Euclid's Theorem

Around 300 B.C., Euclid published a proof that there are infinite primes in *Elements* (Book IX, Proposition 20). It is a simple and rather beautiful proof. For simplicity, we will only work with natural numbers (positive integers) Let's begin with a few definitions:

Definition 1 (Modulo). For any natural number $a, b \in \mathbb{N}$, we can write their quotient as

$$\frac{a}{b} = n + \frac{m}{b}, \tag{7}$$

where n, m are also natural numbers and $0 < m < b$. For the above a, b, the modulo operation is defined as

$$a \bmod b = m, \tag{8}$$

Definition 2 (Primes). A natural number $p \in \mathbb{N},\ p > 1$ is a prime if it is wholly divisible by itself and one[1]. In other words, given any prime p, for any other natural $n \in \mathbb{N}$

$$n \neq p, 1 \implies n \bmod p > 0. \tag{9}$$

It can also be shown that to p is prime if for any other prime q,

$$q \neq p \implies 1 \bmod p > 0. \tag{10}$$

since any natural $n \in \mathbb{N}$ can be constructed from a set of prime factors P_n:

$$\forall n \in \mathbb{N}, \quad \exists P_n = \{p_1, p_2, ..., p_z\} \quad s.t. \quad n = \prod_{i=1}^{z} p_i. \tag{11}$$

Theorem (Euclid's theorem). There are infinite primes. In other words, the set of all primes P has infinite elements.

Proof. By contradiction, assume that the set of all primes P **is finite**, so that

$$P = \{p_1, p_2, ..., p_z\} \tag{12}$$

for some finite z. For example, sorted from lowest to highest, $P = \{2, 3, 5, 7, 11, ..., k\}$ where k is the largest prime number. We will show that any such finite set that presumes to contain all primes actually fails to contain all primes.

Let p^* be the product of all primes in P plus 1:

$$p^* = 1 + \prod_{i=1}^{z} p_i. \tag{13}$$

Then by (4) we have that $p*$ is a prime, since

$$\forall p_i \in P, \quad p_i \bmod p* = 1 > 0. \tag{14}$$

Since $p*$ is larger than any $p_i \in P$, it is not contained in P. Thus, because P does not contain $p*$, P does not contain all primes. $\square$

In other words, for any finite set of primes, you can always construct another prime number by method (7). So there cannot exist a finite set that contains all primes.

[1] For some technical reasons, we do not include 1 as a prime.