ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$

Max A. Alekseyev [a], José María Grau [b], Antonio M. Oller-Marcén [c,*]

[a] Department of Mathematics, George Washington University, Washington, DC, USA
[b] Departamento de Matematicas, Universidad de Oviedo, Avda. Calvo Sotelo s/n, 33007 Oviedo, Spain
[c] Centro Universitario de la Defensa de Zaragoza, Ctra. Huesca s/n, 50090 Zaragoza, Spain

ARTICLE INFO

Article history:
Received 30 June 2017
Received in revised form 9 April 2018
Accepted 9 May 2018
Available online xxxx

Keywords:
Power sums
Primary pseudoperfect numbers
Algorithm

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 $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$ for every prime p. This characterization leads to an algorithm for computing all such solutions, when there is a finite number of them. More generally, our algorithm enables computing all the solutions below a much higher bound as compared to what can be achieved by a naive exhaustive search.

1. Introduction

There exist many Diophantine equations with "few" known solutions, whose search is hard both from the theoretical and computational points of view. One of the best-known examples is given by the *Erdös–Moser equation* $\sum_{i=1}^{m-1} i^n = m^n$, for which it has been proved [2] that there is only a trivial solution $1^1 + 2^1 = 3^1$ when $m < 1.485 \cdot 10^{9321155}$. Other famous examples include *Giuga's conjecture* [4] stating non-existence of composite numbers n such that $\sum_{i=1}^{n-1} i^n \equiv -1 \pmod{n}$, which has been verified [1] for n up to 10^{13800}; and *Lehmer's totient problem* asking for composite numbers n such that $\varphi(n) \mid (n-1)$, which is shown to have no solutions below 10^{22} or with less than 14 prime divisors [3]. Among equations with "few" known solutions, we can mention $\sum_{p|N} \frac{1}{p} - \frac{1}{N} \in \mathbb{N}$ with only 12 known solutions called *Giuga numbers* (sequence A007850 in the OEIS [9]) and $\sum_{p|N} \frac{1}{p} + \frac{1}{N} = 1$ with only 8 known solutions (sequence A054377 in the OEIS [9]) called *primary pseudoperfect numbers* [2].

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, for the equation $1^n + 2^n + \cdots + n^n \equiv 19 \pmod{n}$ that we will show to have exactly 8 solutions, namely $\{1, 2, 6, 19, 38, 114, 798, 34314\}$.

For positive integers k, n, we define $S_k(n) := \sum_{i=1}^{n} i^k$. We will deal with congruences of the form

$$S_n(n) \equiv a \pmod{n}, \tag{1}$$

* Corresponding author.
E-mail addresses: maxal@gwu.edu (M.A. Alekseyev), grau@uniovi.es (J.M. Grau), oller@unizar.es (A.M. Oller-Marcén).

https://doi.org/10.1016/j.dam.2018.05.022
0166-218X/

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

Table 1
Values of a and the sequence indices corresponding to $\mathcal{M}_a$ that are currently present in the OEIS [9]. The stars indicate when $\mathcal{M}_a$ is known to be finite. Finiteness of $\mathcal{M}_p$ for primes $p \in \{2, 3, 7, 19, 43, 79, 193\}$ as well as for p satisfying Theorem 3 is established in the present work.

a	0*	1*	2*	3*	4	5	6
Index	A005408	A014117	A226960	A226961	A226962	A226963	A226964
a	7*	8	9	19*	43*	79*	193*
Index	A226965	A226966	A226967	A280041	A280043	A302343	A302344

which is equivalent to $S_n(n-1) \equiv a \pmod{n}$. The following lemma shows that congruences (1) is also equivalent to

$$n \cdot B_n \equiv a \pmod{n}, \tag{2}$$

where B_n is the nth Bernoulli number. [1]

Lemma 1. *For any positive integer n,*

$$S_n(n) \equiv n \cdot B_n \pmod{n}.$$

Proof. By Faulhaber's formula, we have

$$S_n(n) = \frac{1}{n+1} \sum_{j=0}^{n} (-1)^j \cdot \binom{n+1}{j} \cdot B_j \cdot n^{n+1-j}, \tag{3}$$

where by convention $B_1 = -\frac{1}{2}$. In particular, for $j = 1$, we have that the numerator of $B_j n^{n+1-j} = -\frac{n^n}{2} \equiv 0 \pmod{n}$. For any odd $j \neq 1$, we have $B_j = 0$, and thus the corresponding term in (3) is zero as well.

Consider an even j. The Von Staudt–Clausen theorem implies the denominator of B_j is square-free (in fact, it equals the product of all primes p such that $(p-1) \mid j$) [7]. It follows that the denominator of $B_j \cdot n$ is coprime to n, and thus $B_j \cdot n^{n+1-j} \equiv 0 \pmod{n^{n-j}}$. Hence, $B_j \cdot n^{n+1-j} \equiv 0 \pmod{n}$ for all $j < n$. Now reduction of (3) modulo n completes the proof. □

Let $\mathcal{M}_a$ denote the set of positive n satisfying (1) and (2) (Table 1). From the Von Staudt–Clausen theorem, it is easy to see that $\mathcal{M}_0$ consists of the odd positive integers. It is known [6,8] that $\mathcal{M}_1 = \{1, 2, 6, 42, 1806\}$.

In the present study, we focus on the case of a being prime and address the problem of computing $\mathcal{M}_a$. We encounter both aforementioned situations: in some cases, we are able to compute all the solutions to (1) (and thus prove the finiteness of $\mathcal{M}_a$), while in other cases, we find all solutions below certain large bounds (which are infeasible to reach by brute force).

The main contribution of our work is the characterization of the solutions to the congruence (1) and the development of an algorithm for computing the possible prime divisors of the solutions. Then, if the set of possible prime divisors is finite, the search for solutions can be restricted to products of these divisors and thus determine all the solutions. Furthermore, we establish a connection of this problem to *weak primary pseudoperfect numbers*, which enables computing all the solutions below 10^{30} with little computational effort.

2. Characterization of $\mathcal{M}_p$

The following lemma will be useful in the sequel.

Lemma 2 ([5]). *Let d, k, n, and t be positive integers.*

(i) *If $d \mid n$, then*

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

(ii) *If $p > 2$ is a prime, 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*

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

[1] The congruence $r_1 \equiv r_2 \pmod{n}$ for rational numbers r_1, r_2 is understood as n divides the numerator of $r_1 - r_2$.

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

The following 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 has form $n = p^s q_1 \cdots q_r$, where $p, q_1, \ldots, q_r$ are pairwise distinct primes and $0 \le s \le 2$.*
(ii) *For every $i \in \{1, \ldots, r\}$, $(q_i - 1) \mid n$ 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 case of odd p; for $p = 2$, the proof is similar.

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 $S_n(n) \equiv p \pmod{q_i^{u_i}}$ for all $i \in \{1, \ldots, r\}$.

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

Furthermore, by Lemma 2(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 2(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 $n/p^2 + 1 \equiv 0 \pmod{p^{s-1}}$, with the latter congruence being possible only if $s \le 2$.

Finally, by Lemma 2(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 $p \ne q_i$, it follows from Lemma 2(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 the latter congruence being possible only if $u_i \le 1$. □

Theorem 1 motivates us to consider a decomposition $\mathcal{M}_p = \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$, where

$$\mathcal{M}_p^{(0)} = \{n \in \mathcal{M}_p \,:\, p \nmid n\},$$
$$\mathcal{M}_p^{(1)} = \{n \in \mathcal{M}_p \,:\, p \,||\, n\},$$
$$\mathcal{M}_p^{(2)} = \{n \in \mathcal{M}_p \,:\, p^2 \,||\, n\}.$$

We will now study each of these sets separately, using the following results.

Lemma 3 ([6]). *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 4 ([6]). *Let $\mathcal{N}$ be a set of positive integers ν such that*

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

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

Lemma 4 implies the following result concerning $\mathcal{M}_p^{(0)}$.

Lemma 5. *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 4 and the result follows. □

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

Lemma 6. *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 with p.

Definition 1. For a prime p, we let $\mathcal{Q}_p$ be the set of prime numbers such that $q \in \mathcal{Q}_p$ 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 composed of primes in $\mathcal{Q}_p$:

$$\mathcal{N}_p := \{n \in \mathbb{N} \,:\, n \text{ is square-free}, (p-1) \nmid n, \text{and for every prime } q \mid n,\ q \in \mathcal{Q}_p\}. \tag{4}$$

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

Corollary 1. *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 implies that $n/p \in \mathcal{N}_p$ completing the proof. □

Finally, let us analyze 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 7. *Let $n \in \mathcal{M}_p^{(2)}$. If $q < p$ is a prime such that $q \mid n$, then $q \in \{2, 3, 7, 43\}$.*

Proof. Let us consider the set of primes $\{q : q < p \text{ and } q \mid n \text{ for some } n \in \mathcal{M}_p^{(2)}\}$. Theorem 1 implies that this set satisfies the conditions of Lemma 3, completing the proof. □

Corollary 2. *For any prime $p \notin \{2, 3, 7, 43\}$, the set $\mathcal{M}_p^{(2)}$ 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, for the set of primes $S := \{q : q \mid (p-1)\}$, Lemma 7 implies that $S \subseteq \{2, 3, 7, 43\}$. Thus, p is a prime such that $p-1$ is square-free with prime divisors from the set $\{2, 3, 7, 43\}$. It is easy to see that the only such primes are precisely $\{2, 3, 7, 43\}$. □

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

Corollary 3. *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 $S := \{q : q \neq p,\ q \mid n \text{ for some } n \in \mathcal{M}_p^{(2)}\}$. Theorem 1 implies that the set $S \cup \{p\}$ satisfies the conditions of Lemma 3, and hence $S \cup \{p\} \subseteq \{2, 3, 7, 43\}$, i.e., $S \subsetneq \{2, 3, 7, 43\}$. Now, the statement follows from the fact that every element in $\mathcal{M}_p^{(2)}$ is of the form $p^2 q_1 \cdots q_r$, where each $q_i \in S$. □

Corollary 4. *Let p be a prime. Then*

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

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

Corollary 5.

$$\mathcal{M}_7 = \{1, 2, 6, 7, 14, 294, 12642\},$$
$$\mathcal{M}_{43} = \{1, 2, 6, 42, 43, 86, 258, 77658\}.$$

3. Algorithm for computing $\mathcal{Q}_p$ and $\mathcal{M}_p$

Although Theorem 1 gives a complete characterization of the set $\mathcal{M}_p$ for a prime p, from a practical point of view, Corollary 4 is more useful for effective computation of this set. In particular, Corollary 4 implies that in order to compute $\mathcal{M}_p$, it is enough to compute the set of primes $\mathcal{Q}_p$. Below we propose Algorithm 1 that in the case of finite $\mathcal{Q}_p$ constructs it in a finite number of steps. Namely, for an input prime p, Algorithm 1 constructs a nested sequence of sets $X_1[p] \subseteq X_2[p] \subseteq \ldots$. If this sequence stabilizes, the algorithm returns the limiting set denoted $\mathfrak{X}[p]$, which equals $\mathcal{Q}_p \cup \{p\}$ as we show in Theorem 2.

In Algorithm 1, PrimeParts(S) is defined as the set of primes in the set

$$\text{AllParts}(S) := \{1 + t : t = \prod_{q \in T} q \text{ for some } T \subseteq S,\ (p-1) \nmid t\}.$$

Algorithm 1 Computing the set $\mathfrak{X}[p]$ for a given prime p.

```
Let X_1[p] := {2, p}
for i = 1, 2, 3, ... do
    X_{i+1}[p] := X_i[p] ∪ PrimeParts(X_i[p])
    if X_{i+1}[p] = X_i[p] then
        return 𝔛[p] := X_i[p]
    end if
end for
```

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

Theorem 2. *For every $i \geq 1$, we have that $X_i[p] \subseteq \mathcal{Q}_p \cup \{p\}$. Moreover, Algorithm 1 stops if and only if $\mathcal{Q}_p$ is finite, in which case $\mathfrak{X}[p] = \mathcal{Q}_p \cup \{p\}$.*

Proof. Let $\mathcal{Q}'_p = \mathcal{Q}_p \cup \{p\}$. Clearly, $X_1[p] \subseteq \mathcal{Q}'_p$. Let us assume that there exists an index $i \geq 2$ such that $X_{i-1}[p] \subseteq \mathcal{Q}'_p$, but $X_i[p] \not\subseteq \mathcal{Q}'_p$. Consider the minimum element q in $X_i[p] \setminus \mathcal{Q}'_p$. Since q does not belong to $\mathcal{Q}'_p$, but $q-1$ is squarefree and $(p-1) \nmid (q-1)$, there exists a prime factor q_1 of $q-1$ that is not in $\mathcal{Q}'_p$ and thus not in $X_{i-1}[p]$ either. This contradicts the fact that every element of $X_i[p] \setminus \{2, p\}$ is of the form $1 + p_1 \cdots p_k$ with $p_j \in X_{i-1}[p]$. Hence, $X_i[p] \subseteq \mathcal{Q}'_p$ for every $i \geq 1$ as claimed.

Now, Algorithm 1 constructs sets $X_1[p] \subseteq X_2[p] \subseteq \ldots$, which are all subsets $\mathcal{Q}'_p$. So, if $\mathcal{Q}_p$ is finite (and so is $\mathcal{Q}'_p$), the algorithm stops and returns the limiting set $\mathfrak{X}[p]$. Let us show that $\mathfrak{X}[p] = \mathcal{Q}'_p$. If $\mathfrak{X}[p] \subsetneq \mathcal{Q}'_p$, consider the minimum element q in $\mathcal{Q}'_p \setminus \mathfrak{X}[p]$. Then $q-1 = q_1 \cdots q_r$ is squarefree, where $q_i \in \mathcal{Q}'_p$. Since each $q_i < q$, the definition of q implies that $q_i \in \mathfrak{X}[p]$. Hence, $q = 1 + q_1 \cdots q_r \in \mathfrak{X}[p]$, since otherwise Algorithm 1 would have not stopped. This contradicts the assumption of $\mathcal{Q}'_p \setminus \mathfrak{X}[p]$ being nonempty, and thus completes the proof. □

Once the set $\mathcal{Q}_p$ is obtained, one can easily compute $\mathcal{N}_p = \textsc{AllParts}(\mathcal{Q}_p)$, and then use Corollary 4 to find $\mathcal{M}_p$. Some interesting examples computed with Algorithm 1 are given in the following table.

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}

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

Theorem 3. *Let $A := \{2, 6, 14, 42, 86, 258, 602, 1806\}$ be the set of even divisors of $1806 = 2 \cdot 3 \cdot 7 \cdot 43$. If a prime p is such that the set*

$$\{1 + \alpha p \ : \ \alpha \in A\}$$

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

Proof. It is easy to see that primes $p \in \{2, 3, 7, 43\}$ do not satisfy the condition as numbers $1 + 2 \cdot 2$, $1 + 2 \cdot 3$, $1 + 6 \cdot 7$, and $1 + 1806 \cdot 43$ are prime. On the other hand, for a prime $p \notin \{2, 3, 7, 43\}$ satisfying the theorem condition, Algorithm 1 returns $\mathfrak{X}[p] = \{2, 3, 7, 43, p\}$, implying that $\mathcal{Q}_p = \{2, 3, 7, 43\}$. Then the theorem statement follows from (4) and Corollary 4. □

There seem to exist many primes p satisfying the condition of Theorem 3 (sequence A302345 in the OEIS [9]). For example, the only such primes below 1000 are

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

We remark that there also exist primes p, for which $\mathcal{Q}_p$ and $\mathcal{M}_p$ are finite but do not satisfy the condition of Theorem 3. In particular, this holds for $p \in \{19, 79, 193\}$ present in the table above.

Unfortunately, in some cases we cannot determine if Algorithm 1 stops due to the size of the involved sets of primes. For instance, for $p = 5$, the set $X_5[p]$ contains 77 primes, and it seems infeasible to compute $X_6[p]$.

4. Connection between $\mathcal{M}_p$ and primary pseudoperfect numbers

When $\mathcal{Q}_p$ is infinite, Algorithm 1 never stops. Nevertheless, there is an easy result that allows us to compute the elements of $\mathcal{M}_p$ below $p \cdot (8.49 \times 10^{30})$ as explained below.

We recall that an integer $n \geq 1$ is a *weak primary pseudoperfect number* [6] if it satisfies the congruence:

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

Let $\mathcal{W}$ be the set of all weak primary pseudoperfect numbers (sequence A230311 in the OEIS [9]). The only known elements of $\mathcal{W}$ are

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

It is not even known if $\mathcal{W}$ is finite.

Corollary 6. *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 $n \in \mathcal{M}_1$ by Lemma 5. On the other hand, if $p \mid n$, [6, Corollary 1] states that $n/p \in \mathcal{W}$. □

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

Corollary 6 enables computing all the elements of $\mathcal{M}_p$ below $p \cdot \max \mathcal{W}$. It is enough to determine computationally if $S_n(n) \equiv p \pmod{n}$ for every element of $\mathcal{M}_1 \cup p \cdot \mathcal{W}$, which currently has up to 14 known 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

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

If $\mathfrak{M}_Q \neq \emptyset$, then $Q \in \mathcal{W}$ ([6, Corollary 1]), and furthermore we have the following statement.

Theorem 4 (*[6, Proposition 3]*). *For a given weak primary pseudoperfect number Q, define the integer*

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

Then $\mathfrak{M}_Q = \emptyset$ if and only if $(q-1) \mid \mathfrak{n}_Q Q$ 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 8. *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 $p \in \mathfrak{M}_{n/p}$.*

While it seems to be plausible that the set $\mathcal{M}_p$ is finite for every prime p, there are many primes p for which Algorithm 1 fails to prove its finiteness. Nevertheless, in the previous setting, we can directly prove the finiteness of $\mathcal{M}_p$ for $p = 2$ and 3.

Corollary 7. *If $p \in \{2, 3\}$, then $\mathcal{M}_p$ is finite.*

Proof. By Lemma 5 and Corollary 4, it is enough to show that $\mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$ is finite. Let us assume that $n \in \mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)}$, and observe that $n/p \in \mathcal{W}$ and $p \in \mathfrak{M}_{n/p}$ by Lemma 8.

Let $p = 2$ with $n/2 \in \mathcal{W}$ and $2 \in \mathfrak{M}_{n/2}$. Then Theorem 4 implies that $\mathfrak{n}_{n/p} \mid 2$, i.e., $\mathfrak{n}_{n/2} = 1$ or 2. Now, if $\mathfrak{n}_{n/2} = 2$, Theorem 4 implies that $\mathfrak{M}_{n/2} = \emptyset$, 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 $n/2 \in \mathcal{M}_1$ by Lemma 4. Consequently, $\mathcal{M}_p^{(1)} \cup \mathcal{M}_p^{(2)} \subseteq 2 \cdot \mathcal{M}_1$ is finite and so is $\mathcal{M}_2 \subseteq \mathcal{M}_1 \cup 2 \cdot \mathcal{M}_1$.

Now, 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 $n \neq 3$, Theorem 1 implies that $(q-1) \mid n$ for every prime $q \mid n/3$. In particular, $2 \mid n$ and thus $2 \mid n/3$, so Theorem 4 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. □

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

Corollary 8.

$$\mathcal{M}_2 = \{1, 4, 12, 84, 3612\},$$
$$\mathcal{M}_3 = \{1, 2, 3, 18, 126, 5418\}.$$

In Corollary 5 and Corollary 8, we have established the finiteness and computed the elements of $\mathcal{M}_p$ for $p = 2, 3, 7, 43$. Recall that these are precisely the cases when $\mathcal{M}_p^{(2)}$ may be nonempty. In the remaining cases, $\mathcal{M}_p = \mathcal{M}_p^{(0)} \cup \mathcal{M}_p^{(1)}$. We will conclude this section with a characterization of $\mathcal{M}_p^{(1)}$ for $p \neq 2, 3, 7, 43$.

Lemma 9. *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. The statement directly follows from Theorem 1 and the definition of $\mathcal{M}_p^{(1)}$. □

Corollary 9. *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 $n \in \mathcal{M}_p^{(1)}$. By Lemma 8, $n/p \in \mathcal{W}$ and $p \in \mathfrak{M}_{n/p}$. Hence, $\mathfrak{M}_{n/p} \neq \emptyset$. By Theorem 4, $\mathfrak{n}_{n/p} \mid p$ 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 similarly to the second part of the proof of Corollary 7, we obtain that $n \in p \cdot \mathcal{M}_1 \subset \mathcal{M}_p^{(1)}$. On the other hand, if $\mathfrak{n}_{n/p} = p$, then $\mathfrak{n}_{n/p} - 1 = p - 1 \nmid n/p$, and Theorem 4 implies that $p \in \mathfrak{M}_{n/p}$. Then application of Lemma 8 completes the proof. □

Corollary 9 enables computing (with little effort) all the elements of $\mathcal{M}_p$ below the product of p and the largest known weak primary pseudoperfect number, which today gives the bound $p \cdot 8.49 \times 10^{30}$. It just remains to check if $S_n(n) \equiv p \pmod{n}$ for every element of $p\mathcal{W} \cup \mathcal{M}_1$. Implementing this idea, we obtain the following result.

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.

Corollary 10. *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, since it is the only known prime p for which there exist weak primary pseudoperfect numbers Q satisfying $\mathfrak{n}_Q = p$. Namely, we have $\mathfrak{n}_{47058} = \mathfrak{n}_{2214502422} = 5$. For prime $p = 5$, we obtain the following result:

Corollary 11.

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

So, unless new weak primary pseudoperfect numbers are found, it is impossible to find more than 10 solutions to the congruence $S_n(n) \equiv p \pmod{n}$ with prime p. In other words, for a prime $p \neq 5$, finding a solution not from the set $\mathcal{M}_1 \cup p\mathcal{M}_1$ is equivalent to finding a new weak primary pseudoperfect number.

5. 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 the following analogue of Theorem 1.

Theorem 5. *Let $m = p_1^{r_1} \cdots p_s^{r_s}$ be an integer, where $p_1, \ldots, p_s$ are pairwise distinct primes, $r_1, \ldots, r_s$ are positive integers. A positive integer n belongs to $\mathcal{M}_m$ if and only if the following conditions hold:*

(i) *The prime power factorization of n is given by $n = q_1 \cdots q_r p_1^{t_1} \cdots p_s^{t_s}$, where $q_1, \ldots, q_r$ are pairwise distinct primes not from $\{p_1, \ldots, p_s\}$.*
(ii) *For every $j \in \{1, \ldots, r\}$, $(q_j - 1) \mid n$ and $n/q_j + m \equiv 0 \pmod{q_j}$.*
(iii) *For every $i \in \{1, \ldots, s\}$, we have $t_i \in \{0, r_i, r_i + 1\}$. Furthermore, if $t_i = r_i$, then $(p_i - 1) \nmid n$; and if $t_i = r_i + 1$, then $(p_i - 1) \mid n$ and $n/p_i^{r_i+1} + 1 \equiv 0 \pmod{p_i}$.*

Proof. Clearly, $n \in \mathcal{M}_m$ if and only if $S_n(n) \equiv m \pmod{q_j}$ for every $j \in \{1, \ldots, r\}$ and $S_n(n) \equiv m \pmod{p_i^{t_i}}$ for very $i \in \{1, \ldots, s\}$. It remains to apply Lemma 2 and argue just like in the proof of Theorem 1. □

Theorem 5 enables construction of the set $\mathcal{M}_m$ for some particular values of m as well as developing algorithms for computing the possible prime divisors of the elements of $\mathcal{M}_m$ (similarly to how we have done so 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] D. Borwein, J.M. Borwein, P.B. Borwein, R. Girgensohn, Giuga's conjecture on primality, Amer. Math. Monthly 103 (1) (1996) 40–50.
[2] W. Butske, L.M. Jaje, D.R. Mayernik, On the equation $\sum_{P|N} \frac{1}{P} + \frac{1}{N} = 1$, pseudoperfect numbers, and perfectly weighted graphs, Math. Comp. 69 (2000) 407–420.
[3] G.L. Cohen, P. Hagis Jr., On the number of prime factors of n is $\varphi(n) \mid (n-1)$, Nieuw Arch. Wiskd. 28 (1980) 177–185.
[4] G. Giuga, Su una presumibile propertieta caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. A 83 (1950) 511–528.
[5] J.M. Grau, P. Moree, A.M. Oller-Marcén, Solutions of the congruence $1 + 2^{f(n)} + \cdots + n^{f(n)} \equiv 0 \pmod{n}$, Math. Nachr. 289 (7) (2016) 820–830.
[6] J.M. Grau, A.M. Oller-Marcén, J. Sondow, On the congruence $1^m + 2^m + \cdots + m^m \equiv n \pmod{m}$ with $n \mid m$, Monatsh. Math. 177 (3) (2015) 421–436.
[7] B.C. Kellner, J. Sondow, Power-sum denominators, Amer. Math. Monthly 124 (8) (2017) 695–709.
[8] J. Sondow, K. MacMillan, Reducing the Erdös–Moser equation $1^n + 2^n + \cdots + k^n = (k+1)^n$ modulo k and k^2, Integers 11 (2011) #A34.
[9] The OEIS Foundation, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://oeis.org, 2018.

Please cite this article in press as: M.A. Alekseyev, et al., Computing solutions to the congruence $1^n + 2^n + \cdots + n^n \equiv p \pmod{n}$, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.05.022.