

A Computer-Assisted Proof of Alexa's Primality Criterion

Alper Ferudun*

25 October 2026

Abstract

For $n \geq 8$, let $K = \lfloor n^{1/3}/2 \rfloor$ and let r_i be the least nonnegative residue of $(2i+1)^{n-1}$ modulo n . We prove Alexa's corrected criterion that n is prime if and only if $\sum_{i=1}^K r_i = K$. Residue counting excludes cancellation by zero terms. A classical bound for the least odd quadratic nonresidue excludes even inputs. Prime-product counting treats large prime squares. For odd semiprimes, an integer-parameter version of the Forbes–Kayal–Mittal–Saha polynomial construction bounds an initial odd run in a proper subgroup of order g by $7\sqrt{g} + 50$. Both prime factors of a counterexample would consequently be below 150000. The remaining prime squares and semiprimes are excluded by reproducible exact computations, independently implemented in C++ and Python.

1 The criterion

The corrected formulation of Alexa's conjecture in Open Problem Garden [1] is also recorded as OPG-37413 in *UnsolvedMath* [2]. The residues must be taken individually in $[0, n)$, and the sum is an ordinary integer sum.

Theorem 1. *Let $n \geq 8$ be an integer, put $K = \lfloor n^{1/3}/2 \rfloor$, and define $0 \leq r_i < n$ by $r_i \equiv (2i+1)^{n-1} \pmod{n}$. Then n is prime if and only if $\sum_{i=1}^K r_i = K$.*

Throughout, set $N = 2K + 1$, $t = n^{1/3}$, and write $r(a)$ for the least nonnegative residue of a^{n-1} modulo n . Thus

$$t - 1 < N \leq t + 1 < n, \quad a \in \{3, 5, \dots, N\} \iff (a - 1)^3 \leq n \quad (a \geq 3 \text{ odd}).$$

Every prime passes by Fermat's theorem. We exclude composite inputs. The proof uses the classical odd-nonresidue bound stated in Knapp–Köcher–Schmid [3], the explicit prime-counting bound of Rosser–Schoenfeld [5], and the polynomial method of Forbes–Kayal–Mittal–Saha [4]. We give the needed integer parameter choices and nonvanishing argument explicitly. The finite computations in Section 7 are part of the proof.

2 Zero residues and the possible factorization

Lemma 2. *If $\sum_{i=1}^K r_i = K$, then every $r_i = 1$.*

Proof. Let z count zero terms. The sum condition gives

$$z = \sum_{r(a) > 0} (r(a) - 1).$$

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: [AlperTheKing](https://github.com/AlperTheKing).

A residue is zero exactly when $\text{rad}(n) \mid a$, because every prime-power exponent in n is at most $n - 1$. If $z > 0$, then n is odd and $R = \text{rad}(n) \leq N$.

Suppose R has at least two prime divisors, and let q be its smallest. Then $R \geq 5q$. Put $k = \lfloor N/q \rfloor \geq 5$. The number y of odd multiples of q in the test set is $\lceil k/2 \rceil \geq k/2$, while $z \leq (k/5 + 1)/2$. Each of the $y - z$ multiples of q not divisible by R has a positive residue at least $q \geq 3$. Therefore $3z \geq 2y \geq k$, whereas $3z \leq 3k/10 + 3/2 < k$, a contradiction.

It remains that $n = q^e$ with q an odd prime. The case $e = 1$ cannot have a tested multiple of q . For $e = 2$, the only possibility with $q \leq N$ is $n = 9$, which has sum zero and $K = 1$. Thus $e \geq 3$. Every nonzero residue is 1 modulo q , so z is a positive multiple of q . If $3 \leq e \leq 5$, then

$$z \leq \frac{N/q + 1}{2} \leq \frac{q^{2/3} + q^{-1} + 1}{2} \leq \frac{3q}{8} + \frac{2}{3} < q,$$

using $q^{2/3} \leq 3q/4$ for $q \geq 3$. This is impossible.

For $e \geq 6$, at most z/q nonzero residues differ from 1. The cyclic unit group modulo q^e has exactly $q - 1$ solutions of $x^{q^e-1} = 1$, since $\gcd(q^e - 1, q^{e-1}(q - 1)) = q - 1$. Hence

$$q - 1 \geq K - z - z/q \geq \frac{5N}{18} - \frac{7}{6}, \quad N \leq \frac{18q + 3}{5}.$$

For $q \geq 5$, this contradicts $N > q^2 - 1 > (18q + 3)/5$. For $q = 3, e \geq 7$, we have $t > 12$, hence $N \geq 13 > 57/5$. The last case $n = 729$ has residues $0, 583, 625, 0$, whose sum is 1208, not $K = 4$. Thus $z = 0$, and all the positive terms must be 1. $\square$

A passing input therefore has no odd prime factor at most N . Every such factor is at least $N + 2 > t + 1$. In particular, an odd composite passing input has at most two prime factors, counted with multiplicity: it is p^2 or pq , with $N < p < q$ odd primes.

3 Even inputs

Lemma 3. *Every even integer $n \geq 8$ fails the criterion.*

Proof. All tested residues are odd and positive. If their sum were K , they would all be 1. Testing 3 modulo 4 shows $4 \nmid n$. Write $n = 2m$ with $m \geq 5$ odd. If $m = p$ is prime, then $p > 3$ and $3^{2p-1} \equiv 3 \pmod{p}$, a contradiction. Otherwise choose an odd prime factor $p \leq \sqrt{m}$. We must have $p > N \geq 3$.

The classical bound quoted in [3] supplies an odd quadratic nonresidue $v_p < \sqrt{p}$, except at the eight primes in the table below. Since $n \geq 2p^2$, this gives $v_p < t$, so v_p is a tested base. But $n - 1$ is odd: an element whose $(n - 1)$ -st power is 1 has odd order, and hence is a square in $\mathbb{F}_p^*$. This is impossible. For the exceptional primes use

p	5	7	11	13	23	59	109	131
v_p	3	3	7	5	5	11	11	17

Euler's criterion verifies each nonresidue, and $(v_p - 1)^3 \leq 2p^2 \leq n$ verifies that it is tested. $\square$

4 Prime squares

Lemma 4. *No odd prime square passes the criterion.*

Proof. Suppose $n = p^2$ passes. By Lemma 2, $p > N$ and all tested bases satisfy $a^{p^2-1} \equiv 1 \pmod{p^2}$. In the cyclic unit group this is equivalent to $a^{p-1} \equiv 1 \pmod{p^2}$. These roots form a subgroup of order $p - 1$. If $P = \pi(N) - 1$, all unordered products of two odd primes at most

N , including repeated factors, belong to this subgroup. They are distinct integers less than p^2 , so

$$P(P+1)/2 \leq p-1. \quad (1)$$

For $p \geq 27000000$, put $u = p^{1/3} \geq 300$. The inequality $\pi(x) > x/\log x$ for $x \geq 17$ [5, Corollary 1, (3.5)] gives

$$P > \frac{u^2 - 1}{2 \log u} - 1 \geq \frac{u^2}{(201/100) \log u}.$$

The last inequality follows from $u^2/201 \geq 1 + 2 \log u$. Indeed, $\log u \leq u/10$ and $u^2/201 \geq 1 + u/5$ hold at 300 and their differences increase thereafter. Also $\sqrt{u}/\log u$ increases for $u > \exp(2)$, and at 300 it exceeds $(171/10)/6 = 57/20$. Since $(201/100)\sqrt{2} < 57/20$, this implies $P > \sqrt{2p}$, contradicting (1).

For odd primes $p < 27000000$, the exact computation in Section 7 finds only $p = 11, 1006003$ with $3^{p-1} \equiv 1 \pmod{p^2}$. Both have $N \geq 5$, and

$$5^{10} \bmod 121 = 78, \quad 5^{1006002} \bmod 1006003^2 = 31695130519.$$

Thus base 5 excludes them. $\square$

5 Odd runs in finite-field subgroups

We use an integer-parameter form of the polynomial construction in [4, Section 2]. The following nonvanishing observation is a confluent-Vandermonde argument.

Lemma 5. *Let $a_1, \dots, a_r$ be distinct in $\mathbb{F}_q$, and let D, T be positive integers with $T = (r-1)D$ and $E = rD - 1 < q$. The rD polynomials $x^h(x + a_i)^T$, $0 \leq h < D$, are linearly independent.*

Proof. Suppose a linear functional L on polynomials of degree at most E annihilates their span. Set $P(a) = L((x+a)^E)$. Its derivatives of orders $0, \dots, D-1$ vanish at each a_i , because $(x+a_i)^{E-h}$ lies in the indicated span. The scalar derivative factors are nonzero since $E < q$. Thus P has at least $rD = E+1$ zeros counted with multiplicity, and $P = 0$. All binomial coefficients in $(x+a)^E$ are nonzero modulo q , so $L = 0$. The span is the full rD -dimensional space. $\square$

Lemma 6. *Let H be a proper subgroup of $\mathbb{F}_q^*$, for an odd prime q , of order g . If $1, 3, \dots, N \in H$, where $N < q$ is odd, then*

$$N < 7\sqrt{g} + 50.$$

Proof. For $g < 20$, distinctness gives $N \leq 2g - 1 \leq 37$. For $g \geq 20$, choose integers

$$\begin{aligned} j &= \lfloor \sqrt{g/5} \rfloor, & r &= 2j, & M &= j, \\ s &= -(g + M - 1) \bmod (r-1), & T &= g + M - 1 + s, & D &= T/(r-1). \end{aligned}$$

Here $j \geq 2$, $0 \leq s \leq r-2$, and $g \geq 5r^2/4$. These choices satisfy

$$M(D+s) + \frac{M(M-1)}{2} < rD, \quad E = rD - 1 < 2g < q. \quad (2)$$

For the first inequality it suffices that $g > (5r^2 - 21r + 22)/4$: substitute D and use the worst case $s = r-2$. For the second, $T \leq g + 3r/2 - 3$ implies

$$(r-1)(2g-E) \geq (r-2)g - \frac{3}{2}r^2 + 4r - 1 > 0.$$

Finally, properness gives $q \geq 2g + 1$.

Consider the common roots of $(x + 2i)^g = 1$, $0 \leq i < r$. For polynomials G_i of degree at most $D - 1$, set

$$F(x) = \sum_{i=0}^{r-1} G_i(x)(x + 2i)^T.$$

At a common root, the derivative $F^{(\ell)}$, $0 \leq \ell < M$, reduces by $(x + 2i)^g = 1$ to a polynomial of degree at most $D + M + s - \ell - 2$. Requiring all its coefficients to vanish imposes at most $M(D + s) + M(M - 1)/2$ homogeneous linear conditions on rD coefficients. By (2), a nonzero coefficient vector exists. Lemma 5 ensures $F \neq 0$. It has degree at most E , with multiplicity at least M at each common root. There are therefore at most $\lfloor E/M \rfloor = 2D - 1$ common roots.

Put $L_0 = (N + 1)/2$. If $L_0 \geq r$, the first $L_0 - r + 1$ odd elements are distinct common roots, so $L_0 \leq 2D + r - 2$. The same bound is immediate if $L_0 < r$. Thus $N \leq 4D + 2r - 5$. Since $g \leq 5(j + 1)^2 - 1$,

$$D = \left\lceil \frac{g + j - 1}{2j - 1} \right\rceil < \frac{5j^2 + 11j + 3}{2j - 1} + 1 = \frac{5}{2}j + \frac{31}{4} + \frac{39}{4(2j - 1)}.$$

Consequently

$$N < 14j + 26 + \frac{39}{2j - 1} \leq 14j + 39 < 7\sqrt{g} + 50.$$

□

6 The semiprime cutoff

Proposition 7. *If an odd semiprime $n = pq$, $p < q$, passes, then $p, q < 150000$.*

Proof. We have $N < p < q$. Set $g = \gcd(p - 1, q - 1)$. For every tested a , its order modulo q divides $\gcd(pq - 1, q - 1) = g$. All odd bases through N therefore lie in the proper subgroup of order $g \leq p - 1$ in $\mathbb{F}_q^*$. Lemma 6 gives

$$t < 7\sqrt{p} + 51.$$

If $p \geq 150000$, then $t > p^{2/3}$ would imply

$$p^{1/6} < 7 + \frac{51}{\sqrt{p}} < 7 + \frac{51}{380} < \frac{36}{5},$$

contrary to $(36/5)^6 < 150000$. Hence $p < 150000$.

If $p < 100$, the inequalities $p \geq N + 2$ and $t < N + 1$ give $q < (p - 1)^3/p < p^2 < 10000$. Otherwise $10 \leq \sqrt{p} < 388$, and

$$\begin{aligned} q &< \frac{(7\sqrt{p} + 51)^3}{p} = 343\sqrt{p} + 7497 + \frac{54621}{\sqrt{p}} + \frac{132651}{p} \\ &< 343 \cdot 388 + 7497 + \frac{54621}{10} + \frac{132651}{100} = \frac{14736961}{100} < 150000. \end{aligned}$$

□

7 Finite verification and reproducibility

All primality decisions in the finite endgames use an Eratosthenes sieve. All modular arithmetic is exact. The C++ implementation uses unsigned 128-bit products before reducing to 64 bits; Python uses arbitrary-precision integers. Cube roots and all endpoint decisions are computed with integer arithmetic.

For each odd prime $p < 27000000$, compute $3^{p-1} \bmod p^2$. There are 1683064 such primes. The only residues equal to one occur at 11, 1006003; base 5 excludes both as recorded above.

For distinct odd primes $p < q < 150000$, a factor 3 fails immediately. For $p, q > 3$, put $o_p = \text{ord}_p(3)$, $o_q = \text{ord}_q(3)$. The base-3 Fermat condition is equivalent to

$$o_p \mid q - 1, \quad o_q \mid p - 1.$$

Orders are computed by factoring $p-1$ and testing divisions of the exponent. The C++ checker enumerates the progression $q = p + o_p, p + 2o_p, \dots$, retaining prime values and applying the second divisibility test. The Python audit independently groups primes q by o_q , and visits the groups indexed by divisors of $p-1$. The two enumerations agree on all 4571 base-3-liar pairs. For each pair the accompanying CSV records an odd base $a \leq N$ with $0 < r(a) < pq$ and $r(a) \neq 1$. The largest required witness is 31.

Finite verification domain or outcome	Count
Odd primes $p < 27000000$, square case	1683064
Primes below 150000	13848
Base-3-liar semiprime pairs	4571
Semiprime pairs without a tested witness	0
Prime squares without a tested witness	0

Every residue for a squarefree semiprime and a tested base is positive: a zero would require $pq \mid a$, while $a \leq N < pq$. Thus a recorded witness makes the sum exceed K . Together with Lemmas 2–4 and Proposition 7, the finite endgames prove Theorem 1.

The source package contains `check_finite.cpp`, `check_audit.py`, their outputs, and all 4571 witness rows. From the package’s `reproducibility` directory, the verification can be reproduced using a C++17 compiler and Python 3:

```
c++ -std=c++17 -O2 check_finite.cpp -o check_finite
./check_finite experiments/semiprime-witnesses.csv \
    > experiments/finite.json
python3 check_audit.py > experiments/audit.json
```

The packaged audit skips only the local team’s historical-file integrity check when that optional claim file is absent. Its full mathematical finite domains are unchanged. The audit also checks 19992 literal residue sums and the integer parameter and cutoff identities. These additional regression tests supplement the analytic proof; they do not replace its universal steps.

8 Scope and provenance

The result concerns the corrected 2013 integer-residue formulation, not earlier modular-sum variants in the Garden comments, and not Giuga’s conjecture. It does not claim a practical improvement over modern primality algorithms. The classical nonresidue theorem, prime-counting bound and polynomial method are credited to their sources. A bounded literature search found no proof of this exact criterion; this is not an absolute priority certificate.

An earlier retained computational investigation reduced potential counterexamples to a few factorization shapes and tested integers below $3 \cdot 10^{10}$. The present proof sharpens and writes out the reduction and supplies the missing finite-field bound. Its verification uses the smaller structured domains above and does not rely on that earlier large scan. AI systems assisted the source search, derivations, code and manuscript preparation. This is a self-audited, unrefereed preprint; the two implementations are cross-checks, not independent peer review or a proof-assistant formalization.

References

- [1] Open Problem Garden, *Alexa’s Conjecture on Primality*, posted 28 March 2012, corrected 14 June 2013.
https://www.openproblemgarden.org/op/alexas_conjecture_on_primality.
 Accessed 25 October 2026.
- [2] ulamai, *UnsolvedMath*, version 1.6.0, record OPG-37413 (3361). Frozen commit: `c6e7f41b4eb6ce876feb83e7eb626be1b243fd7e`.
<https://huggingface.co/datasets/ulamai/UnsolvedMath>.
- [3] W. Knapp, M. Köcher and P. Schmid, On the least odd quadratic non-residue, *Beitr. Algebra Geom.* **54** (2013), 483–491. doi:10.1007/s13366-012-0086-6.
- [4] M. Forbes, N. Kayal, R. Mittal and C. Saha, *Square root Bound on the Least Power Non-residue using a Sylvester-Vandermonde Determinant*, 2011.
<https://arxiv.org/abs/1104.4557>.
- [5] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94. doi:10.1215/ijm/1255631807.