

Artin's Primitive Root Conjecture

Bogdan Grechuk • 15 Oct 2026

<https://functor.network/user/3333/entry/2012>

On October 4, 2026, OpenAI released a preprint (OpenAI 2026) claiming to resolve one of the most famous open problems in number theory: *Artin's primitive root conjecture*, formulated almost a century ago. The paper claims that every integer a which is neither -1 nor a perfect square is a primitive root modulo infinitely many primes. Moreover, it gives a quantitative lower bound for the number of such primes. The result is currently a preprint, and its proof has yet to undergo independent verification.

Let us recall the problem. If p is a prime, the nonzero residue classes modulo p form a multiplicative group of order $p - 1$. A classical theorem states that this group is *cyclic*, meaning that there exists an integer a whose powers

$$a, a^2, a^3, \dots, a^{p-1}$$

represent all $p - 1$ nonzero residue classes modulo p .

Such an integer a is called a *primitive root modulo p* . Equivalently, the smallest positive integer k such that

$$a^k \equiv 1 \pmod{p}$$

is $k = p - 1$. This smallest integer is called the *multiplicative order* of a modulo p and is denoted by $\text{ord}_p(a)$.

For example, 2 is a primitive root modulo 5, since

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 3, \quad 2^4 \equiv 1 \pmod{5}.$$

However, 2 is not a primitive root modulo 7, since

$$2^3 \equiv 1 \pmod{7}.$$

Thus, even though every prime has primitive roots, a given integer need not be a primitive root modulo every prime.

In 1927, Emil Artin asked a natural question: if we fix an integer a , are there infinitely many primes p for which a is a primitive root?

There are two obvious exceptions. First, -1 has multiplicative order at most 2, so it cannot be a primitive root modulo any prime greater than 3. Second, if $a = b^2$ is a perfect square, then for every odd prime p not dividing a , Fermat's

little theorem gives

$$a^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

Hence $\text{ord}_p(a) \leq (p-1)/2$, and a cannot be a primitive root.

Artin conjectured that these are the only obstructions: *every integer a which is neither -1 nor a perfect square is a primitive root modulo infinitely many primes.*

In fact, Artin made a stronger prediction. For every such integer a , he conjectured that the number of primes $p \leq x$ for which a is a primitive root is asymptotic to

$$C_a \frac{x}{\log x}$$

for some positive constant C_a . For example, when $a = 2$, the predicted constant is the famous *Artin constant*

$$C_2 = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.3739558.$$

Thus, Artin predicted that 2 is a primitive root modulo approximately 37.4% of all primes.

Despite its elementary formulation, the conjecture proved extremely difficult. In 1967, Hooley (Hooley 1967) established Artin's predicted asymptotic under the generalized Riemann hypothesis for certain number fields. However, this assumption remains unproved.

In 1986, Heath-Brown (Heath-Brown 1986) obtained an important unconditional result: among all prime numbers a , at most two can fail to be primitive roots modulo infinitely many primes. In particular, at least one of 2, 3, and 5 must be a primitive root modulo infinitely many primes. Remarkably, this did not establish the assertion for any one of these three integers individually.

The new OpenAI preprint claims to resolve the infinitude question for every admissible integer, without assuming the generalized Riemann hypothesis.

Theorem 1 (OpenAI) *Let $a \in \mathbb{Z}$ be neither -1 nor a perfect square. Then there exist constants $c_a > 0$ and $x_a \geq 2$ such that, for every $x \geq x_a$,*

$$\#\{p \text{ prime} : x < p < 2x, \quad \text{ord}_p(a) = p-1\} \geq c_a \frac{x}{(\log x)^2}.$$

In particular, the theorem asserts that there are infinitely many primes p for which 2 is a primitive root modulo p . The same conclusion holds for every other integer satisfying Artin's conditions.

Notice that the lower bound is weaker than the conjectured asymptotic. The conjecture predicts approximately $C_a x / \log x$ such primes up to x , whereas the theorem gives a lower bound of order $x / (\log x)^2$ in each sufficiently large interval $(x, 2x)$. Thus, the preprint claims to prove the infinitude part of Artin's conjecture, but not the predicted positive density.

Let us briefly discuss the main idea of the proof. If a is not a primitive root modulo a prime p , then there must be some prime divisor q of $p - 1$ such that

$$a^{(p-1)/q} \equiv 1 \pmod{p}.$$

Thus, to prove that a is a primitive root, it suffices to rule out all such congruences.

The authors construct a large collection of primes p for which $p - 1$ has a particularly convenient factorization. They then show that, for almost all primes in this collection, none of the unwanted congruences can hold. The proof combines elementary counting arguments with sophisticated estimates on the distribution of primes.

The approach is interesting because it combines two very different ideas: constructing primes whose predecessors $p - 1$ have a specially controlled factorization, and using analytic number theory to eliminate all remaining obstructions to maximal multiplicative order.

If the proof withstands independent scrutiny, it will settle the infinitude part of a conjecture that has resisted mathematicians for almost one hundred years. The stronger conjecture predicting the exact positive density of primes with a prescribed primitive root would still remain open.

References

- Heath-Brown, D. R. 1986. "Artin's Conjecture for Primitive Roots." *Quarterly Journal of Mathematics*, Oxford series (2), vol. 37 (1): 27–38. <https://doi.org/10.1093/qmath/37.1.27>.
- Hooley, Christopher. 1967. "On Artin's Conjecture." *Journal für Die Reine Und Angewandte Mathematik* 225: 209–20. <https://doi.org/10.1515/crll.1967.225.209>.
- OpenAI. 2026. *Primitive Roots for Every Admissible Integer Base*. OpenAI Math Release preprint. <https://github.com/openai/math/blob/main/preprints/Primitive-roots-for-every-admissible-integer-base-October-4-2026/primitive-roots-all-integer-bases.pdf>.