The arithmetic progression $n + 1$, $n \geqslant 0$, contains infinitely many primes. A Euclidean proof

About this document

This file has been developed as part of a BSc Thesis in Mathematics by Joan Arenillas i Cases at the Autonomous University of Barcelona. The url https://github.com/joarca01/final-math-bsc-thesis provides full access to the complete Thesis. Please use joanarenillas01@gmail.com to report any typo or express any suggestions.

The fact that the arithmetic progression $\equiv 1 \pmod 1$, that is, $n + 1$, $n \geqslant 0$, contains infinitely many primes, stems from the fact that there exist infinitely many primes. For completeness we shall reproduce here Euclid's proof that there exist infinitely many primes.

Theorem 1 (**Euclid**). *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many primes, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime not in our list. Thus, consider $Q := p_1 p_2 \cdots p_m + 1$. This number has at least one prime divisor, p, since $Q > 1$. If p was one of the p_i for $1 \leqslant i \leqslant m$, then p would divide $p_1 p_2 \cdots p_m$. Since p also divides Q, we deduce that p divides $Q - p_1 p_2 \cdots p_m = 1$, so p must be equal to 1, a contradiction (1 is not a prime). Therefore, p is a prime, and it cannot be in our list, which is a contradiction again. ∎