 8 previously unknown solutions to Equation (1).

Algorithm 2.2.

```
def algorithm_theo2_pollard_rho(start, end, pmax):
    '''spbin is the sum of the digits of p in base 2'''
    k = start
    while (k<=end):
        rk = (binomial(2^(k+1),2^(k))-2^(2^k))
        prime_list=partial_factoring(rk, pmax)
        for p in prime_list:
            if rk%p ==0:
                spbin = sum(ZZ(p).digits(base=2))
                if spbin >= k:
                    print('2^%d x %d = %d' %(k, p, (2^k)*p))
        k=k+1
```

Line 6 of Algorithm 2.2 calls the function `partial_factoring` that can be found in Appendix 5. This function uses the method `is_prime` which employs a strong pseudo-primality test. Using the Algorithm 2.2, we found the following previously unknown solutions to Equation (1):

1. $2^5 \times 29558453816897149$,
2. $2^6 \times 52917841$,
3. $2^6 \times 4181131371869088 1087$,
4. $2^7 \times 3266538383196869458915779068335241011556968075534365464337162308 41$,
5. $2^8 \times 129020293739$,
6. $2^9 \times 1466765681$,
7. $2^{10} \times 412707874957531$,
8. $2^{11} \times 559115197117$.

To find the first 6 solutions we used parameters `start=3`, `end=9` and `pmax=10^8`. That is, we used the command: `algorithm_theo2_pollard_rho(3, 9, 10^8)`.

It was necessary to use 2.1 seconds to get the solutions. To find the last two solutions required 3 minutes and 33 seconds. The parameters were: `start=10`, `end=11` and `pmax=10^4`.

3 A generalization and Wieferich primes

We can observe that it is possible to generalize Theorem 2.1 for any positive integer, in the next Theorem 3.1. It is noteworthy that using this theorem, we show that the Wieferich prime numbers are uniquely determined by Equation (1).

Theorem 3.1. *Let $n = 2^k p_1 \cdots p_s$, where p_j are different prime numbers and $n_j = \frac{n}{p_j}$, then n is solution of the equation*

$$\binom{2n}{n} \equiv 2^n \bmod n \tag{6}$$

if and only if the following conditions are satisfied:

a) p_j divides $\binom{2n_j}{n_j} - 2^{n_j}$;

b) $p_1 \cdots p_s$ has at least k digits 1's in its binary expansion.

Proof. Is the same as in Theorem 2.1 applied to this more general framework. □

Definition 3.1. *A* Wieferich prime *is a prime number p such that p^2 divides $2^{p-1} - 1$.*

The Wieferich primes were defined in 1909 by Arthur Wieferich in his studies of Fermat's Last Theorem. There is a lot of connection with this class of primes and important topics in number theory like *ABC* conjecture, pseudoprimes, Mersenne primes, and others. Until today, in March of 2023, there are only two known Wieferich primes, 1093 and 3511.

Theorem 3.2. *Let $n = p^2$ with p a prime number. We have that p is a Wieferich prime if and only if n is a solution of Equation* (1).

Proof. Supposing that p is a Wieferich prime we are going to prove that n is a solution of Equation (1), that is,

$$\binom{2p^2}{p^2} \equiv 2^{p^2} \bmod p^2. \tag{7}$$

Using Lucas's Theorem we have that left-hand side of Equation (7) is

$$\binom{2p^2}{p^2} \equiv \binom{2}{1} \equiv 2 \bmod p^2.$$

In the right-hand side of (7) note that $2^{p^2} = 2^{p(p-1)} \cdot 2^p$, by Euler's Theorem $2^{p(p-1)} \equiv 1 \bmod p^2$ then

$$2^{p^2} \equiv 2^{p(p-1)} \cdot 2^p \equiv 2^p \equiv 2^p - 2 + 2 \equiv 2 \cdot (2^{p-1} - 1) + 2 \bmod p^2.$$

Now apply the hypothesis of p being a Wieferich prime then

$$2 \cdot (2^{p-1} - 1) + 2 \equiv 2 \bmod p^2.$$

Thus, we show that Equation (7) is valid, since both sides are congruent to 2 modulo p^2.

For the converse in the same lines we have that $2^p \equiv 2 \bmod p^2$ simplifying by 2 we obtain $2^{p-1} \equiv 1 \bmod p^2$ which is the definition of a Wieferich prime. □

One natural question arose here: *How many of the known solutions of Equation* (1) *are explained by the theorems of this article?* In Table 1 we can see that there is only one previously known solution ($n = 233850649$) that cannot be explained by the theorems of this article. All the new solutions found in this article are of the form $2^k p$, where p is a prime number. Hence they are explained by Theorem 2.1.

Solution	**Solution factorization**	$\boldsymbol{k}$	**Ones in bin. exp. of** $\boldsymbol{p_1 \cdots p_s}$	**Theorem**
12	$2^2 \cdot 3$	2	2	Theorem 2.1
30	$2 \cdot 3 \cdot 5$	1	4	Theorem 3.1
56	$2^3 \cdot 7$	3	3	Theorem 2.1
424	$2^3 \cdot 53$	3	4	Theorem 2.1
992	$2^5 \cdot 31$	5	5	Theorem 2.1
16256	$2^7 \cdot 127$	7	7	Theorem 2.1
58288	$2^4 \cdot 3643$	4	8	Theorem 2.1
119984	$2^4 \cdot 7499$	4	8	Theorem 2.1
356992	$2^7 \cdot 2789$	7	7	Theorem 2.1
1194649	1093^2	–	–	Theorem 3.2
9973504	$2^8 \cdot 38959$	8	8	Theorem 2.1
12327121	3511^2	–	–	Theorem 3.2
13141696	$2^6 \cdot 205339$	6	8	Theorem 2.1
22891184	$2^4 \cdot 607 \cdot 2357$	4	12	Theorem 3.1
67100672	$2^{13} \cdot 8191$	13	13	Theorem 2.1
233850649	$3919 \cdot 59671$	–	–	?

Table 1. Prior known solutions of (1) explained by Theorems 2.1 and 3.2.

4 Conclusion

In this article, we describe algorithms that facilitate the search for solutions to Equation (1), and with it, we were able to find new solutions. Furthermore we related the set of solutions with even perfect numbers and Wieferich primes. Much remains to be done, we describe solutions of the form $n = 2^k p_1 p_2 \cdots p_r$ or $n = p^2$. However, there is a lot to wonder about solutions with exponents greater than 1.

5 Appendix

In this Appendix we have the functions that are called, directly or indirectly, by Algorithm 2.2.

Algorithm 5.1.

```
1  def pollard_rho_ref(n):
2      i=1
3      x=randint(0, n-1)
4      y=x
5      k=2
6      while True:
7          i=i+1
8          x=(x^2-1)%n
9          d=gcd(y-x, n)
10         if d!= 1 and d!=n:
11             if d.is_prime():
12                 return d
13             else:
14                 f = list(d.factor())[0][0]
15                 return f
16         elif i==k:
17             y=x
18             k=2*k
```

The Algorithm 5.1 is a SageMath adaptation of the pseudocode of page 976 of [2]. The differences here are in lines 11 to 15. The original pseudocode prints the value of d, while the Algorithm 5.1 returns a prime that divides d.

Algorithm 5.2.

```
def partial_factoring(n, max=oo):
    prime_list=[]
    while n!=1:
        if n.is_prime():
            prime_list.append(n)
            return prime_list
        else:
            p=pollard_rho_ref(n)
            while n%p==0:
                n=ZZ(n/p)
            prime_list.append(p)
            if p>=max:
                return prime_list
```

The Algorithm 5.2 tries to create a divisor list of n, it has the inputs n and max. This algorithm stops adding the primes to the list when it finds all the primes of n or when it finds a prime number greater than the input max. This algorithm executes Algorithm 5.1 to search for primes, divides n by the prime number found and runs the Algorithm 5.1 again with the new value.

Acknowledgements

We would like to thank Paulo Ribenboim, for his books, his lecture, and his entire life dedicated to mathematics. To the Department of Mathematics of the Federal Rural University of Pernambuco - UFRPE, for the excellent work environment, with the appreciation of the broad spectrum that academic life can have.

Also, we would like to express our gratitude to the editors and anonymous referees for their feedback including the suggestion to use Pollard's Rho Algorithm to improve our algorithm and find more solutions to Equation (1). Our sincere thanks.

References

[1] Chuan-Chong, C., & Khee-Meng, K. (1992). *Principles and Techniques in Combinatorics.* World Scientific, Singapore.

[2] Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to Algorithms.* (3rd ed.). MIT Press, Cambridge, Massachusetts.

[3] Granville, A. (2020). *Number Theory Revealed: A Masterclass.* American Mathematical Society, Providence, Rhode Island.

[4] Guy, R. (2004). *Unsolved Problems in Number Theory.* Springer Science + Business Media, New York.

[5] McIntosh, R. J. (1995). On the converse of Wolstenholme's theorem. *Acta Arithmetica*, 71(4), 381–389.

[6] Mersenne.org (2023). List of known Mersenne prime numbers. Available online at: https://www.mersenne.org/primes/.

[7] OEIS Foundation Inc. (2023). Composite integers n such that binomial $(2 * n, n) == 2^n \bmod n$. Entry A084699. *The On-Line Encyclopedia of Integer Sequences*. Available online at: https://oeis.org/A084699.

[8] Ribenboim, P. (2004). *The Little Book of Bigger Primes.* (Vol. 811). Springer, New York.