

There are “Infinitely” Many Primes!

We will use the symbols $a|b$ to mean that a divides b . All numbers will be assumed to be positive integers. A number which has no factors other than itself and 1 is called *prime*; if a number isn't prime it's called *composite*.

Lemma 1. *Every number N has a prime factor.*

Proof: If the number N is prime, then it has itself as a prime factor. If it's composite, it has some factor F_1 not equal to 1; if F_1 isn't prime, it has a factor F_2 , not equal to 1, smaller than F_1 ; if F_2 isn't prime, it has a factor F_3 , not equal to 1, smaller than it. Continuing in this way, we get a sequence of positive whole numbers:

$$N > F_1 > F_2 > F_3 \dots$$

where each one divides the previous. This must terminate since there are only a finite number of numbers less than N . The last of these F 's must then be a prime factor of N .

Lemma 2. *A never divides $MA + 1$.*

Proof: When you divide A into $MA + 1$ you get a quotient of M with a remainder of 1.

Theorem (Euclid). *There are infinitely many primes.*

Proof: Suppose there are only finitely many; call them p_1, p_2, \dots, p_n . So these are the *only* primes. Let $N = p_1 p_2 \dots p_n + 1$ (multiply all the primes together and add 1). By Lemma 1, N must have a prime factor P ; by Lemma 2, P can't be any of the primes $p_1 \dots p_n$. Since by assumption these are the *only* primes, this is a contradiction, so there can't have been only a finite number of primes.

Please note that the use of the word “infinitely” here is not from Euclid. The Greeks never conceived of an infinite collection of anything as existing in reality. What Euclid proved might be more accurately phrased as “the list of primes is never-ending,” or “for any collection of primes there is always another not on that list.”