Cyclic self-sumset recognition: a credited corollary of the integer hardness theorem

Alec Kriebel
Independent researcher
ORCID: 0009-0001-9320-500X

Version 1.0, October 14, 2026

Abstract

We give a short explicit cyclic corollary of the integer hardness theorem of Abboud, Fischer, Safier, and Wallheimer. For unbounded positive input n, deciding whether a given $B \subseteq \mathbb{Z}/n\mathbb{Z}$ equals $A + A$ for some subset A of the same group is NP-complete in each of two explicit representations: binary n with a binary residue list, and an n-bit characteristic vector. Sums include repeated summands. Hardness already holds for odd n and nonempty B containing zero with every canonical representative b satisfying $2b < n$. The proof normalizes integer targets and forces a zero anchor in every cyclic root, after which no sum wraps. Dense hardness uses the source's polynomial numerical universe, separately from the sparse bit-length argument. This is credited exposition; no new hardness gadget, novelty, first-publication, or independent-discovery claim is made.

Status and license. AI-assisted, unrefereed preprint; no external human peer review or formal proof-assistant certification. Copyright 2026 Alec Kriebel. CC BY 4.0.

1 Claim, input models, and credit

For $G_n = \mathbb{Z}/n\mathbb{Z}$ and $A \subseteq G_n$, write

$$A + A = \{a + a' : a, a' \in A\},$$

including $a = a'$. The modulus n is a positive integer supplied with the input, without a fixed upper bound. Canonical residues are $0, \ldots, n-1$. The sparse representation gives binary n and a sorted list of distinct binary canonical residues of B. The dense representation gives binary n and exactly n indicator bits. Malformed encodings are NO strings; syntax, lengths, ordering, and residue bounds are checked in polynomial time.

Theorem 1. *Ordinary self-sumset recognition $B = A + A$ in the same G_n is NP-complete under deterministic polynomial-time many-one reductions, separately in the sparse and dense representations above. Each remains NP-complete when restricted to odd n, nonempty B, $0 \in B$, and $2b < n$ for every canonical $b \in B$.*

The original motivation is Campos's Problem 15, attributed to Alon and Granville, in Oberwolfach Report 22/2022, printed p. 1228 [2]. Both sets there lie in $\mathbb{Z}/n\mathbb{Z}$; ordinary all-pair notation appears on p. 1174. The question specifies neither an encoding nor a formal meaning of "efficient." Theorem 1 gives a conventional deterministic polynomial-time exact-decision interpretation in the

two stated models. In either model such an algorithm exists if and only if P = NP. This does not assert P ≠ NP.

All integer NP-hardness and the bounded uniform 3SAT construction used below are due to Aboud, Fischer, Safier, and Wallheimer (AFWS) [1]. Standard 3SAT NP-completeness is established background. We use Theorem 1.2 and the integer composition on p. 23 of arXiv:2410.18661v2, dated October 26, 2024. The separately verified publication record is SODA 2025, pp. 4484–4506, DOI 10.1137/1.9781611978322.153; its full typeset body was not separately inspected. For a 3-CNF formula with $q = v + c \geq 1$, the needed source interface constructs, in polynomial time,

$$S \subseteq [0, 2^{57}q^4] \cap \mathbb{Z}, \qquad \varphi \text{ satisfiable} \iff (\exists R \subseteq \mathbb{Z})\ S = R + R. \tag{1}$$

The source's relevant integer mechanisms have been reconstructed in the accompanying source note. Literal v2 presentation slips require care, but the bound in (1) is preserved; this dependency is not a claim to have reproved the whole source bibliography. The separate AFWS theorem for $\mathbb{F}_p^d$ is not used: for $d > 1$ this additive group is not cyclic of order p^d.

2 Normalization and the universal cyclic transfer

Let S be a finite nonempty integer set with $S = R + R$. Then R is nonempty and finite: fixing $r_0 \in R$ injects R into S by $r \mapsto r + r_0$. Extremal diagonal sums give

$$\min S = 2 \min R, \qquad \max S = 2 \max R.$$

Thus an odd $t = \min S$ is impossible. If t is even, put

$$B = S - t, \qquad M = \max S - \min S.$$

Translation of roots by $-t/2$, with inverse translation by $t/2$, proves

$$S \text{ is an integer self-sumset} \iff B \text{ is an integer self-sumset.} \tag{2}$$

This includes negative t. Here $0 \in B \subseteq [0, M]$; any integer root of B has minimum zero and maximum $M/2$.

Lemma 1. *Let $M \geq 0$, $0 \in B \subseteq [0, M] \cap \mathbb{Z}$, and let n be positive and odd with $n > 2M$. Then B is an integer self-sumset if and only if it is a self-sumset in G_n. Moreover, the canonical representatives of every cyclic root are an integer root of B.*

Proof. An integer root of B projects to a cyclic root. Conversely, suppose $A + A = B$ in G_n. Since $0 \in B$, some $a, -a$ belong to A. Diagonal sums put $2a, -2a$ in B. Their canonical representatives b_1, b_2 satisfy

$$b_1 + b_2 \equiv 0 \pmod{n}, \qquad 0 \leq b_1 + b_2 \leq 2M < n.$$

They must both be zero. Hence $2a = 0$ in G_n, and oddness of n gives $a = 0$. Thus $0 \in A$, and $x = x + 0$ shows that $A \subseteq B$.

Let T be the canonical representatives of A. Then $T \subseteq B \subseteq [0, M]$. Every integer pair sum of T is at most $2M < n$ and has residue in B, so $T + T \subseteq B$. Every $b \in B$ is a cyclic pair sum from A; its canonical pair sum and b both lie in $[0, n-1]$, so their congruence implies integer equality. Therefore $B \subseteq T + T$ as well. □

The diagonal sums and anchor are essential to this proof. For example, the integer target $\{1\}$ is NO but equals $\{3\} + \{3\}$ modulo 5. Oddness is essential to the statement about *every canonical root*: $\{2\} + \{2\} = \{0\}$ modulo 4, but its integer sum is $\{4\}$. Mere anchored existence equivalence can also hold at even order after an order-two root translation; no necessity assertion about oddness for existence is made here. The lemma includes $n = 1$, where its hypotheses force $M = 0$ and $B = \{0\}$.

3 The total reduction and its size

For a valid explicit finite signed-integer set S, define the following map:

1. If $S = \varnothing$, output $(3, \varnothing)$.
2. If $S \neq \varnothing$ and $\min S$ is odd, output $(5, \{0, 1\})$.
3. Otherwise output (n, B) with $B = S - \min S$, $M = \max B$, and $n = \max(3, 2M + 1)$.

The empty case is YES, with empty root on both sides. The fixed target in case 2 is NO: Lemma 1 would give an integer root of $\{0, 1\}$, whose maximum would have to be $1/2$. In case 3, n is odd and $n > 2M$, so (2) and Lemma 1 prove the exact YES/NO equivalence. For $M = 0$ the output is $(3, \{0\})$. Invalid source strings may be sent to the fixed NO after a syntax check. The map uses no prime search or factorization.

For the restricted nonempty target language, replace the empty-source output by $(3, \{0\})$. Every output then has odd n, is nonempty, contains zero, and has $2b < n$ for every canonical b. Both fixed outputs satisfy these restrictions.

For a sparse integer source of binary length L, translating coordinates and forming $2M + 1$ requires only $O(L)$-bit arithmetic and emits at most $|S|$ residues. This map is polynomial in bit length, even for numerically enormous M.

For dense hardness, compose *directly* with the bounded 3SAT construction (1). Delete unused variables and relabel occurring variables first, so $q = v + c$ is polynomial in explicit formula length. Whenever the nonconstant branch applies,

$$M \leq 2^{57} q^4, \qquad n \leq \max(3, 2^{58} q^4 + 1).$$

Writing the n-bit vector is therefore polynomial in formula length. The large fixed coefficient does not affect polynomial reducibility. Constant exceptional formulas, including $q = 0$, are evaluated directly and mapped to the fixed YES or NO. A valid empty conjunction is YES. Expanding an *arbitrary* binary integer instance into a dense vector would not justify this argument. The same bounded 3SAT composition also proves sparse hardness without relying on a formal source encoding convention.

4 NP membership and exact scope

For sparse input with nonempty $B = A + A$, fix $a_0 \in A$. The translation $a \mapsto a + a_0$ injects A into B, so $|A| \leq |B|$ for every positive n, including even n and $n = 1$. A witness has at most $|B|$ canonical binary residues, using $O(|B| \log(n + 1))$ bits. After checking syntax and bounds, the verifier computes all at most $|B|^2$ modular pair sums, including diagonal pairs, deduplicates them, and tests exact equality with B. Binary arithmetic and sorting take polynomial bit time. Empty B has the empty witness; a nonempty witness cannot have empty sumset.

For dense input, an n-bit witness for A suffices. All pair sums and comparison of the resulting n bits take polynomial time in the input length. The restricted language additionally checks its stated restrictions in polynomial time. Together with the reductions, these verifiers prove Theorem 1.

The conclusion concerns deterministic exact decision and ordinary all-pair self-sums in the same cyclic group, with unbounded input n. It asserts no prime-only classification or conclusion about distinct summands, unrelated summand sets, succinct circuits, oracle descriptions, randomized algorithms, approximation, average case, or promised-root search.

5 Antecedents, verification, and authorship

The recognition question and root-containment search observation already occur in Croot–Lev (2007), Problem 4.11 [3]. Dose's 2016 revision 5 records even integer-translation invariance in Lemma 4.32 and discusses SUMSET complexity [4]. Antoniou–Tringali's v3 has closely related canonical no-wrap lifts under anchored-factor and maximum-additivity hypotheses [5]. These are mechanism antecedents; the integer hardness construction used here is AFWS's. The exact historical priority of the full cyclic formulation remains unknown. Bounded literature comparison establishes neither first publication nor current worldwide openness.

The support kit contains the complete eight-file original edition, later AI-assisted transfer, source-interface, and priority reports with their frozen derivations and selected receipts, root acceptance records, authored checkers, and fresh reproducibility commands. Historical verdicts remain unchanged as historical records. The October 14, 2026 preparation snapshot records the new whole-package review stage separately. Finite enumeration checks corroborate the universal proof and test boundary controls; they do not prove asymptotic hardness, and omitted historical scripts are not claimed to have been replayed.

Alec Kriebel is the sole named author and takes responsibility for this exposition. OpenAI Codex AI systems were used extensively in mathematical reasoning, source retrieval and interpretation, adversarial checking, coding, computational verification, writing, and preparation. The accompanying audits are AI-assisted checks, not independent human peer review. No external human peer review or formal proof-assistant certification is claimed. No external individual was contacted on behalf of this work.

References

[1] A. Abboud, N. Fischer, R. Safier, and N. Wallheimer, *Recognizing Sumsets is NP-Complete*, SODA 2025, 4484–4506. doi:10.1137/1.9781611978322.153. Inspected proof: arXiv:2410.18661v2, October 26, 2024, Theorem 1.2 and p. 23.

[2] *Combinatorics, Probability and Computing*, Oberwolfach Report 22/2022. Campos, Problem 15 (Alon–Granville), p. 1228; ordinary sumset notation p. 1174. doi:10.4171/owr/2022/22.

[3] E. Croot and V. F. Lev, *Open problems in additive combinatorics* (2007), Problem 4.11, p. 17 of the primary author copy.

[4] T. Dose, *Complexity of Constraint Satisfaction Problems over Finite Subsets of Natural Numbers*, ECCC TR16-031, revision 5 (2016), Lemma 4.32 and SUMSET discussion. Primary revision record.

[5] A. A. Antoniou and S. Tringali, *On the arithmetic of power monoids and sumsets in cyclic groups*, inspected arXiv:1804.10913v3 (December 1, 2020), pp. 18–21; published in Pacific Journal of Mathematics (2021).