THEOREM OF THE DAY

Euclid's Infinity of Primes There are infinitely many prime numbers.



A prime number is an integer greater than one which cannot be divided exactly by any other integer greater than one. Euclid's proof, well over two thousand years old, that such numbers form an infinity, is often cited by mathematicians today as the prototype of a beautiful mathematical argument. Thus, suppose there are just N primes, where N is a positive integer. Then we can list the primes: p_1, p_2, \ldots, p_N . Calculate $q = 1 + p_1 \times p_2 \times \ldots \times p_N$. Now q cannot be prime since it is larger than any prime in our list. But dividing q by any prime in our list leaves remainder 1, so q cannot be divided exactly by any prime in our list. So it cannot be divided by any integer greater than 1 other than q and is therefore prime by definition. This contradiction refutes the assertion that there were only N primes. So no such assertion can be made.

Remarks: (1) Euclid's proof uses the fact that non-divisibility by a prime implies non-divisibility by a non-prime (a composite). This is the content of **Book 7, Proposition 32** of his *Elements*.

(2) It would be a mistake to think that we always get a new prime directly from q since, for example, $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$ and 1 + 30030 is not prime, being the product of the two prime numbers 59 and 509.

Scant record exists of any such person as Euclid of Alexandria (325–265 BC) having existed. However, the *Elements* certainly date from third century BC Alexandria and although Greek mathematics, rooted in geometry, did not recognise the concept of infinity, this theorem with what is effectively this proof appears as *Proposition 20* in *Book IX*.

Web link: aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html. Is 1 prime? Find out here: arxiv.org/abs/1209.2007. **Further reading:** *Ancient Mathematics (Sciences of Antiquity)*, by Serafina Cuomo, Routledge, 2001.