Euclid’s proof of infinite primes

- Assume that there are a finite number of primes that can be listed in order $p_1, p_2, \ldots, p_n$
- Now construct the number:

$$M = (p_1 \times p_2 \times \cdots \times p_n) + 1$$

- None of the existing primes, $p_1, \ldots, p_n$, can divide M exactly (as each leaves a remainder 1)
- Therefore **either** M is itself a prime and $M > p_n$ **or** M is a product of other primes all of which must be $> p_n$
- So we can always generate a larger prime than our last prime p_n. This contradicts our assumption and proves that there are an infinite number of primes