**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**2025, Volume 31, Number 4, 776–784**
**DOI: 10.7546/nntdm.2025.31.4.776-784**

# Proofs of some geometric conjectures on the power sum congruence modulo a prime

**Pentti Haukkanen**

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

**Received:** 15 September 2025 **Revised:** 29 October 2025
**Accepted:** 2 November 2025 **Online First:** 5 November 2025

**Abstract:** The main purpose of this paper is to verify the geometric conjectures of Mustonen (2022) concerning the solutions and the number of solutions of the congruence

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

where $p$ is a prime. For $p > 2$, the nontrivial solutions lie on the "lines" $y \equiv cx \pmod{p}$, where $c$ ranges over the $n$-th roots of $-1$ modulo $p$. The total number of solutions is $1 + (p-1)d$ if $d$ divides $(p-1)/2$, and $0$ otherwise, where $d = \gcd(n, p-1)$. For each $c$, the lines are equally spaced.

**Keywords:** Congruence of powers, Experimental geometry, Power residue, Primitive root, Cyclic group.
**2020 Mathematics Subject Classification:** 11A07, 11A15, 11Y99, 51M04.

## 1 Introduction

In this note, we study the congruence

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

where $p$ is a prime. Equivalently, we look for solutions of $x^n + y^n = 0$ over the finite field

$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. Seppo Mustonen examined this congruence experimentally with the aid of the *Survo* system [4]. He observed that the solution set in the region $0 < x, y < p$ can be divided into straight lines (or line segments), and he recorded the following observations without providing proofs [5]:

1. The number of directions of straight lines covering all roots is $\gcd(p-1, n)$.
2. The number of nontrivial roots in each direction is $p-1$ in the region $0 < x, y < p$.
3. Each nontrivial root is covered by only one of these straight lines. Hence the total number of nontrivial roots in the region $0 < x, y < p$ is $(p-1)\gcd(p-1, n)$.

It can be seen from the figures [5] that lines with the same direction are equidistant. Merikoski *et al.* [3] studied the solvability of this congruence modulo $m$ and reported Mustonen's observations on the congruence modulo $p$.

The structure of the paper is as follows. In Section 2 we study the algebraic structure of the congruence, describe its solution set, and determine its cardinality. In Section 3 we take a geometric perspective and formalize and verify Mustonen's observations 1–3, illustrating them with examples. In Section 4 we prove that the parallel lines are equidistant, and in Section 5 we propose directions for further research.

# 2 Solution of the congruence

**The case $p = 2$.** For every integer $t$ and $n \geq 1$ we have $t^n \equiv t \pmod 2$, since

$$t^n - t = t\big(t^{\,n-1} - 1\big)$$

has an even factor. Hence the congruence reduces to $x + y \equiv 0 \pmod 2$, i.e., $x \equiv y \pmod 2$. Over $\mathbb{F}_2$ there are precisely two solutions: $(x, y) \equiv (0, 0)$ and $(1, 1)$.

**The case $p$ is odd.** If $x \equiv 0 \pmod p$, then $y^n \equiv 0 \pmod p$ and thus $y \equiv 0 \pmod p$. So $(0, 0)$ is the only solution with a zero coordinate. For $x \not\equiv 0 \pmod p$, put $c = yx^{-1} \in \mathbb{F}_p^\times$, where $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$ is the finite cyclic group of order $p-1$. Then

$$x^n + y^n \equiv x^n\big(1 + c^n\big) \pmod p,$$

so $x^n + y^n \equiv 0 \pmod p$ if and only if

$$c^n \equiv -1 \pmod p. \tag{1}$$

Thus the problem reduces to counting the $n$th roots of $-1$ in the cyclic group $\mathbb{F}_p^\times$. We then obtain the solution as

$$y \equiv cx \pmod p,$$

where $c$ goes through the solutions of $c^n \equiv -1 \pmod p$ and $x$ goes through the values $1, 2, \ldots, p-1$.

**Theorem 2.1.** *Let $p$ be an odd prime and $n \geq 1$, and set $d = \gcd(n, p-1)$. Then the congruence $x^n + y^n \equiv 0 \pmod{p}$ has*

$$1 + (p-1)\, N_p(n)$$

*solutions $(x, y) \in \mathbb{F}_p^2$, where $N_p(n)$ is the number of solutions $c \in \mathbb{F}_p^\times$ to* (1)*. Moreover,*

$$N_p(n) = \begin{cases} d, & \text{if } d \mid \dfrac{p-1}{2}, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

*Equivalently,* (1) *is solvable if and only if the 2-adic valuation satisfies $\nu_2(n) < \nu_2(p-1)$; in that case there are exactly $d$ distinct solutions $c$ of* (1)*.*

*Proof.* The map $\phi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $\phi(u) = u^n$, is a homomorphism onto a subgroup of size $(p-1)/d$ with kernel of size $d = \gcd(n, p-1)$. Hence, for any $a \in \mathbb{F}_p^\times$, the equation $u^n = a$ has either $d$ or $0$ solutions $u$, according as $a$ does or does not lie in the image of $\phi$.

Write $-1 = g^{(p-1)/2}$ for a fixed primitive root $g$ modulo $p$ [1]. Then $u^n = -1$ is equivalent to

$$g^{kn} \equiv g^{(p-1)/2} \pmod{p} \quad \Longleftrightarrow \quad kn \equiv \frac{p-1}{2} \pmod{p-1}.$$

This linear congruence has solutions in $k$ if and only if $d \mid \frac{p-1}{2}$, and in that case there are exactly $d$ incongruent solutions $k$ modulo $p-1$, yielding $d$ distinct $c = g^k$ that solve (1). This proves (2).

Finally, for each such $c$ and each $x \in \mathbb{F}_p^\times$, we obtain a solution $(x, y) = (x, cx)$ to the original congruence. These are precisely all the solutions with $x \neq 0$, and each such solution is counted exactly once. Indeed, if $c_1 x \equiv c_2 x \pmod{p}$, then $c_1 \equiv c_2 \pmod{p}$ since $x \neq 0$; similarly, if $cx_1 \equiv cx_2 \pmod{p}$, then $x_1 \equiv x_2 \pmod{p}$ since $c \neq 0$ (see also Section 3.)

Thus, the total number is $1 + (p-1)\, N_p(n)$, where the extra '1' accounts for $(0, 0)$. The equivalence with $\nu_2(n) < \nu_2(p-1)$ follows from noting that $d \mid \frac{p-1}{2}$ is automatically satisfied at all odd primes dividing $d$, so the only restriction is on the power of 2. □

**Remark 2.1** (Explicit solutions via a primitive root)**.** Assume $d \mid \frac{p-1}{2}$ and let $g$ be a primitive root modulo $p$. Put $M = \frac{p-1}{d}$, $n' = \frac{n}{d}$ (so $\gcd(n', M) = 1$), and $T = \frac{1}{d} \cdot \frac{p-1}{2}$. Then the linear congruence

$$n'k \equiv T \pmod{M}$$

has the unique solution class $k \equiv n'^{-1} T \pmod{M}$, and the $d$ solutions of (1) are

$$c = g^{\,k+tM} \qquad (t = 0, 1, \ldots, d-1).$$

For each such $c$ and any $x \in \mathbb{F}_p^\times$, the pair $(x, y) = (x, cx)$ is a solution, together with $(0, 0)$.

**Corollary 2.1.** *If $p \equiv 3 \pmod{4}$ and $n$ is even, then $x^n + y^n \equiv 0 \pmod{p}$ has only the trivial solution $(0, 0)$.*

**Example 2.1.**

- $p = 5$, $n = 2$: $p - 1 = 4$, $d = \gcd(2, 4) = 2$ and $d \mid \frac{p-1}{2} = 2$, so there are $N_p(n) = 2$ values of $c$ with $c^2 \equiv -1 \pmod{5}$ (namely $c \equiv \pm 2$), giving $(p-1)N_p(n) + 1 = 9$ solutions in total.
- $p = 7$, $n = 2$: $p - 1 = 6$, $d = 2 \nmid \frac{p-1}{2} = 3$, so there are no nontrivial solutions. Thus, we have only the trivial solution $(x, y) = (0, 0)$.
- $p = 7$, $n = 3$: $p-1 = 6$, $d = 3 \mid \frac{p-1}{2} = 3$, so $N_p(n) = 3$ and there are $(p-1)N_p(n)+1 = 19$ solutions.

**Example 2.2** (Case $n = p$)**.** Let $p$ be prime and take $n = p$. Over $\mathbb{F}_p$ the Frobenius endomorphism [2] gives $t^p = t$ for all $t \in \mathbb{F}_p$, hence

$$x^p + y^p \equiv x + y \pmod{p}.$$

So $x^p + y^p \equiv 0 \pmod{p}$ if and only if $x + y \equiv 0 \pmod{p}$, i.e., $y \equiv -x \pmod{p}$. Therefore the solutions are exactly the $p$ pairs $(x, -x)$ with $x \in \mathbb{F}_p$. This agrees with Theorem 2.1: here $d = \gcd(p, p-1) = 1$, so $N_p(p) = 1$ and the total number of solutions is $1 + (p-1) \cdot 1 = p$. An illustration for $n = p = 7$ is presented in Figure 1.

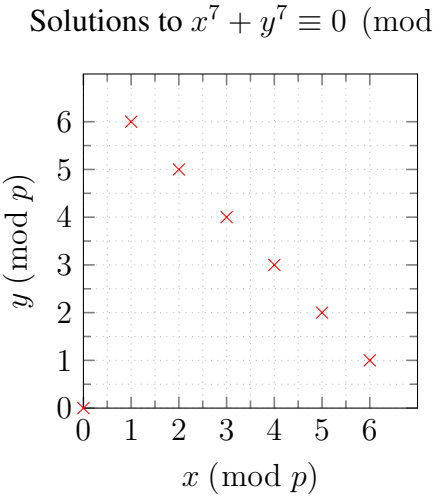
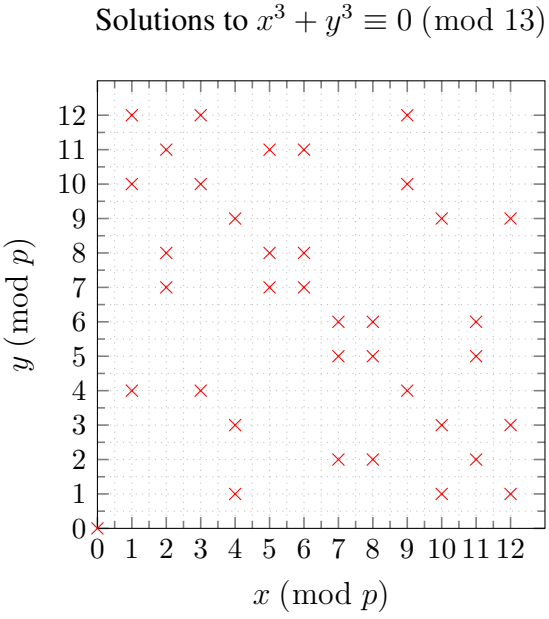
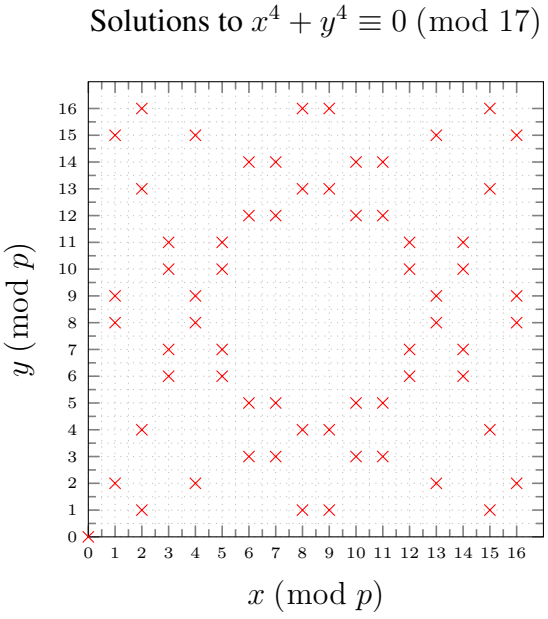



**Figure 1.** Solutions of $x^7 + y^7 \equiv 0 \pmod{7}$ in $\mathbb{F}_7^2$: the anti-diagonal $y \equiv -x$ and the origin.

We conclude this section with two figures illustrating solutions to congruences of the type considered in this paper.




**(a)** $p = 13,\ n = 3$




**(b)** $p = 17,\ n = 4$

**Figure 2.** Two examples of solution sets $\{(x, y) \in \mathbb{F}_p^2 :\ x^n + y^n \equiv 0 \pmod{p}\}$.

# 3 Proofs of Mustonen's observations

In this section, we verify Mustonen's observations as reviewed in the introduction. Some of the reasoning from Section 2 is repeated here for clarity.

We start with an overview. Let $p$ be an odd prime and $n \geq 1$. Put $d = \gcd(n, p-1)$ and

$$S = \{\, c \in \mathbb{F}_p^\times : \; c^n \equiv -1 \pmod{p} \}.$$

Then $|S| \in \{0, d\}$, and in fact $|S| = d$ if and only if $d \mid \frac{p-1}{2}$ (otherwise $|S| = 0$). Here, $S$ is the set of directions. (Each direction corresponds to a class of slopes congruent modulo $p$. By convention we usually take representatives with $0 < c < p$, but one may also use $-p < c < 0$. The latter choice only affects the apparent geometry of the picture, not the solution set itself.)

For each direction $c \in S$, the "line" of solutions is

$$L_c \;=\; \{(x, y) \in \mathbb{F}_p^2 : \; y \equiv cx \pmod{p}\}.$$

It contains exactly $p-1$ nontrivial solutions $(x, y)$ of $x^n + y^n \equiv 0 \pmod{p}$. When drawn in the square $0 \leq x, y \leq p-1$, $L_c$ appears as one or more straight-line segments of slope $c$; when the slope is positive breaks occur at the wrap-around points where $(c(x+1) \bmod p) < (cx \bmod p)$, where $(cx \bmod p)$ denotes the residue of $cx$ modulo $p$. If the slope is negative, breaks occur at the wrap-around points where $(c(x+1) \bmod p) > (cx \bmod p)$. (By a "line" we mean either the set of pairs $(x, y)$ such that $y \equiv cx \pmod{p}$, or its chosen set of representatives.)

The lines $\{L_c : c \in S\}$ are pairwise disjoint on the set of nontrivial solutions, and their union equals the set of all nontrivial solutions. Consequently, the number of nontrivial solutions with $0 < x, y < p$ is

$$(p-1)\,|S| = \begin{cases} (p-1)\,\gcd(n, p-1), & \text{if } \gcd(n, p-1) \mid \dfrac{p-1}{2}, \\ 0, & \text{otherwise.} \end{cases}$$

We next present detailed proofs of the Properties 1–3 given by Mustonen [5].

*Proof.* Property 1: Number of directions. Directions are solutions $c$ of the congruence $c^n \equiv -1 \pmod{p}$. We look at this algebraically. Because $\mathbb{F}_p^\times$ is cyclic of order $p-1$, the map $u \mapsto u^n$ has kernel of size $d = \gcd(n, p-1)$ and image of size $(p-1)/d$. Thus $c^n = a$ has either $d$ or $0$ solutions. In our application, $a = -1$. This proves Property 1.

Property 2: Number of roots in each direction. For each direction $c \in S$, the "line" of solutions is

$$L_c \;=\; \{(x, y) \in \mathbb{F}_p^2 : \; y \equiv cx \pmod{p}\}.$$

The elements $x = 1, 2, \ldots, p-1$ give distinct solutions in $L_c$. In fact, assume $cx_1 \equiv cx_2 \pmod{p}$; then $x_1 \equiv x_2 \pmod{p}$ since $c \neq 0$. Thus, the number of nontrivial roots in each direction in $p-1$. This proves Property 2.

Property 3: Total number of nontrivial roots. We analyze Property 3 in the four subtitles below.

*Lines from solutions (each solution is on a line).* Let $(x, y)$ be a nontrivial solution, so $x, y \neq 0$. Set $c = yx^{-1} \in \mathbb{F}_p^\times$. Then

$$0 \equiv x^n + y^n \equiv x^n\big((yx^{-1})^n + 1\big) = x^n(s^n + 1) \pmod{p},$$

so $c^n \equiv -1 \pmod{p}$, i.e. $c \in S$, and $(x, y)$ lies on the line $y \equiv cx \pmod{p}$, where $c \in S$.

*Solutions from lines (each integer point in a line is a solution).* Conversely, assume $(x, y)$ lies in a line $y \equiv cx \pmod{p}$. If $c \in S$ and $x \in \mathbb{F}_p^\times$, then with $y = cx$ we have $x^n + y^n \equiv x^n(c^n + 1) \equiv 0 \pmod{p}$. So, $(x, y)$ is a solution.

*Disjointness of the lines.* If $(x, y)$ lies on both $L_{c_1}$ and $L_{c_2}$, then $y \equiv c_1 x \equiv c_2 x \pmod{p}$ with $x \neq 0$: hence $c_1 \equiv c_2 \pmod{p}$. So, the lines are disjoint.

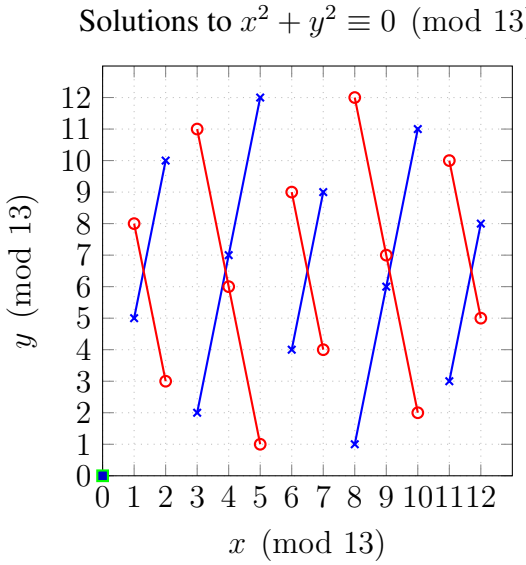
*Conclusion of Property 3.* Combining the above parts, we see that every nontrivial solution lies on exactly one line $L_c$, $(c \in S)$, and each $L_c$ contributes one solution for each $x \in \mathbb{F}_p^\times$, i.e., exactly $p - 1$ nontrivial solutions. This proves that each nontrivial root is covered by exactly one of these straight lines and the total number of nontrivial roots in the region $0 < x, y < p$ is $(p - 1)|S|$. □

We illustrate the geometry of the solutions with a couple of examples.

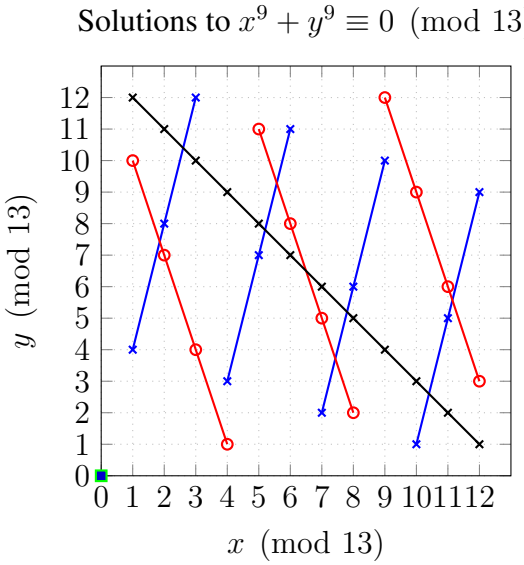
**Example 3.1.** Consider the congruence $x^2 + y^2 \equiv 0 \pmod{13}$ with $p = 13$ and $n = 2$. Then $d = \gcd(n, p - 1) = 2$, and thus $d \mid (p - 1)/2$. Now, $S = \{5, 8\} = \{5, -5\} \subset \mathbb{F}_{13}^\times$, the set of square roots of $-1$ modulo 13. Hence there are $d = 2$ directions, and the "lines" are $L_5$ and $L_8 = L_{-5}$, which together partition the set of nontrivial solutions. Moreover, $|L_5| = p - 1 = 12$, and likewise $|L_{-5}| = 12$. Thus the total number of solutions, including the trivial solution $(0, 0)$, is $1 + d(p - 1) = 1 + 2 \cdot 12 = 25$.

The set $L_5$ consists of the points in blue line segments in Figure 3a. In these line segments the slope is $c = 5 \in \mathbb{Z}$. The set $L_{-5}$ consists of the points in red line segments in Figure 3a. In these line segments the slope is $c = -5 \in \mathbb{Z}$. Although $L_8 = L_{-5}$ as sets, the decomposition into line segments differs: the first segment for $L_8$ is the single point $(1, 8)$, the second segment runs from $(2, 3)$ to $(3, 11)$, and so on.

Thus the nontrivial solutions are exactly $L_5 \cup L_{-5}$, as depicted in Figure 3a.




**(a)** The lines correspond to $y \equiv cx \pmod{13}$ with $c^2 \equiv -1 \pmod{13}$, here $c = -5$ (red) and $c = 5$ (blue). The origin is marked in green.




**(b)** The lines correspond to $y \equiv cx \pmod{13}$ with $c^9 \equiv -1 \pmod{13}$, here $c = 4$ (red), $c = -3$ (blue) and $c = -1$ (black). The origin is marked in green.

**Figure 3.** Geometric illustration of solution sets $\{(x, y) \in \mathbb{F}_p^2 : x^n + y^n \equiv 0 \pmod{p}\}$.

**Example 3.2.** Consider the congruence $x^9 + y^9 \equiv 0 \pmod{13}$ with $p = 13$ and $n = 9$. Then $d = \gcd(n, p-1) = 3$, and thus $d \mid (p-1)/2$. Now, $S = \{4, 10, 12\} = \{4, -3, -1\} \subset \mathbb{F}_{13}^{\times}$, the set of 9-th roots of $-1$ modulo 13. Hence there are $d = 3$ directions, and the "lines" are $L_4$, $L_{10} = L_{-3}$, and $L_{12} = L_{-1}$, which together partition the set of nontrivial solutions. Each of these sets has cardinality $p - 1 = 12$. Thus the total number of solutions, including the trivial solution $(0, 0)$, is $1 + d(p-1) = 1 + 3 \cdot 12 = 37$.

The set $L_4$ consists of the points in blue line segments in Figure 3a. In these line segments the slope is $c = 4 \in \mathbb{Z}$. The set $L_{-3}$ consists of the points in red line segments in Figure 3a. In these line segments the slope is $c = -3 \in \mathbb{Z}$. Although $L_{10} = L_{-3}$, the line segments related to $L_{10}$ and $L_{-3}$ are different. The line segments related to $L_{10}$ have the slope $c = 10 \in \mathbb{Z}$. The set $L_{-1}$ consists of the points in the black line segment. Now, $L_{12} = L_{-1}$ but there are 12 "line segments" related to $L_{12}$, and each line segment consists only of one point. The first "line segment" is $(1, 12)$, the second is $(2, 11)$, and so on.

Thus the nontrivial solutions are exactly $L_4 \cup L_{-3} \cup L_{-1}$, as shown in Figure 3a.

**Remark 3.1.** It should be noted that the set of nontrivial solutions can also be partitioned into parallel and equidistant line segments that are not of the form $y \equiv cx \pmod{p}$ with $c \in S$. For example, in Figure 3a, the red points can be grouped so that $(2, 3)$ is connected to $(5, 1)$, and so on. These segments have slope $-2/3$. A similar phenomenon can also be observed in Figure 3b. A closer study of such line segments suggests that they can be described by congruences of the form

$$ax + by \equiv 0 \pmod{p}.$$

For instance, the line through the points $(2, 3)$ and $(5, 1)$ has the equation

$$2x + 3y - 13 = 0,$$

which modulo 13 takes the form $2x + 3y \equiv 0 \pmod{13}$. In the finite field $\mathbb{F}_{13}$, we obtain $y = (-2/3)x = (-5)x = 8x$. We do not pursue this direction further in the present paper.

# 4 Distance of line segments

In this section, we prove that for each direction $c \in S$ the line segments are equally spaced. For example, in Figure 3b, the blue line segments are equally spaced, and similarly for the red line segments.

Let $c \in S$ be a direction with $-p < c < p$, and consider the line

$$y \equiv cx \pmod{p}.$$

Then each line segment in the region $0 \le x, y < p$ is of the form

$$\ell_k : \ y = cx - kp$$

for a suitable value of $k$ and certain values of $x$. To be more precise, if $0 < c < p$, then

$$0 < cx - kp < p \quad \Longleftrightarrow \quad \frac{kp}{c} < x < \frac{(k+1)p}{c},$$

and if $-p < c < 0$, then $(k+1)p/c < x < kp/c$.

One easily checks that $\ell_k$ and $\ell_{k+1}$ are two consecutive line segments (the order depends on the sign of $c$). For example, if $0 < c < p$, then $\ell_0$ is the left-most line segment and $\ell_1$ is the next one.

Applying elementary geometry to the equations $\ell_k : \ y = cx - kp$ and $\ell_{k+1} : \ y = cx - (k+1)p$, we see that their perpendicular distance is equal to

$$\frac{p}{\sqrt{1+c^2}}.$$

Since the distance is independent of $k$, the line segments are equally spaced.

# 5 Concluding remarks

The nontrivial solutions of the congruence $x^n + y^n \equiv 0 \pmod{p}$ are the "lines"

$$y \equiv cx \pmod{p},$$

where $c$ goes through the solutions of $c^n \equiv -1 \pmod{p}$ and $x$ goes through the values $1, 2, \ldots, p-1$. This gives every solution exactly once. Here, $c$ determines the direction of a line, and each line has a distinct direction, [5].

However, a single line $y \equiv cx \pmod{p}$ does not extend to infinity. Instead, it is represented within the region $0 < x, y < p$; whenever the line crosses the boundary of this region, the points are mapped back into the region by modular reduction. Consequently, the graph of the line inside this region consists of a collection of line segments that are parallel and equally spaced, as is shown in Section 4. The line segments can also be described by

$$y = (cx \bmod p).$$

In this paper, we proved the conjectures of Mustonen [5] concerning the geometry of the congruence solutions.

This is a rich area of research, and we hope that these results will stimulate further investigations into the number-theoretic, algebraic, and geometric properties of such congruences.

In particular, Merikoski *et al.* [3] studied the solvability of this congruence for arbitrary moduli $m \ (\geq 2)$, and the reader is invited to examine their solutions.

# Acknowledgements

The author is grateful to Seppo Mustonen for introducing this topic, and to Jorma Merikoski and Timo Tossavainen for their valuable and encouraging comments.

# References

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

[2] Lang, S. (2002). *Algebra* (Revised 3rd edition), Graduate Texts in Mathematics Series, Vol. 211, Springer.

[3] Merikoski, J. K., Haukkanen, P., & Tossavainen, T. (2024). The congruence $x^n \equiv -a^n \pmod{m}$: Solvability and related OEIS sequences. *Notes on Number Theory and Discrete Mathematics*, 30(3), 516–529.

[4] 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`.

[5] 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`.