MATCH
Communications in Mathematical and in Computer Chemistry

MATCH Commun. Math. Comput. Chem. **96** (2026) 43–52
ISSN: 0340–6253
doi: 10.46793/match.96-1.29025

Discussing Diophantine Problems with a Large Language Model

Sanja Stevanović[a,*], **Dragan Stevanović**[b]

[a] *Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia*

[b] *Abdullah Al Salem University, Khaldiya, Kuwait*

sanja.stevanovic@mi.sanu.ac.rs, dragan.stevanovic@aasu.edu.kw

(Received November 5, 2025)

Abstract

Recent versions of large language models have become increasingly reliable in providing mathematical arguments, especially in classical topics such as Diophantine problems. We exemplify this development here by using ChatGPT to solve an open Diophantine problem from Majstorović Ergotić and Došlić [MATCH Commun. Math. Comput. Chem. 95 (2026) 265–283].

1 Introduction

During the 1980s expert systems generated high expectations, as rule-based programs were seen as a route to codified human expertise. Those expectations generally failed to be realized in practice, because acquiring and encoding domain knowledge at scale, handling uncertainty and exceptions, and keeping rule sets consistent and up to date all turned out to be far harder than anticipated. Limited computational resources of the

*Corresponding author.

era and poor integration with statistical learning meant that such systems could not generalize beyond narrow, well curated scenarios [1–5]. Nevertheless, numerous methodological insights from that period (knowledge representation, ontologies, rule engines) later informed more successful hybrid and learning-based approaches.

Current large language models (LLMs) have become ubiquitous in research, industry and consumer applications, powering search, coding assistants, chatbots and content generation. Their rapid emergence over the last decade was enabled by a confluence of different factors: the transformer architecture and empirical scaling laws that made model performance improve predictably with size, the availability of vast, web-scale text corpora and better data curation practices, dramatic increases in computing power (GPUs/TPUs and cloud infrastructure) and distributed training techniques, as well as numerous algorithmic advances. Open research, shared toolchains, and large public datasets further accelerated their deployment and adoption.

While there are certainly limitations to what LLMs can achieve, they can still be quite effective as math-capable assistants, especially in well developed mathematical theories, such as Diophantine problems, and Pell equations in particular. This effectiveness mainly stems from their broad training on well established methods combined with rapid pattern recognition and robust symbolic manipulation.

Our goal here is to exemplify this effectiveness on a recent open Diophantine problem from this journal. Majstorović Ergotić and Došlić [6] recently showed that complete split graphs maximize generalized complementary second Zagreb index among connected graphs of order n. Recall that a complete split graph $CS_{k,n-k}$ consists of a complete subgraph on k vertices and an empty subgraph on $n-k$ vertices, such that each vertex of the complete subgraph is adjacent to each vertex of the empty subgraph. Majstorović Ergotić and Došlić [6, Theorem 2] proved that the extremal complete split graph is unique, unless $17n^2 - 28n + 4$ is a perfect square such that $\sqrt{17n^2 - 28n + 4}$ is congruent to $n - 6$ modulo 8, in which case there are two extremal complete split graphs. After presenting a few concrete examples of small such orders $n \in \{2, 12, 117, 450\}$, and observing their rarity among natural numbers less than 10^9, they left as an open problem to show that there are infinitely many such orders.

Here we solve this open problem through a short discussion with a particular LLM—free version of ChatGPT's GPT-5 Thinking model—using a few natural prompts:

- *Can you characterize when is* $17n^2 - 28n + 4$ *a perfect square?*
- *Can you now characterize when is, for the values of* n *from your previous answer, the square root of* $17n^2 - 28n + 4$ *congruent to* $n - 6$ *modulo 8?*
- *How do we know that these are all such values of* n*?*

Following sections represent mostly unabridged replies to these prompts, which have been—nevertheless—thoroughly checked for correctness. The affirmative answer to the open problem of Majstorović Ergotić and Došlić is evident from these replies.

2 Reply to the first prompt

Start with

$$17n^2 - 28n + 4 = m^2.$$

Multiply both sides by 68 and set

$$k := 34n - 28.$$

A direct computation gives

$$k^2 - 68m^2 = 512.$$

Conversely, any integer solution (k, m) of $k^2 - 68m^2 = 512$ with $k \equiv -28 \pmod{34}$ yields an integer

$$n = \frac{k + 28}{34}$$

solving the original equation. Thus integer solutions (n, m) are equivalent to integer solutions (k, m) of the Pell-type equation

$$k^2 - 68m^2 = 512, \qquad k = 34n - 28. \tag{1}$$

The homogeneous Pell equation

$$x^2 - 68y^2 = 1$$

has fundamental unit

$$\varepsilon = 33 + 4\sqrt{68},$$

because $33^2 - 68 \cdot 4^2 = 1$. Every solution of the inhomogeneous equation (1) is obtained from a finite set of primitive solutions (k_0, m_0) by multiplying by arbitrary integer powers of ε:

$$k_t + m_t\sqrt{68} = (k_0 + m_0\sqrt{68})\,\varepsilon^t, \qquad t \in \mathbb{Z}, \tag{2}$$

which is equivalent to the recurrence

$$\begin{aligned} k_{t+1} &= 33k_t + 272m_t, \\ m_{t+1} &= 4k_t + 33m_t. \end{aligned}$$

For each such pair (k_t, m_t) we recover

$$n_t = \frac{k_t + 28}{34} \in \mathbb{Z}.$$

3 Reply to the second prompt

Lemma 1. *Let* $a, b \in \mathbb{Z}$. *If* $a^2 \equiv b^2 \pmod{16}$ *then:*

(i) If $b \not\equiv 0, 4 \pmod 8$, *then* $a \equiv \pm b \pmod 8$.

(ii) If $b \equiv 0, 4 \pmod 8$, *then* $a \equiv 0, 4 \pmod 8$.

Proof. Reduce residues modulo 8. The squares of residues $r \in \{0, \ldots, 7\}$

modulo 16 are:

r	0	1	2	3	4	5	6	7
$r^2 \pmod{16}$	0	1	4	9	0	9	4	1

From the table the value 1 arises only from $\{\pm 1\}$, 4 only from $\{\pm 2\}$, and 9 only from $\{\pm 3\}$; thus for those square classes equality of squares modulo 16 forces the residues to be negatives of each other modulo 8. The value 0 arises from $\{0, 4\}$, which are not negatives of each other modulo 8; hence the exceptional behaviour in (ii). ■

From

$$m^2 - (n-6)^2 = 16(n-2)(n+1)$$

we deduce $m^2 \equiv (n-6)^2 \pmod{16}$. Applying the lemma:

- If $n - 6 \not\equiv 0, 4 \pmod 8$ (equivalently $n \not\equiv 2, 6 \pmod 8$), then

  $$m \equiv \pm(n-6) \pmod 8.$$

  The choice of sign $(+)$ or $(-)$ is invariant on each Pell orbit (2), so it suffices to test one primitive representative per orbit.

- If $n \equiv 2 \pmod 8$ or $n \equiv 6 \pmod 8$ (the *exceptional classes*), then $(n-6)^2 \equiv 0 \pmod{16}$ and the congruence modulo 16 only gives $m \equiv 0$ or $4 \pmod 8$. In these exceptional classes one must use more information (for instance the primitive Pell representative) to determine whether $m \equiv n - 6$ or $m \equiv 6 - n$ modulo 8.

Below we list a convenient choice of one primitive representative per Pell orbit (2) that yields integer $n_0 = (k_0 + 28)/34$. For each seed we give (k_0, m_0), the corresponding n_0, and the value of $m_0 \pmod 8$ and $n_0 - 6 \pmod 8$ so the sign is immediate.

orbit	k_0	m_0	n_0	$n_0 - 6 \pmod 8$	$m_0 \pmod 8$	sign
1	-28	2	0	2	2	+
2	40	4	2	4	4	+
3	142	17	5	7	1	-
4	380	46	12	6	6	+
5	1468	178	44	6	2	-
6	3950	479	117	7	7	+

There are six Pell orbits of solutions represented above by the six listed seeds. Using (2) each seed produces infinitely many integers n with $17n^2 - 28n + 4$ a perfect square. For each infinite orbit the congruence $m \equiv n - 6 \pmod 8$ (or the opposite sign) is constant; the explicit table above tells which sign occurs for each orbit. In particular the infinite orbits with representatives $n_0 \in \{0, 2, 12, 117\}$ satisfy $m \equiv n - 6 \pmod 8$, while the infinite orbits with representatives $n_0 \in \{5, 44\}$ satisfy $m \equiv 6 - n \pmod 8$.

4 Reply to the third prompt

We consider integer solutions of the inhomogeneous Pell equation

$$k^2 - 68m^2 = 512. \tag{3}$$

Two solutions (k, m) and (k', m') are *equivalent* if

$$k' + m'\sqrt{68} = (k + m\sqrt{68})\varepsilon^t \qquad (t \in \mathbb{Z}),$$

where $\varepsilon = 33 + 4\sqrt{68}$ is the fundamental unit of $\mathbb{Z}[\sqrt{68}]$. The equivalence classes under this action are the *Pell orbits*. A solution (k_0, m_0) is called *primitive* if its equivalence class is not obtained by multiplying a smaller integer solution by a unit; equivalently, primitive solutions are representatives of distinct Pell orbits.

Lemma 2. *There are only finitely many primitive solutions to* (3)*. More-*

over, every primitive representative (k_0, m_0) *has*

$$|k_0| \le \left\lfloor \frac{\varepsilon + 512}{2} \right\rfloor \quad \text{and} \quad |m_0| \le \left\lfloor \sqrt{\frac{\left(\lfloor(\varepsilon+512)/2\rfloor\right)^2 - 512}{68}} \right\rfloor,$$

so the set of primitive representatives can be found by a finite (and quite small) search.

Proof. Let $\alpha = k + m\sqrt{68} \in \mathbb{Z}[\sqrt{68}]$ satisfy $N(\alpha) = k^2 - 68m^2 = 512$. Write the two real embeddings

$$\varphi_1(\alpha) = k + m\sqrt{68}, \qquad \varphi_2(\alpha) = k - m\sqrt{68},$$

so that $\varphi_1(\alpha)\varphi_2(\alpha) = 512$. The unit $\varepsilon > 1$ acts by $\varphi_1(\alpha) \mapsto \varepsilon\varphi_1(\alpha)$, $\varphi_2(\alpha) \mapsto \varepsilon^{-1}\varphi_2(\alpha)$, hence for every orbit there exists a unique representative α with

$$1 \le \varphi_1(\alpha) < \varepsilon.$$

(Choose the unique integer t so that $\varphi_1(\alpha)\varepsilon^{-t} \in [1, \varepsilon)$.)

For such a representative we have

$$\varphi_2(\alpha) = \frac{512}{\varphi_1(\alpha)} \le \frac{512}{1} = 512,$$

and therefore

$$|k| = \left| \frac{\varphi_1(\alpha) + \varphi_2(\alpha)}{2} \right| \le \frac{\varepsilon + 512}{2}.$$

Setting

$$K := \left\lfloor \frac{\varepsilon + 512}{2} \right\rfloor,$$

we obtain the uniform bound $|k| \le K$ for any representative chosen in the fundamental interval. From (3) we then have

$$68m^2 = k^2 - 512 \le K^2 - 512,$$

hence

$$|m| \le \sqrt{\frac{K^2 - 512}{68}}.$$

Since k, m are integers, there are only finitely many pairs (k, m) satisfying these bounds; each such pair can be tested in the Diophantine equation (3) to decide whether it is a representative. This proves finiteness and reduces the classification of primitive orbits to a finite search. ■

Numerically $\sqrt{68} \approx 8.2462112512$ and

$$\varepsilon = 33 + 4\sqrt{68} \approx 65.9848450049,$$

so

$$K = \left\lfloor \frac{\varepsilon + 512}{2} \right\rfloor = \left\lfloor \frac{577.9848450049}{2} \right\rfloor = 288.$$

Hence any primitive representative with $1 \le \varphi_1(\alpha) < \varepsilon$ obeys

$$|k| \le 288, \qquad |m| \le \left\lfloor \sqrt{\frac{288^2 - 512}{68}} \right\rfloor = 34.$$

Thus the exhaustive search can be performed over the small finite box

$$k \in \{-288, \dots, 288\}, \quad m \in \{-34, \dots, 34\},$$

which is readily checked by a short computation.

Carrying out the finite search described above (or, equivalently, performing elementary congruence sieving followed by a bounded search) yields exactly six distinct primitive Pell–orbits for (3). One convenient choice of primitive seeds (one representative per orbit) is

$$(k_0, m_0) \in \{(-28, 2),\ (40, 4),\ (142, 17),\ (380, 46),\ (1468, 178),\ (3950, 479)\}.$$

Each of these pairs satisfies $k_0^2 - 68m_0^2 = 512$. The corresponding values

$$n_0 = \frac{k_0 + 28}{34}$$

are integers and give the small nonnegative orbit representatives

$$n_0 \in \{0,\ 2,\ 5,\ 12,\ 44,\ 117\},$$

which are the representatives used in Section 3 to separate the orbits according to the congruence of the square root modulo 8.

Remark. The occurrence of exactly six primitive orbits is a concrete instance of the general phenomenon that, for a fixed nonzero norm N in a real quadratic order, the set of algebraic integers of norm N splits into finitely many orbits under the multiplicative action of the unit group (which is infinite cyclic). The elementary numeric bounds above make this finiteness effective and allow one to determine the orbits by a trivial finite computation.

5 Concluding remarks

The affirmative solution to the open Diophantine problem from [6] is evident already from the replies to the first two prompts. We have added the third prompt only to make sure that the reply to the second prompt did not miss any of the primitive representatives.

Despite the fact that it provided a concrete solution to a concrete open problem, the main purpose of this note is to inform the readers of MATCH of the usefulness of modern LLMs. Anyway, this is not to say that this usefulness should be blindly trusted. While repeating the same prompts from different accounts, we noticed that GPT-5 Thinking model produces different, but equivalent replies. Our observations suggest that the model actually tends to shape its replies to the history of exchanges with the researcher: the model may reply with sloppier or partially incorrect replies to less careful researchers who do not point out discrepancies in its replies. Hence the readers should always be cautious and properly check the validity of all replies.

***Acknowledgment*:** This research was supported by the Science Fund of the Republic of Serbia, #6767, Lazy walk counts and spectral radius of threshold graphs—LZWK, and by the Croatian Science Foundation under the project number HRZZ-IP-2024-05-2130.

References

[1] D. M. Cvetković, L. L. Kraus, S. K. Simić, Discussing graph theory with a computer, I: Implementation of graph theoretic algorithms, *Publ. Elektrotehn. Fak. Ser. Mat. Fiz.* **716–734** (1981) 100–104.

[2] D. M. Cvetković, Discussing graph theory with a computer, II: Theorems suggested by the computer, *Publ. Inst. Math. Nouv. Sér.* **33(47)** (1983) 29–33.

[3] D. Cvetković, I. Pevac, Discussing graph theory with a computer, III: Man-machine theorem proving, *Publ. Inst. Math. Nouv. Sér.* **34(48)** (1983) 37–47.

[4] D. M. Cvetković, Discussing graph theory with a computer, IV: Knowledge organization and examples of theorem proving, in: D. Cvetković, I. Gutman, T. Pisanski, R. Tošić (Eds.), *Proc. 4th Yugosl. Semin. Graph Theory*, Univ. Novi Sad, Novi Sad, 1983, pp. 43–68.

[5] D. Cvetković, Discussing graph theory with a computer, VI: Theorems proved with the aid of the computer, *Bull. Cl. Sci. Math. Nat. Sci. Math.* **16** (1988) 51–70.

[6] S. Majstorović Ergotić, T. Došlić, Graphs with maximum generalized complementary second Zagreb index, *MATCH Commun. Math. Comput. Chem.* **95** (2026) 265–283.