Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 March 2021 doi:10.20944/preprints202103.0281.v1

CONSIDERATIONS FOR GOLDBACH'S STRONG CONJECTURE

Author: Carleilton Severino da Silva
ORCID iD - https://orcid.org/0000-0001-9461-2785
INSTITUIÇÃO: SEDUC-SP (Secretaria de Educação do Estado de São Paulo)

ABSTRACT

Since 1742, the year in which the Prussian Christian Goldbach wrote a letter to Leonhard Euler with his Conjecture in the weak version, mathematicians have been working on the problem. The tools in number theory become the most sophisticated thanks to the resolution solutions. Euler himself said he was unable to prove it. The weak guess in the modern version states the following: any odd number greater than 5 can be written as the sum of 3 primes. In response to Goldbach's letter, Euler reminded him of a conversation in which he proposed what is now known as Goldbach's strong conjecture: any even number greater than 2 can be written as a sum of 2 prime numbers. The most interesting result came in 2013, with proof of weak version by the Peruvian Mathematician Harald Helfgott, however the strong version remained without a definitive proof. The weak version can be demonstrated without major difficulties and will not be described in this article, as it becomes a corollary of the strong version. Despite the enormous intellectual baggage that great mathematicians have had over the centuries, the Conjecture in question has not been validated or refuted until today.

Keywords: Goldbach's conjecture, numbers prime, Arithmetic Theorem.

DEFINITIONS AND SOME PROPERTIES OF WHOLE NUMBERS

Let $n \in Z$, where Z is the Set of Integers then follows: $\forall\, n \in Z,\ \exists\, I \,|\, I = \{2n+1\}$, where I is the Set of Odd Numbers, $I \subseteq \mathbb{Z}$.

Let $n \in \mathbb{Z}$, Where $\mathbb{Z}$ is the Set of Integers, then follows: $\forall\, n \in \mathbb{Z},\ \exists\, P \,|\, P = \{2n\}$, where P is the Set of Even numbers, $P \subseteq \mathbb{Z}$.

There are numbers that can only be divided by itself and by the unit. These numbers form the Prime Numbers Set and will be represented here generically by $\Lambda = \{q_1, q_2, q_3, \dots, q_k\}$, where k is a positive integer. Since $q = 1.q = q.1$, then the only possible divisors of q are 1 and q, itself, so that $mmc(1,q) = q$, which characterizes q as a prime. In this article the letter y and x will be used for composite whole numbers and they can be written in terms of prime numbers.

Consider $y = x_k x_s$, where $x = \prod_{k=1}^{k} q_k$ and $x_s = \prod_{s=1}^{s} \varphi_s$, rewriting $y = \prod_{k=1}^{k} q_k \prod_{s=1}^{s} \varphi_s = q_1 \dots q_k \varphi_1 \dots \varphi_t$, where $q_1 \leq q_2 \leq \cdots \leq q_k$, $\varphi_1 \leq \varphi_2 \leq \cdots \leq \varphi_t \in \Lambda$. This is the formalization of the Fundamental Theorem of Arithmetic, which in words "every composite whole number can be written in terms of prime factors and each number has a unique decomposition signature, except in the order of its factors".

DEMONSTRATION OF THE EXISTENCE OF DECOMPOSITION

Sinse y is a prime, then $y = q$, it is trivial $\{y, 1\} = \{q, 1\}$. If y is composed, then $\exists x_k \,|\, 1 < x_k < y$ that divides y so that $y = x_k x_s$ e $1 < x_s, < y$. Hypothetically, x_k and x_s can be written as the multiplication of prime factors, such that, $x_k = \prod_{k=1}^{k} q_s = q_1 q_2 q_3 \dots q_k$ and $x_s = \prod_{s=1}^{s} \varphi_s = \varphi_1 \varphi_2 \varphi_3 \dots \varphi_s$, rewriting it comes; $y = (q_1 q_2 \dots q_k)(\varphi_1 \varphi_2 \dots \varphi_s) = \prod_{k=1}^{k} q_k \prod_{s=1}^{s} \varphi_s$, where $k, s, \geq 1$ are positive integers. Since x_k and x_s can be decomposed into their prime factors, the decomposition of y is also obtained.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 March 2021 doi:10.20944/preprints202103.0281.v1

In the above demonstration, it is considered that the primes are not necessarily distinct, so it is possible to regroup them so that the Fundamental Theorem of Arithmetic can be rewritten in its standard form, known as canonical form, that is: $y = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$, where $\alpha_1, \dots, \alpha_k$ are positive integers and represent the exponents generated by the clusters of primes that eventually repeat, in this case, each prime forms a power $q_k^{\alpha_k}$, after this rearrangement, there is $q_1 < q_2 < \cdots < q_k$.

DEMONSTRATION OF THE UNIQUENESS OF DECOMPOSITION

Each number, when decomposed into its prime factors has a unique signature, is called the uniqueness of the decomposition. Let $y = q_1 q_2 q_3 \dots q_k$, where $q_1 \leq q_2 \leq \cdots \leq q_k$, it is known that the decomposition is unique and in this case the length is k. To prove that given a decomposition of length k, it is unique, suppose there is another decomposition for this case and has length 1, so, $\varphi_1 = y = q_1 q_2 q_3 \dots q_k$, where φ_1 is prime. Like $q_1 | q_1 q_2 q_3 \dots q_k$, $\rightarrow q_1 | \varphi_1 \rightarrow \varphi_1 = q_1 \Rightarrow 1 = q_2 q_3 \dots q_k$, absurd, because for $k > 1$, there is $\frac{1}{q_2} = q_3 \dots q_k$, an invertible $\mathbb{Z}$ impossible product. We conclude that for $k = 1$, $y = \varphi_1 = q_1$, which proves that this decomposition is unique. By induction, it is proved that the proposition will be valid for $s + 1$. In fact, doing $y = \varphi_1 \varphi_2 \varphi_3 \dots \varphi_{s+1} = q_1 q_2 q_3 \dots q_k$, like $q_1 | q_1 q_2 q_3 \dots q_k \rightarrow q_1 | \varphi_1 \varphi_2 \varphi_3 \dots \varphi_{k+1}$, for some $j \in \{1, 2, 3, \dots, s, s+1\}$, $q_1 \varphi_j \Rightarrow q_1 = \varphi_j$. How the two factors coincide on both sides of the above equation; $\not{\varphi_1} \varphi_2 \varphi_3 \dots \varphi_{s+1} = \not{q_1} q_2 q_3 \dots q_k \Rightarrow \varphi_2 \varphi_3 \dots \varphi_{s+1} = q_2 q_3 \dots q_k$. This equality shows that factors φ_j and q_i are equal for all i and $j \in \{2, 3, 4, \dots, s, s+1\}$. The length of the decomposition in the first member is é $s = (s+1) - 1$, -1 comes from the fact that in the first member φ_1 it was canceled. Furthermore, for equality, we have $k = s + 1$, which justifies the coincidence between the factors φ_j and q_i, proving that the uniqueness of the decomposition is also valid for $s + 1$. Before starting the demonstration proposed in this article, it will be important to look at other properties of whole numbers. Let $y \in I$ and $p \in P$:

Property 1: the multiplication of an odd number by an odd number will always result in an odd number. Demonstration: let two integers be any n and m;
$(2n+1)(2m+1) = 4mn + 2n + 2m + 1 = 2(2mn + n + m) + 1$. Calling the portion $(2mn + n + m)$ of k, where $k \in \mathbb{Z}$, we have: $2(2mn + n + m) + 1 = 2k + 1 = y$

Property 2: multiplying an odd with an even number will always result in an even number. Demonstration: let two integers be any n and m; $(2n)(2m+1) = 4mn + 2n = 2(mn + n)$. Calling $(nm + n)$ of k, where $k \in \mathbb{Z}$, we have: $2k = p$

Property 3: multiplying a pair with a pair will always result in an even number. Demonstration: let two integers be any n and m; $(2n)(2m) = 4mn = 2(2mn)$. Calling $(2nm)$ of k, where $k \in \mathbb{Z}$, we have: $2k = p$

Property 4: adding an odd to an odd will always result in an even number. Demonstration: let any two integers be n and m; $(2n+1) + (2m+1) = 2n + 2m + 2 = 2(n + m) + 2$. Calling $(n + m)$ de k, where $k \in \mathbb{Z}$, we have: $2(n + m) + 2 = 2k + 2 = p$

Property 5: adding an odd to a pair will always result in an odd number. Demonstration: let two integers be any n and m; $(2n) + (2m+1) = 2n + 2m += 2(n + m) + 1$. Calling $(n + m)$ de k, where $k \in \mathbb{Z}$, we have: $2(n + m) + 1 = 2k + 1 = y$

Property 6: adding a pair to a pair will always result in an even number.
Demonstration: let two integers be any n and m; $(2n) + (2m) = 2(n + m)$. Calling $(n + m)$ of k, where $k \in \mathbb{Z}$, we have: $2(n + m) = 2k = p$
Property 4 says that the sum of two odd numbers always results in an even number, however, although the primes other than 2 are odd, it has never been possible to prove that the sum of any prime numbers any other than 2 generates even numbers, this it happens because the quoted property is valid for compound

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 March 2021 doi:10.20944/preprints202103.0281.v1

numbers. There is no guarantee that this property will work if the odd ones are prime. However, with a proof, the Goldbach's Conjecture turns into Theorem and then it will be an extension of property 4.

MOTTO

Proposition: Let $y = x_k x_s \in I$, where $I = \{2n+1\} \subseteq \mathbb{Z}$, x_k and x_s are odd integers and $p = x_k + x_s$, $p \in \mathbb{Z}$, then there is: $x^2 - px + y = 0$, where x_k e x_s are roots of this equation.

Demonstration

$$y = x_k x_s \quad \Rightarrow \quad x_k = \frac{y}{x_s} \qquad EQ.1$$

$$p = x_k + x_s \quad \Rightarrow \quad x_k = p - x_s \qquad EQ.2$$

Joining $EQ.1$ and $EQ.2$ we have;

$$y = x_s(p - x_s) =$$

$$x_s p - x_s^2 \quad \Rightarrow \quad x^2 - px + y = 0 \qquad EQ.3$$

The following conclusions are limited to the Set of Natural Numbers, but are valid for the Whole Set of Integers, since there are odd numbers and negative pairs.

Conclusion 1: y is prime if, and only if, there is only one possibility for the value of p, that is, $p = y + 1 = q + 1$. In this case the only factors are; $x_k = y = q$ and $x_s = 1$ or $x_k = 1$ and $x_s = y = \varphi$, where $\{q, \varphi\} \in \Lambda$.

Conclusion 2: y is composed if, and only if, there are factors $\{x_k,\ x_s\} \mid x_k \neq (y,\ 0,\ 1,)$ and $x_s \neq (1,\ 0,\ y,)$ being $1 < \{x_k, x_s\} < y$. For $x_k \neq 0$ and $x_s \neq 0 \Rightarrow y \neq 0$. In the case where the two factors are prime, we have $x_k = q$ and $x_s = \varphi$ and thus $y = q\varphi$. In this case, $p = q + \varphi$.

Conclusion 3: if and only if, $p = x_k + x_s$ is knawn, a $EQ.3$ will determine the factors $x_k,\ x_s$ for a given y, since the pair $\{x_k, x_s\}$ is the solution of the equation (trivial conclusion).

As already noted, the factors $x_k,\ x_s$ may or may not be composed. It is known that all composite numbers also have divisors, 1 and himself, in addition to non-trivial divisors, so for such numbers, $\exists p \mid p = x_k + x_s$, where $\{x_k, x_s\} \neq 1$ and $\{x_k, x_s\} \neq y$ and also $\exists p \mid p = y + 1$ for $y = x_k = q$ and $x_s = 1$ or for $y = x_s = \varphi$ and $x_k = 1$. If the number y for primo, is prime, it is only possible to obtain $p = y + 1$. This means that the equation $EQ.3$ is valid for compound numbers and for prime numbers. A simple check that $EQ.3$ is valid for primes follows as follows: let y be a number of the form $y = q.1 = q$, where q is prime, then from equation $EQ.3$ we have: $q^2 - (q+1)q + q = 1^2 - (q+1)1 + q = 0$. That is, the pair $\{q, 1\}$ satisfies the equation. Conclusions 1 and 2 complement each other as, once the numerical value of p, is known, it is possible to state whether y is prime or composed from the found roots.

THE STRONG GOLDBACH CONJECTURE

Let $y = q\varphi$, where $y \in I$, $\{q, \varphi\} \in \Lambda$ and $q \neq 2$ and $\varphi \neq 2 \rightarrow \{q, \varphi\} \in \Lambda$, $\Lambda \subseteq I \subseteq \mathbb{Z}$, then $\{q, \varphi\} \in \mathbb{Z}$.

Consider $q + \varphi = p$ $\qquad EQ.4$

Where p is an integer. One must arrive at the hypothesis;

$q + \varphi = p = 2k, k \in Z$ $\qquad EQ.5$

Joining $(EQ.1)$ and $(EQ.4)$, of property 4 results;

$yq + y\varphi = (q\varphi)q + (q\varphi)\varphi = (q\varphi)p = 2(kq\varphi) = 2n = p'$ $\qquad EQ.6$

With p' and $\in \mathbb{Z}, p' \subseteq P$.

Note that, for property 1, $(q\varphi)q$ and $(q\varphi)\varphi$ are odd. From $(EQ.4)$ can be obtained;

$\varphi = p - q$ $\qquad EQ.7$

Joining the equations $(EQ.6)$ and $(EQ.7)$, we obtain;

$2n = (q\varphi)q + q\varphi(p - q) =$

$(q\varphi)q + q\varphi p - (q\varphi)q =$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 March 2021 doi:10.20944/preprints202103.0281.v1

$p' = 2n = q\varphi p = 2kq\varphi$ $EQ.8$

If the Conjecture is correct, property 2 implies that p must be even.

So, $q + \varphi = p = 2k$ por $\{q, \varphi\} \neq 2$ e $2k > 4$. This is Goldbach's strong guess.

PROOF OF STRONG GOLDBACH CONJECTURE

It is known that there is $p = x_k + x_s$ for the equation $x^2 - px + y = 0$. Then;

$x_{k,s} = \frac{-p \pm \sqrt{(p^2 - 4ay}}{2a}$ $EQ.9.$

Follow the test;

$x = \frac{-p \pm \sqrt{(p^2 - 4ay}}{2a} \rightarrow$

$2ax = -p + \sqrt{(p^2 - 4ay)} \rightarrow$

$2ax + p = \sqrt{(p^2 - 4ay)}$, raising the two members of the equation come;

$(2ax + p)^2 = (p^2 - 4ay) =$

$(2ax + p)(2ax + p) = p^2 - 4ay =$

$4a^2x^2 + 2axp + 2axp + p^2 = p^2 - 4ay =$

$4a^2x^2 + 4axp + \cancel{p^2} = \cancel{p^2} - 4ay \rightarrow$

$4axp = -4a^2x^2 - 4ay \rightarrow$

$p = \frac{-4a(ax^2 + y)}{4ax} =$

$p = \frac{-(ax^2 + y)}{x} = 2k,\ x \neq 0$ $EQ.10$

Remembering that $p \in Z$, because it is the result of the sum of two integers. It is also defined that $y \in I \Rightarrow \{x_k, x_s\} \in I$. Keeping this in mind, property 4 guarantees that the numerator of $EQ.10$ will always be even. Even though $x = q$, where q is an odd prime, property 4 remains valid because $x^2 = q^2$ becomes a composite odd. Note that x is guaranteed to be an odd one, because if it weren't, y wouldn't be either, which guarantees that $ax^2 + y$ is of the form $2l$, where $l \in Z$. Property 2 also guarantees that $p = x_k + x_s = 2k$ is always true, since $px = 2kx = ax^2 + y = 2l$. This equation remains valid even when $\{x_k,\ x_s\} = \{q, \varphi\}$, because in which case $\{x_k,\ x_s\}$ are prime, they will be prime such that $\{x_k,\ x_s\} = \{q, \varphi\} \neq 2$, otherwise, y could not be odd. So for $y = q\varphi$ the $EQ.10$ is;

$p = \frac{-(aq^2 + y)}{q} \quad \Longrightarrow \quad p = \frac{-(aq^2 + q\varphi)}{q} = \frac{-q(aq + \varphi)}{q} = -(aq + \varphi).$

The coefficient a arises from the equation $EQ.3$, it is trivial that $a = 1$, therefore; $p = \frac{-(q^2 + y)}{q} = -(q + \varphi).$

The direct proof that $EQ.10$ results in an even number, regardless of whether x is prime or does not proceed as follows:

$p = \frac{-(aq^2 + y)}{q} = \frac{-(q^2 + y)}{q};$

As q^2 and $y \in I$, one can write$q^2 = 2n + 1$ and $y = 2m + 1$, so $EQ.10$ stays;

$-\left(\frac{q^2 + y}{q}\right) = -\left(\frac{2n + 1 + 2m + 1}{q}\right) = -2\left(\frac{n + m + 1}{q}\right).$ $EQ.11$

It is known that $q^2 = 2n + 1$ and $y = 2m + 1$, that $n = \frac{q^2 - 1}{2}$ and $m = \frac{y - 1}{2}$, like this;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 March 2021 doi:10.20944/preprints202103.0281.v1

$-\left(\frac{n+m+1}{q}\right) = -\left(\frac{q^2-1+y-1}{2q} + \frac{1}{q}\right) = -\left(\frac{q^2-1+y-1+2}{2q}\right) = -\frac{(q^2+y)}{2q}$. Knowing that q^2 and y são are odd, by property 4, $q^2 + y$ results in an even number, therefore $2|(q^2 + y)$. As well as $q|(q^2)$ and $q|(y)$, it can be done; $\frac{q^2}{q} + \frac{y}{q} = \left(\frac{q^2+y}{q}\right) = z$. Note that z is an integer. Since 2 and q are factors of $q^2 + y$, by the Fundamental Theorem of Arithmetic $2q|(q^2 + y)$, then;

$-\frac{(n+m+1)}{q} = -\frac{(q^2+y)}{2q} = k$, where $k \in \mathbb{Z}$. Substituting k in $EQ.11$ comes:

$$-2\left(\frac{n+m+1}{q}\right) = 2k = p = q + \varphi. \qquad EQ.12$$

Goldbach's conjecture is proven to be true. As the equation is valid for any prime greater than or equal to 3, the first even number that is obtained must be greater than 4, that is, $p = 2k > 4$, so $p = 3 + 3 = 6$ is the first even number that it is obtained with the sum of two odd prime numbers. In this case $y = 9$ and the value of $k = 3$. Substituting k at $p = 2k$, the number $p = 6$. is again reached. The demonstration of the weak Goldbach's Conjecture becomes just a Corollary of this work and easy to demonstrate. This will be left to the reader.

REFERENCES

SOUZA, José Emanuel. **Conjectura de Goldbach - Uma visão Aritmética**. Universidade dos Açores. Departamento de Matemática. Ilha de são Miguel – Portugal, Abril de 2013. Disponível em: https://repositorio.uac.pt/handle/10400.3/2881, consultado em: 02 de Janeiro, 2021.

BERTNONE, Ana Maria Amarillo. **Introdução à Teoria dos Números.** Universidade Federal e Uberlândia, Uberlândia-MG, 2014.

FILHO, Edgar de Alencar. Teoria Elementar dos Números. São Paulo, Nobel 1981.

FILHO, Ivan De Oliveira Holanda; Da CRUZ, Marcos Paulo Mesquita; Da COSTA, Ernandes Farias; GOMES, Rickardo Léo Ramos. **Números primos: os átomos da Matemática.** Revista Atlante. Cuadernos de Educación y Desarrollo, ISSN: 1989-4155, Setembro, 2020. Disponível em: https://www.eumed.net/rev/atlante/2020/09/numeros-primos.html, consultado em: 02, Janeiro, 2021.

BURTON, David M. **Elementary Number Theory.** University of New Hampshire. McGraw-Hill, 2007. 6th ed. Disponível em: https://napocaro.files.wordpress.com/2015/02/david_m-_burton_elementary_number_theory_sixth_bookfi-org.pdf, consultado em: 02, Janeiro, 2021.

SUTOY, Marcus. A música dos Números primos: A história de um problema não resolvido na Matemática. Rio de Janeiro, Jorge Zahar, ed. 2007.

“It is stated that there are no conflicts of interest of any kind in this article”.