

## ON THE CONGRUENCE

$$1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$$

MAX ALEKSEYEV, JOSÉ MARÍA GRAU, AND ANTONIO M. OLLER-MARCÉN

ABSTRACT. It is well-known that the congruence  $\sum_{i=1}^n i^n \equiv 1 \pmod{n}$  has exactly five solutions:  $\{1, 2, 6, 42, 1806\}$ . In this work, we characterize the solutions to the congruence in the title for every prime  $p$ . This characterization leads to an algorithm that allows to compute all such solutions when there is finite number of them and, in general, to find all the solutions up to very high bounds in comparison to the computational complexity appearing if the problem is naively addressed by exhaustive search.

AMS 2010 Mathematics Subject Classification 11B99, 11A99, 11A07

Keywords: Power sum, primary pseudoperfect numbers, algorithm

## 1. INTRODUCCION

Very often in the literature we find equations with “few” solutions whose search is a hard both from the theoretical and computational point of view. One of the best-known examples is possibly the so-called Erdős-Moser Equation,  $\sum_{i=1}^{m-1} i^n = m^n$ , for which it has been proved that there only exists the trivial solution  $1^1 + 2^1 = 3^1$  if  $m < 1.485 \times 10^{9321155}$  [2]. Another famous examples are Giuga’s Conjecture [4], that states that there is no composite  $n$  such that  $\sum_{i=1}^{n-1} i^n \equiv -1 \pmod{n}$  and that has been verified up to  $10^{13800}$  [1] or Lehmer’s Totient Problem asking if there exists any composite number  $n$  such that  $\varphi(n) \mid (n-1)$  and having no solution smaller than  $10^{22}$  or with less than 14 prime divisors [3]. If we have a look at equations with “few” known solutions, we can mention  $\sum_{p|N} \frac{1}{p} - \frac{1}{N} \in \mathbb{N}$  for which only 12 solutions are known (the so-called Giuga numbers, sequence A007850 in OEIS) or  $\sum_{p|N} \frac{1}{p} + \frac{1}{N} = 1$  having only 8 known solutions (the Primary pseudoperfect numbers [2], sequence A054377 in OEIS).

In some cases, the search for new solutions to an equation only leads to the extension of the set of integers for which no solution is known. In other cases, theoretical and computational effort succeed in finding all the solutions. This is the case, for instance, of the equation  $1^n + 2^n + \cdots + n^n \equiv 19 \pmod{n}$  that we will show to have only 8 solutions, namely  $\{1, 2, 6, 19, 38, 114, 798, 34314\}$ .

Let us define  $S_k(n) := \sum_{i=1}^n i^k$ . Throughout the paper we deal with congruences of the form  $S_n(n) \equiv a \pmod{n}$ . We will denote its set of solutions by  $\mathcal{M}_p$ . It is easy to see that  $n \in \mathcal{M}_0$  if and only if  $n$  is odd [5, Theorem 1]. In [6, Proposition 1] the set  $\mathcal{M}_1$  was determined. Namely,  $\mathcal{M}_1 = \{1, 2, 6, 42, 1806\}$ .

In this work, we focus on the case when  $a$  is prime. Both of the situations described above appear. In some cases we will be able to prove the finiteness of the set of solutions (and to compute them) and in other cases we will find the

solutions up to very high bounds (which would be unreachable only by “brute force” methods). The main contribution of this paper is the characterization of the solutions to the previous congruence and the implementation of an algorithm by which the possible prime divisors of the solutions are found. Hence, if this set of possible prime divisors is finite, the search for solutions can restrict to products of them. Moreover, the relation of this problem with *weak primary pseudoperfect numbers* will allow us to compute all the solutions up to  $10^{30}$  with very little computational effort.

## 2. CHARACTERIZATION AND COMPUTATION OF $\mathcal{M}_p$ WITH PRIME $p$

The following lemma (see [5]) will be useful in the sequel.

**Lemma 1.** *Let  $d, k, n$ , and  $t$  be positive integers.*

i) *If  $d$  divides  $n$ , then*

$$S_k(n) \equiv \frac{n}{d} S_k(d) \pmod{d}.$$

ii) *Let  $p^t$  be an odd prime power. Then*

$$S_k(p^t) \equiv \begin{cases} -p^{t-1} \pmod{p^t}, & \text{if } p-1 \mid k; \\ 0 \pmod{p^t}, & \text{otherwise.} \end{cases}$$

iii) *We have*

$$S_k(2^t) \equiv \begin{cases} 2^{t-1} \pmod{2^t}, & \text{if } t = 1, \text{ or } t > 1 \text{ and } k > 1 \text{ is even;} \\ -1 \pmod{2^t}, & \text{if } t > 1 \text{ and } k = 1; \\ 0 \pmod{2^t}, & \text{if } t > 1 \text{ and } k > 1 \text{ is odd.} \end{cases}$$

Next theorem gives a characterization of the set  $\mathcal{M}_p$  in terms of the prime power factorization of its elements.

**Theorem 1.** *Let  $p$  be a prime number. Then  $n \in \mathcal{M}_p$  if and only if the following conditions hold:*

i) *The prime power factorization of  $n$  is given by  $n = p^s q_1 \cdots q_r$ , with  $0 \leq s \leq 2$ .*

ii) *For every  $i \in \{1, \dots, r\}$ ,  $q_i - 1 \mid n$  and  $n/q_i + p \equiv 0 \pmod{q_i}$ .*

iii) *If  $s = 1$ , then  $p - 1 \nmid n$ .*

iv) *If  $s = 2$ , then  $p - 1 \mid n$  and  $n/p^2 + 1 \equiv 0 \pmod{p}$ .*

*Proof.* We will work out the odd  $p$  case, if  $p = 2$  the proof is identical. Let  $n = 2^t p^s q_1^{u_1} \cdots q_r^{u_r}$  be the prime power factorization of  $n$ . Then  $S_n(n) \equiv p \pmod{n}$  if and only if  $S_n(n) \equiv p \pmod{2^t}$ ,  $S_n(n) \equiv p \pmod{p^s}$  and  $S_n(n) \equiv p \pmod{q_i^{u_i}}$ .

Due to Lemma 1,  $S_n(n) \equiv \frac{n}{2^t} S_n(2^t) \pmod{2^t}$  so  $S_n(n) \equiv p \pmod{2^t}$  if and only if  $r \leq 1$  with  $n/2 + p \equiv 0 \pmod{2}$  if  $t = 1$  by Lemma 1 iii).

Furthermore, by Lemma 1 i)  $S_n(n) \equiv \frac{n}{p^s} S_n(p^s) \pmod{p^s}$  so  $S_n(n) \equiv p \pmod{p^s}$  if and only if  $\frac{n}{p^s} S_n(p^s) \equiv p \pmod{p^s}$  and we apply Lemma 1 ii) repeatedly. If  $s = 1$  the latter congruence holds if and only if  $p - 1 \nmid n$ . If  $s > 1$ , it holds if and only if  $p - 1 \mid n$  and  $n/p^2 + 1 \equiv 0 \pmod{p^{s-1}}$  and this latter congruence is possible only if  $s \leq 2$ .

Finally, by Lemma 1 i) again,  $S_n(n) \equiv \frac{n}{q_i^{u_i}} S_n(q_i^{u_i}) \pmod{q_i^{u_i}}$  and hence, since  $p \neq q_i$ , it follows from Lemma 1 iii) that  $S_n(n) \equiv p \pmod{q_i^{u_i}}$  if and only if  $q_i - 1 \mid n$  and  $n/q_i + p \equiv 0 \pmod{q_i^{u_i}}$  with this latter congruence being possible only if  $u_i \leq 1$ .  $\square$

This result motivates a decomposition  $\mathcal{M}_p = \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$ , with

$$\begin{aligned}\mathcal{M}_p^{(0)} &= \{n \in \mathcal{M}_p : p \nmid n\}, \\ \mathcal{M}_p^{(1)} &= \{n \in \mathcal{M}_p : p \parallel n\}, \\ \mathcal{M}_p^{(2)} &= \{n \in \mathcal{M}_p : p^2 \parallel n\}.\end{aligned}$$

We will now study each of these sets separately. To do so, the following results will be useful. Their proofs can be found in [6].

**Lemma 2.** *Let  $\mathcal{P}$  be a non-empty set of primes  $p$  such that*

- i)  $p - 1$  is square-free, and
- ii) if  $q$  is a prime divisor of  $p - 1$ , then  $q \in \mathcal{P}$ .

*Then  $\mathcal{P}$  is one of the sets  $\{2\}$ ,  $\{2, 3\}$ ,  $\{2, 3, 7\}$ , or  $\{2, 3, 7, 43\}$ .*

**Lemma 3.** *Let  $\mathcal{N}$  be a set of positive integers  $\nu$  such that*

- i)  $\nu$  is square-free, and
- ii) if  $p$  is a prime divisor of  $\nu$ , then  $p - 1$  divides  $\nu$ .

*Then  $\mathcal{N} \subseteq \{1, 2, 6, 42, 1806\}$ .*

Lemma 3 provides the following result regarding  $\mathcal{M}_p^{(0)}$ .

**Proposition 1.** *Let  $p$  be a prime. Then,  $\mathcal{M}_p^{(0)} \subseteq \{1, 2, 6, 42, 1806\} = \mathcal{M}_1$*

*Proof.* Let  $n \in \mathcal{M}_p^{(0)}$ . Theorem 1 i) implies that  $n$  is square-free. Moreover, Theorem 1 ii) implies that if  $q$  is a prime divisor of  $n$ , then  $q - 1$  divides  $n$ . Hence, we can apply Lemma 3 and the result follows.  $\square$

In fact, the following result is straightforward and completely determines the set  $\mathcal{M}_p^{(0)}$ .

**Proposition 2.** *Let  $p$  be a prime. Then,  $\mathcal{M}_p^{(0)} = \{n \in \mathcal{M}_1 : p \equiv 1 \pmod{n}\}$ .*

To study the set  $\mathcal{M}_p^{(1)}$  we introduce the following set of primes associated to  $p$ .

**Definition 1.** Let  $p$  be a prime. The set  $\mathcal{Q}_p$  is the set of prime numbers defined by the property:  $q \in \mathcal{Q}_p$  if and only if the following conditions hold:

- i)  $q - 1$  is square-free.
- ii)  $p - 1 \nmid q - 1$ .
- iii) If  $t$  is a prime divisor of  $q - 1$ , then  $t = p$  or  $t \in \mathcal{Q}_p$ .

In addition, we define the following set of integers associated to each  $\mathcal{Q}_p$ ,

$$\mathcal{N}_p := \{n \in \mathbb{N} : n \text{ is square-free, } p - 1 \nmid n \text{ and } q \in \mathcal{Q}_p, \text{ for every prime } q \mid n\}.$$

**Proposition 3.** *Let  $p$  be a prime. Then,  $\mathcal{M}_p^{(1)} \subseteq p \cdot \mathcal{N}_p$ .*

*Proof.* Let  $n \in \mathcal{M}_p^{(1)}$ . Theorem 1 i), ii) and iii) clearly imply that  $n/p \in \mathcal{N}_p$  and hence the result.  $\square$

Finally, let us turn to the set  $\mathcal{M}_p^{(2)}$ . We will see that this set is empty in most cases. To do so we first need the following lemma.

**Lemma 4.** *Let  $n \in \mathcal{M}_p^{(2)}$ . If  $q$  is a prime such that  $p > q \mid n$ , then  $q \in \{2, 3, 7, 43\}$ .*

*Proof.* Let us consider the set of primes  $\{q : p > q, q \mid n, \text{ for some } n \in \mathcal{M}_p^{(2)}\}$ . Theorem 1 implies that this set is in the conditions of Lemma 2 and hence the result.  $\square$

**Proposition 4.** *Let  $p \neq 2, 3, 7, 43$  be a prime. Then  $\mathcal{M}_p^{(2)}$  is empty.*

*Proof.* Assume that  $n \in \mathcal{M}_p^{(2)}$ . Since theorem 1 implies that  $n = p^2 q_1 \cdots q_r$  and  $p - 1 \mid n$ , it follows that  $p - 1$  is square-free. Moreover, if we consider the set of primes  $S = \{q : q \mid p - 1\}$ , Lemma 4 implies that  $S \subseteq \{2, 3, 7, 43\}$ . Thus,  $p$  is a prime such that  $p - 1$  is square-free and the only possible prime divisors of  $p - 1$  are  $\{2, 3, 7, 43\}$ . The only primes in these conditions are precisely  $\{2, 3, 7, 43\}$  as can be directly checked.  $\square$

The following result shows that in the remaining cases; i.e., if  $p = 2, 3, 7$  or  $43$  the set  $\mathcal{M}_p^{(2)}$  is also finite.

**Proposition 5.** *Let  $p \in \{2, 3, 7, 43\}$ . Then,  $\mathcal{M}_p^{(2)} \subseteq p^2 \cdot \mathcal{M}_1$*

*Proof.* Define the set of primes  $\{q \neq p : q \mid n, \text{ for some } n \in \mathcal{M}_p^{(2)}\}$ . Theorem 1 implies that the set  $S \cup \{p\}$  is in the conditions of Lemma 2 and hence  $S \cup \{p\} \subseteq \{2, 3, 7, 43\}$ . But, since  $p \in \{2, 3, 7, 43\}$  it follows that also  $S \subseteq \{2, 3, 7, 43\}$ . Thus, the result follows from the fact that every element in  $\mathcal{M}_p^{(2)}$  is of the form  $p^2 q_1 \cdots q_r$  with  $q_i \neq p$  prime.  $\square$

**Corollary 1.** *Let  $p$  be a prime. Then,*

$$\mathcal{M}_p = \begin{cases} \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)} \subseteq \mathcal{M}_1 \cup p \cdot \mathcal{N}_p, & \text{if } p \neq 2, 3, 7, 43; \\ \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)} \subseteq \mathcal{M}_1 \cup p \cdot \mathcal{N}_p \cup p^2 \cdot \mathcal{M}_1, & \text{otherwise.} \end{cases}$$

*In particular if  $\mathcal{N}_p$  is finite then so is  $\mathcal{M}_p$ .*

**Corollary 2.**

$$\mathcal{M}_7 = \{1, 2, 6, 7, 14, 294, 12642\},$$

$$\mathcal{M}_{43} = \{1, 2, 6, 42, 43, 86, 258, 77658\}.$$

Although Theorem 1 gives a complete characterization of the set  $\mathcal{M}_p$  for a prime  $p$ , from a practical point of view, Corollary 1 is more useful if we want to effectively compute the elements of this set. In particular, Corollary 1 implies that in order to compute  $\mathcal{M}_p$  we need to compute the set of primes  $\mathcal{Q}_p$ . Since this set is not necessarily finite and it is constructed iteratively, we need stopping criteria in case they are finite. We give one in the following result.

**Proposition 6.** *Let  $K \in \mathcal{Q}_p$ . Given a subset  $\Omega \subset \{q \in \mathcal{Q}_p : q < K + 1\}$ , we define integers*

$$w_\Omega := 1 + \prod_{q \in \Omega} q, \quad w'_\Omega := 1 + p \prod_{q \in \Omega} q$$

*If  $w_\Omega$  and  $w'_\Omega$  are not prime for any subset  $\Omega$ , then  $\mathcal{Q}_p$  is finite and  $K = \max \mathcal{Q}_p$ .*

*Proof.* Let  $K \in \mathcal{Q}_p$  assume that it is not the maximum. Then, define  $\bar{q} = \min\{q \in \mathcal{Q}_p : K < q\}$ . Since  $\bar{q} \in \mathcal{Q}_p$  we can put  $\bar{q} - 1 = \prod t_i$  with  $t_i$  primes. Consider  $\bar{\Omega} = \{t_i : t_i \neq p\}$ . Since  $\bar{q} \in \mathcal{Q}_p$ , it follows that  $\bar{\Omega} \subseteq \mathcal{Q}_p$  and the minimality of  $\bar{q}$  implies that  $t_i < K + 1$ . But in this situation either  $w_{\bar{\Omega}}$  or  $w'_{\bar{\Omega}}$  is a prime (depending on whether  $p \mid \bar{\Omega}$  or not) and the result follows.  $\square$

The following algorithm constructs, for any given prime  $p$ , an increasing sequence of sets  $X_i[p]$ . In the cases when this sequence stabilizes, it does at a set  $\mathfrak{X}[p]$  that will be shown to be  $\mathcal{Q}_p \cup \{p\}$ . In fact, the stabilization criterion is given by Proposition 6.

**Algorithm.** INPUT:  $p, i = 1; X_1[p] := \{2, p\};$

$$\text{ProdParts}(X_i[p]) := \{1 + \prod_{q \in \Omega} q : \Omega \subseteq X_i[p]\} \cap \{n : p - 1 \nmid n - 1\};$$

STEP1 If  $\text{ProdParts}(X_i[p]) \setminus X_i[p] = \emptyset$  then  $\mathfrak{X}[p] = X_i[p]$ . STOP .

STEP2

$$X_{i+1}[p] := X_i[p] \cup \{q \text{ prime} : q \in \text{ProdParts}(X_i[p])\}.$$

STEP3:  $i = i + 1$ ; GOTO STEP1.

**Theorem 2.** For every  $i$ , we have that  $X_i[p] \subseteq \mathcal{Q}_p \cup \{p\}$ . Moreover, the algorithm stops if and only if  $\mathcal{Q}_p$  is finite, in which case  $\mathfrak{X}[p] = \mathcal{Q}_p \cup \{p\}$ .

*Proof.* Clearly  $X_1[p] \subseteq \mathcal{Q}_p \cup \{p\}$ . Let us assume that  $X_{i-1}[p] \subseteq \mathcal{Q}_p$  while  $X_i[p] \setminus (\mathcal{Q}_p \cup \{p\}) \neq \emptyset$ . Let  $q$  the minimum of  $X_i[p] \setminus (\mathcal{Q}_p \cup \{p\})$ . Since  $q$  no pertenece a  $\mathcal{Q}_p \cup \{p\}$  but  $q - 1$  is square free and  $p - 1 \mid q - 1$ , there must exist a prime  $q_1$  dividing  $q - 1$  not in  $\mathcal{Q}_p \cup \{p\}$  and, consequently, not in  $X_{i-1}[p]$  either. This contradicts the fact that every element of  $X_i[p]$  is of the form  $1 + p_1 \dots p_k$  with  $p_j \in X_{i-1}[p]$ . Hence,  $X_i[p] \subseteq \mathcal{Q}_p \cup \{p\}$  for every  $i$  as claimed.

Now, if  $\mathcal{Q}_p$  is finite it is clear that the algorithm stops. Let us see that, if it stops, the output is  $\mathcal{Q}_p \cup \{p\}$ . If it was not the case, put  $q = \min\{(\mathcal{Q}_p \cup \{p\}) \setminus \mathfrak{X}[p]\}$ . Then,  $q - 1 = q_1 \dots q_r$  is squarefree with  $q_i \in \mathcal{Q}_p \cup \{p\}$ . But, in this case,  $q_i \in \mathfrak{X}[p]$  so  $q = 1 + q_1 \dots q_r \in \mathfrak{X}[p]$  because otherwise the algorithm would not have stopped. This contradicts the assumption of  $(\mathcal{Q}_p \cup \{p\}) \setminus \mathfrak{X}[p]$  being non empty so the result follows.  $\square$

**Example 1.** For  $p = 19$  the algorithm stops because  $X_7[19] = X_8[19]$  and its output is  $\mathcal{Q}_{19} \cup \{19\} = \{2, 3, 7, 19, 43, 4903, 168241543, 5773040306503\}$ . This implies that  $\mathcal{M}_{19}$  is finite.

The following result determines the finiteness of  $\mathcal{Q}_p$  (and hence of  $\mathcal{M}_p$ ) for a family of primes.

**Corollary 3.** If  $p \notin \{2, 3, 7, 43\}$  and the set

$$\{1 + 2p, 1 + 1806p, 1 + 6p, 1 + 14p, 1 + 86p, 1 + 42p, 1 + 258p, 1 + 602p\}$$

does not contain any prime, then  $\mathcal{M}_p \subseteq \mathcal{M}_1 \cup p\mathcal{M}_1$  and thus, it is finite.

*Proof.* In this situation the above algorithm stops giving  $\mathfrak{X}[p] = \{2, 3, 7, 43, p\}$ . Hence,  $\mathcal{Q}_p = \{2, 3, 7, 43\}$  and the result follows.  $\square$

There seem to exist many primes  $p$  satisfying the condition of Corollary 3. The following are those smaller than 1000:

{67, 97, 127, 163, 307, 317, 337, 349, 409, 521, 523, 547, 643, 709, 757, 811, 839, 857, 919, 967, 997}

There also exist primes for which  $\mathcal{Q}_p$  and  $\mathcal{M}_p$  are finite that do not satisfy the condition of Corollary 3. The following table gives some examples.

$p$	stop	$\mathcal{Q}_p$	$\mathcal{M}_p$
19	i=8	{2, 3, 7, 43, 4903, 168241543, 5773040306503}	{1, 2, 6, 19, 38, 114, 798, 34314}
79	i=5	{2, 3, 7, 43, 3319, 1573207}	{1, 2, 6, 79, 158, 474, 3318, 142674}
193	i=5	{2, 3, 7, 43, 348559}	{1, 2, 6, 193, 386, 1158, 8106, 348558}

Unfortunately, in some cases we cannot determine if the algorithm stops due to the size of the involved sets of primes. For instance, if  $p = 5$ , we have that  $X_5[5]$  contains 77 primes and it was impossible to compute  $X_6[5]$ .

### 3. RELACIÓN ENTRE THE PRIMARY PSEUDOPERFECT NUMBERS AND $\mathcal{M}_p$

When  $\mathcal{Q}_p$  is infinite, the previous algorithm never stops. Nevertheless, there is an easy result that allows us to compute the elements of  $\mathcal{M}_p$  up to  $p \cdot (8.49 \times 10^{30})$ . Before we introduce this result, we recall the set  $\mathcal{W}$  of *weak primary pseudoperfect numbers* defined in [6]. An integer  $n \geq 1$  is a *weak primary pseudoperfect number* if it satisfies the congruence

$$\sum_{p|n} \frac{n}{p} + 1 \equiv 0 \pmod{n}.$$

The only known weak primary pseudoperfect numbers are:

1, 2, 6, 42, 1806, 47058, 2214502422, 52495396602, 8490421583559688410706771261086.

and it is not even known whether  $\mathcal{W}$  is finite.

**Proposition 7.** *Let  $p$  be a prime. Then,  $\mathcal{M}_p \subseteq \mathcal{M}_1 \cup p \cdot \mathcal{W}$ .*

*Proof.* Let  $n \in \mathcal{M}_p$ . If  $p \nmid n$ , then  $n \in \mathcal{M}_1$  due to Proposition 1. On the other hand, if  $p \mid n$  [6, Corollary 1] states that  $n/p \in \mathcal{W}$  and hence the result.  $\square$

Thus, this proposition allows us to compute all the elements of  $\mathcal{M}_p$  up to  $p \cdot \max \mathcal{W}$ . It is enough to determine computationally if  $S_n(n) \equiv p \pmod{n}$  for every element of  $\mathcal{M}_1 \cup p \cdot \mathcal{W}$ . Observe that this set has, to this day, only 14 elements.

In some cases it is possible to use *ad hoc* arguments to prove that  $\mathcal{M}_p$  is finite and, hence, to compute its elements. This is the case, e.g., for  $p = 2, 3$ . To see that both  $\mathcal{M}_2$  and  $\mathcal{M}_3$  are finite we need to recall some ideas from [6]. For every  $Q \in \mathbb{N}$  we define

$$\mathfrak{M}_Q := \{n \in \mathbb{N} : S_{Qn}(Qn) \equiv n \pmod{n}\}.$$

If  $\mathfrak{M}_Q \neq \emptyset$ , then  $Q \in \mathcal{W}$  [6, Corollary 1] and, moreover, we have that [6, Proposition 3]

**Proposition 8.** *Given a weak primary pseudoperfect number  $Q$ , define the integer*

$$\mathfrak{n}_Q := \begin{cases} \text{lcm} \left\{ \frac{p-1}{\gcd(p-1, Q)} : p \mid Q \right\}, & \text{if } Q \neq 1; \\ 1, & \text{if } Q = 1. \end{cases}$$

*Then  $\mathfrak{M}_Q = \emptyset$  if and only if  $q - 1 \mid Q\mathfrak{n}_Q$  for some prime  $q \mid \mathfrak{n}_Q$ . Moreover, if  $\mathfrak{M}_Q \neq \emptyset$ , then  $\mathfrak{n}_Q \mid n$  for every  $n \in \mathfrak{M}_Q$  and, in particular,  $\mathfrak{n}_Q = \min \mathfrak{M}_Q$ .*

The following lemma is straightforward.

**Lemma 5.** *Let  $p$  be a prime. Then,  $n \in \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$  if and only if  $n/p \in \mathcal{W}$  and  $p \in \mathfrak{M}_{n/p}$ .*

Even if it might be true that the set  $\mathcal{M}_p$  is finite for every prime  $p$ , there are many primes  $p$  for which the algorithm fails to prove the finiteness of  $\mathcal{Q}_p$ . Nevertheless, in the previous setting, we can directly prove the finiteness of  $\mathcal{M}_p$  in a couple of easy cases.

**Proposition 9.** *If  $p \in \{2, 3\}$ , then  $\mathcal{M}_p$  is finite.*

*Proof.* Due to Proposition 1 and Corollary 1 it is enough to prove that  $\mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$  is finite. Thus, assume that  $n \in \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$  and observe that, due to Lemma 5,  $n/p \in \mathcal{W}$  and  $p \in \mathfrak{M}_{n/p}$ .

Let  $p = 2$  with  $n/2 \in \mathcal{W}$  and  $2 \in \mathfrak{M}_{n/2}$ . It follows from Proposition 8 that  $\mathfrak{n}_{n/p} \mid 2$ ; i.e.,  $\mathfrak{n}_{n/2} = 1$  or  $2$ . Now, if  $\mathfrak{n}_{n/2} = 2$ , Proposition 8 implies that  $\mathfrak{M}_{n/2} = \emptyset$  which is a contradiction. Hence,  $\mathfrak{n}_{n/2} = 1$  which implies that  $p - 1 \mid n/2$  for every  $p \mid n/2$ ; i.e., that  $n/2 \in \mathcal{M}_1$  due to Lemma 3. Consequently,  $\mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)} \subseteq 2 \cdot \mathcal{M}_1$  is finite and so is  $\mathcal{M}_2 \subseteq \mathcal{M}_1 \cup 2 \cdot \mathcal{M}_1$ .

On the other hand, Let  $p = 3$  with  $n/3 \in \mathcal{W}$  and  $3 \in \mathfrak{M}_{n/3}$ . Again, we obtain that  $\mathfrak{n}_{n/3} = 1$  or  $3$ . Since  $n \in \mathcal{M}_p$  and  $3 \mid n$ , if  $n \neq 3$ , it follows from Theorem 1 that  $q - 1 \mid n$  for every prime  $q \mid n/3$ . In particular  $2 \mid n$ , so  $2 \mid n/3$  and Proposition 8 implies that  $\mathfrak{M}_{n/3} = \emptyset$  which is a contradiction. Hence,  $\mathfrak{n}_{n/3} = 1$  and  $\mathcal{M}_3 \subseteq \mathcal{M}_1 \cup 3 \cdot \mathcal{M}_1$  is finite.  $\square$

As a consequence, it is easy to compute the elements of  $\mathcal{M}_p$  for  $p = 2, 3$ .

**Corollary 4.**

$$\mathcal{M}_2 = \{1, 4, 12, 84, 3612\},$$

$$\mathcal{M}_3 = \{1, 2, 3, 18, 126, 5418\}.$$

In Proposition 2 and Corollary 4 we have determined the finiteness and we have computed the elements of  $\mathcal{M}_p$  for  $p = 2, 3, 7, 43$ . Recall that these are precisely the cases when  $\mathcal{M}_p^{(2)}$  might be non-empty. In the remaining cases  $\mathcal{M}_p = \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)}$ . To end this section we are going to give a characterization of  $\mathcal{M}_p^{(1)}$  when  $p \neq 2, 3, 7, 43$ .

**Lemma 6.** *Let  $p \neq 2, 3, 7, 43$  be a prime. Then,  $p \cdot \mathcal{M}_1 = \{p, 2p, 6p, 42p, 1806p\} \subset \mathcal{M}_p^{(1)}$ .*

*Proof.* It is enough to apply Theorem 1 and recall the definition of  $\mathcal{M}_p^{(1)}$ .  $\square$

**Proposition 10.** *Let  $p \neq 2, 3, 7, 43$  be a prime. Then,  $n \in \mathcal{M}_p^{(1)}$  if and only if  $n/p \in \mathcal{W}$ ,  $\mathfrak{n}_{n/p} \mid p$  and  $\mathfrak{n}_{n/p} - 1 \nmid n/p$ .*

*Proof.* Assume that  $n \in \mathcal{M}_p^{(1)}$ . Then, by Lemma 5,  $n/p \in \mathcal{W}$  and  $p \in \mathfrak{M}_{n/p}$ . Hence,  $\mathfrak{M}_{n/p} \neq \emptyset$  and due to Proposition 8  $\mathfrak{n}_{n/p} \mid p$  and  $\mathfrak{n}_{n/p} - 1 \nmid n/p$ .

Conversely, assume that  $n/p \in \mathcal{W}$ ,  $\mathfrak{n}_{n/p} \mid p$  and  $\mathfrak{n}_{n/p} - 1 \nmid n/p$ . If  $\mathfrak{n}_{n/p} = 1$ , then like in the second part of the proof of Proposition 9 we obtain that  $n \in p \cdot \mathcal{M}_1 \subset \mathcal{M}_p^{(1)}$ . On the other hand, if  $\mathfrak{n}_{n/p} = p$ , since  $\mathfrak{n}_{n/p} - 1 = p - 1 \nmid n/p$  we apply Proposition 8 to obtain that  $p \in \mathfrak{M}_{n/p}$ . Lemma 5 applies and the proof is complete.  $\square$

Proposition 10 above allows us to compute, without great computational effort, all the elements of  $\mathcal{M}_p$  up to the product of  $p$  and the largest known weak primary pseudoperfect number which is today of the order of  $p \cdot 8.49 \times 10^{30}$ . We just have to check if  $S_n(n) \equiv p \pmod{n}$  for every element of  $p\mathcal{W} \cup \mathcal{M}_1$ . Following this idea, we have the following result.

**Proposition 11.** *For every prime  $p \neq 5$ , we have that*

$$[1, p \cdot 8.49 \times 10^{30}] \cap \mathcal{M}_p \subseteq \mathcal{M}_1 \cup p\mathcal{M}_1.$$

The prime  $p = 5$  is exceptional because it is the only known prime for which weak primary pseudoperfect numbers  $Q$  exist satisfying  $\mathfrak{n}_Q = 5$ . Namely,  $\mathfrak{n}_{47058} = \mathfrak{n}_{22214502422} = 5$ . In this case, we obtain the following result.

**Proposition 12.**  $\mathcal{M}_5 \cap [1, 10^{31}] = \{1, 2, 5, 10, 30, 210, 9030, 235290, 11072512110\}$ .

So, while no new weak primary pseudoperfect numbers are found it will not be possible to find more than 10 solutions to the congruence  $S_n(n) \equiv p \pmod{n}$  with prime  $p$ . In other words, to find a solution not lying on the set  $\mathcal{M}_1 \cup p\mathcal{M}_1$  for some prime  $p \neq 5$  would be equivalent to find a new weak primary pseudoperfect number.

#### 4. FURTHER WORK

A natural extension of this work is, of course, to have a closer look at  $\mathcal{M}_m$  with composite  $m$ . In this general case we have an analogue to Theorem 1.

**Theorem 3.** *Let  $m = p_1^{r_1} \cdots p_s^{r_s}$  be an integer and let  $n \in \mathbb{N}$ . Then  $n \in \mathcal{M}_m$  if and only if the following conditions hold:*

- i) *The prime power factorization of  $n$  is given by  $n = q_1 \cdots q_r p_1^{t_1} \cdots p_s^{t_s}$ , with  $0 \leq t_i \leq r_i + 1$ .*
- ii) *For every  $i \in \{1, \dots, r\}$ ,  $q_i - 1$  divides  $n$  and  $n/q_i + m \equiv 0 \pmod{q_i}$ .*
- iii) *For every  $j \in \{1, \dots, s\}$ , if  $0 < t_j \leq r_j$  then  $p_j - 1 \nmid n$ .*
- iv) *For every  $j \in \{1, \dots, s\}$ , if  $t_j = r_j + 1$  then  $p_j - 1 \mid n$  and  $n/p_j^{r_j+1} + 1 \equiv 0 \pmod{p_j}$ .*

*Proof.* Clearly  $n \in \mathcal{M}_m$  if and only if  $S_n(n) \equiv m \pmod{n}$ ; i.e., if and only if  $S_n(n) \equiv m \pmod{q_i}$  for every  $i \in \{1, \dots, r\}$  and  $S_n(n) \equiv m \pmod{q_j^{t_j}}$  for every  $j \in \{1, \dots, s\}$ . To get the proof it is enough to apply Lemma 1 and reason just like in the proof of Theorem 1.  $\square$

This result allows us to construct the set  $\mathcal{M}_m$  for some particular values of  $m$  and to develop algorithms to determine the possible prime divisors of the elements of  $\mathcal{M}_m$  like we have just done in the prime case, but they are not operative. New ideas will have to be developed in order to attack this general situation. In any case, the following conjecture seems plausible.

**Conjecture 1.** *For every  $m \in \mathbb{N}$  the set of solutions to the congruence  $S_n(n) \equiv m \pmod{n}$  is finite.*



## REFERENCES

- [1] Borwein, D.; Borwein, J.M.; Borwein, P.B. and Girgensohn, R. Giuga's Conjecture on Primality. *Amer. Math. Monthly*, 103:40–50, 1996.
- [2] Butske, W.; Jaje, L.M. and Mayernik, D.R. On the equation  $\sum_{P|N} \frac{1}{P} + \frac{1}{N} = 1$ , pseudoperfect numbers, and perfectly weighted graphs. *Math. Comp.*, 69:407–420, 2000.
- [3] Cohen, G.L. and Hagis, P.Jr. On the Number of Prime Factors of  $n$  is  $\phi(n)|(n-1)$ . *Nieuw Arch. Wisk.*, 28:177–185, 1980.
- [4] Giuga, G. Su una presumibile proprietà caratteristica dei numeri primi.. *Ist. Lombardo Sci. Lett. Rend. A*, 83:511–528, 1950.
- [5] Grau, J.M.; Moree, P. and Oller-Marcén, A.M. Solutions of the congruence  $\sum_{k=1}^n k^{f(n)} \equiv 0 \pmod{n}$ . *Math. Nachr.*, to appear, DOI: 10.1002/mana.201500057.
- [6] Grau, J.M; Oller-Marcén, A.M. and Sondow, J. On the congruence  $1^m + 2^m + \cdots + m^m \equiv n \pmod{m}$  with  $n \mid m$  *Monatsh. Math.*, 177:421–436, 2015.

*E-mail address:* maxal@gwu.edu

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE OVIEDO, AVDA. CALVO SOTELLO S/N,  
33007 OVIEDO, SPAIN

*E-mail address:* grau@uniovi.es

CENTRO UNIVERSITARIO DE LA DEFENSA DE ZARAGOZA, CTRA. HUESCA S/N, 50090 ZARAGOZA,  
SPAIN

*E-mail address:* oller@unizar.es