The concept of prime number and the Legendre conjecture

Jamel Ghanouchi
Professor of Mathematics
RIME Department of Mathematics
6 Rue Khansa 2070 Marsa Tunisia

Keywords: Primes ; Legendre ; Conjecture ; Proof.

Abstract
In this paper, we generalize the concept of prime number and define new primes. It allows to apply the new concept to the Legendre conjecture and to prove it.

Introduction
The prime numbers are called primes because they are the bricks of the numbers: Each number \( n \) can be written as \( \prod \limits_j \left( P_j \right)^{n_j} \) where \( P_j \) 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 is allowed, 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 \( 2^4 = 16 \) and each number can be written according to \( 2 \) and its rational exponent instead of \( 2 \).
If we decide conventionally that each Fermat number is prime, and it is possible by the fact that they are coprime two by two, 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, the fifth Fermat number \( F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417 \) is prime, we can decide that it replaces \( 641 \) which becomes compound when \( 6700417 \) remains prime or \( 641 \) remains prime and it replaces \( 6700417 \) which becomes 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.

The Legendre’s conjecture
The Legendre conjecture states that there is always a prime number between the squares of two consecutive integers. So \( \exists p \mid n^2 < p \leq (n+1)^2 \; ; \forall n \in \mathbb{N} \) where \( p \) is prime. What does it become with our new definition? It remains true! Effectively:

Proof:
We have \( (2m)^2 = 4m^2 + 1 \leq (2m + 1)^2 \leq 4m^2 + 8m + 1 \leq (2m + 2)^2 \)
But we will prove now that (CD : common divisor)

SciPress applies the CC-BY 4.0 license to works we publish: https://creativecommons.org/licenses/by/4.0/
\[ CD(4m^2 + 1, 4k^2 + 1) = 5; m \neq k \]
\[ CD(4m^2 + 8m + 1, 4k^2 + 8k + 1) = 3; m \neq k \]
\[ GCD(4m^2 + 1, 4p^2 + 8p + 1) = 1 \]

It is true for the two first assertions and for the third, let us suppose \( d \) dividing both the two equations, we have:

\[
d \mid 4m^2 + 1;\ d \mid 4p^2 + 8p + 1 \text{ hence } \\
\Rightarrow d \mid 4p^2 + 8p + 1 - 4m^2 - 1 = d \mid p^2 - m^2 + 2p \\
\Rightarrow d \mid 4p^2 + 8p + 1 + 4m^2 + 1 = d \mid 2p^2 + 2m^2 + 4p + 1 \\
= 2(p + m)^2 - 2pm + 4p + 1 \\
\Rightarrow d \mid (p - m)(p + m)^2 + 2p(p + m) \\
\Rightarrow d \mid 2(p - m)(p + m)^2 - 2pm(p - m) + 4p(p - m) + p - m \\
\Rightarrow d \mid -2pm(p - m) + p - m = -2p^2m + 2pm^2 + p - m \\
\Rightarrow d \mid -4p^2m - 8pm - m + 8pm + m + 4pm^2 - p - p - m \\
\Rightarrow d \mid pm \Rightarrow d \mid p - m \Rightarrow d \mid m \Rightarrow d = 1 \\
\]

because \( d \) is odd. And

\[ m = 5(k + k') \pm 1 \]
\[ p = 5(k - k') \pm 1 \neq m \]
\[ \Rightarrow 4m^2 + 1 = 5(20k^2 + k'k)^2 \pm 8(k - k') + 1 \]
\[ 4p^2 + 1 = 5(20k^2 + k'k)^2 \pm 8(k - k') + 1 \]

And

\[ m = 3(k + k') + 2 \]
\[ p = 3(k - k') + 2 \neq m \]
\[ 4m^2 + 8m + 1 = (2m + 1)^2 - 3 = (6(k + k') + 6)^2 - 3 = 3w \]
\[ 4p^2 + 8p + 1 = (2p + 1)^2 - 3 = (6(k - k') + 6)^2 - 3 = 3w' \]

And \( 4m^2 + 1 \leq 4m^2 + 8m + 1 \) and can be taken primes simultaneously with our definition of the primes, for example, the first \( 4m^2 + 1 \) divisible by 5 is for \( m = 4 \) and then \( 4m^2 + 1 = 65 = 13.5 + 1 = 65.13^{-1} \) is no more prime and 65 is prime, the second is for \( m = 6 \) and then \( 4m^2 + 1 = 29.5 \Rightarrow 29 = 145.5^{-1} = 145.13.65^{-1} \) is no more prime and 145 is prime, etc… until infinity. By the same way, the first \( 4m^2 + 8m + 1 \) divisible by 3 is for \( m = 2 \) and then \( 4m^2 + 8m + 1 = 33 = 11.3 \Rightarrow 3 = 33.11^{-1} \) is no more prime and 33 is prime, etc… until infinity; but \( (2m)^2 \leq 4m^2 + 1 \leq (2m + 1)^2 \leq 4m^2 + 8m + 1 \leq (2m + 2)^2 \)

The Legendre conjecture is true for the new definition of the primes, we have proved it.

**Back to the traditional definition of primes**

Let now the Legendre conjecture, we have found that for the new definition

\[ (2n)^2 < p' < (2n + 1)^2 < q' < (2n + 2)^2 \]
Where \( p', q' \) are new primes. If Legendre conjecture is false for old and true for new primes. There exists \( x \), for which \((p' : \text{new prime}, p : \text{old prime}, q' : \text{new prime})\)

\[
p' - ux^2 - (1 - u)(1 + x)^2 = 0; 0 < u < 1
\]

\[
\exists x; p - u'x^2 - (1 - u')(1 + x)^2 = b; \forall p; 0 < u' < 1; b \neq 0
\]

\[
a \neq 0
\]

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

\[
a^2 p - u'(ax)^2 - (1 - u')(a(1 + x))^2 = a^2 b
\]

\[
= a^2 p - q' + (u'' - u')a^2(x^2 - (x + 1)^2)
\]

\[
\Rightarrow -\frac{q'}{a^2} = b - p' + (u'' - u')a^2(x^2 - (x + 1)^2) \in \mathbb{Z}; \forall a
\]

\[
a = a' \Rightarrow a' = 1
\]

Impossible ! It means that for all \( x \), there exists \( p \) old prime number, for which \( b = 0 \) and the conjecture is also true for the old definition !

**Conclusion**

We have generalized the definition of the primes and proved the Legendre conjecture for the generalization of the definition of primes, a reasoning which led to absurdity allowed to prove that this conjecture is true for the old definition too.