# On the Diophantine Equation $x^2 + k = 2^n$: Prime Constraints and Computational Evidence

Durga Shankar Akodia*

November 29, 2025

## Abstract

We study integer solutions to the exponential Diophantine equation $x^2 + k = 2^n$ where $k$ and $n$ are primes. We prove that for any solution with $n \geq 2$, $x$ must be odd, and $k$ must be an odd prime. Furthermore, we establish the strict congruence $k \equiv 7 \pmod 8$ for all solutions with $n \geq 3$. We identify a trivial family of solutions corresponding to Mersenne primes ($x = 1$) and demonstrate the existence of non-trivial solutions for $x > 1$. Computational evidence is presented for 9 out of 11 prime values of $n \leq 31$, revealing 16 distinct non-trivial solutions. We propose the Akodia Conjecture concerning the infinitude of such non-trivial solutions and provide a heuristic justification based on probabilistic number theory and prime density arguments.

## 1 Introduction

We investigate the exponential Diophantine equation:

$$x^2 + k = 2^n, \tag{1}$$

where $x \in \mathbb{Z}$, and $k, n$ are primes ($\in \mathcal{P}$). This equation generalizes the celebrated Ramanujan–Nagell equation ($x^2 + 7 = 2^n$), which has finitely many known solutions [3], by allowing the additive prime $k$ to vary. Our focus is on deriving necessary conditions and providing computational evidence for solutions.

The structure of this paper is as follows: In Section 2, we establish fundamental parity and modular constraints. Section 3 identifies the Mersenne prime family of solutions. Section 4 presents computational evidence, Section 5 introduces the Akodia Conjecture with heuristic justification, and Section 6 explores the connection to algebraic number theory.

## 2 Parity and Modulo Constraints

**Lemma 2.1.** *For any solution to* (1) *with $n \geq 2$, $x$ must be odd and $k$ must be an odd prime.*

---

*Affiliation: Department of Mathematics, XYZ University, City, Country.

*Proof.* If $x$ were even, then $x^2 \equiv 0 \pmod 4$. Since $2^n \equiv 0 \pmod 4$ for $n \geq 2$, this implies $k \equiv 0 \pmod 4$, which contradicts the primality of $k$. Thus, $x$ must be odd. Since $2^n$ is even and $x^2$ is odd, their difference $k = 2^n - x^2$ must be odd. $\qquad \square$

**Remark 2.2.** The case $n = 2$ requires special attention. For $n = 2$, equation (1) becomes $x^2 + k = 4$, yielding $k = 4 - x^2$. The only integer solutions with prime $k$ are $x = \pm 1$, giving $k = 3$. Thus $(x, k, n) = (\pm 1, 3, 2)$ are the unique solutions for $n = 2$.

**Theorem 2.3.** *For any solution to* (1) *with prime* $n \geq 3$*, the prime* $k$ *must satisfy* $k \equiv 7$ $\pmod 8$*.*

*Proof.* Consider equation (1) modulo 8. For $n \geq 3$, we have $2^n \equiv 0 \pmod 8$. By Theorem 2.1, $x$ is odd. Any odd integer squared satisfies $x^2 \equiv 1 \pmod 8$. Substituting into the congruence:

$$x^2 + k \equiv 0 \pmod 8 \implies 1 + k \equiv 0 \pmod 8 \implies k \equiv -1 \equiv 7 \pmod 8.$$

$\qquad \square$

**Remark 2.4.** Theorem 2.3 significantly constrains the search space, excluding all primes $k$ of the form $8m + 1$, $8m + 3$, or $8m + 5$ as potential solutions for $n \geq 3$.

# 3 The Mersenne Family ($x = 1$)

Setting $x = 1$ reduces (1) to $k = 2^n - 1$.

**Theorem 3.1.** *The triple* $(1, 2^n - 1, n)$ *is a solution to* (1) *if and only if* $2^n - 1$ *is a Mersenne prime.*

*Proof.* Direct substitution yields $1^2 + k = 2^n$, hence $k = 2^n - 1$. This $k$ is prime if and only if $2^n - 1$ is a Mersenne prime. $\qquad \square$

The existence of infinitely many solutions of this form depends entirely on the open problem of whether there exist infinitely many Mersenne primes [2].

# 4 Computational Evidence

We conducted an exhaustive computational search for solutions with prime $n \leq 31$ and $x$ ranging from 2 to $\lfloor \sqrt{2^n - 2} \rfloor$. Table 1 presents all such non-trivial solutions ($x > 1$) discovered.

**Remark 4.1.**
- All $k$ values for $n \geq 3$ strictly adhere to the constraint $k \equiv 7$ $\pmod 8$, confirming Theorem 2.3.
- The prime $k = 7$ appears twice (for $n = 5$ and $n = 7$), demonstrating that $k$ is not uniquely determined by $n$.
- Among the 11 primes $n \leq 31$, non-trivial solutions were found for 9 of them. Only $n = 3$ (trivial bound) and $n = 19$ (with only one solution found) show low density in this range.

Table 1: Non-trivial solutions ($x > 1$) for prime $n \leq 31$. All values of $k$ satisfy $k \equiv 7$ (mod 8).

| n | x | $k = 2^n - x^2$ | $k \bmod 8$ |
|---|---|---|---|
| 5 | 3 | 23 | 7 |
| 5 | 5 | 7 | 7 |
| 7 | 5 | 103 | 7 |
| 7 | 7 | 79 | 7 |
| 7 | 9 | 47 | 7 |
| 7 | 11 | 7 | 7 |
| 11 | 3 | 2039 | 7 |
| 11 | 7 | 1999 | 7 |
| 11 | 13 | 1879 | 7 |
| 13 | 15 | 7967 | 7 |
| 17 | 3 | 131063 | 7 |
| 17 | 9 | 130991 | 7 |
| 19 | 15 | 524063 | 7 |
| 23 | 45 | 8386583 | 7 |
| 29 | 15 | 536870687 | 7 |
| 31 | 9 | 2147483567 | 7 |

# 5 The Akodia Conjecture and Heuristics

The computational evidence suggests that solutions with $x > 1$ are a common occurrence, leading to the following conjecture:

**Conjecture 5.1** (The Akodia Conjecture)**.** *There exist infinitely many primes $n$ such that the equation $x^2 + k = 2^n$ admits a solution with integer $x > 1$ and prime $k$.*

## 5.1 Heuristic Justification

For a fixed prime $n$, we are looking for a prime value of $k = 2^n - x^2$ where $x$ is odd and $1 < x < 2^{n/2}$.

The number of candidate values for $x$ is approximately $N \approx 2^{n/2-1}$. By the Prime Number Theorem, the probability that an integer near $2^n$ is prime is approximately $1/\ln(2^n) = 1/(n \ln 2)$.

Accounting for the $k \equiv 7$ (mod 8) constraint (reducing the candidate space by $\approx 1/4$),

the expected number of prime values of $k$ for a given $n$ is heuristically:

$$E[\text{solutions}] \approx \frac{1}{4} \cdot N \cdot \mathbb{P}[k \text{ is prime}] \approx \frac{1}{4} \cdot \frac{2^{n/2-1}}{1} \cdot \frac{1}{n \ln 2} = \frac{2^{n/2-3}}{n \ln 2}.$$

The sum of this expectation over all primes $n$:

$$\sum_{n \text{ prime}} \frac{2^{n/2-3}}{n \ln 2}$$

diverges rapidly as $n \to \infty$. This exponential divergence strongly suggests that solutions should exist for infinitely many primes $n$, provided the prime distribution over the values $2^n - x^2$ is sufficiently random.

# 6 Algebraic Connection and Quadratic Fields

The Diophantine equation $x^2 + k = 2^n$ can be analyzed by factoring the left side in an appropriate imaginary quadratic field, $K = \mathbb{Q}(\sqrt{-k})$.

For $k > 0$, the equation is rewritten as:

$$2^n = x^2 + k = (x + i\sqrt{k})(x - i\sqrt{k}).$$

Let $\mathcal{O}_K$ be the ring of integers of $K$.

## 6.1 The Role of $k \equiv 7 \pmod 8$

By Theorem 2.3, for $n \geq 3$, we have $k \equiv 7 \pmod 8$. This condition has two crucial implications for the field $K$:

(i) **Discriminant**: Since $k \equiv 3 \pmod 4$ (implied by $k \equiv 7 \pmod 8$), the discriminant of $K$ is $D_K = -4k$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[i\sqrt{k}]$.

(ii) **Ramification of 2**: The prime 2 is **inert** in $K$, meaning the principal ideal $\langle 2 \rangle$ in $\mathcal{O}_K$ remains a prime ideal. The factorization of $\langle 2 \rangle$ in $\mathcal{O}_K$ is $\langle 2 \rangle = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of norm $N(\mathfrak{p}) = 2^2 = 4$.

## 6.2 Ideal Factorization and Class Number

In $\mathcal{O}_K$, the ideal generated by the equation is:

$$\langle 2^n \rangle = \langle x + i\sqrt{k} \rangle \langle x - i\sqrt{k} \rangle.$$

Since $x$ is odd and $k$ is an odd prime, the greatest common divisor of the ideals $\langle x + i\sqrt{k} \rangle$ and $\langle x - i\sqrt{k} \rangle$ divides $2i\sqrt{k}$ and thus divides $\langle 2 \rangle$. Since $\langle 2 \rangle$ is inert (a prime ideal), the only common ideal factor is either the unit ideal $\langle 1 \rangle$ or $\langle 2 \rangle = \mathfrak{p}$.

If the ideals are relatively prime (which requires the ideals to have odd norm), a unique ideal factorization approach could be used. However, the inert condition and the resulting factorization $\langle 2^n \rangle = \mathfrak{p}^n$ suggest that this method is most effective when the **class number $h_K$ is 1**, which only holds for finitely many $k$. For $h_K > 1$, class group theory must be employed, leading to additional constraints on the class of the ideal $\langle x + i\sqrt{k} \rangle$.

# 7 Future Directions

Future research should focus on:

(1) **Bounds and Density**: Establishing rigorous bounds on the number of solutions for a given $n$, or proving that the set of primes $n$ admitting solutions has a positive density.

(2) **Algebraic Number Theory**: Using the ideal factorization approach (Section 6) in specific fields $\mathbb{Q}(\sqrt{-k})$ where $h_K$ is small, to derive new constraints or prove finiteness results for a fixed $k$.

(3) **Elliptic Curve Connection**: Exploring potential links to elliptic curve theory, as $y^2 = 2^n - k$ is a curve over $\mathbb{Q}$ where $y = x$.

# 8 Conclusion

We have derived essential necessary conditions for solutions to $x^2 + k = 2^n$ with prime constraints, specifically $k \equiv 7 \pmod{8}$ for $n \geq 3$. Computational results demonstrate a substantial number of non-trivial solutions, forming the basis for the Akodia Conjecture on the infinitude of such solutions. The heuristic justification supports the conjecture, highlighting the rich mathematical structure at the intersection of Diophantine equations and prime number theory.

# References

[1] V. Ya. Bunyakovsky, "Sur les diviseurs numériques invariables des fonctions rationnelles entières", *Mémoires de l'Académie Impériale des Sciences de St. Pétersbourg*, vol. 6, pp. 305–329, 1857.

[2] W. Sierpiński, "Sur les nombres de Mersenne", *Elemente der Mathematik*, vol. 15, no. 6, pp. 113–115, 1960.

[3] T. Nagell, "The Diophantine equation $x^2 + 7 = 2^n$", *Arkiv för Matematik*, vol. 4, no. 3, pp. 185–187, 1961.

[4] R. Scott and R. Styer, "On the generalized Pillai equation $\pm a^x \pm b^y = c$", *Journal of Number Theory*, vol. 118, no. 2, pp. 236–265, 2006.