Forbidden Sidon subsets of perfect difference sets, featuring a human-assisted proof

Boris Alexeev ChatGPT* Lean† Dustin G. Mixon‡§

Abstract

We resolve a $1000 Erdős prize problem, complete with formal verification generated by a large language model.

In over a dozen papers, beginning in 1976 and spanning two decades, Paul Erdős repeatedly posed one of his "favourite" conjectures: every finite Sidon set can be extended to a finite perfect difference set. We establish that $\{1, 2, 4, 8, 13\}$ is a counterexample to this conjecture.

During the preparation of this paper, we discovered that although this problem was presumed to be open for half a century, Marshall Hall, Jr. published a different counterexample three decades *before* Erdős first posed the problem. With a healthy skepticism of this apparent oversight, and out of an abundance of caution, we used ChatGPT to vibe code a Lean proof of both Hall's and our counterexamples.

1 Introduction

We note that this paper is written mostly in the style of an ordinary mathematics paper, so we suggest skipping ahead to Section 7 if the reader is primarily curious about the role of artificial intelligence in this paper, including the sense in which this features a "human-assisted proof".

Paul Erdős wrote many papers on the subject of *Sidon sets/sequences*, also called $B_2[1]$ *(or* B_2 *for short) sets/sequences*. We give a definition and an equivalent restatement:

Definition 1. A set A (typically of integers) is a *Sidon set* if all differences $a - a'$ of distinct $a, a' \in A$ are distinct.

Remark. Beware that harmonic analysts use the term "Sidon set" to mean something entirely different.

✓ **Observation 2.** *Equivalently, A is a Sidon set if all sums $a + a'$ with $a, a' \in A$ are distinct, up to re-ordering of the terms $a + a' = a' + a$.*

Proof. The equivalence follows from the fact that $a - b = c - d$ is equivalent to $a + d = b + c$, though note that in the case of differences we ignore all differences $a - a = 0$, whereas in the case of sums we *do* consider the sums $a + a$. For example, $\{1, 2, 3\}$ is not a Sidon set because of the identity $2 - 1 = 3 - 2$ using differences or the identity $1 + 3 = 2 + 2$ using sums. □

Erdős posed many problems about Sidon sets, especially regarding their sizes, many of which are still open. For example, Erdős asked how quickly the elements grow in "the greedy Sidon set", also known as the "Mian–Chowla sequence" [40] (OEIS sequence A005282 [42]):

Problem 3. *Let $A = \{1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, \dots\}$ be the greedy Sidon sequence, constructed at each step by picking the smallest positive integer that preserves the Sidon property. What is the order of growth of A?*

*ChatGPT with GPT-5, the large language model (LLM) from OpenAI [43]. Nota bene: ChatGPT did not write any of the text of this paper.

†Lean 4, the open-source programming language and proof assistant [41], using results from Mathlib [38], the community-developed library of formalized mathematics. Lean was used to verify the correctness of results.

‡Department of Mathematics, The Ohio State University, Columbus, OH

§Translational Data Analytics Institute, The Ohio State University, Columbus, OH

✓ denotes that the corresponding result has been verified in Lean.

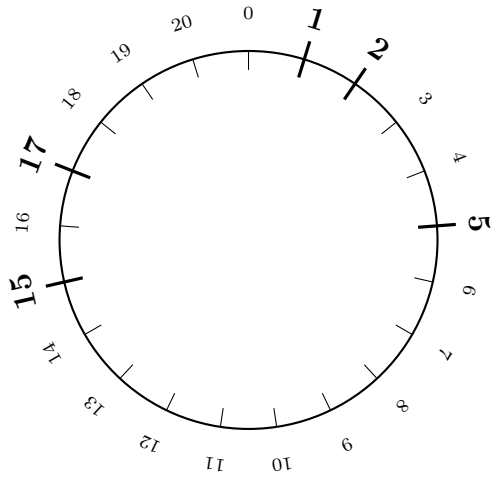


Figure 1: An illustration of the perfect difference set $B = \{1, 2, 5, 15, 17\}$ mod 21. One can check that every difference from 1 to 20 appears exactly once between the bold ticks; for example, 6 is witnessed by $2 - 17 \pmod{21}$. Suppose you have a favorite set, such as $A = \{1, 5, 15\}$. Erdős's conjecture asks whether or not it is always possible to find a perfect difference set B modulo *some* v that contains your favorite set A, assuming of course that A doesn't already have a repeated difference. In this paper, we disprove this conjecture: you will be disappointed if your favorite set is $\{1, 2, 4, 8, 13\}$.

Erdős did not believe that the Mian–Chowla sequence was optimally dense. Instead, he made a specific conjecture about the maximum asymptotic size of a Sidon set of natural numbers:

Conjecture 4. *There exists a Sidon set of natural numbers $A \subset \mathbb{N}$ so that*

$$\limsup_{n\to\infty} \frac{|A \cap \{1, \ldots, n\}|}{\sqrt{n}} = 1.$$

Erdős and Turán [25] proved that this lim sup is at most 1 for every Sidon set A by analyzing the finite case. Meanwhile, Erdős showed that there exists a Sidon set A achieving $1/2$, and Krückeberg [36] achieved $1/\sqrt{2}$. Erdős saw one potential path to proving Conjecture 4 via perfect difference sets.

Definition 5. Given an abelian group G, a set $B \subset G$ is a *perfect difference set* for G if the differences $d = b - b'$ of distinct $b, b' \in B$ represent every nonzero element $d \in G$ exactly once. If B is a set of integers, then we say that B represents a perfect difference set modulo $v > 0$ if the images of B modulo v form a perfect difference set in the cyclic group $\mathbb{Z}/v\mathbb{Z}$ (the integers modulo v). In the sequel, we say *finite perfect difference set* when the group is $\mathbb{Z}/v\mathbb{Z}$, and we say *infinite perfect difference set* when the group is $\mathbb{Z}$.

Remark. Note that if B represents a perfect difference set modulo v, we insist that the elements of B be distinct modulo v, as otherwise $b_1 \equiv b_2$ would induce a zero difference $b_1 - b_2 \equiv 0$ of distinct elements in B. Also, the name v is chosen for the modulus to align with standard practice in the theory of designs, where we also mention that the word "perfect" (the condition that each nonzero residue is represented exactly once) corresponds to $\lambda = 1$.

✓ **Observation 6.** *Every perfect difference set is a Sidon set.*

By a simple counting argument, a perfect difference set modulo v can exist only if $v = q^2 + q + 1$ for some integer q, in which case its size is $|B| = q + 1$. Singer [44] proved that such a perfect difference set exists for each prime power q.

Erdős made the following optimistic[1] conjecture, which would imply Conjecture 4:

Conjecture 7. *Every finite Sidon set can be extended to a finite perfect difference set.*

[1] Besides optimism, Erdős also mentioned as motivation similar results by Treash, Lindner, and others, for Steiner systems and other more complicated combinatorial structures.

Indeed, one could then start with any Sidon set A and repeatedly perform two operations: arbitrarily extending A with some new element (which is always possible) and extending A to a perfect difference set (taking the smallest positive representatives modulo v). Since a perfect difference set up to q^2+q+1 has size $q+1$ (which is asymptotically equivalent to $\sqrt{q^2+q+1}$), Conjecture 4 follows.

Erdős posed Conjecture 7 in at least 16 papers [10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 31] with publication dates from 1976 to 1997, differing slightly in the meaning of "extended" as well as which perfect difference sets are allowed. This problem also appears in both sections **C9** ("Packing sums of pairs", including Sidon sequences) and **C10** ("Modular difference sets and error correcting codes", including perfect difference sets) of Guy's "Unsolved Problems in Number Theory" [32]. In 1980 [13], Erdős wrote:

> [Conjecture 4] would follow from one of my favourite recent conjectures: Let $1 \leq a_1 < \cdots < a_k$ be a finite B_2 sequence. Prove that it can be imbedded into a perfect difference set, i.e. there is a prime p and a set of $p+1$ residues $u_1, \ldots, u_{p+1} \bmod p^2+p+1$ so that all the differences $u_i - u_j$ are incongruent mod p^2+p+1 and the a's all occur amongst the u's. I offer a thousand dollars for a proof or disproof of this conjecture.

The main difference regarding the perfect difference sets is whether one requires p to be prime (as in the text above). Sometimes there is no restriction, whereas other times there is an unqualified $p = q^\alpha$, thus presumably referring to a prime power. At least once [19], he wondered whether perhaps it might be true for all sufficiently large primes p.

Erdős famously offered prizes for solutions to many of his favorite problems. The dollar amounts covered a wide range, ranging from ten dollars to thousands of dollars. Only three problems are known [8] to have a prize larger than $1000. (One regarding prime gaps was solved by Maynard [39] and Ford, Green, Konyagin, and Tao [26]. The other two are still unsolved; both ask about the density of sets avoiding arithmetic progressions in different ways. One is the Erdős conjecture on arithmetic progressions, which states that if A is a set of positive integers such that $\sum_{n\in A} 1/n$ diverges, then A contains arbitrarily long arithmetic progressions.)

If one requires p to be prime (as in Erdős's statement of his $1000 problem above), then we exhibit a particularly simple counterexample with four elements (the first powers of two):

✓ **Theorem 8.** *The finite Sidon set $\{1,2,4,8\}$, which is the first* four *terms of the Mian–Chowla sequence, does not extend to a finite perfect difference set modulo $v = p^2+p+1$ for any prime p.*

If one allows for an arbitrary perfect difference set (as in our statement of Conjecture 7), then we exhibit a counterexample with five elements:

✓ **Theorem 9.** *The finite Sidon set $\{1,2,4,8,13\}$, which is the first* five *terms of the Mian–Chowla sequence, does not extend to a finite perfect difference set modulo any $v > 0$.*

During the preparation of this paper, we were surprised to learn that Marshall Hall, Jr. already disproved Conjecture 7 in 1947 [34], writing the following:

> From this theorem it immediately follows that there are many sets of integers satisfying the conditions of [Definition 1] which cannot be extended to any finite [perfect] difference set. For example the set $-8, -6, 0, 1, 4$ may not be so extended.

Because one can translate perfect different sets, an equivalent counterexample containing only positive integers can be produced by adding 9 to obtain $\{1,3,9,10,13\}$.

Clearly, it appears that Erdős was not aware of this result. The authors of this paper were also unaware of this result, even though they performed a reasonably deep literature search prior to starting this project. (In fact, no large language model could find Hall's result, even with substantial prompting that the result indeed exists.) Instead, the paper was discovered by accident when searching for support for Conjecture 14.

We were completely taken aback by our discovery of Hall's result. Hall's paper appeared in a famous journal, and it is clear that the paper is well-known, since, for example, it is cited by Guy [32] just two sentences before stating Conjecture 7 in section **C10**. So then why is Hall's counterexample not an accepted resolution of this conjecture? Maybe there's a missing hypothesis? Maybe it contains a deeper flaw? In pursuit of the truth, we were determined to obtain a formal proof; we chose Lean [41] as our proof assistant because many other mathematicians have done the same recently. However,

since we're not experts in Lean (nor any other proof assistant), we prompted ChatGPT [43] to write the code for us. In the end, we obtained a human-assisted Lean proof of Hall's counterexample, and of Theorems 8 and 9 (mind the double check marks ✓✓ above).

The resulting formal proof is thousands of lines, nearly all of which were written by ChatGPT. Accordingly, we believe that ChatGPT is properly *an author* of the formal proof accompanying this paper. Unfortunately, large language models are known to hallucinate and otherwise produce incorrect results, so we would not be able to trust this proof unless it was in a formal language. Therefore, we believe Lean is also an author, or perhaps ChatGPT and Lean may be credited together. Even so, while our formal proofs were written and verified by the second and third authors, we stress that this paper was written the old-fashioned way by the first and fourth authors.

Before diving into the proof, we briefly discuss *infinite* Sidon and perfect difference sets in Section 2. In Section 3, we give a direct proof of Theorem 8. In Sections 4 and 5, we follow Hall's proof by building up some mathematical structure involving projective planes in order to prove Theorems 8 and 9, as well as the correctness of Hall's original counterexample. Section 6 discusses our Lean proof, which we vibe coded using ChatGPT, while Section 7 discusses the broader role of AI in this paper. We conclude in Section 8 with ideas for future directions.

Acknowledgments

The online collection `erdosproblems.com` includes Problem 3 as #340 [6], Conjecture 4 as #329 [5], and Conjecture 7 as #707 [7]. (Problem #44 [4] may also be of interest, as it is intermediate between #707 and #329.) The authors thank Thomas Bloom for creating and curating this very useful resource. We also appreciate the lively community that has arisen around it.

Our formalization would have been much more difficult without the proof assistant Lean. The authors are especially grateful to the Mathlib community for their unified library of mathematics in Lean4. Even with this extensive library, we found it surprisingly painful to successfully write proofs in Lean, so we also thank OpenAI for producing a large language model (namely, ChatGPT with GPT-5) that is capable of meeting a human mathematician halfway (or at least partway).

DGM was partially supported by NSF DMS 2220304.

2 Some minor remarks on infinite sets

The following table summarizes whether a finite/infinite Sidon set can always be extended to a finite/infinite perfect difference set:

Does a Sidon set always extend to a perfect difference set?		**perfect difference set**	
		finite	*infinite*
Sidon set	*finite*	No (this paper)	Yes (see Claim 10)
	infinite	No (pigeonhole)	No (see Reference [9])

We briefly mention the infinite case.

Claim 10. *Every finite Sidon set can be extended to an infinite perfect difference set.*

Proof. This result and its proof are stated formally by Hall [34, Theorem 3.1], but the proof is essentially a "just-do-it" [29, 30] greedy construction wrapped around the observation that there are only finitely many obstructions to adding a missing difference. □

Alternatively, one may ask whether an *infinite* Sidon set can always be extended to an infinite perfect difference set. Here, the answer is no, as pointed out by Cilleruelo and Nathanson [9]. An easy counterexample is $A = \{2b \mid b \in B\}$, where B is an infinite perfect difference set. Indeed, A is a Sidon set, but adding an even number to A causes an immediate problem, while adding two odd numbers also results in a contradiction. Thus, A cannot be extended to a perfect difference set.

Finally, obviously an infinite Sidon set cannot be extended to a finite perfect difference set.

Having briefly discussed these infinite cases, the remainder of this paper will focus on *finite* Sidon and perfect difference sets, as Erdős had done in Conjecture 7.

3 A direct solution to Erdős's $1000 problem

The next two sections build up various structures involving projective planes in order to prove Theorems 8 and 9 and confirm Hall's original counterexample following his original proof. In what follows, we present a short, direct proof of Theorem 8 that bypasses all of this extra structure.

✓ **Theorem 8.** *The finite Sidon set* $\{1, 2, 4, 8\}$*, which is the first* four *terms of the Mian–Chowla sequence, does not extend to a finite perfect difference set modulo* $v = p^2 + p + 1$ *for any prime* p*.*

Proof. Suppose, for contradiction, that B represents a perfect difference set modulo $v = p^2 + p + 1$ that contains $\{1, 2, 4, 8\}$. We identify B with the set of residues comprising its images modulo v, and write an equals sign to denote modular equality. (Note that $\{1, 2, 4\}$ is a perfect difference set modulo $7 = 2^2 + 2 + 1$, but this does not count as an extension of $\{1, 2, 4, 8\}$ precisely because 1 and 8 are identical modulo 7.)

As Erdős already observed in the quotation in Section 1, the perfect difference set B has cardinality $p+1$ because there are $v-1 = p^2+p = (p+1)\cdot p$ nonzero residues modulo v and $|B|\cdot(|B|-1)$ ordered pairs of distinct elements of B. Since B contains at least four elements by assumption, we have $p \geq 3$, whence the prime p is odd and $|B| = p + 1$ is even.

We prove a small result inline that will be useful later. Consider an arbitrary $a \notin B$. Define the function $f_a \colon B \to B$ by $f_a(b) = c$ if $a - b = c - d$ in the unique representation of $a - b$ with $c, d \in B$. (The residue $a - b$ is nonzero precisely because $a \notin B$.) This function f_a is an involution, because if $f_a(b) = c$ then clearly $a - c = b - d$ is the corresponding representation of $a - c$ and thus $f_a(c) = b$. Finally, note that if f_a has a fixed point b, i.e., $f_a(b) = b$, that implies that $a-b = b-d$ or equivalently $2b = a + d$.

As the main part of the proof, for each $x \in B$, we will find two elements $b_x, d_x \in B$ so that

$$2b_x = 2(x - 1) + d_x,$$

where moreover d_x is different for different x. If $x = 2$, then we choose $b_2 = d_2 = 2$ as in $2 \cdot 2 = 2 \cdot (2 - 1) + 2$. Otherwise, we will use the construction from the previous paragraph with $a = 2(x - 1)$. Observe that $a \notin B$ because otherwise $x-2 = a-x$ would be two distinct representations of the nonzero residue $x - 2$ as differences in B. Because f_a is an involution on the set B with even cardinality, it has an even number of fixed points. One such fixed point is x because $2(x - 1) - x = x - 2$, so it has another fixed point, say $b_x \neq x$. Together with its corresponding d_x, we obtain our desired identity $2b_x = 2(x - 1) + d_x$.

Suppose $x \neq x'$ but $d_x = d_{x'}$. Then we may subtract $2b_x = 2(x-1)+d_x$ and $2b_{x'} = 2(x'-1)+d_{x'}$ to get $2(b_x - b_{x'}) = 2(x - x')$ or equivalently (because the modulus v is odd) $b_x - b_{x'} = x - x'$. These two representations must be identical, so $b_x = x$ and $b_{x'} = x'$. But in choosing b_x and $b_{x'}$, we insisted that $b_x \neq x$ and $b_{x'} \neq x'$ except possibly if $x = 2$ and $x' = 2$, a contradiction.

Finally, since we have a different d_x for each x, the d_xs are a permutation of the finite set B and there exists an x for which $d_x = 4$. Expanding the corresponding identity gives $2b_x = 2(x - 1) + 4$ or (again because v is odd) $b_x = x + 1$. The only representation of 1 as a difference $b_x - x$ in B is as $1 = 2 - 1$, so $x = 1$ and thus $d_1 = 4$. Similarly, there exists an x' for which $d_{x'} = 8$. Reasoning similarly, noting the only representation of 3 as $3 = 4 - 1$, we obtain $x' = 1$ as well and thus $d_1 = 8$, a contradiction. □

Remark. The condition that p is prime is necessary for this counterexample. Indeed,

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256\} \equiv \{1, 2, 4, 8, 16, 32, 64, 55, 37\} \pmod{73}$$

is a perfect difference set mod $73 = 8^2 + 8 + 1$. Accordingly, we need another element in our counterexample in Theorem 9.

4 Cyclic projective planes

Throughout the more structured solution of the problem, we use the terminology of (finite) projective planes. We will gradually build up progressively more structure, which will prove very useful.

Definition 11. A projective plane is an incidence structure between *points* and *lines* such that

- given any two distinct points, there is exactly one line incident with both of them,
- given any two distinct lines, there is exactly one point incident with both of them, and
- the plane is not degenerate.

The specific phrasing of non-degeneracy varies across different sources. Often the condition is that there are four points, no three of which are collinear. At the present moment, Mathlib has the condition

$$p_1 \notin l_2 \wedge p_1 \notin l_3 \wedge p_2 \notin l_1 \wedge p_2 \in l_2 \wedge p_2 \in l_3 \wedge p_3 \notin l_1 \wedge p_3 \in l_2 \wedge p_3 \notin l_3,$$

described as "three points in general position".

✓ **Observation 12.** *There exists a positive integer $q \geq 2$, called the* order *of the plane, such that there are q^2+q+1* points *(each on $q+1$ lines) and q^2+q+1* lines *(each with $q+1$ points).*

Proof. Pleasantly, these basic results about projective planes are already known to Mathlib. □

We very quickly recap some well-known facts about projective planes: Given a finite field of order q, one can construct a projective plane of order q. Thus, there exist projective planes of order q for all prime powers q. It is unknown whether there is a projective plane of any other order. Order 12 is the smallest for which it is unknown whether a projective plane exists.

Desargues's theorem states that "Two triangles are in perspective axially if and only if they are in perspective centrally" (but because it is inessential for the remainder of the paper, we do not elaborate on what this means). A projective plane satisfying Desargues's theorem is called *Desarguesian*, which includes all planes defined from a field (as mentioned above). There exist non-Desarguesian projective planes (though the known finite examples are still of prime power order).

We mention all of this background because perfect difference sets correspond to *cyclic* projective planes. This is a projective plane with the additional structure of a regular action by a cyclic group (a kind of *collineation*). We do not prove the equivalence of these two notions here, but rather only the single direction we need:

✓ **Lemma 13** (one direction of Theorem 2.1 in Hall [34], but likely implicitly known to Singer [44] and others)**.** *Suppose B is a perfect difference set modulo $v = q^2+q+1$ with $q \geq 2$. Considering the residues x modulo v as points, the translates $B+y$ (also modulo v) of B as lines, and incidence as set membership (so point x is on line $B+y$ if $x \in B+y$, or equivalently $x-y \in B$) produces a projective plane of order q.*

Proof. The axioms of the projective plane follow straightforwardly from the unique representations of all nonzero residues modulo v as differences in B. For example, if $x - x' = b - b'$ is the unique representation of the nonzero residue $x - x'$ with $b, b' \in B$, then $B + (x - b) = B + (x' - b')$ is the unique line through the distinct points x and x'. □

Singer [44] showed that the projective planes constructed from finite fields are cyclic, and thus perfect difference sets exist modulo $v = q^2+q+1$ when q is a prime power. The "prime power conjecture" states that there are no cyclic projective planes (and thus no perfect difference sets) for any other order. Unlike the situation above without the extra "cyclic" condition, this has been verified at least up to two billion [3]. Because projective planes constructed from fields are Desarguesian, a related conjecture is the following:

Conjecture 14. *Every finite cyclic projective plane (and thus perfect difference set) is Desarguesian.*

We mention this conjecture for a couple reasons. First, if it were known to be true, we have constructed alternate proofs of Theorem 9 (which we do not describe here). Intuitively, this is because Desargues's theorem is a fairly strong restriction and interacts with the perfect difference set condition. Second, it is precisely researching the support for this conjecture that led the authors to find Hall's paper [34], where he says

> The properties found in [that paper's Section 4] make it highly plausible that every finite cyclic plane is Desarguesian.

However, because Conjecture 14 is open, we will not mention Desargues's theorem in the remainder of this work.

We note here an observation about Singer's construction that was useful to us during the exploratory phase of this work. The usual exposition of this construction is algebraic and chooses a primitive root in the field $GF(q^3)$, seen as a field extension of $GF(q)$, and then reasons about the (cyclic!) multiplicative group of $GF(q^3)$. This construction is very nice, but we found it very practical to work with a different one on the computer:

Construction 15 ([33], according to [34])**.** Given constants $a_1, a_2, a_3 \in GF(q)$, define a sequence (x_k) of elements of $GF(q)$ via the initial conditions $x_0 = 0$, $x_1 = 0$, $x_2 = 1$, and the third-order linear recurrence relation $x_k = a_1 x_{k-1} + a_2 x_{k-2} + a_3 x_{k-3}$ for $k \geq 3$. Then consider the indices k for which $x_k = 0$. For some values of the constants a_1, a_2, a_3, these indices are periodic modulo $q^2 + q + 1$ and form a perfect difference set.

Of course, the astute reader will see the relationship between this construction and Singer's. Moreover, it is possible to make the imprecise words "for some values of the constants a_1, a_2, a_3" exact and to classify which values work. The reason we wanted to share this construction is that we found that randomly choosing a_1, a_2, a_3, then simply checking whether the construction succeeded (and retrying otherwise) was very effective in practice and required minimal coding.

5 Polarities and the remainder of Hall's proof

Hall's proof factors through a handful of geometric results from Baer [1, 2] that identify intricate aspects of the well-known duality between points and lines in projective planes. We start by introducing the notions of *polarity* and *absolute* points and lines.

Definition 16. A *polarity* (an involutive duality/correlation) for a projective plane is a map π that switches its points and lines, preserves incidence, and has order two (applying it twice gives the identity).

✓ **Lemma 17** (Theorem 2.3 in Hall [34])**.** *The map π given by $x \rightleftharpoons B - x$ (swapping the point x with the line $B - x$) is a polarity for the construction from Lemma 13.*

Proof. The map π is clearly an involution that swaps points and lines, and it preserves incidence:

$$x \in B + y \iff x - y = (-y) - (-x) \in B \iff -y \in B - x \iff \pi(B + y) \in \pi(x). \quad \square$$

Definition 18. Fix a polarity π for a projective plane. A point p is called *absolute* (with respect to the polarity π) if p lies on its polar line $\pi(p)$. Dually, a line ℓ is called *absolute* if ℓ contains its polar $\pi(\ell)$.

✓ **Lemma 19** (Lemma 4.1 in Hall [34])**.** *A point x is absolute with respect to the polarity π from Lemma 17 if and only if $2x \in B$. It follows that there are exactly $q + 1$ absolute points.*

Proof. For the first part, we have

$$\text{point } x \text{ is absolute} \iff x \text{ lies on the line } B - x \iff 2x = x - (-x) \in B.$$

We know from earlier that $v = q^2 + q + 1$, so v is odd and 2 has a multiplicative inverse modulo v. Thus, for each $b \in B$, there is a unique residue x such that $2x = b$, and there are exactly $q+1$ absolute points, one corresponding to each element of B. $\square$

✓ **Proposition 20** (Lemma in Baer [1])**.** *For an arbitrary polarity for an arbitrary projective plane: An absolute line contains one and only one absolute point.*

Proof. By definition, an absolute line ℓ contains its polar $\pi(\ell)$, which is also absolute by definition, so it contains at least one absolute point.

Suppose p is an absolute point lying on the absolute line ℓ. By the polarity property, the point $\pi(\ell)$ lies on the line $\pi(p)$. It follows that p and $\pi(\ell)$ are two points that both lie on the lines ℓ and $\pi(p)$. If p did not equal $\pi(\ell)$, we would have two distinct lines passing through two distinct points in a projective plane, a contradiction. Thus $\pi(\ell)$ is the unique absolute point lying on an absolute line ℓ. $\square$

Proposition 21 (Lemma in Baer [2]). *For an arbitrary polarity for an arbitrary projective plane: If a line is not absolute, then the number of points on it which are not absolute is even.*

Proof. Suppose the line ℓ is not absolute, so it does not contain its polar $\pi(\ell)$. If p is a point on ℓ, then denote by p' the intersection of the lines ℓ and $\pi(p)$. By the properties of a polarity, $\pi(p)$ is the unique line passing through $\pi(\ell)$ and p'. It also follows that p is absolute if and only if $p = p'$, and that $p'' = p$. The points on ℓ which are not absolute therefore occur in pairs, proving our contention. □

Proposition 22 (Theorem 2 in Baer [2]). *For an arbitrary polarity for an arbitrary projective plane, of **odd** order q: A line is absolute if and only if it carries exactly one absolute point.*

Proof. The proof is immediate. If ℓ is absolute, then it contains exactly one absolute point by Proposition 20. Otherwise, ℓ contains $q+1$ points in total by Observation 12, which is even. An even number of those are not absolute by Proposition 21, so the remainder comprise an even number of absolute points. In particular, there is not exactly one absolute point. □

Proposition 23 (one direction of Corollary 1 (of Theorem 5) in Baer [2]). *For an arbitrary polarity for an arbitrary projective plane of **odd** order q: If the polarity has exactly $q+1$ absolute points, then there are no more than two absolute points on any line.*

Proof. Consider an absolute point p, which by definition lies on its polar line $\pi(p)$. Consider any other line $\ell \neq \pi(p)$ through p. By Proposition 22, it must contain at least one more absolute point. (If the line ℓ were absolute, it would contain the absolute point $\pi(\ell) \neq p$, which would suffice for the claim. But that actually contradicts Proposition 20, so ℓ is not absolute.)

We have identified all $q+1$ absolute points: besides p, there are the q distinct absolute points on each of the q other lines through p. (The points are distinct because different lines through p intersect only at p.) Hence every line through p contains at most one absolute point other than p.

This result applied to ℓ proves that ℓ contains at most two absolute points in total. □

Theorem 8. *The finite Sidon set $\{1, 2, 4, 8\}$, which is the first* four *terms of the Mian–Chowla sequence, does not extend to a finite perfect difference set modulo $v = p^2 + p + 1$ for any prime p.*

Another proof (see Section 3 for the first proof). Construct the projective plane from Lemma 13, and fix the polarity from Lemma 17.

From Lemma 19, we see that 1, 2 and 4 are absolute points that all lie on the single line $B + 0$. Thus, p is not odd by Proposition 23. Unfortunately, the sole even prime $p = 2$ is too small to extend the set A. □

Proposition 24 (Theorem 1 in Baer [2]). *For an arbitrary polarity for an arbitrary projective plane of **even** order q: Every line carries an odd number of absolute points.*

Proof. If q is even, then every line contains $q + 1$ points, which is odd. By Proposition 21, an even number of these are not absolute, leaving an odd number of absolute points as desired. □

Proposition 25 (The direction (i) implies (iii), from Corollary 2 (of Theorem 5) in Baer [2]). *For an arbitrary polarity for an arbitrary projective plane of **even** order q: If the polarity has exactly $q+1$ absolute points, then all absolute points lie on a line.*

Proof. Suppose the line ℓ contains a point p which is not absolute. Each of the $q + 1$ lines through p contain an absolute point by Proposition 24, which are all distinct and different from p. (As a few proofs ago: the points are distinct because different lines through p intersect only at p.) This accounts for all $q+1$ absolute points, so each line through p contains exactly one absolute point. In other words, if a line ℓ contains a point which is not absolute, then it contains exactly one absolute point.

There are at least $q + 1 \geq 2$ absolute points, so if we consider a line through any two of them, all points on that line must be absolute. Furthermore, again by counting, that accounts for all $q+1$ absolute points. □

Theorem 9. *The finite Sidon set $\{1, 2, 4, 8, 13\}$, which is the first* five *terms of the Mian–Chowla sequence, does not extend to a finite perfect difference set modulo any $v > 0$.*

Proof. Construct the projective plane from Lemma 13, and fix the polarity from Lemma 17. Note that this projective plane has some order q, which of course is either even or odd.

As before, from Lemma 19, we see that 1, 2 and 4 are absolute points that all lie on the single line $B+0$. Thus, q is not odd by Proposition 23.

But if q is even, all points on the line $B+0$ are absolute by Lemma 25. In particular, 8 is absolute and thus $2 \cdot 8 = 16 \in B$ by Lemma 19.

We obtain a contradiction because $16 - 13 = 4 - 1$ violates the defining property of a perfect difference set. □

✓ **Theorem 26** (the paragraph following Theorem 4.3 in Hall [34])**.** $\{-8, -6, 0, 1, 4\}$ *doesn't extend to a perfect difference set.*

Proof. Construct the projective plane from Lemma 13, and fix the polarity from Lemma 17.

By Lemma 19, we see that -4, -3, 0, and 2 are absolute points. Of these, -4, -3, and 0 lie on the line $B-4$. However, 2 does not lie on the line $B-4$ because otherwise $6 \in B$ and the two equal differences $6-0 = 0-(-6)$ would violate the defining property of a perfect difference set.

This causes a problem for both odd and even q. If q were odd, then too many absolute points lie on the same line, violating Proposition 23. If q were even, then not all absolute points lie on the same line, violating Proposition 25. □

✓ **Corollary 27.** $\{1, 3, 9, 10, 13\}$ *is a Sidon set that doesn't extend to a perfect difference set.*

Proof. If B is a perfect difference set and c is an arbitrary constant, then $B + c$ is also a perfect difference set. (The cs cancel when computing differences in B.)

Therefore, $\{-8, -6, 0, 1, 4\}$ extends to a perfect difference set if and only if $9 + \{-8, -6, 0, 1, 4\} = \{1, 3, 9, 10, 13\}$ does as well. Hence we are done by Theorem 26. □

6 Lean statement

We used ChatGPT to vibe code[2] a proof. The resulting proof consists of thousands of lines of spaghetti code, with many missteps and convoluted arguments. Normally for programming code, this would be reason to distrust the code; however, Lean is a proof assistant that formally verifies arguments, and so we can be sure that the argument is correct even if its code is ugly. As the Lean website [37] says: "Lean's minimal trusted kernel guarantees absolute correctness in mathematical proof, software and hardware verification." Even so, there is still one potential source of error: the statement that Lean verifies may not correspond properly to the statement that the human mathematician believes is being proven.

The Formal Conjectures [28] project is an initiative by Google DeepMind to create a large, open corpus of formalized statements of open conjectures (into Lean). In particular, they are attempting to translate all of Erdős's problems, and we were lucky that this particular Erdős problem had already been translated [27]. Several variants were included. The principal one included the condition that $v = q^2 + q + 1$ and q is a prime power. We were interested in proving the conjecture with no restriction on the modulus v, which was included as well. However, the corresponding statement in Lean was in fact incorrect for a subtle reason! The statement in Lean conjectured that every finite Sidon set can be extended to a perfect difference set modulo v, but it accidentally allowed $v = 0$. The case $v = 0$ means that $\mathbb{Z}/v\mathbb{Z}$ is simply $\mathbb{Z}$ itself, so this corresponds to the infinite case handled in Claim 10. In particular, this case is both relatively easy and has the opposite resolution.

While our Lean *proof* was generated entirely by ChatGPT, we did carefully check that our statement matched what we believed we were proving. As an extra precaution, we proved several "consistency checks" that were not needed for the main proof, but would support the claim that the statement of the conjecture was translated correctly. Specifically, this included Observations 2 and 6.

The Lean proof itself is included as a supplementary file, but for the avoidance for doubt, we include a portion of the file here so that one can see the *statement* being proven:

[2] Vibe coding [48] refers to a style of programming where the user interacts with a large language model in order to generate code, which they do not verify except via the use of tools. The term was popularized by Andrej Karpathy [35] in February 2025. (The reference there also describes using voice interaction, which we did not use and does not seem to be an essential part of the accepted usage of the term now.) As we discuss in Section 7, Lean is an ideal use case for vibe coding.

```
import Mathlib

/-- A Sidon set `A` is a set where all pairwise sums `i + j` are unique,
up to swapping the addends. -/
def IsSidon {α : Type*} [AddCommMonoid α] (A : Set α) : Prop :=
  ∀ {i₁ i₂ j₁ j₂ : α}, i₁ ∈ A → i₂ ∈ A → j₁ ∈ A → j₂ ∈ A →
    i₁ + i₂ = j₁ + j₂ →
      (i₁ = j₁ ∧ i₂ = j₂) ∨ (i₁ = j₂ ∧ i₂ = j₁)

/-- `B` is a perfect difference set modulo `v` if there is a bijection between
non-zero residues mod `v` and distinct differences `a - b`, where `a, b ∈ B`. -/
def IsPerfectDifferenceSetModulo (B : Set ℤ) (v : ℕ) : Prop :=
  B.offDiag.BijOn (fun (a, b) => (a - b : ZMod v)) {x : ZMod v | x ≠ 0}

-- (6216 lines omitted)

/--
**Erd\H{o}s problem 707**:
Any finite Sidon set of natural numbers can be embedded in a perfect difference
set modulo `v` for some `v ≠ 0`.
-/
def erdos_707 : Prop :=
  ∀ A : Set ℕ, A.Finite → IsSidon A →
    ∃ (B : Set ℤ) (v : ℕ),
      v ≠ 0 ∧
      (↑) '' A ⊆ B ∧
      IsPerfectDifferenceSetModulo B v

-- (101 lines omitted)

/--
The Sidon set {1, 2, 4, 8, 13} does not extend to a perfect difference set
modulo v for any nonnegative v.
-/
theorem not_erdos_707AM : ¬ erdos_707 :=
  not_erdos_707_given_counterexample
    counterexampleAM
    counterexampleAM_finite
    counterexampleAM_Sidon
    counterexampleAM_noExt
```

We can verify that the statement of Erdős's conjecture indeed says that any finite Sidon set can be extended to a perfect difference set. Because this Lean file compiles without any issues, it verifies that the theorem `not_erdos_707AM` indeed has the type `¬ erdos_707`. This means we have proven the negation of Erdős's conjecture. (One cannot ascertain from the snippet provided above specifically which counterexample is verified, as it is only mentioned in a comment.)

In the interest of reproducibility, we include here information about our versions of Lean [41] and the Mathlib [38] dependency:

```
Lean version4.24.0-rc1 919e297292280cdb27598edd4e03437be5850221
mathlib4               c69734131b8f3aff48af48197fe0480d6cc304cb
```

Our resulting proof is over 6000 lines (over a quarter of a megabyte) and consists of 26 definitions, 169 lemmas, and 4 theorems (the final verification of counterexamples). On our ordinary laptop, the code takes slightly under half a minute to verify. These metrics provide some data in the discussion of the "de Bruijn factor" [47], which is defined as the ratio of the size of a formal proof over the size of the informal proof. We will abstain from computing a specific number to represent this, but we wanted to note that unlike in de Bruijn's original work, we found that the factor varied heavily depending on the details of the argument. If an argument was straightforward and involved only some projective planes and polarities, then usually the factor was tiny. If, however, an argument involved cardinalities and parities, it would explode.

As discussed more in the following section, the most egregious example was a basic claim about involutions that took us over 250 lines of code, but which comprises a single sentence in this paper.

7 Discussion of the uses of artificial intelligence

Modern large language models, such as ChatGPT from OpenAI, Claude from Anthropic, and Gemini from Google DeepMind, have proven to be very useful in many aspects of mathematical research.

One popular use case of LLMs is literature search. In particular, there have been several recent success stories on `erdosproblems.com` with using LLMs to locate solutions to Erdős problems in the existing literature; see Tao [46] for a discussion. Unfortunately, LLMs completely failed to locate Hall's solution to our Erdős problem. Why? There seems to be a confluence of issues here:

1. Hall didn't state his result as a theorem, but rather as a throwaway sentence after a theorem. (Of course, he couldn't predict that Erdős would later make a huge fuss out of this problem, so he didn't know that a theorem statement would be necessary to signal the result's existence.)

2. No human mathematician appeared to have noticed Hall's result. As an egregious example, Guy [32] cites Hall's paper two sentences before stating this Erdős problem in section **C10**. Despite being aware of (some of) the contents of Hall's paper, Guy failed to connect the dots. As another perspective, it seems that the folks who solve Erdős problems are generally good at analytic number theory or analytic aspects of combinatorics, but they are perhaps less familiar with the study of combinatorial designs.

3. One might expect AI to help close this gap by reading the literature and responding to appropriately engineered prompts, but alas, it appears that the contents of Hall's paper might have been blocked from the AI's training set thanks to a paywall. As evidence of this, we searched a verbatim passage from the first page of Hall's paper and got a Google hit, but a similar search using text from later pages fails.

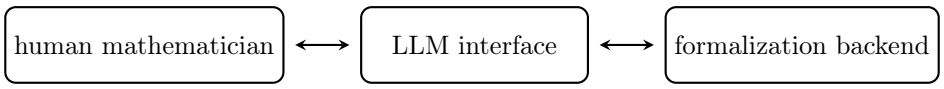
In various projects, LLMs are very helpful in writing exploratory code. This is almost an ideal use case. We began our project by generating many perfect difference sets to see which Sidon sets were evidently forbidden. Accordingly, we could have used LLMs to help with this, but instead, the first author found it mildly amusing to discover and use Construction 15. Through these investigations, we found that $\{1, 2, 4, 8\}$ appeared to be forbidden for primes (and odd prime powers), and $\{1, 2, 4, 8, 13\}$ was forbidden even for powers of two. These observations ultimately led to Theorems 8 and 9.

Sometimes, LLMs are helpful with brainstorming ideas, suggesting techniques, or even proving theorems. In fact, various authors have reported LLMs identifying a crucial idea for a proof, supplying a lemma, or otherwise making it possible to complete a project that they were stuck on. Sadly, for our problem, LLMs were not terribly helpful in this way. Even after we knew what exactly to prove, it couldn't help us close the gap.

At some point during the course of this project, we eventually found Hall's paper and thus learned that the problem had been solved. This was very confusing for us. Was Hall's proof correct, or was it generally understood by the community to be flawed in some way? It was clear to us that Lean would help us determine the truth, but we didn't know Lean, and it isn't terribly user-friendly. However, ChatGPT can write Lean, so we decided to vibe code the whole proof. It took a long time (about a week), and the process was extremely annoying, but somehow it succeeded.

One thing we came to realize is that Lean is actually a perfect setting for vibe coding. In general, vibe coding is good for generating code that appears to work well, but might contain some bugs. As such, one must carefully test the resulting code before deploying it in important settings. Modern applications of vibe coding include quick prototypes or fun side projects, i.e., settings in which bugs are not catastrophic. It turns out that Lean is also a great match for vibe coding, but for a completely different reason: if the code runs, you can trust it!

People think of Lean proofs as *computer-assisted* proofs, but this was entirely backwards from our experience. What we experienced was much more like a *human-assisted* (formal) proof. An idealized version of our experience would look like this:



In particular, the human mathematician engages in a productive conversation with an LLM, discussing a mathematical argument in natural language. The LLM then translates and extrapolates the core ideas in Lean code, fighting with syntax and compile errors on its own, keeping the human away from this level of tedium. When the LLM gets stuck on a fundamental logical step, it asks an appropriate followup question to the human mathematician. After a few iterations, the LLM successfully formalizes the human mathematician's proof.

From this perspective, our very first interaction with ChatGPT was stunning. We asked for it to state Proposition 20 in Lean (meaning to state the proposition without proof), and it quickly replied not only with the statement but also with a correct proof. In particular, we did not yet supply it with any argument, which we presumed would be necessary.

Sadly, most of the rest of our actual experience with human-assisted proof wasn't nearly this pleasant, though we are hopeful for a future that is closer to the above idealization. One of the early frustrations was while proving the next result, Proposition 21. It was promising at first, as ChatGPT itself constructed and proved the properties of the involution $p \mapsto p'$ without any hints at all. However, it was completely stuck finishing the final step: that since the not-absolute points occur in pairs, there is an even number of them.

This is a curious inversion of the experience of describing the proof of Proposition 21 to another human mathematician: The interesting and possibly "difficult" part to a human is the definition of p' from p. It may also be interesting to verify the desired properties of this map, but the final step (that if a finite number of items occur in pairs, then there are an even number of them) is so simple that depending on the verbosity of the writer, it may occupy only one or even no sentences in a writeup.

For us, however, convincing ChatGPT to formally prove the result that "if f is a fixed point–free involution on a finite set S, then S has even cardinality" was a multi-day struggle! Furthermore, the resulting argument is 250 lines of code, many of which deal with entirely trivial claims. (This is not an inherent feature of Lean; in fact, almost certainly a succinct and nice proof exists and can be written by a competent human. However, it was the best we could do vibe coding with our particular model.)

There were multiple recurring sources of difficulty with Lean and ChatGPT during the vibe coding process. One was the multitude of notions of *cardinality* in Mathlib, as applied to sets, finite sets, subtypes, etc. Perhaps they all make sense when viewed appropriately, but ChatGPT was not helpful in translating between all of them. Routinely we would seek to prove a basic lemma involving cardinality, only to be stymied because there were issues involving which specific cardinality was known or sought.

Another, very simple but frequent issue that arose involved parity. Perhaps the ChatGPT model we used was trained heavily on mathlib3, the previous version of Mathlib, which has different definitions of basic concepts like even/odd and lemmas involving them. We were often unsuccessful with prompting ChatGPT to look up the appropriate definitions and use them. Thankfully this usually did not delay the work very much, as it's a very simple matter. We mention it specifically because of the interaction between incompatible programming language version and large language models trained on the "wrong" version (from the perspective of the user).

Many of the issues we encountered would be alleviated greatly if the large language model interface we interacted with were integrated with Lean and reinforced appropriately with training in this interaction. We believe that even a small amount of such fine tuning would have made our specific "human-assisted proof" a much more pleasant interaction.

Finally, when it came to writing the paper, we knew that ChatGPT would probably do a decent job, but we decided to do our part and write it the old-fashioned way.

8 Future directions

In this paper, we identified forbidden Sidon sets of finite perfect difference sets. There are a few opportunities for future work.

First, let s denote the size of the smallest forbidden Sidon set. Both our example and Hall's example establish that $s \leq 5$. Meanwhile, the lower bound $s \geq 3$ follows from the fact that there are arbitrarily large finite perfect difference sets. What is s? Also, what are the forbidden Sidon sets of size s? One might interpret this as a challenge to "beat the AI", à la [45].

Can one find other Erdős problems that were solved before they were posed? Can AI help solve either of the two (ostensibly) open Erdős problems that are worth more than $1000? Finally, how

long until AI gets to the point where human-assisted proof is easier than conventional mathematics research?

References

[1] R. Baer, Null systems in projective space, Bull. Amer. Math. Soc. **51** (1945), 907–910.

[2] R. Baer, Polarities in finite projective planes, Bull. Amer. Math. Soc. **52** (1946), 77–93.

[3] L. D. Baumert and D. M. Gordon, On the existence of cyclic difference sets with small parameters, in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI, 2004, 61–68.

[4] Thomas F. Bloom, Erdős Problem #44, https://www.erdosproblems.com/44, retrieved October 21, 2025.

[5] Thomas F. Bloom, Erdős Problem #329, https://www.erdosproblems.com/329, retrieved October 21, 2025.

[6] Thomas F. Bloom, Erdős Problem #340, https://www.erdosproblems.com/340, retrieved October 21, 2025.

[7] Thomas F. Bloom, Erdős Problem #707, https://www.erdosproblems.com/707, retrieved October 21, 2025.

[8] Thomas F. Bloom, Erdős Problem Prizes, https://www.erdosproblems.com/prizes, retrieved October 21, 2025.

[9] J. Cilleruelo and M. B. Nathanson, Perfect difference sets constructed from Sidon sets, Combinatorica **28** (2008), 401–414.

[10] P. Erdős, Problems and results in graph theory and combinatorial analysis, in *Proceedings of the Fifth British Combinatorial Conference (Univ. Aberdeen, Aberdeen, 1975)*, Congr. Numer. **15** (1976), 169–192. [See p. 189.]

[11] P. Erdős, Problems and results on combinatorial number theory. III, in *Number Theory Day (Proc. Conf., Rockefeller Univ., New York, 1976)*, Lecture Notes in Math. **626**, Springer, Berlin, 1977, 43–72. [See p. 55.]

[12] P. Erdős, Some old and new problems in various branches of combinatorics, in *Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1979)*, Congr. Numer. **23** (1979), 19–37. [See p. 13.]

[13] P. Erdős, A survey of problems in combinatorial number theory, Ann. Discrete Math. **6** (1980), 89–115. [See p. 99.]

[14] P. Erdős, On the combinatorial problems which I would most like to see solved, Combinatorica **1** (1981), 25–42. [See p. 5.]

[15] P. Erdős, On some problems in graph theory, combinatorial analysis and combinatorial number theory, in *Graph Theory and Combinatorics (Cambridge, 1983)*, Academic Press, London, 1984, 1–17. [See p. 16.]

[16] P. Erdős, Extremal problems in number theory, combinatorics and geometry, in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, PWN, Warsaw, 1984, 51–70. [See p. 55.]

[17] P. Erdős, On some of my problems in number theory I would most like to see solved, in *Number Theory (Ootacamund, 1984)*, Lecture Notes in Math. **1122**, Springer, Berlin, 1985, 74–84. [See p. 77.]

[18] P. Erdős, Some applications of probability methods to number theory. Successes and limitations, in *Sequences: Combinatorics, Compression, Security, and Transmission (Naples/Positano, 1988)*, R. M. Capocelli (ed.), Springer-Verlag, New York, 1990, 182–194. [See p. 186.]

[19] P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, in *Graph Theory, Combinatorics, and Applications, Vol. 1 (Kalamazoo, MI, 1988)*, Wiley-Intersci. Publ., Wiley, New York, 1991, 397–406. [See p. 405.]

[20] P. Erdős, On some of my favourite problems in various branches of combinatorics, in *Fourth Czechoslovakian Symposium on Combinatorics, Graphs and Complexity (Prachatice, 1990)*, Ann. Discrete Math. **51** (1992), 69–79. [See p. 73.]

[21] P. Erdős, Problems and results in discrete mathematics, Discrete Math. **136** (1994), 53–73. [See p. 57.]

[22] P. Erdős, Some of my favorite problems and results, in *The Mathematics of Paul Erdős, I*, Algorithms Combin. **13**, Springer, Berlin, 1997, 47–67. [See p. 54.]

[23] P. Erdős and R. Freud, A Sidon-problémakör (Hungarian) [On Sidon sequences and related problems], Mat. Lapok **1991**, no. 1–2, 1–44. [See p. 9.]

[24] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de L'Enseignement Mathématique, Vol. 28, Univ. Genève, Geneva, 1980. [See p. 49.]

[25] P. Erdős and P. Turán, On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. **16** (1941), 212–215.

[26] K. Ford, B. Green, S. Konyagin and T. Tao, Large gaps between consecutive prime numbers, Ann. of Math. (2) **183** (2016), no. 3, 935–974.

[27] Formal Conjectures authors, Erdős Problem #707 (Lean file), in *Formal Conjectures* (Lean 4 repository), Google DeepMind, 2025. https://github.com/google-deepmind/formal-conjectures/blob/main/FormalConjectures/ErdosProblems/707.lean, retrieved October 21, 2025.

[28] Google DeepMind, *Formal Conjectures* (open repository of conjectures formalized in Lean). https://github.com/google-deepmind/formal-conjectures and https://google-deepmind.github.io/formal-conjectures/, retrieved October 21, 2025.

[29] W. T. Gowers, Just-do-it proofs, Gowers's Weblog, 16 Aug 2008. https://gowers.wordpress.com/2008/08/16/just-do-it-proofs/, retrieved October 21, 2025.

[30] W. T. Gowers, Just-do-it proofs, Tricki (wiki article). https://www.tricki.org/article/Just-do-it_proofs, retrieved October 21, 2025.

[31] R. K. Guy (ed.), *Western Number Theory Problems, 1991-12-19 & 22*, problem list prepared for mailing prior to the 1992 Corvallis meeting, 1991. [See p. 10.] https://westcoastnumbertheory.org/wp-content/uploads/2018/02/wcnt-problems-1991.pdf

[32] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Mathematics, Springer, New York, 2004. [See Sections C9 and C10.]

[33] M. Hall, An isomorphism between linear recurring sequences and algebraic rings, Trans. Amer. Math. Soc. **44** (1938), no. 2, 196–218.

[34] M. Hall, Jr., Cyclic projective planes, Duke Math. J. **14** (1947), 1079–1090.

[35] A. Karpathy, "There's a new kind of coding I call 'vibe coding'...", X (formerly Twitter), 2 Feb 2025. https://x.com/karpathy/status/1886192184808149383, retrieved October 21, 2025.

[36] F. Krückeberg, B_2-Folgen und verwandte Zahlenfolgen, J. Reine Angew. Math. **206** (1961), 53–60.

[37] Lean Prover community, The Lean theorem prover (official website). https://lean-lang.org/, retrieved October 21, 2025.

[38] The mathlib Community, The Lean mathematical library, in *Proc. 9th ACM SIGPLAN Int. Conf. on Certified Programs and Proofs (CPP 2020)*, ACM, 2020, 367–381.

[39] J. Maynard, Large gaps between primes, Ann. of Math. (2) **183** (2016), no. 3, 915–933.

[40] A. M. Mian and S. Chowla, On the B_2-sequence of integers, Proc. Indian Acad. Sci. Sect. A **17** (1943), 75–80.

[41] L. de Moura and S. Ullrich, The Lean 4 Theorem Prover and Programming Language, in *Automated Deduction – CADE 28*, LNAI **12699**, Springer, 2021, 625–635. https://doi.org/10.1007/978-3-030-79876-5_37 https://pp.ipd.kit.edu/uploads/publikationen/demoura21lean4.pdf

[42] OEIS Foundation Inc. (2025), Mian-Chowla sequence, Entry A005282 in The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A005282, retrieved October 21, 2025.

[43] OpenAI, *ChatGPT* 5 [Large language model]. https://chat.openai.com/, used throughout October 2025.

[44] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. **43** (1938), 377–385.

[45] T. Tao, Answer to "Is the least common multiple sequence $\mathrm{lcm}(1, 2, \ldots, n)$ a subset of the highly abundant numbers?", https://mathoverflow.net/a/501125/1079, retrieved October 21, 2025.

[46] T. Tao, Mathstodon post, https://mathstodon.xyz/@tao/115385022005130505, retrieved October 21, 2025.

[47] F. Wiedijk, The De Bruijn factor, manuscript, 2006. https://www.cs.ru.nl/~freek/factor/factor.pdf

[48] Wikipedia contributors, Vibe coding, *Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/wiki/Vibe_coding, retrieved October 21, 2025.