

Is there a largest prime number?

Juan Segurola · All Rights Reserved

QUE · Article 043 · Simple Questions, Deep Answers · Version 0.1 EN

No prime number is the last. This answer does not depend on how far a computer has searched, and discovering another very large prime would not make the underlying argument stronger. The claim concerns every possible finite list of primes, including lists whose entries nobody has written down.

The distinction is between extending a collection and proving that it cannot be complete. Computation can establish the properties of particular integers. A proof can explain why no finite collection contains them all. Euclid's Elements, Book IX, Proposition 20, gives an argument that prime numbers exceed any assigned finite multitude. [1]

1. What is a prime?

Here a prime is an integer greater than one whose only positive divisors are one and itself. Thus two and three are prime, while six is not: two and three divide it. The number one is excluded by the definition. The question is about this precise class of positive integers, not about how large a written numeral can be.

A preliminary fact makes the argument work: every integer greater than one has a prime divisor. To see why, choose its smallest divisor greater than one. If that divisor were composite, it would itself have a smaller divisor greater than one, which would also divide the original number. This contradicts the choice of the smallest divisor. The chosen divisor must therefore be prime.

The proof uses the ordering of positive integers and ordinary divisibility. It does not require that we already know how to factor a huge number efficiently. Existence of a divisor and a practical method for finding it quickly are distinct issues.

2. Take any proposed complete list

Suppose someone gives us a finite list of all primes, p_1 through p_n . Multiply every entry to obtain P , and form $N = P + 1$. Each listed prime divides P exactly. Dividing N by any one of them therefore leaves remainder one.

Consequently, no prime on the list divides N . Yet N is greater than one and so has a prime divisor by the preliminary argument. That divisor is absent from the proposed complete list. The list cannot have been complete.

Nothing in the reasoning depended on which finite list we started with. That is what gives the proof its reach. It does not test the first thousand possibilities and guess that the pattern continues; it supplies a contradiction for any finite claim of completeness. The product construction is a familiar modern presentation of the divisibility argument. [1]

3. The number we construct need not be prime

This is the place where an otherwise convincing explanation often goes wrong. The proof does not say that multiplying consecutive primes and adding one always produces a prime. It says that the result has a prime divisor outside the starting list.

For the list 2, 3 and 5, the construction gives 31, which is prime. But using 2, 3, 5, 7, 11 and 13 gives 30,031, and $30,031 = 59 \times 509$. This example is composite, while still doing exactly what the proof requires. Neither 59 nor 509 is among the six starting primes.

A composite result is not a failed test of the theorem. It is one of the two cases the argument allows. Confusing the constructed integer with the new prime divisor changes a valid proof into an invalid recipe. The difference is small in wording and decisive in logic.

4. Does the new prime have to be larger?

If the starting list really contains all primes up to some bound, an absent prime divisor must exceed that bound. If the list is merely an arbitrary selection, the absent divisor might instead be a smaller prime that was omitted. Both cases are compatible with the proof.

The theorem therefore defeats a claim of a largest prime as follows. If a largest prime existed, every prime would occur among the finitely many integers from two to that value. We could list them, and the construction would show that the list was incomplete. This contradicts the assumption.

A useful exercise is to distinguish “not on this list” from “larger than every item on this list”. They coincide only when the list has the appropriate completeness property. Keeping track of that condition prevents a common hidden step in popular presentations.

5. What computation can still contribute

The theorem gives no efficient general procedure for finding a prime of a desired size. Building P may require an enormous integer, and extracting a factor of $P + 1$ can be computationally difficult. A proof of unbounded existence and an algorithm's running time are different achievements.

Similarly, a largest known prime is a statement about a body of verified knowledge at a particular time. A largest prime would be a statement about the integers themselves. Updating a record can change the first statement and cannot change the theorem ruling out the second. No numerical record is needed to understand the distinction.

There is no scientific uncertainty about the conclusion within ordinary integer arithmetic and the stated definitions. The relevant cautions concern the scope of the proof, the validity of each step and the error of replacing it with an experimental trend. Other questions about how primes are distributed or how efficiently they can be found are not settled merely by showing that there are infinitely many.

The answer is exact: there is no largest prime because any finite purportedly complete list can be shown to omit a prime divisor of a specifically constructed integer. The strength of the result lies in its general argument, not in the size of any number we have happened to calculate.

References

[1] Euclid. Elements, Book IX, Proposition 20. Online edition and commentary by David E. Joyce, Clark University. <https://mathcs.clarku.edu/~djoyce/elements/bookIX/propIX20.html>

Related reading

Article 044: How can we know that a knot cannot be undone?