Goldbach's Conjecture Finally Proven

Ed de Almeida, PhD

July 28, 2024

Abstract

This paper introduces a complete proof for Goldbach's Conjecture, based on simple Number Theory techniques.

1 Introduction

Since June 7th, 1742, when Christian Goldbach wrote to his friend Leonard Eüler stating something like

> "I believe all even numbers greater than four may be written as a sum of two prime numbers, but I couldn't find a proof for this claim."

many mathematicians tried to find such a proof. All of them failed until now.

In my opinion, there are two main reasons to explain this massive failure, which includes some of the greatest mathematicians of all time, even the most prolific of us all, Leonard Euler.

First reason is the complexity of prime numbers' distribution among positive integers. Even with all computational resources we have today, the simple task of checking if a number is prime or not requires an enormous computational effort when we enter the space of huge numbers.

The second reason, I think, is the unnecessary complexity we mathematicians introduced even in simple problems, specially since the 20th century.

High order algebras, complex spaces and morphisms of all sorts are always introduced in solutions, even when dealing with simple problems. It's almost

as if we needed to show how good we are with these complex things, despite the fact we could apply simple techniques to simple problems.

I've always used a "rule of thumb" when solving math problems, and my rule is only raising the complexity of my tools when this represents a proportional reduction of the problem's complexity as a whole.

My "rule of thumb", of course, is not mine. It's just a way to rephrase Occam's Razor, a well-known principle by William of Occam, a medieval monk.

I'll remind here late Professor William Boyce. In his foreword to "Partial differential Equations and Boundary Value Problems", which he wrote with Richard DiPrima, Professor Boyce criticizes, with his natural humour, those mathematicians who skip lines in complex demonstrations they publish, in order to pretend to be smarter than they really are with sentences like "then we easily find".

Nothing in this paper was easily found. and this is the reason why I will neither skip lines, nor pretend I am smarter than I really am. This means I will include demonstrations which will be considered too elementary by most. And I'll do this as a gift to the young undergraduate student I was forty years ago. I used to feel very dumb when reading some papers written by mathematicians like those mentioned by Professor Boyce. When I first read his book I noticed I wasn't as dumb as some of us are pretentious.

2   Introductory definitions

2.1   Some special sets

Thru this paper we shall use some sets here defined.

Definition 1: Let $\mathfrak{P}$ be the set of all prime numbers.

Definition 2: Let $\mathfrak{G}$ be the set of all numbers mentioned by Goldbach in his conjecture, i.e., $\mathfrak{G} = \{n \in \mathbb{N} : n > 4 \text{ and } 2|n\}$.

Definition 3: Let $\mathbb{N}^* = \mathbb{N} \cup \{0\}$, i.e., the of all natural numbers, plus the zero.

2.2   Some entities

These are some of the tools we shall use to prove Goldbach's Conjecture.

Definition 4: Let the sequence $< s_i >$ be such that $s_i = 3 + 2i$ for all $i \in \mathbb{N}^*$.

This sequence is a very special tool, because being $(3, 2) = 1$ a well-known result by Dirichlet assures us that this sequence contains infinite prime numbers. In fact, it contains all primes greater than two. For the rest of this paper I shall use s_i or $s(i)$, making no difference between these notations.

Definition 5: Let $\mathbf{g} : \mathfrak{G} \to \mathbb{N}^*$ be such that $\mathbf{g}(n) = \frac{n-6}{2}$, $\forall n \in \mathfrak{G}$.

It is easy to see that $\mathbf{g}$ is a bijection. Given $n_1, n_2 \in \mathfrak{G}$, with $n_1 \neq n_2$, we have $n_1 \neq n_2 \Rightarrow n_1 - 6 \neq n_2 - 6 \Rightarrow \frac{n_1-6}{2} \neq \frac{n_2-6}{2} \Rightarrow \mathbf{g}(n_1) \neq \mathbf{g}(n_2)$. On the other hand, given $i \in \mathbb{N}^*$ we may take $n = 2i + 6$. Of course, $2|n$ and $n > 4$, $\forall i \in \mathbb{N}^*$. Then, $n \in \mathfrak{G}$, according to Definition 2.

Definition 6: Given an arbitrary $n \in \mathfrak{G}$, let's define the set $S_n = \{i \in \mathbb{N}^* : i \leq \mathbf{g}(n)\}$.

2.3   Some preliminary results

In this section I shall introduce some small results that will help us ahead.

Result 1: The only three successive odd prime numbers p, $p+2$ and $p+4$ are 3, 5 and 7.

Proof: Let's consider $p \in \mathfrak{P}$, $(p+2) \in \mathfrak{P}$ and $(p+4) \in \mathfrak{P}$, with $p \neq 3$. Of course $p = 3q + 1$ or $p = 3q + 2$, with $q \in \mathbb{N}$, because $p = 3q$ would imply $3|p$ and, since $pin\mathfrak{P}$, it would be $p = 3$, which contradicts outr hypothesis. Being $p = 3q + 1$, then $p + 2 = 3a + 3$, and then $3|(p+2)$ and, therefore, $p + 2 = 3$. But this makes $p = 1$ and contradicts $p \in \mathfrak{P}$. Finally, being $p = 3q + 2$, then $p + 4 = 3q + 6$. This makes $3|(p+4)$ and, therefore, $p + 4 = 3$, i.e., $p = -1$, which contradicts $p \in \mathfrak{P}$. So, it must be $p = 3$ and the proof is done.

It happens that, by Definition 4, $s(0) = 3$, $s(1) = 5$ and $s(2) = 7$.

This result is quite simple, indeed, but it will help us a lot, when we shall need to "break" the $\mathfrak{G}$ set into smaller parts.

Result 2: $\forall n \in \mathfrak{G}$, then $s_i + s_j = n$ if, and only if, $i + j = \mathbf{g}(n)$.

Proof: $i + j = \mathbf{g}(n) \Leftrightarrow i + j = \frac{n-6}{2} \Leftrightarrow 2(i+j) = n - 6 \Leftrightarrow 2i + 2j + 6 = n \Leftrightarrow (3 + 2i) + (3 + 2j) = n \Leftrightarrow s_i + s_j = n$.

3   Breaking things appart

Now it's time for putting all these things together. And I shall start by recalling, for a given $n \in \mathfrak{G}$, the S_n set in Definition 6.

According to Result 2, a certain n may always be written as a sum of two elements of Sn. The point now is to prove that, $\forall n \in \mathfrak{G}$ we may find such a sum with the two parts being prime numbers.

Let's start by excluding elementary cases, so we can concentrate on the difficult ones.

The first elementary case which occurs to me is when $s(\mathbf{g}(n)) \in \mathfrak{P}$. It is elementary because $\mathbf{g}(n) + 0 = \mathbf{g}(n)$. Since $s(0) = 3 \in \mathfrak{P}$, our hypothesis gives us n as a sum of two primes. To make thing even better, the Dirichlet's result previously mentioned assures us that we have an infinite number of such situations.

Definition 7: Let $\mathfrak{G}^0 = \{n \in \mathfrak{G} : s(\mathbf{g}(n)) \in \mathfrak{P}\}$.

Of course, this takes us nowhere. We have an infinite number of elements in $\mathfrak{G}^0$, but also have an infinite numberof elements of $\mathfrak{G}$ out of this set. But we shall not give up, for it's time for another definition.

Definition 8: Let $\mathfrak{G}^1 = \{n \in \mathfrak{G} : s(\mathbf{g}(n) - 1) \in \mathfrak{P}\}$.

Here again we have $s(\mathbf{g}(n) - 1) + 1 = \mathbf{g}(n)$ and n may be written as a sum of two primes, since $s(1) = 5 \in \mathfrak{P}$.

Please be patient and endure one more definition, pretty similar to the previous ones.

Definition 9: Let $s(\mathbf{g}) - 2) = \{n in \mathfrak{G} : s(\mathbf{g}(n) - 2) \in \mathfrak{P}\}$.

Like in the previous definitions, the n's in this set may be written as a sum of two primes, because $s(2) = 7$ is a prime number.

These three sets would be useless without something connecting them. This is why we now have

Result 3: Let $n \in \mathfrak{G}^0$. Then $(n + 2) \in \mathfrak{G}^1$.

Proof: $n \in \mathfrak{G}^0 \Rightarrow s(\mathbf{g}(n)) \in \mathfrak{P}$. It happens that $\mathbf{g}(n + 2) = \frac{(n+2)-6}{2} = \frac{(n-6)+2}{2} = \frac{n-6}{2} + \frac{2}{2} = \frac{n-6}{2} + 1 = \mathbf{g}(n) + 1$. Then $\mathbf{g}(n + 2) = \mathbf{g}(n) + 1 \Rightarrow \mathbf{g}(n + 2) - 1 = \mathbf{g}(n)$ and $s(\mathbf{g}(n + 2) - 1) = s(\mathbf{g}(n)) \in \mathfrak{P}$.

The same strategy may be used to prove that $n \in \mathfrak{G}^0 \Rightarrow (n + 4) \in \mathfrak{G}^2$ and also that $n \in \mathfrak{G}^1 \Rightarrow (n + 2) \in \mathfrak{G}^2$. Unfortunatelly we can't go farther, because $s(3) = 9$ is not a prime.

These results, whose demonstration I'm going to skip, with Result 3, allow me to write $\mathfrak{G}$ as a union of the following four sets

$$\mathfrak{G} = \mathfrak{G}^0 \cup \mathfrak{G}^1 \cup \mathfrak{G}^2 \cup \mathfrak{G}^*$$

where $\mathfrak{G}^*$ is the complementary of the union of the other three in relation to $\mathfrak{G}$.

We know for sure that all elements of the three initial sets may be written as a sum of two primes. Our goal now is to prove that the same holds $\forall n \in \mathfrak{G}^*$. And this is what will be done in the next section.

4 Yes, it holds for the rest

Contents