The arithmetic progression $2n+1$, $n \geqslant 0$, 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.

We will prove that the arithmetic progression $\equiv 1 \pmod 2$ contains infinitely many primes. Equivalently, we will see that there are infinitely many primes of the form $2n+1$, $n \geqslant 0$.

Lemma 1. *There are infinitely many primes* $\equiv 1 \pmod 2$.

Proof. Suppose there are finitely many primes $\equiv 1 \pmod 2$, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime $\equiv 1 \pmod 2$ not in our list. For this goal, consider $Q := p_1 p_2 \cdots p_m$ and the polynomial $f(x) := 2x - 1$. Now, $f(Q) = 2p_1 p_2 \cdots p_m - 1 = 2Q - 1$. This number has at least one prime divisor, p, since it is greater than one. We then have that p divides $2Q-1$.

Next, observe that $p \neq p_i$ for every i such that $1 \leqslant i \leqslant m$: if $p = p_i$ for some i, then p would divide $2Q$. Since p also divides $2Q-1$, we get that p divides 1, so $p = 1$, which is a contradiction (1 is not a prime). Therefore, p is a prime divisor of $2Q-1$ not in our list. Finally, note that $2Q-1$ has all its prime divisors $\equiv 1 \pmod 2$ since it is odd, so p is a new prime $\equiv 1 \pmod 2$.

This gives us an infinitude of primes $\equiv 1 \pmod 2$ provided we have one. Since 3 is a prime $\equiv 1 \pmod 2$, the desired result is finally settled. ■