Euclid's proof that there are infinitely many primes.

Euclid ~ 300 BC

Proof from Prop. 20 in BOOK IX of "The Elements"

Modern language

<u>Theorem</u> Any finite list of primes can be extended

<u>Proof</u> Let $p_1, \ldots, p_j$ be a list of prime numbers.

Consider the integer

$$P = (p_1 p_2 \cdots p_j) + 1$$

$$= \left(\prod_{i=1}^{j} p_i \right) + 1.$$

<u>Case 1</u> P might be prime and so it's a new prime not on our original list.

Case 2 P is not prime, i.e. composite

But then there exists a prime factor q of P.

Claim: q is not on the original list. Suppose it was

let's $q = p_i$, for some $1 \le i \le j$

and consider

$$1 = P - (p_1 \cdots p_j)$$

Since q is a factor of both terms on the right. Therefore q is a factor of 1. This impossible.

So q is not on the original list.

So in all the cases the list of primes can be extended.

$2, 3, 5, 7, 11, 13, \ldots$