

Small exact values for Green's Problem 37 ($m(N, 3)$ for $N \leq 17$, bounds beyond) and a reproduction of the table for Problem 27

Lluis Eriksson

22 October 2026

Abstract

Let $m(N, k)$ be the least size of a finite set of integers containing, for every $d = 1, \dots, N$, a k -term arithmetic progression of common difference d (Problem 37 in Green's list; $k = 3$ unless stated). I could not find a table of its values in the literature. With CP-SAT in $\mathbb{Z}$ I obtain $m(N, 3) = 3, 4, 5, 6, 7, 8, 8, 8, 9, 10, 11, 11, 12, 12, 12, 13, 13$ for $N = 1, \dots, 17$; for $N \leq 10$ this is also supported by DRUP proofs of SAT instances whose reduction to a finite window is proved in the note. For $N \leq 27$ I give verified witnesses (upper bounds) and, inside the window $[0, 2N]$, DRUP-certified lower bounds up to $N = 23$. The window is *not* harmless: for $N = 15$ the true value is 12 but no 12-element set fits in $[0, 30]$ (the optimum has diameter 35), so for $N > 17$ the lower bounds are only window bounds. I also give a few values for $k = 4$. For Problem 27 ($m(p)$ in $\mathbb{Z}/p\mathbb{Z}$) I recomputed $m(p)$ for primes $p \leq 31$; these values were already published, so this is a reproduction, not new. Everything is computational, produced by AI agents, without human review or formal verification of the pipeline.

1 The problems

Problem 37. Green's *100 open problems* [1] asks for the smallest subset of $\mathbb{N}$ containing, for each $d = 1, \dots, N$, an arithmetic progression of length k and common difference d . Green writes $F_k(N)$ for it, conjectures $F_k(N) \gg_k N^{1-c_k}$ with $c_k \rightarrow 0$, and notes (with Ruzsa [2]) that this is equivalent to the arithmetic Kakeya conjecture of Katz and Tao. The formal-conjectures file `GreensOpenProblems/37.lean` [3] defines $m(N, k) = \min\{|A| : A \subset \mathbb{N} \text{ finite}, \forall 1 \leq d \leq N \exists a : a, a+d, \dots, a+(k-1)d \in A\}$ and records only the trivial bound $m(N, k) \leq kN + 1$. Translating `A` shows that it makes no difference whether $A \subset \mathbb{N}$ or $A \subset \mathbb{Z}$.

Problem 27. For a prime p , $m(p)$ is the least $|A|$, $A \subset \mathbb{Z}/p\mathbb{Z}$, $|A| \geq 2$, such that every element of $A + A$ has at least two representations $a + b$ as an *unordered* pair (the definition `HasNoUniqueRepresentation` in [3]; $a = b$ allowed). It was studied by Straus and Bedert [4].

2 Results

Theorem 1 (Problem 37, $k = 3$). $m(N, 3) = 3, 4, 5, 6, 7, 8, 8, 8, 9, 10, 11, 11, 12, 12, 12, 13, 13$ for $N = 1, \dots, 17$, and $m(N, 3) \leq \text{UB}(N)$, the column `UB` of Table 1, for $N \leq 27$.

Table 1 lists, for each N : $m_{[0, 2N]}$, the least size of a set inside the window $\{0, \dots, 2N\}$ that works (an *upper* bound for $m(N, 3)$, exact for the window); `UB`, the smallest verified witness found (the window value, or the CP-SAT witness in $\mathbb{Z}$ for $N \leq 17$; it is smaller than $m_{[0, 2N]}$ only for $N \in \{15\}$; for $N = 18, \dots, 27$ searches for smaller sets in the windows $[0, 3N]$, $[0, 4N]$, $[0, 6N]$ with a 240 s limit per instance all ended in `TIMEOUT`, which is inconclusive); $m_{\mathbb{Z}}$, the true value in $\mathbb{Z}$ when proved (a dagger marks values forced by monotonicity: $m(N, 3)$ is non-decreasing in N , and the window value equals a proven lower bound for a smaller N); and the certificates: `W`

= a DRUP proof that no set of size $m_{[0,2N]} - 1$ fits in $[0, 2N]$ was checked; Z = a DRUP proof of the same size bound for *all* finite sets of integers, via Lemma 1.

N	$m_{[0,2N]}$	UB	$m_{\mathbb{Z}}$	cert	N	$m_{[0,2N]}$	UB	$m_{\mathbb{Z}}$	cert
1	3	3	3	–	15	13	12	12	W-
2	4	4	4	–	16	13	13	13	W-
3	5	5	5	WZ	17	13	13	13	W-
4	6	6	6	WZ	18	14	14	13–14	W-
5	7	7	7	WZ	19	14	14	13–14	W-
6	8	8	8	WZ	20	15	15	13–15	W-
7	8	8	8	WZ	21	15	15	13–15	W-
8	8	8	8	WZ	22	16	16	13–16	W-
9	9	9	9	WZ	23	16	16	13–16	W-
10	10	10	10	WZ	24	17	17	13–17	–
11	11	11	11	W-	25	17	17	13–17	–
12	11	11	11	W-	26	17	17	13–17	–
13	12	12	12	W-	27	18	18	13–18	–
14	12	12	12	W-					

Table 1: $k = 3$. An entry a – b in the $m_{\mathbb{Z}}$ column means only $a \leq m(N, 3) \leq b$ is proved.

For $k = 4$ (windows $[0, 3N]$, Table 2) the true value in $\mathbb{Z}$ was computed by CP-SAT only for $N \leq 11$.

N	$m_{[0,3N]}$	$m_{\mathbb{Z}}$	N	$m_{[0,3N]}$	$m_{\mathbb{Z}}$
1	4	4	11	15	15
2	6	6	12	16	–
3	7	7	13	17	–
4	9	9	14	17	–
5	10	10	15	18	–
6	11	11	16	19	–
7	11	11	17	20	–
8	13	13	18	21	–
9	14	14	19	21	–
10	15	15	20	22	–

Table 2: $k = 4$ (CP-SAT in $\mathbb{Z}$, no DRUP certificate).

The window is not harmless. For $N \leq 14$ and $N = 16, 17$ the CP-SAT value in $\mathbb{Z}$ equals $m_{[0,2N]}(N)$, but for $N = 15$ it is $12 < 13 = m_{[0,2N]}(15)$: the set $\{0, 5, 10, 12, 13, 14, 17, 20, 24, 26, 28, 35\}$ (diameter $35 > 2N$) works. So the W-certificates do not by themselves give lower bounds in $\mathbb{Z}$; only the Z-certificates and CP-SAT do. For $N > 17$ I have no true lower bound beyond monotonicity, and UB may overestimate $m(N, 3)$. For $N = 18$ the value is 13 or 14 (lower bound by monotonicity from $N = 17$). CaDiCaL (gap-clause instance, i.e. any set of ≤ 13 integers of diameter $\leq W$) gave UNSAT for $W = 40$, $W = 45$. CP-SAT for 13-element sets of diameter ≥ 37 : unknown (time 2712 s). The CP-SAT run on the full $\mathbb{Z}$ instance ($N = 18$, $s = 13$, 3000 s limit) returned UNKNOWN.

Problem 27. Table 3 reproduces $m(p)$ for $p \leq 31$ (SAT with $0, 1 \in A$ by the affine symmetry; upper bound = verified witness; lower bound = DRUP proof of “no valid A of size $m(p) - 1$ ”, same checker). **These values are not new.** The README of the repository [mkwatson/unique-sums-notes](#) [5] (read 22 Oct. 2026) states $m(3) = 3, \dots, m(59) = 15$ as values that already appear in Scheinerman’s dissertation (I did not see that thesis), with solver-certified

p	$m(p)$	lower bound	p	$m(p)$	lower bound
3	3	DRUP checked	17	8	DRUP checked
5	4	DRUP checked	19	9	DRUP checked
7	5	DRUP checked	23	10	DRUP checked
11	7	DRUP checked	29	11	proof logged, not checked
13	7	DRUP checked	31	11	proof logged, not checked

Table 3: Problem 27.

$m(53) = 14$, $m(59) = 15$, and cites Kwaczyński for $m(61) = 15$, $m(67) = m(71) = m(73) = 16$ at “search only” level. I did not get beyond $p = 31$, so I add no new value for Problem 27.

3 From $\mathbb{Z}$ to a finite search

Lemma 1. *Let $A \subset \mathbb{Z}$ be finite and suppose that for each $1 \leq d \leq N$ it contains a k -term AP of difference d . Then there is B with $|B| = |A|$, $\min B = 0$, with the same property and with all gaps between consecutive elements $\leq N$; in particular $\text{diam } B \leq N(|B| - 1)$.*

Proof. Translate so that $\min A = 0$. Let $a < b$ be consecutive elements of A with $b - a > N$. A k -AP $P \subset A$ of difference $d \leq N$ cannot have a term $\leq a$ and a term $\geq b$: two consecutive terms $y < y + d$ would satisfy $y \leq a < b \leq y + d$, so $d \geq b - a > N$. Hence each such P lies in $L = A \cap (-\infty, a]$ or in $R = A \cap [b, \infty)$. Replace A by $L \cup (R - (b - a - 1))$: the elements of R are moved to the right of a , no two elements merge, translating R preserves all APs inside R , so the new set has the same size and still contains all required APs. Each step reduces the number of large gaps. $\square$

Consequently the SAT instance “ $x_0 = 1$; for each $d \leq N$ some $y_{d,a}$ with $y_{d,a} \rightarrow x_a \wedge x_{a+d} \wedge x_{a+2d}$; at most s of the x_a ($0 \leq a \leq W$); gap clauses” with $W = N(s - 1)$ is satisfiable iff some set of at most s integers works. This is the Z-certificate. With $W = 2N$ and no gap clauses the same formula decides the window problem (W-certificate); $W = 2N$ is only a restriction, not a reduction. The gap clauses are $x_a \wedge t_{a+N+1} \rightarrow \bigvee_{j=a+1}^{a+N} x_j$ with $t_a \leftrightarrow x_a \vee t_{a+1}$. Lemma 1 is the only reduction used for the Z results.

4 Methods and verification

CP-SAT in $\mathbb{Z}$. For each (N, s) : integers $0 = x_0 < \dots < x_{s-1}$ with gaps in $[1, N + 1]$, a Boolean for every k -subset of indices and every d forcing consecutive differences $= d$, and one clause per d ; a reflection symmetry break. Sizes are increased until feasible. OR-Tools 9.15, 8 workers, status INFEASIBLE/OPTIMAL as reported by the solver; **no independent certificate exists for these results**, except those marked Z in Table 1. In addition CaDiCaL on the Z-instance for $N = 13$, $s = 11$ ($W = 130$, 360 s) also reported UNSAT.

Window SAT and proofs. Windows were solved with CaDiCaL (PySAT); each UNSAT instance (size $m - 1$) was re-solved with Glucose 4 logging DRUP, and the proof was checked by `rup.exe`, a forward RUP checker in Go with two watched literals (the one written for the Gowers–Long note; deletions ignored). Negative controls on the $N = 8$ proof: it is rejected against the satisfiable size-8 formula (at lemma 6), cut in half (no empty clause), with a false first lemma $\neg x_0$ prepended, and the bare empty clause is rejected. The checker is **not** drat-trim nor a verified checker; encoder and checker are trusted. Altogether 29 DRUP proofs of the $k = 3$ instances were accepted (21 window, 8 Z); the longest has 175187 lemmas ($N = 22$, $W = 44$, $s = 15$; 25242143 bytes; checked in 1522 s). SHA-256 of every CNF and proof are in `g37/cert37.jsonl`; proof files for small N are in the supplement, larger ones can be regenerated with `cert37.py`.

Proofs for the Z-instances $N = 11, 12$, for the window instance $N = 24$ and for $m(29), m(31)$ in Problem 27 were produced but the checker runs were interrupted when I stopped; they are not counted anywhere.

Witnesses. All witnesses are checked by `verify_witnesses.py`, a naive loop sharing no code with the solvers, and by Lean 4 (core, no Mathlib): `lean/Green2737.lean` defines Boolean checkers `covers` and `noUnique` and proves each witness by `native_decide` (trusts the compiler); small cases also by `decide +kernel`. The file compiled with exit code 0. No Lean statement connects these checkers to the formal-conjectures definitions.

Problem 27 encoding. Variables x_a and y_{ab} ($a \leq b$, $y_{ab} \rightarrow x_a \wedge x_b$); for each pair, $x_a \wedge x_b \rightarrow \bigvee y_{cd}$ over the other pairs with the same sum; $0, 1 \in A$ (an affine map $x \mapsto ux + v$ preserves the property, and any A with $|A| \geq 2$ can be mapped to contain $0, 1$); cardinality $\leq k$ by a sequential counter. PySAT's CaDiCaL prints a harmless message `found falsified original clause` (also seen in the Green 22 note); results were checked by witnesses and proofs.

5 What is not verified

(i) For $N > 17$ no lower bound in $\mathbb{Z}$ is proved beyond monotonicity; UB there is only an upper bound and, as $N = 15$ shows, may not be sharp. (ii) The Z values for $N > 10$ rest on CP-SAT's reported status (cross-checked once by CaDiCaL for $N = 13$). (iii) The RUP checker is home-made. (iv) No theorem links the encodings or Lean checkers to the formal-conjectures statements. (v) No asymptotic information: these small values say nothing about N^{1-c_k} . (vi) The literature search was limited (Green's list, Green–Ruzsa, two OEIS searches, a few web searches); I found no earlier values for $m(N, 3)$, but this is not a priority claim. (vii) No human review.

6 Source disclosure

This is exploratory computational work carried out with AI assistance: the code, formulas, certificates, Lean files and this text were produced by Claude Sonnet 5.5 agents under the direction of the author. There has been no human refereeing and no complete formal verification. The CPU was shared with other jobs, so timings are only indicative. The supplement (code, witnesses, SHA-256 of proofs, logs) allows rerunning everything.

References

- [1] B. Green, *100 open problems*, manuscript (Dec. 2025), Problems 27 and 37. <https://people.maths.ox.ac.uk/greenbj/papers/open-problems.pdf>
- [2] B. Green and I. Ruzsa, *On the arithmetic Kakeya conjecture of Katz and Tao*, Period. Math. Hungar. (2018), arXiv:1712.02108.
- [3] Google DeepMind, *formal-conjectures*, `GreensOpenProblems/27.lean`, `37.lean`, <https://github.com/google-deepmind/formal-conjectures>.
- [4] B. Bedert, *On unique sums in Abelian groups*, Combinatorica **44** (2024), 269–298, arXiv:2303.15134.
- [5] M. K. Watson, *unique-sums-notes*, <https://github.com/mkwatson/unique-sums-notes>.

A A witness

$k = 3$, $N = 27$, $|A| = 18$, $A = \{0, 2, 4, 6, 10, 15, 16, 20, 22, 27, 28, 29, 30, 33, 38, 48, 50, 54\}$. All other witnesses are in `g37/witnesses37.json` and `g27/witnesses27.json`.