

Conjectures.io

Formal proof verified through Conjectures

GREEN'S PROBLEM 47: A COUNTEREXAMPLE TO EXACT QUADRATIC CONTAINMENT

JENSEN KOHLMAYER AND LIAM KRUER

ABSTRACT. Let A be the set consisting of 2 and the squares of primes congruent to 1 modulo 8. For every odd prime p , its reduction occupies at most $(p+1)/2$ residue classes. Nevertheless, its counting function is not $O(\sqrt{X}/(\log X)^{100})$, and A is not contained in $P(\mathbb{Z})$ for any quadratic polynomial $P \in \mathbb{Q}[x]$. This gives a negative answer to the exact-containment question in Problem 47 of Green's collection. The obstruction to quadratic containment is a first- and second-moment identity for quadratic images over finite fields. Deleting 2 leaves a subset of the squares, so the example satisfies a quadratic-structure conclusion allowing finitely many exceptions. We also describe the correspondence with the submitted Lean proof.

1. INTRODUCTION

For a set $A \subseteq \mathbb{N}$, write

$$A(X) = |A \cap [1, X]|, \quad A_p = \{a \bmod p : a \in A\} \subseteq \mathbb{F}_p.$$

The exact-containment question in Green's Problem 47 [1] asks whether the condition $|A_p| \leq (p+1)/2$ for all sufficiently large primes forces either

$$A(X) \ll \frac{\sqrt{X}}{(\log X)^{100}} \quad (X \rightarrow \infty) \tag{1}$$

or containment of all of A in the integer-input image of a rational quadratic. Here and throughout, a quadratic has degree exactly two, and an implied constant in (1) must be independent of X .

Define

$$\mathcal{P} = \{q : q \text{ is prime and } q \equiv 1 \pmod{8}\}, \quad A = \{2\} \cup \{q^2 : q \in \mathcal{P}\}. \tag{2}$$

Theorem 1.1. *The set A in (2) has all three of the following properties:*

- (1) $|A_p| \leq (p+1)/2$ for every odd prime p ;
- (2) its counting function does not satisfy (1);
- (3) for every $P \in \mathbb{Q}[x]$ of degree two, $A \not\subseteq P(\mathbb{Z})$.

The role of the added element is essential to the claim being made: $A \setminus \{2\}$ is contained in the image of $x \mapsto x^2$ on $\mathbb{Z}$. Green–Harper's Conjecture 1.7 [2] allows finitely many exceptions in its quadratic alternative; it also uses rational inputs and a different quantifier over counting scales. The present example does not refute that conjecture. It shows that exact containment, as stated in the particular question above, is too strong.

Date: Working draft — 12 September 2026.

Key words and phrases. Inverse large sieve, quadratic residues, primes in arithmetic progressions, finite fields, Lean formalization.

1.1. Historical context and scope. Green and Harper's paper on the inverse large sieve problem first appeared in November 2013 [2], nearly thirteen years before the September 2026 verification of the present counterexample. Their Conjecture 1.7 allows finitely many exceptions and is not refuted by this construction. The date of that related paper should therefore not be read as the first-proposal date of the exact-containment formulation resolved here.

1.2. Outline of the argument. The proof has three parts. The congruence restriction on q makes it possible to insert 2 without violating the modular cardinality bound. Dirichlet's theorem then makes the modular image large enough to obstruct any containing quadratic. Finally, a divergent prime sum prevents the counting function from being as small as (1).

2. QUADRATIC IMAGES OVER A PRIME FIELD

Fix a prime $p > 5$, and let $S = \{x^2 : x \in \mathbb{F}_p\}$, including zero. All sums in this section are taken in $\mathbb{F}_p$, with each element of a set counted once. The squaring map is two-to-one away from zero, so

$$|S| = \frac{p+1}{2}, \quad \sum_{s \in S} s = 0, \quad \sum_{s \in S} s^2 = 0. \quad (3)$$

Indeed, twice either sum on the right is respectively $\sum_{x \in \mathbb{F}_p} x^2$ or $\sum_{x \in \mathbb{F}_p} x^4$. Both vanish: for $0 < j < p-1$, multiplication by a suitable nonzero field element shows that $\sum_x x^j = 0$. The restriction $p > 5$ ensures this applies to $j = 2, 4$.

Lemma 2.1 (A moment identity). *Let $a, b, c \in \mathbb{F}_p$, with $a \neq 0$, and put*

$$T = \{ax^2 + bx + c : x \in \mathbb{F}_p\}.$$

Then $|T| = (p+1)/2$ and

$$\sum_{t \in T} t^2 = 2 \left(\sum_{t \in T} t \right)^2. \quad (4)$$

Proof. Complete the square and put $v = c - b^2/(4a)$. Then $T = v + aS$, and this affine map on S is injective. The cardinality assertion follows. As a scalar in $\mathbb{F}_p$, $|S| = (p+1)/2$ equals $1/2$. Thus (3) gives

$$\sum_{t \in T} t = \sum_{s \in S} (v + as) = \frac{v}{2},$$

and

$$\sum_{t \in T} t^2 = \sum_{s \in S} (v^2 + 2vas + a^2s^2) = \frac{v^2}{2}.$$

These two equalities imply (4). □

Lemma 2.2 (Replacing zero by a nonsquare). *Suppose 2 is a nonsquare in $\mathbb{F}_p$. Then*

$$E_p = (S \setminus \{0\}) \cup \{2\}$$

is not contained in the image of any degree-two polynomial over $\mathbb{F}_p$.

Proof. The set E_p has $(p+1)/2$ elements. By (3),

$$\sum_{t \in E_p} t = 2, \quad \sum_{t \in E_p} t^2 = 4.$$

If E_p were contained in a quadratic image, the two sets would have the same cardinality and hence would be equal. Lemma 2.1 would then give $4 = 2 \cdot 2^2 = 8$ in $\mathbb{F}_p$, which is impossible for an odd prime. □

3. THE MODULAR BOUND AND FAILURE OF CONTAINMENT

We use the supplementary law of quadratic reciprocity in the form

$$2 \text{ is a square modulo an odd prime } p \iff p \equiv 1 \text{ or } 7 \pmod{8}. \quad (5)$$

We also use Dirichlet's theorem: if r is relatively prime to a positive integer m , there are arbitrarily large primes congruent to r modulo m . These are standard arithmetic inputs; the corresponding Lean development uses Mathlib's quadratic-residue and primes-in-progressions results.

Proposition 3.1. *For every odd prime p , $|A_p| \leq (p+1)/2$.*

Proof. If 2 is a square modulo p , every element of A reduces to a square, so the assertion follows from the number of quadratic residues including zero. If 2 is a nonsquare, no $q \in \mathcal{P}$ can equal p : otherwise $p \equiv 1 \pmod{8}$, contradicting (5). Since both p and q are prime, q^2 therefore reduces to a nonzero square. Hence

$$A_p \subseteq (S \setminus \{0\}) \cup \{2\},$$

whose cardinality is $(p-1)/2 + 1 = (p+1)/2$. $\square$

Lemma 3.2. *For every odd prime p , the set A_p contains every nonzero square in $\mathbb{F}_p$, as well as 2.*

Proof. Fix $u \in \mathbb{F}_p^\times$. The Chinese remainder theorem gives a residue class r modulo $8p$ with

$$r \equiv 1 \pmod{8}, \quad r \equiv u \pmod{p}.$$

This class is relatively prime to $8p$. Dirichlet's theorem supplies a prime q in it. Then $q \in \mathcal{P}$ and $q^2 \bmod p = u^2$, as required. The element 2 belongs to A by definition. $\square$

Proposition 3.3. *The set A is not contained in $P(\mathbb{Z})$ for any $P \in \mathbb{Q}[x]$ of degree two.*

Proof. Write

$$P(x) = \frac{ax^2 + bx + c}{d}, \quad a, b, c, d \in \mathbb{Z}, \quad a \neq 0, \quad d \neq 0.$$

Choose, by Dirichlet's theorem, a prime

$$p \equiv 3 \pmod{8}, \quad p > \max\{5, |a|, |d|\}.$$

Reduction modulo p defines a polynomial

$$\overline{P}(x) = \overline{d}^{-1}(\overline{a}x^2 + \overline{b}x + \overline{c}) \in \mathbb{F}_p[x]$$

of degree two. If $A \subseteq P(\mathbb{Z})$, clearing the denominator in each equality $n = P(z)$ and reducing it modulo p gives $A_p \subseteq \overline{P}(\mathbb{F}_p)$.

By (5), 2 is a nonsquare modulo this p . Lemma 3.2 gives $E_p \subseteq A_p$, contradicting Lemma 2.2. $\square$

4. THE COUNTING FUNCTION

The quantitative input needed here is weaker than the prime number theorem for arithmetic progressions. We use the classical divergence statement

$$\sum_{q \in \mathcal{P}} \frac{\log q}{q} = \infty. \quad (6)$$

This is precisely the specialization to the reduced residue class 1 modulo 8 of the weighted prime-sum result used in the submitted formalization; see [3]. Infinitude of $\mathcal{P}$ alone would not suffice for the following argument.

Proposition 4.1. *The counting function $A(X)$ is not $O(\sqrt{X}/(\log X)^{100})$.*

Proof. Write $\pi_{1,8}(Y) = |\mathcal{P} \cap [1, Y]|$. The map $q \mapsto q^2$ is injective on positive integers, so

$$\pi_{1,8}(Y) \leq A(Y^2).$$

Suppose the asserted big- O bound held. Evaluating it at Y^2 gives, for sufficiently large Y ,

$$\pi_{1,8}(Y) \leq C \frac{Y}{(\log Y)^{100}}$$

for some constant $C > 0$, after absorbing the factor 2^{100} . In particular there is $C_1 > 0$ such that

$$\pi_{1,8}(2^{k+1}) \leq C_1 \frac{2^{k+1}}{(k+1)^{100}}$$

for all sufficiently large integers k . For $2^k \leq q < 2^{k+1}$, $\log q/q \leq (k+1) \log 2/2^k$. Therefore

$$\begin{aligned} \sum_{\substack{q \in \mathcal{P} \\ 2^k \leq q < 2^{k+1}}} \frac{\log q}{q} &\leq \pi_{1,8}(2^{k+1}) \frac{(k+1) \log 2}{2^k} \\ &\leq \frac{2C_1 \log 2}{(k+1)^{99}}. \end{aligned}$$

The right-hand side is summable over k . Adding the finitely many initial blocks would make the series in (6) convergent, a contradiction. $\square$

Propositions 3.1, 3.3, and 4.1 prove Theorem 1.1. Since $0 \notin A$, the use of $[1, X]$ here agrees with the formal statement's counting convention $A \cap \{n : n \leq X\}$.

5. LEAN PROOF CORRESPONDENCE AND VERIFICATION EVIDENCE

The formalization develops the counterexample in the namespace `Green47Counterexample`. Conjectures' public verification report records successful compilation, acceptance by Lean's default kernel, comparison with the negation of `Green47.green_47`, and a permitted-axiom check. The final declaration is `Bounty.target`. The correspondence between the mathematical argument and the submitted declarations is as follows.

Argument in this paper	Submitted declaration
Lemma 2.1	<code>quadratic_moment</code>
Lemma 2.2	<code>exceptionalImage_not_subset_quadImage</code>
Proposition 3.1	<code>local_bound</code>
Lemma 3.2	<code>goodPrime_in_residue</code>
Proposition 3.3	<code>no_rational_quadratic</code>
Proposition 4.1	<code>not_small</code>
Negation of the published target	<code>target</code>

5.1. Public artifacts and verification scope. The artifacts are linked from the [public result record](#). The [complete Lean source](#) and [machine-readable verification report](#) are publicly accessible. The source is also available as the `source` field of the [solution API response](#). The UTF-8 source consists of 24,478 bytes with SHA-256

`eddeff2c83de970aab5390fb0684a147712897ef4ed2e8b9cf755d4631152388`.

The public report identifies the full original report by SHA-256

`b87ddf938a8f9032a42d33d87557dab5da852e5defcbc9e0fb16be7ff8193849`.

This second digest commits to the full report, not to its public JSON projection.

The verification used Lean 4.33.1 and the revisions below. The complete revisions and dependency fingerprints are recorded in the [dependency lock file](#).

Component	Revision
Mathlib	0df444a360ea
Formal Conjectures, patched	8432eac99811
Conjectures verifier	428166381eba
Statement comparator	68a064109f01

The verification permits `propext`, `Quot.sound`, and `Classical.choice`. The optional Nanoda checker was disabled. The recorded checks concern the Lean target and its dependencies; they do not mechanically verify the prose exposition. No new Lean verification was performed for this manuscript revision.

ACKNOWLEDGMENTS

OpenAI Codex assisted with drafting, revising, and typesetting the exposition from the Lean proof and its verification records.

REFERENCES

- [1] B. Green, *100 Open Problems*, Problem 47, p. 23, online collection, version consulted 9 September 2026. <https://people.maths.ox.ac.uk/greenbj/papers/open-problems.pdf>.
- [2] B. Green and A. J. Harper, *Inverse questions for the large sieve*, Geometric and Functional Analysis **24** (2014), 1167–1203. Preprint first submitted 24 November 2013. See Conjecture 1.7 and Appendix A. <https://arxiv.org/abs/1311.6176>.
- [3] The Mathlib Community, *Primes in arithmetic progressions*, at the library revision recorded in the final section. Its weighted prime-sum divergence theorem gives (6); the submitted proof uses the corresponding Mathlib declaration. [Pinned source](#).