



**HAL**  
open science

# The concept of prime number and the Legendre and Goldbach conjectures

Jamel Ghannouchi

► **To cite this version:**

Jamel Ghannouchi. The concept of prime number and the Legendre and Goldbach conjectures. Bulletin of Mathematical Sciences and Applications, 2014, 3 (4), pp.25. hal-01067727v2

**HAL Id: hal-01067727**

**<https://hal.science/hal-01067727v2>**

Submitted on 3 Oct 2014 (v2), last revised 19 Jan 2015 (v4)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# The concept of prime number and the Legendre, De Polignac and Goldbach conjectures

Jamel Ghanouchi

jamel.ghanouchi@live.com

Ecole Supérieure des Sciences et Techniques de Tunis

## Abstract

(MSC=11D04) In this document, we deal with the concept of prime number together with the Legendre, De Polignac and Goldbach conjectures.

Keywords : Primes ; Legendre ; De Polignac ; Goldbach ; Conjectures.

## Defintion

The prime numbers are called primes because they are the bricks of the numbers : Each number  $n$  can be written as  $n = p_1^{n_1} p_2^{n_2} \dots p_i^{n_i}$  when  $p_j$  are primes and  $n_j$  are integers.

This writing is called the decomposition in prime factors of the number  $n$ . In fact, this definition is a very particular case of a much more general one. Indeed, if  $n_j$  are rationals, everything changes.

Considering that the decomposition in prime factors of an integer  $n$  when  $n_j$  are rationals  $n = p_1^{n_1} p_2^{n_2} \dots p_i^{n_i}$ . In this writing, then the  $p_j$  have no reason to be the same than before and they become a convention. For example, if we decide that 16 is conventionally prime, we have  $2 = 16^{\frac{1}{4}}$  and each number can be written according to 16 and its rational exponent instead of 2.

If we decide conventionally that  $F_n = 2^{2^n} + 1$  is prime  $\forall n \geq 0$ , and it is possible by the fact that  $GCD(F_n, F_m) = 1$  when  $n \neq m$ , then each new prime (new primes=bricks with rational exponents in the writing) replaces another one in the list of the old primes (old primes=bricks with integral exponents in the writing).

Example : If by convention,  $F_5 = 2^{2^5} + 1 = 4294967297 = 641.6700417$  is prime, we can decide that it replaces  $641 = F_5.6700417^{-1}$  which becomes compound and 6700417 is prime or 641 is prime and  $6700417 = F_5.641^{-1}$  is compound.

In all cases, the advantage is that we have a formula which gives for each

$n$  a prime. And we can see the the primes are infinite.

There is a result which is enough interesting : Let Ulam spiral. The Fermat numbers are all situated in the same line.

Let us apply it to the real numbers !

The following numbers can be called bricks or elements, because they constitute the bricks of the numbers. They exist, of course, and we prefer to call them prime numbers because they really generalize the concept of primes. Let us see this : A real number is compound if it is equal to  $\pm p_1^{n_1} \dots p_i^{n_i}$  where  $p_j$  are prime numbers and  $n_j$  are rationals. We define other real prime numbers which can not be expressed like this :  $\pi, e, \ln(2)$ .

Thus  $\sqrt[p]{p} = p^{\frac{1}{p}}$  for example is compound.

We can notice that such numbers really generalize the concept of prime, as they can be written only as  $p = p.1$

Furthermore  $\sqrt[p]{p} + 1$  is conventionally prime, with  $p$  prime, hence  $\sqrt[p]{p} - 1 = (p - 1)(\sqrt[p]{p} + 1)^{-1}$  is compound !

And

$$\sqrt[p]{p} - 1 = (p - 1)(\sqrt[p]{p} + 1)^{-1}(\sqrt[p]{p} + 1)^{-1} \dots (\sqrt[p]{p} + 1)^{-1}$$

And, conventionally,  $\pi$  and  $e$  are primes instead of  $\pi^{n_0}$  and  $e^{m_0}$  with  $(n_0 - 1)(m_0 - 1) \neq 0$  which are compound.

We define the GCD of two numbers as following : If  $p_1$  and  $p_2$  are prime real numbers

$$p_1 \neq p_2 \Rightarrow GCD(p_1, p_2) = 1$$

$$n_1 n_2 < 0 \Rightarrow GCD(p_1^{n_1}, p_1^{n_2}) = 1$$

$$n_1 n_2 > 0; n_1 > 0 \Rightarrow GCD(p_1^{n_1}, p_1^{n_2}) = p_1^{\min(n_1, n_2)}$$

$$n_1 n_2 > 0; n_1 < 0 \Rightarrow GCD(p_1^{n_1}, p_1^{n_2}) = p_1^{\max(n_1, n_2)}$$

$$GCD(p_1^{n_1} p_2^{n_2} \dots p_i^{n_i}, p_1^{m_1} p_2^{m_2} \dots p_j^{m_j}) = \prod_{i,j} (GCD(p_i^{n_i}, p_j^{m_j}))$$

And if  $x = p_1^{n_1} p_2^{n_2} \dots p_i^{n_i}$  and  $y = p_1^{m_1} \dots p_i^{m_i}$  then  $y$  divides  $x$  if  $GCD(x, y) = y$ . Thus  $\frac{3}{2}$  does not divide the prime 3, for example.

## The Legendre conjecture

The Legendre conjecture states that there is always a prime number between the squares of two consecutive integers. What does it become with our new definition ? It remains true ! Effectively :

Proof :

We always have

$$(2n)^2 < 4n^2 + 1 < (2n + 1)^2 < 4n^2 + 8n + 1 < (2(n + 1))^2$$

Let us prove that

$$CD(4n^2 + 1, 4p^2 + 1) = 5; p \neq n$$

$$CD(4n^2 + 8n + 1, 4p^2 + 8p + 1) = 3, p \neq n$$

$$GCD(4n^2 + 1; 4p^2 + 8p + 1) = 1$$

We have

$$\begin{aligned} d|4n^2 + 1; \quad d|4p^2 + 8p + 1 \\ \Rightarrow d|4(p^2 - n^2) + 8p \end{aligned}$$

And  $4n^2 + 1$  is odd then  $d$  is odd and

$$d|p^2 - n^2 + 2p$$

But

$$d|4n^2 + 4p^2 + 8p + 2 \Rightarrow d|2(n + p)^2 - 4np + 4p + 1$$

Thus

$$d|2(p - n)(p + n)^2 + 4p(n + p)$$

And

$$d|2(p - n)(p + n)^2 + p - n + 4np(n - p) + 4p(p - n)$$

Hence

$$d|p - n + 4np(n - p) = p - n + 4pn^2 - 4np^2 - 8np + 8np$$

Or

$$d|8np \Rightarrow d|np$$

Thus

$$d|p - n \Rightarrow d|n \Rightarrow d = 1$$

Also

$$\begin{aligned} n = 5(k + k') \pm 1; p = 5(k - k') \pm 1 \neq n \\ \Rightarrow 5|4n^2 + 1; 5|4p^2 + 1 \end{aligned}$$

And

$$\begin{aligned} n = 3(k + k') + 2; p = 3(k - k') + 2 \neq n \\ \Rightarrow 3|4n^2 + 8n + 1; 3|4p^2 + 8p + 1 \end{aligned}$$

And  $4m^2 + 1$  and  $4p^2 + 8p + 1$  can be taken primes simultaneously by the new definition of the primes. Here is how : the first  $4m^2 + 1$  divisible by 5 is for  $m = 4$  and then  $4m^2 + 1 = 65 = 13 \cdot 5$ . We consider 65 prime and then  $5 = 65 \cdot 13^{-1}$  is not a prime. The second  $4m^2 + 1$  divisible by 5 is for  $m = 6$  and then  $4m^2 + 1 = 145 = 29 \cdot 5$ , 145 is now prime and  $29 = 145 \cdot 5^{-1} = 145 \cdot 65^{-1} \cdot 13$  is not a prime. All this because there is only one decomposition in prime factors. Etc...

Now by the same way, the first  $4m^2 + 8m + 1$  divisible by 3 is for  $m = 2$  and then  $4m^2 + 8m + 1 = 33 = 11 \cdot 3$  is prime and  $3 = 33 \cdot 11^{-1}$  is not a prime, etc...

By this definition of the primes, as

$$(2n)^2 < 4n^2 + 1 < (2n + 1)^2 < 4n^2 + 8n + 1 < (2(n + 1))^2$$

Means that between all  $x^2$  and  $(x + 1)^2$  there is a prime  $\forall x \in \mathbb{N}$ .

## De Polignac conjecture

By the same way than before, we consider that  $4m^2 + 4k' + 1$ ,  $4m^2 + 4k' + 3$ ,  $4m^2 + 4k' + 7$ ,  $4m^2 + 4k' - 3$ ,  $4m^2 + 4k' - 1$ ,  $4m^2 + 4k' - 7$  and  $4p^2 + 8p + 4k + 1$ ,  $4p^2 + 16p + 4k + 3$ ,  $4p^2 + 16p + 4k + 7$  are always primes.

then

$$\begin{aligned} \forall 2(2n + 1), \exists(p, m, k, k') | n = p^2 - m^2 + 2p + k - k' + 2 \text{ or } n = p^2 - m^2 + 2p + k - k' + 2 \\ \text{or } n = p^2 - m^2 + 2p + k - k' + 3 \text{ or } n = p^2 - m^2 + 2p + k - k' - 1 \\ \Rightarrow 2(2n + 1) = 4p^2 + 8p + 4k + 1 - 4m^2 - 4k' - 1 \text{ or } 2(2n + 1) = -4m^2 - \\ 4k' + 7 + 4p^2 + 8p + 4k + 3 \text{ or } 2(2n + 1) = -4m^2 - 4k' + 7 + 4p^2 + 8p + 4k + 7 \\ \text{or } 2(2n + 1) = 4p^2 + 8p + 4k + 1 - 4m^2 - 4k' - 3 \end{aligned}$$

And  $2(2n + 1)$  is always the difference of two primes. And

$$\begin{aligned} \forall 2(2n), \exists(p, m, k, k') | n = p^2 - m^2 + k - k' + 1 \text{ or } n = p^2 - m^2 + k - k' - 1 \text{ or } \\ n = p^2 - m^2 + k - k' + 2 \text{ or } n = p^2 - m^2 + k - k' - 2 \\ \Rightarrow 2(2n) = 4p^2 + 4k + 3 + 4m^2 + 4k' + 1 \text{ or } 2(2n) = 4p^2 + 4k - 3 + 4m^2 + 4k' - \\ 1 \text{ or } 2(2n) = 4p^2 + 4k + 7 + 4m^2 + 4k' + 1 \text{ or } 2(2n) = 4p^2 + 4k - 7 + 4m^2 + 4k' - 1 \\ \text{And } 2(2n) \text{ is always the difference of two primes!} \end{aligned}$$

Thus  $2n$  is always the difference of two primes,  $\forall n \in \mathbb{N}$ .

## Goldbach conjecture

By the same way than before, we consider that  $4m^2 + 4k' + 1$ ,  $4m^2 + 4k' + 3$ ,  $4m^2 + 4k' + 7$ ,  $4m^2 + 4k' - 3$ ,  $4m^2 + 4k' - 1$ ,  $4m^2 + 4k' - 7$  and  $4p^2 + 8p + 4k + 1$ ,  $4p^2 + 16p + 4k + 3$ ,  $4p^2 + 16p + 4k + 7$  are always primes.

then

$$\begin{aligned} \forall 2(2n + 1), \exists(p, m, k, k') | n = p^2 + m^2 + 2p + k + k' \text{ or } n = p^2 + m^2 + 2p + k + k' + 2 \\ \text{or } n = p^2 + m^2 + 2p + k + k' + 3 \text{ or } n = p^2 + m^2 + 2p + k + k' - 1 \\ \Rightarrow 2(2n + 1) = 4p^2 + 8p + 4k + 1 + 4m^2 + 4k' + 1 \text{ or } 2(2n + 1) = 4m^2 + 4k' + \\ 7 + 4p^2 + 16p + 4k + 3 \text{ or } 2(2n + 1) = 4m^2 + 4k' + 7 + 4p^2 + 16p + 4k + 7 \text{ or } \\ 2(2n + 1) = 4p^2 + 16p + 4k + 1 + 4m^2 + 4k' - 3 \end{aligned}$$

And  $2(2n + 1)$  is always the sum of two primes. And

$$\begin{aligned} \forall 2(2n), \exists(p, m, k, k') | n = p^2 + m^2 + k + k' + 1 \text{ or } n = p^2 + m^2 + k + k' - 1 \text{ or } \\ n = p^2 + m^2 + k + k' + 2 \text{ or } n = p^2 + m^2 + k + k' - 2 \\ \Rightarrow 2(2n) = 4p^2 + 4k + 3 + 4m^2 + 4k' + 1 \text{ or } 2(2n) = 4p^2 + 4k - 3 + 4m^2 + 4k' - \\ 1 \text{ or } 2(2n) = 4p^2 + 4k + 7 + 4m^2 + 4k' + 1 \text{ or } 2(2n) = 4p^2 + 4k - 7 + 4m^2 + 4k' - 1 \\ \text{And } 2(2n) \text{ is always the sum of two primes!} \end{aligned}$$

Thus  $2n$  is always the sum of two primes,  $\forall n \in \mathbb{N}$ .

## Theorem

All the properties concerning integers and their relations with  $n$  primes that are true for the new definition of primes are true for the old definition of primes.

### Proof of the theorem

Let us suppose a property implying an integer  $x$  and  $m$  primes :

$$F(x, p_1, p_2, \dots, p_m) = 0$$

(for example : an even is always the sum of two primes  $2x = p + q$

or there is always a prime between the square of two consecutive integers

$$p = ux^2 + (1 - u)(x + 1)^2; 0 < u < 1)$$

available for the new definition of primes and false for the old one  $P(x, p_1, \dots, p_m = 0)$  and there exists  $x$  for which  $F(x, p_1', \dots, p_m') = b \neq 0; \forall p_i'$

(there exists an even  $2x$  which is equal to  $2x = p' + q' + 2b; b \neq 0$ , for all  $p', q'$  old primes ;

there exists  $x^2$ , for which there exists  $b \neq 0$  verifying  $p' - ux^2 - (1 - u)(x + 1)^2 = b, \forall p$  old prime).

$$F(x, p_1, \dots, p_m) = 0$$

$$a \neq 0; F(ax, ap_1, \dots, ap_m) = 0 = F(ax, q_1, \dots, q_m)$$

$$F(x, p_1', \dots, p_m') = b$$

$$F(ax, ap_1', \dots, ap_m') = b' = F(ax, q_1, \dots, q_m)$$

Example : Goldbach : True for new primes

$$2x - p_1 - p_2 = 0$$

Flase for old

$$2x - p_1' - p_2' = 2b$$

Thus

$$2ax - ap_1 - ap_2 = 0 = 2ax - q_1 - q_2$$

$$2ax - ap_1' - ap_2' = 2ab = a(p_1 + p_2 - p_1' - p_2') = q_1 + q_2 - a(p_1' + p_2'); \forall a \neq 0$$

Particularly  $a = q_1 + q_2$

$$2ab = (q_1 + q_2)(1 - (p_1' + p_2')) = a(1 - (p_1' + p_2'))$$

$$2b - 1 = -p_1' - p_2'$$

But  $p_1' + p_2'$  is even then it is impossible and it means that for all  $x$  there exists an old prime  $p$  for which  $b = 0$

Another example : De Polignac :

True for new primes

$$2x - p_1 + p_2 = 0$$

Flase for old

$$2x - p_1' + p_2' = 2b$$

Thus

$$2ax - ap_1 + ap_2 = 0 = 2ax - q_1 + q_2$$

$$2ax - ap_1' + ap_2' = 2ab = a(p_1 - p_2 - p_1' + p_2') = q_1 - q_2 - a(p_1' - p_2'); \forall a \neq 0$$

Particularly  $a = q_1 - q_2$

$$2ab = (q_1 - q_2)(1 - (p_1' - p_2')) = a(1 - (p_1' - p_2'))$$

$$2b - 1 = -p_1' + p_2'$$

But  $p_1' - p_2'$  is even then it is impossible and it means that for all  $x$  there exists an old prime  $p$  for which  $b = 0$

Another example : Legendre : True for new primes

$$p - ux^2 - (1 - u)(x + 1)^2 = 0$$

And false for old

$$p' - u''x^2 - (1 - u'')(x + 1)^2 = b$$

But for  $a \neq 0$

$$a^2p - u(ax)^2 - (1 - u)(a(1 + x))^2 = 0 = q - u'(ax)^2 - (1 - u')(a(x + 1))^2$$

$$a^2p' - u''(ax)^2 - (1 - u'')(a(x + 1))^2 = a^2b = a^2(p' - p) = a^2p' - q + a^2(u' - u'')(x^2 - (x + 1)^2)$$

But

$$-\frac{q}{a^2} = b - p' + (u - u')(x^2 - (x + 1)^2) \in \mathbb{Z}$$

$\forall a$ . Particlarly  $a = q$  and then  $q = 1$  : impossible ! It means that for all  $x$ , there exists  $p$  old prime for which  $b = 0$ .

## Conclusion

We deal with the concept of prime number and gave a new definition of primes. It allowed to prove the Goldbach and Legendre conjectures for the new definition of primes and to transopose the proof to the old one.

## Références

- [1] Alan Baker, Transcendental number theory *Cambridge University Press*, (1975).