Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 3, 516–529
DOI: 10.7546/nntdm.2024.30.3.516-529

The congruence $x^n \equiv -a^n \pmod{m}$: Solvability and related OEIS sequences

Jorma K. Merikoski[1], **Pentti Haukkanen**[2] **and Timo Tossavainen**[3]

[1] Faculty of Information Technology and Communication Sciences,
Tampere University
FI-33014 Tampere, Finland
e-mail: jorma.merikoski@tuni.fi

[2] Faculty of Information Technology and Communication Sciences,
Tampere University
FI-33014 Tampere, Finland
e-mail: pentti.haukkanen@tuni.fi

[3] Department of Arts, Communication and Education,
Lulea University of Technology
SE-97187 Lulea, Sweden
e-mail: timo.tossavainen@ltu.se

Received: 24 May 2024 **Revised:** 15 September 2024
Accepted: 29 September 2024 **Online First:** 30 September 2024

Abstract: We study the solvability of the congruence $x^n \equiv -a^n \pmod{m}$, where $n, m \in \mathbb{Z}_+$, $a \in \mathbb{Z}$, and $\gcd(a, m) = 1$. Our motivation arises from computer experiments concerning a geometric property of the roots of the congruence $x^n + y^n \equiv 0 \pmod{p}$, where $n \in \mathbb{Z}_+$ and $p \in \mathbb{P}$. We encounter several OEIS sequences. We also make new observations on some of them.
Keywords: Congruence of powers, Integer sequence, Experimental geometry.
2020 Mathematics Subject Classification: 11A07, 11B83, 11Y99, 51M04.

1 Introduction

All variables and constants written by lower case letters are integer-valued. As suggested by Graham, Knuth, and Patashnik [6, p. 115], $x \perp y$ denotes that x and y are coprime.

1.1 Mustonen's experiments

Mustonen [9] experimentally studied with the computing environment *Survo* [8] the congruence

$$x^n + y^n \equiv 0 \pmod{p}, \tag{1}$$

where $n > 0$ and $p \in \mathbb{P}$. He observed the following.

1. All its roots are in a set L of parallel equidistant lines with $\gcd(n, p-1)$ different slopes.
2. All integer points of L are roots.
3. Each nontrivial root (that is, $p \nmid x, y$) lies on exactly one line.

We tried without success to prove these observations. As a promising step in this direction. we were able to solve (1) by the following procedure.

Step 1. Fix a with $p \nmid a$.

Step 2. Substitute $y = a$ in (1).

Step 3. Solve x.

Step 4. Go through all a's.

Unfortunately, we obtained a quite complex formula (not given here), and we could not go ahead. So, we must leave this problem open.

1.2 Solvability of (1)

Instead, we succeeded to give a complete description on the solvability of (1), and, more generally, on that of

$$x^n + y^n \equiv 0 \pmod{m},$$

where $n, m > 0$. An equivalent problem (see the above procedure) concerns the solvability of the congruence

$$x^n \equiv -a^n \pmod{m}, \tag{2}$$

where $a \perp m$. This is the topic of our paper.

When referring to (2), *we assume its background* ($n, m > 0$ *and* $a \perp m$).

We need to do nothing if $n = 1$, and all congruences are solvable if $m = 1$, but we include these trivial cases for completeness.

If n is odd, then (2) is solvable, because the trivial solution $x \equiv -a \pmod{m}$ always exists. But what about the nontrivial solvability, i.e., the existence of nontrivial roots $x \not\equiv -a \pmod{m}$? If n is even, then the answer is easy.

Theorem 1.1. *If n is even and the congruence (2) is solvable, then the following conditions are equivalent.*

(a) *All possible roots of (2) are nontrivial.*

(b) $m > 2$.

Proof. All congruences are modulo m.

(b)⇒(a). Let $x^n \equiv -a^n$. We show that $x \not\equiv -a$. If $x \equiv -a$, then, since n is even, also $x^n \equiv a^n$. Therefore $a^n \equiv -a^n$, and further $2a^n \equiv 0$, i.e., $m \mid (2a^n)$. Since $a \perp m$, it follows that $m \mid 2$, contradicting (b).

¬(b)⇒ ¬(a). If $m = 1$, then any x is a trivial root of (2). If $m = 2$, then, since a is odd and $x^n = -a^n$, also x is odd and hence trivial. □

We study the solvability and nontrivial solvability of (2) in Sections 3–4, present some further results in Section 5, and complete our paper with discussion in Section 6. Many OEIS sequences [11] relate to our topics. We consider some of them.

2 Preliminaries

We need certain well-known results. Our primary reference is Apostol [1], but we also use Lozano-Robledo [7].

2.1 Euler's totient

Let us begin with Euler's totient $\phi(m)$.

Lemma 2.1. [1, Theorem 2.5] *Let $p \in \mathbb{P}$ and $\alpha > 0$. If $p \neq 2$, then*

$$\phi(p^\alpha) = p^{\alpha-1}(p-1) = \phi(2p^\alpha).$$

If $p = 2$, then the first equation holds, while the second does not.

Lemma 2.2. [1, Theorem 10.10c] *If $m > 2$, then*

$$\operatorname{ind}(-1) = \frac{\phi(m)}{2},$$

where ind *stands for the index modulo m (to a given base).*

There are several OEIS sequences on Euler's totient. We introduce one of them.

A023022. a_t is the number of expressions of t as a sum of two positive, relatively prime numbers. For example, $15 = 14 + 1 = 13 + 2 = 11 + 4 = 8 + 7$, so $a_{15} = 4$. If $t > 2$, then $a_t = \phi(t)/2$. Thus we have a comment to add: if $t > 2$, then $a_t = \operatorname{ind}(-1)$ modulo t.

2.2 Primitive roots

Studying (2) becomes easier if m has a primitive root (i.e., there is a primitive root modulo m).

Lemma 2.3. [1, p. 212] *The set of positive numbers having a primitive root is*

$$R = H \cup K,$$

where

$$H = \{1, 2, 4\}, \quad K = \{up^\gamma : u \in \{1, 2\},\ 2 \neq p \in \mathbb{P},\ \gamma > 0\}. \tag{3}$$

We consider also the larger set

$$\tilde{H} = \{2^\gamma : \gamma \geqslant 0\}.$$

A033948. a_t is the t-th positive integer having a primitive root.

A001918. a_t is the smallest positive primitive root modulo the t-th prime.

2.3 Congruences

We apply Lemma 2.4 if $m \in R$, and Lemma 2.5 in the general case.

Lemma 2.4. [7, Theorem 8.6.11] *Let $n > 0$, $m \in R$, and $c \perp m$. The following conditions are equivalent.*

(a) *The congruence $x^n \equiv c \pmod m$ is solvable.*

(b) $c^{\frac{\phi(m)}{d}} \equiv 1 \pmod m$, *where* $d = \gcd(n, \phi(m))$.

If the congruence in (a) *is solvable, then it has* (*precisely*) d (*pairwise*) *incongruent roots.*

Lemma 2.5. [1, Theorem 5.28] *Let f be a polynomial with integer coefficients, and let $m_1, \ldots, m_k > 0$ be* (*pairwise*) *coprime. The congruence*

$$f(x) \equiv 0 \pmod{m_1 \cdots m_k}$$

is solvable if and only if all congruences

$$f(x) \equiv 0 \pmod{m_1}, \ \ldots, \ f(x) \equiv 0 \pmod{m_k}$$

are solvable. Moreover,

$$\nu(m_1 \cdots m_k) = \nu(m_1) \cdots \nu(m_k),$$

where $\nu(l)$ denotes the number of (*pairwise*) *incongruent roots of the congruence $f(x) \equiv 0 \pmod l$.*

3 Solvability of (2)

If n is odd, then, as already said in the Introduction, the congruence (2) is solvable. We can therefore assume that

throughout this section, $n(> 0)$ is even.

Actually, most of our results are trivially true also for odd n.

3.1 The case $m \in K$

We find convenient to use Lemma 2.4 only for $m \in K$, and tie $m \in H$ to the case $m \in \tilde{H}$.

Theorem 3.1. *Let $m = up^\gamma \in K$ as in (3), $d = \gcd(n, \phi(m))$, and*

$$n = 2^k l, \quad \phi(m) = 2^i j, \quad 2 \nmid l, j. \tag{4}$$

The following conditions are equivalent:

(a) *The congruence (2) is solvable.*

(b) $d \mid \phi(m)/2$.

(c) $k \leqslant i - 1$.

(d) $p \equiv 1 \pmod{2^{k+1}}$.

Proof. The congruences are modulo m.

(a)⇔(b). By simple calculation and the Euler–Fermat theorem [1, Theorem 5.17], we obtain

$$(-a^n)^{\frac{\phi(m)}{d}} = (-1)^{\frac{\phi(m)}{d}} a^{\frac{n\phi(m)}{d}} = (-1)^{\frac{\phi(m)}{d}} (a^{\phi(m)})^{\frac{n}{d}} \equiv (-1)^{\frac{\phi(m)}{d}} \cdot 1^{\frac{n}{d}} = (-1)^{\frac{\phi(m)}{d}}.$$

Consequently,

$$(-a^n)^{\frac{\phi(m)}{d}} \equiv 1 \iff \frac{\phi(m)}{d} \text{ is even},$$

verifying the claim by Lemma 2.4.

(b)⇔(c). Since

$$d = \gcd(2^k l, 2^i j) = 2^{\min(k,i)} \gcd(l, j),$$

it follows that

$$d \mid \frac{\phi(m)}{2} \iff d \mid 2^{i-1} j \iff k \leqslant i - 1.$$

(c)⇔(d). By (4) and Lemma 2.1,

$$2^i j = \phi(m) = p^{\gamma-1}(p - 1).$$

Therefore,

$$i \geqslant k + 1 \iff 2^{k+1} \mid (p - 1),$$

completing the proof. □

Remark 3.1. Let $n = 2$, $a = 1$, and $2 \neq p \in \mathbb{P}$. Then (a) with $m = p$ states that -1 is a quadratic residue modulo p. The Legendre symbol

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$$

[1, Theorem 9.4], which is just (d).

Remark 3.2. Dence and Dence [2, Corollary 7.2] studied the case $n = 4$.

Corollary 3.1. *Let $m \in K$. The following conditions are equivalent.*

(a) *The congruence (2) is solvable for some a.*

(b) *The congruence (2) is solvable for any a.*

Proof. The conditions (b)–(d) in Theorem 3.1 do not depend on a. □

Corollary 3.2. *Let* $2 \neq p \in \mathbb{P}$ *and*

$$K_p = \{up^\gamma : u \in \{1, 2\}, \gamma > 0\}.$$

The following conditions are equivalent.

(a) *The congruence* (2) *is solvable modulo some* $m \in K_p$*.*

(b) *The congruence* (2) *is solvable modulo any* $m \in K_p$*.*

Proof. The conditions (b)–(d) of Theorem 3.1 do not depend on u and γ. □

Corollary 3.3. *Let* $m = up^\gamma \in K$ *be as in* (3)*. The following conditions are equivalent.*

(a) *The congruence* (2) *is solvable.*

(b) *The congruence* $x^n \equiv -1 \pmod{p}$ *is solvable.*

Proof. Apply Corollaries 3.1 and 3.2. □

When studying the solvability of (2) with $m = up^\gamma \in K$, the congruence

$$x^n \equiv -1 \pmod{p} \tag{5}$$

is therefore enough.

Theorem 3.2. *The congruence* (5) *is solvable for infinitely many* p*'s.*

Proof. Let $n = 2^k l$ be as in (4). By Dirichlet's theorem on arithmetic progressions [1, Theorem 7.9], there are infinitely many primes of the form $p = 2^{k+1}t + 1$. All they apply by Theorem 3.1. □

3.2 More OEIS sequences

The condition (d) of Theorem 3.1 with $k = 1$ yields the primes satisfying

$$p \equiv 1 \pmod{4}, \tag{6}$$

and with $k = 2$ those satisfying

$$p \equiv 1 \pmod{8}. \tag{7}$$

A002144. a_t is the t-th prime of the form (6).

A080109. The above sequence squared termwise.

A002314. a_t is the smallest positive root of (5), where $n = 2$ and m is the t-th term of A002144.

A007519. a_t is the t-th prime of the form (7).

A218028. a_t is the smallest positive root of (5), where $n = 4$ and m is the t-th term of A007519.

We also introduce a quite curious sequence.

A262998. a_t is the t-th positive composite number satisfying

$$1^{\phi(m)} + 2^{\phi(m)} + \cdots + \phi(m)^{\phi(m)} \equiv \phi(m) \pmod{m}.$$

This sequence contains all numbers $2p$, where $p \in \mathbb{P}$ satisfies (6), but has also some other terms. Only five of them are known: $320, 480, 22113, 44226, 66339$.

3.3 The case $m \in \tilde{H}$

This case is easy.

Theorem 3.3. *If $m \in \tilde{H}$, then the following conditions are equivalent.*

(a) *The congruence (2) is solvable.*

(b) $m \in \{1, 2\}$.

Proof. (b)⇒(a). Trivial.

¬(b)⇒ ¬(a). Let $n = 2h$. The case $m = 4$ is enough. Since a $(\perp 4)$ is odd, $a = 2t + 1$ for some t. If

$$x^n + a^n \equiv 0 \pmod 4,$$

then also x must be odd, $x = 2s + 1$. But now,

$$x^n + a^n = (2s + 1)^{2h} + (2t + 1)^{2h} \equiv 2 \pmod 4,$$

implying wrongly that $2 \equiv 0 \pmod 4$. □

Remark 3.3. Corollaries 3.1 and 3.3 hold also for $m \in \tilde{H}$. All their statements are by Theorem 3.3 true if $m = 1, 2$, and false otherwise.

Remark 3.4. Dence and Dence [3] studied the congruence $x^n \equiv c \pmod{2^\gamma}$ with $n = 2, 3, 4$.

3.4 The case $m > 0$

Theorem 3.4. *Let $m > 0$, and let $n = 2^k l$ be as in (4). The following conditions are equivalent.*

(a) *The congruence (2) is solvable.*

(b) *$4 \nmid n$, and any odd prime factor p of m satisfies*

$$p \equiv 1 \pmod{2^{k+1}}. \tag{8}$$

Proof. Let

$$m = 2^\alpha p_1^{\alpha_1} \cdots p_h^{\alpha_h}, \tag{9}$$

where $\alpha \geqslant 0$, $\alpha_1, \ldots, \alpha_h > 0$, and $p_1, \ldots, p_h$ are (distinct) odd primes. The "empty product" $(h = 0)$ equals one.

By Lemma 2.5, (a) holds if and only if all congruences

$$x^n \equiv -a^n \pmod{2^\alpha},\ x^n \equiv -a^n \pmod{p_1^{\alpha_1}},\ \ldots,\ x^n \equiv -a^n \pmod{p_h^{\alpha_h}}$$

are solvable. By Theorem 3.3, the first one is solvable if and only if $\alpha < 2$, i.e., $4 \nmid m$. By Theorem 3.1, the remaining ones are solvable if and only if $p_1, \ldots, p_h$ satisfy (8). □

Corollaries 3.1–3.3 are generalized easily. The proofs are analogous.

Corollary 3.4. *Let $m > 0$. The following conditions are equivalent.*

(a) *The congruence* (2) *is solvable for some* a.

(b) *The congruence* (2) *is solvable for any* a.

Corollary 3.5. *Let* $2 \neq p_1, \dots, p_h \in \mathbb{P}$ (*distinct*), *and*

$$K_{p_1,\dots,p_h} = \{up_1^{\alpha_1} \cdots p_h^{\alpha_h} : u \in \{1,2\}, \alpha_1, \dots, \alpha_h > 0\}.$$

The following conditions are equivalent.

(a) *The congruence* (2) *is solvable modulo some* $m \in K_{p_1,\dots,p_h}$.

(b) *The congruence* (2) *is solvable modulo any* $m \in K_{p_1,\dots,p_h}$.

Corollary 3.6. *Let* m *be as in* (9). *The following conditions are equivalent.*

(a) *The congruence* (2) *is solvable.*

(b) *The congruence* $x^n \equiv -1 \pmod{p_1 \cdots p_h}$ *is solvable.*

(c) *The congruence* $x^n \equiv -1 \pmod{2p_1 \cdots p_h}$ *is solvable.*

Remark 3.5. Dence and Dence [4, Theorem 6] studied also the solvability of (2). Some of our results are special cases of theirs, but our approach is independent and more suitable for our purpose.

4 Nontrivial solvability of (2)

Let us recall that the congruence (2) is nontrivially solvable if it has a solution $x \not\equiv -a \pmod{m}$. Having already considered even n in Theorem 1.1, we can assume that

throughout this section, n (> 0) *is odd.*

Contrary to what said in the beginning of Section 3, most of our results here are not true for even n.

4.1 The case $m \in K$

Theorem 4.1. *Let* $m = up^\gamma \in K$ *be as in* (3). *If* $p \nmid n$, *then the following conditions are equivalent.*

(a) *The congruence* (2) *is nontrivially solvable.*

(b) $n \not\perp (p-1)$.

If $p \mid n$, *then* (a) *is equivalent to*

(c) $p^2 \mid m$ *or* $n \not\perp (p-1)$.

Proof. *Case $p \nmid n$.* By Lemma 2.4, (a) holds if and only if $d := \gcd(n, \phi(m)) > 1$. Since

$$d = \gcd(n, p^{\gamma-1}(p-1)) = \gcd(n, p-1)$$

by Lemma 2.1, the claim follows from the last sentence of Lemma 2.4.
Case $p \mid n$. Let $n = tp^\beta$, where $p \nmid t$ and $\beta > 0$. As above, (a) holds if and only if

$$\gcd(n, \phi(m)) = \gcd(tp^\beta, p^{\gamma-1}(p-1)) > 1,$$

i.e.,

$$\gamma > 1 \text{ or } t \not\perp (p-1). \tag{10}$$

This is clearly equivalent to (c). □

We continue as in Subsection 3.1. The proofs are analogous.

Corollary 4.1. *Let $m \in K$. The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable for some a.*

(b) *The congruence (2) is nontrivially solvable for any a.*

Corollary 4.2. *Let K_p be as in Corollary 3.2, and $p \nmid n$. The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable modulo some $m \in K_p$.*

(b) *The congruence (2) is nontrivially solvable modulo any $m \in K_p$.*

Corollary 4.3. *Let $m = up^\gamma \in K$ be as in (3). The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable.*

(b) *The congruence (5) is nontrivially solvable.*

Theorem 4.2. *The congruence (5) is nontrivially solvable for infinitely many p's.*

4.2 The case $m \in \tilde{H}$

We factorize

$$x^n + a^n = (x+a) f_{n-1}(x, a), \tag{11}$$

where

$$f_{n-1}(x,a) = x^{n-1} - x^{n-2}a + \cdots + x^2 a^{n-3} - xa^{n-2} + a^{n-1} =: g_{n-1}(x,a) + a^{n-1}.$$

We also define that $f_0(x,a) = 1$ and $g_0(x,a) = 0$.

Lemma 4.1. *If a is odd, then $f_{n-1}(x,a)$ is odd for all x.*

Proof. If x is even, then $g_{n-1}(x,a)$ is even, so $f_{n-1}(x,a)$ is odd. If x is odd, then $g_{n-1}(x,a)$ is a sum of $n-1$ odd numbers (or zero). Since $n-1$ is even, this sum is even, and $f_{n-1}(x,a)$ is again odd. □

Theorem 4.3. *If $m \in \tilde{H}$, then (2) has only the trivial solution.*

Proof. The congruences are modulo m. If $m = 1$, then any $x \equiv -a$, implying the claim in this case. If $m = 2^\gamma$, $\gamma > 0$, then, because $a(\perp m)$ is odd, $f_{n-1}(x, a)$ is always odd by Lemma 4.1. Hence, by (11), if x satisfies (2), then $x \equiv -a$. □

Remark 4.1. Corollaries 4.1 and 4.3 hold also for $m \in \tilde{H}$. All statements are false by Theorem 4.3.

4.3 The case $m > 0$

Theorem 4.4. *Let $m > 0$. The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable.*

(b) *m has a prime factor p satisfying the condition* (b) *of Theorem* 4.1.

Proof. By (9) and Lemma 2.5, the congruence (2) holds if and only if

$$x^n \equiv -a^n \pmod{2^\alpha},\ x^n \equiv -a^n \pmod{p_1^{\alpha_1}},\ \ldots,\ x^n \equiv -a^n \pmod{p_h^{\alpha_h}}. \tag{12}$$

If m has no odd prime factor, then (12) reduces to $x^n \equiv -a^n \pmod{2^\alpha}$, which has by Theorem 4.3 only the trivial solution.

Otherwise, by Lemma 2.5 and Theorem 4.3,

$$\nu(m) = \nu(p_1^{\alpha_1}) \cdots \nu(p_h^{\alpha_h}).$$

So, $\nu(m) > 1$ if and only if at least one $\nu(p_i^{\alpha_i}) > 1$, i.e., $\gcd(n, \phi(p_i^{\alpha_i})) > 1$. The claim now follows from Theorem 4.1. □

The proofs of the following corollaries are similar to those of Corollaries 3.4–3.6.

Corollary 4.4. *Let $m > 0$. The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable for some a.*

(b) *The congruence (2) is nontrivially solvable for any a.*

Corollary 4.5. *Let $K_{p_1,\ldots,p_h}$ be as in Corollary* 3.5. *The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable modulo some $m \in K_{p_1,\ldots,p_h}$.*

(b) *The congruence (2) is nontrivially solvable modulo any $m \in K_{p_1,\ldots,p_h}$.*

Corollary 4.6. *Let m be as in (9). The following conditions are equivalent.*

(a) *The congruence (2) is nontrivially solvable.*

(b) *The congruence $x^n \equiv -1 \pmod{p_1 \cdots p_h}$ is nontrivially solvable.*

(c) *The congruence $x^n \equiv -1 \pmod{2p_1 \cdots p_h}$ is nontrivially solvable.*

4.4 The case $2 \neq n \in \mathbb{P}, n \neq p$

Writing $q = n$, the congruence (5) reads in this case

$$x^q \equiv -1 \pmod{p}. \tag{13}$$

Theorem 4.5. *The following conditions are equivalent.*

(a) *The congruence* (13) *is nontrivially solvable.*

(b) $p \equiv 1 \pmod{q}$.

(c) $p \equiv 1 \pmod{2q}$.

Proof. (a)⇔(b). The condition (b) is that of Theorem 4.1.

(b)⇔(c). Since p is odd, it follows that $p - 1$ is even. □

A002476. a_t is the t-th prime satisfying (b) (equivalently, (c)) for $q = 3$.

A030430. As above, but $q = 5$.

A140444. As above, but $q = 7$.

Let $p \in \mathbb{P}$. It is a classical result [5] that if $p = a^2 + ab + b^2$ for some $a, b > 0$, then p satisfies the condition (b) (and (c)) of Theorem 4.5. Nair [10, Theorem 8] proved the converse, and that the representation (with $a \geqslant b$) is unique. He called p a $\mathcal{B}$*-prime*. An integer having this representation is a $\mathcal{B}$*-number*. Probably the symbol $\mathcal{B}$ comes from "binary quadratic form". We also apply Nair's certain other results.

Theorem 4.6. *Let* $3 \neq p \in \mathbb{P}$. *The following conditions are equivalent to those of Theorem* 4.5 *for* $q = 3$.

(d1) $p = a^2 + ab + b^2$ *for some* a, b.

(d2) $p = a^2 - ab + b^2$ *for some* a, b.

(e1) $p = a^2 + ab + b^2$ *for some* $a, b > 0$.

(e2) $p = a^2 - ab + b^2$ *for some* $a, b > 0$.

Proof. (b)⇔(e1). See above.

(d1)⇔(e1). [10, Theorem 3].

(e1)⇔(e2). [10, Section 8].

(d1)⇔(d2). Proceed as in the proof of [10, Theorem 8]. □

Can this theorem be extended?

Conjecture 1. *The following conditions are equivalent to those of Theorem* 4.5.

(d1) $p = a^{q-1} + a^{q-2}b + \cdots + ab^{q-2} + b^{q-1}$ *for some* a, b.

(d2) $p = a^{q-1} - a^{q-2}b + \cdots - ab^{q-2} + b^{q-1}$ *for some* a, b.

(e1) $p = a^{q-1} + a^{q-2}b + \cdots + ab^{q-2} + b^{q-1}$ *for some* $a, b > 0$.

(e2) $p = a^{q-1} - a^{q-2}b + \cdots - ab^{q-2} + b^{q-1}$ *for some* $a, b > 0$.

5 Further results

5.1 The case $a \not\perp m$

This case can be reduced to $a \perp m$ through a rather technical process. Because we do not find its details interesting, we only outline how to study the solvability of (2) if $m \in K$.

Let

$$m = up^\gamma,\ a = tp^\alpha,\ x = sp^\xi, \quad u \in \{1, 2\},\ p \nmid t, s,\ \gamma, \alpha > 0,\ \xi \geqslant 0.$$

Then (2) reads

$$s^n p^{\xi n} + t^n p^{\alpha n} \equiv 0 \pmod{up^\gamma}, \tag{14}$$

and we must find s and ξ.

Case 1. $\alpha n \geqslant \gamma$. Then $x = a$ satisfies (14), because

$$x^n + a^n = 2a^n = 2t^n p^{\alpha n} \quad \text{and} \quad up^\gamma \mid 2t^n p^{\alpha n}.$$

Case 2. $\alpha n < \gamma$, $\xi \neq \alpha$. If $\xi < \alpha$, then

$$x^n + a^n = (s^n + t^n p^{(\alpha-\xi)n}) p^{\xi n} \not\equiv 0 \pmod{p^\gamma}.$$

If $\xi > \alpha$, then

$$x^n + a^n = (s^n p^{(\xi-\alpha)n} + t^n) p^{\alpha n} \not\equiv 0 \pmod{p^\gamma},$$

so (14) is not solvable.

Case 3. $\alpha n < \gamma$, $\xi = \alpha$. Now, (14) reads

$$(s^n + t^n) p^{\alpha n} \equiv 0 \pmod{up^\gamma},$$

equivalently

$$(s^n + t^n) \equiv 0 \pmod{up^{\gamma-\alpha n}}. \tag{15}$$

Writing

$$x' = s, \quad a' = t, \quad m' = up^{\gamma-\alpha n},$$

(15) reads

$$(x')^n \equiv -(a')^n \pmod{m'}. \tag{16}$$

If

$$a' \perp m', \tag{17}$$

then we can apply Theorem 3.1 to (16).

If $u = 1$ or if $u = 2$ and t is odd, then (17) holds. If $u = 2$ and t is even, then s is even (since $2 \mid (s^n + t^n)$). So, we can cancel $u = 2$ in (15), and (17) becomes satisfied.

5.2 The primitive-rooted factorization

As an alternative to the prime factorization, can we use the *primitive-rooted factorization* ("prd-factorization" in short) of m? That is,

$$m = m_1 \cdots m_k,$$

where $m_1, \ldots, m_k \in R \backslash \{1\}$ are distinct and (pairwise) coprime. We also define that the prd-factorization of 1 is 1.

The answer is affirmative. However, the prd-factorization, compared to the prime factorization, has no advantage but has disadvantages. It may not exist, and if it exits, then it may not be unique. We can easily prove that m has a prd-factorization if and only $8 \nmid m$. For example, $30 = 2 \cdot 3 \cdot 5 = 6 \cdot 5 = 3 \cdot 10$. We can also easily prove that m has a unique prd-factorization if and only if $m = 2$ or $m\ (> 0)$ is odd.

A047501. a_t is the t-th positive number not divisible by 8. We have a comment to add: a_t is the t-th positive number having a prd-factorization.

A004280. The sequence consisting of the number 2 and all odd positive integers. We have a comment to add: the numbers having a unique prd-factorization.

5.3 The congruence $x^n \equiv a^n \pmod m$

Let us have a quick look at the congruence

$$x^n \equiv a^n \pmod m, \tag{18}$$

where $n > 0$, $m = up^\gamma \in K$ as in (3), and $a \perp m$.

Solvability. The congruence (18) is always solvable, having the trivial solution $x \equiv a \pmod m$. Instead, the congruence (2) is not always solvable if n is even.

Nontrivial solvability, n odd. We can proceed as in Section 4.

Nontrivial solvability, n even. The congruences are modulo p. It is reasonable to say that, besides the solution $x \equiv a$, also the solution $x \equiv -a$ is trivial. We show that $a \not\equiv -a$. An equivalent claim is that $2a \not\equiv 0$. If $2a \equiv 0$, then $p \mid a$, contradicting $a \perp m$. Hence, (18) is nontrivially solvable if and only if it has more than two incongruent roots. By the last sentence of Lemma 2.4 and the above, this happens if and only if $\gcd(n, p^{\gamma-1}(p-1)) > 2$. An equivalent condition,

$$\gcd\left(\frac{n}{2},\, p^{\gamma-1}\frac{p-1}{2}\right) > 1,$$

leads to the condition (b) of Theorem 4.1.

A closer look shows that everything in Section 4 hold as such or with minor changes.

6 Discussion

Certain computer experiments [9] led us to (1) and, more generally, to (2). In this paper, we studied its solvability. If m has a primitive root, then we applied Lemma 2.2, which can be proved by index calculus. In the general case, we used the prime factorization and the Chinese remainder theorem. If n is odd, then (2) has always the trivial solution $x \equiv -a \pmod m$. So, we got another task: to study nontrivial solvability in this case.

The congruence (2) and related congruences have been considered in the literature. However, the solvability of (2) has not (according to our knowledge) been studied in all detail, which motivated us to write this paper. As an additional topic of possible interest, we found many direct or indirect connections with OEIS sequences. We also encountered Conjecture 1, which is (according to our knowledge) open.

References

[1] Apostol, T. M. (1986). *Introduction to Analytic Number Theory* (3rd printing), Springer.

[2] Dence, J. B., & Dence, T. P. (1995). Cubic and quartic residues modulo a prime. *Missouri Journal of Mathematical Sciences*, 7, 24–31.

[3] Dence, J. B., & Dence, T. P. (1996). Residues – Part II: Congruences modulo powers of 2. *Missouri Journal of Mathematical Sciences*, 8, 26–35.

[4] Dence, J. B., & Dence, T. P. (1997). Residues – Part III: Congruences to general composite moduli. *Missouri Journal of Mathematical Sciences*, 9, 72–78.

[5] Dickson, L. E. (1999). *History of the Theory of Numbers, Vol. 3*, AMS-Chelsea.

[6] Graham, R. L., Knuth, D. E., & Patashnik, O. (1994). *Concrete Mathematics: A Foundation of Computer Science* (2nd edition). Addison–Wesley.

[7] Lozano-Robledo, Á. (2019). *Number Theory and Geometry: An Introduction to Arithmetic Geometry*. American Mathematical Society.

[8] Mustonen, S. (1992). *Survo: An Integrated Environment for Statistical Computing and Related Areas*. Survo Systems. Available online at: `https://www.survo.fi/kirjat/index.html`.

[9] Mustonen, S. (2022). *Diophantine equations $X^n + Y^n \equiv 0 \pmod{P}$. Additional results and graphical presentations*. Available online at: `https://www.survo.fi/papers/Dioph2022.pdf`.

[10] Nair, U. P. (2004). *Elementary results on the binary quadratic form $a^2 + ab + b^2$*. Preprint. arXiv:math/0408107.

[11] Sloane, N. J. A. (2024). *The On-line Encyclopedia of Integer Sequences*. Available online at: `https://oeis.org/`.