Contents

On Legendre's conjecture

March 26, 2014

msc 11A41
A.Garcés Doz
angel1056510@gmail.com

I thank God Almighty for giving me the knowledge, and the Lord Jesus Christ, our savior.

Abstract

Legendre's conjecture, stated by Adrien-Marie Legendre (1752-1833), says there is always a prime between n^2 and $(n+1)^2$. This conjecture is part of Landau's problems. In this paper a proof of this conjecture is presented, using the method of generating prime numbers between consecutive squares, and proving that for every pair of consecutive squares with $n \geqq 3$ may be generated at least one prime number that belongs to the interval $\left[n,(n+1)^2\right]$

Since in the intervals $\left[1,(1+1)^2\right]$ and $\left[2,(2+1)^2\right]$, there are prime numbers; 3, 5 and 7, respectively, then the Legendre conjecture is true for every pair of consecutive squares.

1 Prior Definitions.

In this section, elements and mathematical functions, which will be used to establish the algorithm generating prime numbers in the interval between two consecutive squares will be defined.

Definition 1.1. Primorial

For the nth prime number p_n the primorial $p_n\#$ is defined as the product of the first n primes: $p_n\# = \prod_{k=1}^{p_k} p_k$

Definition 1.2. Euler's totient function.

Euler's totient or phi function, $\varphi(n)$, is an arithmetic function that counts the totatives of n, that is, the positive integers less than or equal to n that are relatively prime to n.

Definition 1.3. Euler totient function of primorials.

$$\varphi(p_n\#) = \prod_{k=1}^{p_k}(p_k - 1)$$

Theorem 1.1. *Bertrand-Chebyshev theorem: states that for any integer $n > 3$, there always exists at least one prime number p with $n < p < 2n - 2$. A weaker but more elegant formulation is: for every $n > 1$ there is always at least one prime p such that $n < p < 2n$.*

Ramanujan, S. (1919). "A proof of Bertrand's postulate". Journal of the Indian Mathematical Society 11: 181–182

2 Algorithm prime number generator in the range $\left[a^2, (a-1)^2\right]$; through primorials and Bertrand-Chebyshev theorem.

Lemma 2.1. *If between two consecutive squares there is at least one prime number, with $a \geqq 3$, then this prime number can be generated by the following algorithm: being $p_n \geqq 3$; $p_y \in [a, 2a]$ (Bertrand-Chebyshev theorem); $p_n \leqq a < p_{n+1}$*

If $\exists\, p_z \in \left[a^2,\ (a-1)^2\right] \longrightarrow \exists \prod_p p_x$; $\prod_p p_x > a^2$ such that: $\left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor \not\equiv 0(mod\ \forall p_k)$ and $\left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor \equiv 1(mod\ 2)$; $p_k \in [2,\ p_n]$; then it holds:

$p_y \cdot \left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor + r(p_y) - a^2 = \prod_p p_x \cdot p_n\#$; *and* $p_y \cdot \left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor - \prod_p p_x \cdot p_n\# = a^2 - r(p_y) = p_z$; *where* $r(p_y)$ *is the residue of* p_y ; $p_z \in \left[a^2,\ (a-1)^2\right]$; $p_y \cdot \left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor - \prod_p p_x \cdot p_n\# = a^2 - r(p_y) \not\equiv 0(mod\ \forall p_k)$; *Since all* $n \leqq a^2$ *is prime or* $n \equiv 0(mod\ p_k)$

Proof. Inasmuch as $p_n\# \equiv 0(mod\ \forall p_k)$ and $\exists\, p_z \in \left[a^2,\ (a+1)^2\right]$; $r(p_y) < 2a$; $\forall p_z \in \left[a^2,\ (a-1)^2\right] \rightarrow p_z = a^2 - d$; $d \leqq 2a - 1 \rightarrow d \in \{r(p_y)\}$ □

If for all , $\forall \left\lfloor (\prod_p p_x \cdot p_n\# + a^2)/p_y \right\rfloor$ *and* $\forall p_y \in [a,\ 2a]$; was fulfilled

$$\left\{\left\lfloor(\prod_p p_x \cdot p_n\# + a^2)/p_y\right\rfloor \equiv 0(mod\ p_k)\right\} \to \left\{p_y \cdot \left\lfloor(\prod_p p_x \cdot p_n\# + a^2)/p_y\right\rfloor + r(p_y) - a^2 = \prod_p p_x \cdot p_n\#\right\} \to p_y \cdot \left\lfloor(\prod_p p_x \cdot p_n\# + a^2)/p_y\right\rfloor - \prod_p p_x \cdot p_n\# = a^2 - r(p_y)$$

And $a^2 - r(p_y) \equiv 0(mod\ p_k)$ But this last statement is contrary to the starting, ie: $\exists\, p_z \in \left[a^2,\ (a-1)^2\right]$

So, by contradiction, Lemma 2.1 is proved.

2.1 Examples of prime numbers generation between consecutive squares.

Example 2.1. $p_n\# = p_2\# = 2 \cdot 3 = 6$; $3 \leqq a < p_{n+1}$; $a = 3$; $p_y \in [3,\ 2 \cdot 3]$; $p_y = 5$; $\prod_p p_x = 2^2 \cdot 17 > 3^2$

$$\left\{\left\lfloor(2^2 \cdot 17 \cdot p_2\# + 3^2)/5\right\rfloor = 83\ (prime\ number)\right\} \to \left\lfloor(2^2 \cdot 17 \cdot p_2\# + 3^2)/5\right\rfloor \cdot 5 - 2^2 \cdot 17 \cdot p_2\# = 7\ (prime\ number)\ ;\ 7 \in \left[3^2, (3-1)^2\right]$$

Example 2.2. $p_n\# = p_2\# = 2 \cdot 3 = 6$; $3 \leqq a < p_{n+1}$; $a = 4$; $p_y \in [4,\ 4 \cdot 2]$; $p_y = 5$; $\prod_p p_x = 37 > 4^2$ $(prime\ number)$

$$\left\{\left\lfloor(37 \cdot p_2\# + 4^2)/5\right\rfloor = 47\ (prime\ \ number)\right\} \to \left\lfloor(37 \cdot p_2\# + 4^2)/5\right\rfloor \cdot 5 - 37 \cdot p_2\# = 13\ (prime\ number)\ ;\ 13 \in \left[4^2,\ (4-1)^2\right]$$

Example 2.3. $p_n\# = p_3\# = 2 \cdot 3 \cdot 5 = 30$; $5 \leqq a < p_{n+1}$; $a = 5$; $p_y \in [5,\ 5 \cdot 2]$; $p_y = 7$; $\prod_p p_x = 29 > 5^2$ $(prime\ number)$

$$\left\{\left\lfloor(29 \cdot p_3\# + 5^2)/7\right\rfloor = 127\ (prime\ \ number)\right\} \to \left\lfloor(29 \cdot p_3\# + 4^2)/7\right\rfloor \cdot 7 - 29 \cdot p_3\# = 19\ (prime\ number)\ ;\ 19 \in \left[5^2,\ (5-1)^2\right]$$

Example 2.4. $p_n\# = p_4\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$; $7 \leqq a < p_{n+1}$; $a = 9$; $p_y \in [7,\ 7 \cdot 2]$; $p_y = 11$; $\prod_p p_x = 251 > 7^2$ $(prime\ number)$

$$\left\{\left\lfloor(251 \cdot p_4\# + 9^2)/11\right\rfloor = 4799\ (prime\ number)\right\} \to \left\lfloor(251 \cdot p_4\# + 9^2)/11\right\rfloor \cdot 11 - 251 \cdot p_4\# = 79\ (prime\ number)\ ;\ 79 \in \left[9^2,\ (9-1)^2\right]$$

3 The existence of at least, a prime number between consecutive squares, for every interval $\left[a^2,\ (a-1)^2\right]$

By Bertrand-Chebyshev's theorem the following lemma is derived:

Lemma 3.1. *Be any primorial. And let the Euler functions* $\varphi_{\#}(p_n\# + 2a)$; $\varphi_{\#}(p_n\# + a)$; $p_n \leqq a < p_{n+1}$

Symbolizing $\varphi_{\#}(p_n\# + 2a)$ *and* $\varphi_{\#}(p_n\# + a)$; *the functions that count the number of relatively prime integers; with respect to a given primorial, and in the intervals* $[1,\ p_n\# + 2a]$; $[1,\ p_n\# + a]$.

By Bertrand-Chebyshev's theorem: in the interval $[a,\ 2a]$ *there, at a minimum, a prime number. So is fulfilled:* $\varphi_{\#}(p_n\# + 2a) - \varphi_{\#}(p_n\# + a) \geqq 1$

Proof. Any number that is prime relative to $\varphi(p_n\#)$; and that belongs to the interval $z \in [p_n\# + 2a,\ p_n\# + a]$; satisfies: $z - p_n\# = p$; $p \in [a,\ 2a]$

In fact: $\left\{\ (z,\ p_n\#) = 1 \rightarrow z \not\equiv 0(mod\ \forall p_k)\right\}$; $p_k \leqq p_n$ $\left\{\ (z,\ p_n\#) = 1 \rightarrow z \not\equiv 0(mod\ \forall p_k)\right\} \rightarrow \forall z \in [p_n\# + 2a,\ p_n\# + a]$ $z - p_n\# = p$; $p \in [a,\ 2a]$

Therefore, Lemma 3.1 is proved and the equivalence with Bertrand-Chebyshev's theorem:

$\left\{\forall\ [a,\ 2a]\ \exists\, p \in [a,\ 2a]\right\} \equiv \left\{\forall\ a\ ;\ p_n \leqq a < p_{n+1}\ ;\ \exists\, z\ (z,\ p_n\#) = 1\ ;\ z \in [p_n\# + 2a,\ p_n\# + a]\ ;\ z - p_n\# = p\ ;\ p \in [a,\ 2a]\right\}$

□

Example 3.1. $\{\ \varphi_{\#}(p_3\# + 2\cdot 6) - \varphi_{\#}(p_3\# + 6)\} = \{37,\ 41\}$; $\varphi(p_3\#) = \varphi(2\cdot 3\cdot 5) = \varphi(30)$

$\{37,\ 41\} - p_3\# = \{7,\ 11\}$; $7 = p \in [6,\ 2\cdot 6]$; $11 = p \in [6,\ 2\cdot 6]$; $p_3 \leqq 6 < p_{3+1}$; $\varphi_{\#}(p_3\# + 2\cdot 6) - \varphi_{\#}(p_3\# + 6) \geqq 1$

3.0.1 The floor function and Lemma 3.1

Let the floor function $\lfloor x \rfloor$. One of its properties to the sum of two integers, it is: $\left\lfloor \frac{x_1+x_2}{n} \right\rfloor = \left\lfloor \frac{x_1}{n} \right\rfloor + \left\lfloor \frac{x_2}{n} \right\rfloor$; $n, x_1, x_2 \in \{N\}$; $x_1 \geqq x_2$

Likewise is fulfilled: $\left\lfloor \frac{x_1-x_2}{n} \right\rfloor = \left\lfloor \frac{x_1}{n} \right\rfloor - \left\lfloor \frac{x_2}{n} \right\rfloor$; $n, x_1, x_2 \in \{N\}$

Equivalence between Bertrand-Chebyshev's theorem and Lemma 3.1, together with the above properties of the floor function, imply the following result:

$$\varphi_{\#}(p_n\#+2a) - \varphi_{\#}(p_n\#+a) = \left\lfloor p_n\# \cdot \prod_{k=1}^{p_k}(1-\frac{1}{p_k}) \right\rfloor + \left\lfloor 2a \cdot \prod_{k=1}^{p_k}(1-\frac{1}{p_k}) \right\rfloor - \left\lfloor p_n\# \cdot \prod_{k=1}^{p_k}(1-\frac{1}{p_k}) \right\rfloor - \left\lfloor a \cdot \prod_{k=1}^{p_k}(1-\frac{1}{p_k}) \right\rfloor \geqq 1$$

$$\varphi_{\#}(p_n\#+2a)-\varphi_{\#}(p_n\#+a)=\left\lfloor 2a\cdot\prod_{k=1}^{p_k}(1-\frac{1}{p_k})\right\rfloor-\left\lfloor a\cdot\prod_{k=1}^{p_k}(1-\frac{1}{p_k})\right\rfloor \geqq 1$$

The same lower bound is obtained for intervals between consecutive squares. So that the interval is equal in amount to the integer which includes; to the interval $[a,\ 2a]$; the interval between consecutive squares for the same a , be modified to obtain the same amount; ie:

$\varphi_{\#}(p_n\#+a^2)-\varphi_{\#}(p_n\#+(a-1)^2+a-1) \to \left[a^2,\ (a-1)^2+a-1\right]$; $(a^2-(a-1)^2-a+1)=a=(2a-a)$

Therefore, we have: $\left\{\varphi_{\#}(p_n\#+a^2)-\varphi_{\#}(p_n\#+(a-1)^2+a-1) \equiv \varphi_{\#}(p_n\#+2a)-\varphi_{\#}(p_n\#+a)\right\} \to \varphi_{\#}(p_n\#+a^2)-\varphi_{\#}(p_n\#+(a-1)^2+a-1) \geqq 1$

Therefore: $\forall a\, \exists p_z \in \left[a^2,\ (a-1)^2+a-1\right]$, as between consecutive squares $(1^2,\ 2^2)$; $(2^2,\ 3^2)$; there are prime number; 3, 5 and 7, respectively, then the Legendre conjecture is true for every pair of consecutive squares.

3.0.2 Condition should meet algorithm (lemma 2.1), generating prime numbers between consecutive squares, to the inexistence of at least one prime number between consecutive squares.

For the algorithm derived from Lemma 2.1, there is a particular case of this algorithm given by: $p_n \geqq 3$; $p_n \leqq a < p_{n+1}$; $p_y \in [a,\ 2a]$; $p_k \leqq p_n$

$\prod_p p_x > a^2$; $\prod_p p_x = 2^n\cdot p_x$; $p_x > a^2$; $(p_x,\ p_n\#)=1$. By Lemma 2.1 we have that if is true: $\left\lfloor(2^n\cdot p_x\cdot p_n\#+a^2)/p_y\right\rfloor \not\equiv 0(mod\ \forall p_k)$; and $\left\lfloor(2^n\cdot p_x\cdot p_n\#+a^2)/p_y\right\rfloor \equiv 1(mod\ 2)$; then: $p_y\cdot\left\lfloor(2^n\cdot p_x\cdot p_n\#)/p_y\right\rfloor - 2^n\cdot p_x\cdot p_n\# = p$; $p\in\left[a,\ (a-1)^2\right]$

Condition must meet the algorithm derived from lemma 2.1, so that there is not a prime number between two consecutive squares:

Only if: $\left\{\forall\, 2^n,\ p_x \left\lfloor(2^n\cdot p_x\cdot p_n\#+a^2)/p_y\right\rfloor \equiv 0(mod\ p_k)\right\} \to \left\{\forall\, p_y\cdot\left\lfloor(2^n\cdot p_x\cdot p_n\#)/p_y\right\rfloor - 2^n\cdot p_x\cdot p_n\# \neq p\right\} \to \nexists\, p_z \in \left[a,\ (a-1)^2\right]$

Definition 3.1. If the previous condition is fulfilled for all $2^n\cdot p_x$; then all prime number p_x greater than a^2 ; could be represented by:

Definition. $\left\lfloor(2^n\cdot p_x\cdot p_n\#+a^2)/p_y\right\rfloor = Z_n\cdot p_k$; $\left\{Z_n\cdot p_k\cdot p_y+r(p_y)=2^n\cdot p_x\cdot p_n\#+a^2\right\} \to a^2-r(p_y)\equiv 0(mod\, p_k)$; $p_x=\frac{Z_{n2}\cdot p_k}{2^n\cdot p_n\#}$

Forming the product: $\prod_p p_x = \prod_p \frac{Z_{n2}\cdot p_k}{2^n\cdot p_n\#}$, If the condition is fulfilled, given by Definition 3.1, then you would have to: $\prod_p \frac{Z_{n2}\cdot p_k}{2^n\cdot p_n\#}+1=\prod_p \frac{Z_{n3}\cdot p_k}{2^n\cdot p_n\#}$

But this last equality, it is obviously impossible. So will exist infinite solutions which fulfill: $\left\lfloor (2^n \cdot p_x \cdot p_n\# + a^2)/p_y \right\rfloor \not\equiv 0(mod\ \forall p_k)$; and $\lfloor (2^n \cdot p_x \cdot p_n\# + a^2)/p_y \rfloor \equiv 1(mod\ 2)$; $then:$ $p_y \cdot \left\lfloor (2^n \cdot p_x \cdot p_n\#)/p_y \right\rfloor - 2^n \cdot p_x \cdot p_n\# = p$; $p \in \left[a,\ (a-1)^2\right]$

And finally we have that, between any pair of consecutive squares, there is at least one prime number.

References

[1] Dusart, Pierre, Autour de la fonction qui compte le nombre de nombres premiers, http://www.unilim.fr/laco/theses/1998/T1998_01.pdf, 1998

[2] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th ed., Oxford University Press, p. 494.,2008

[3] Nagura, J, On the interval containing at least one prime number, Proceedings of the Japan Academy, Series A 28,pp. 177–181, 1952

[4] Ramanujan, S, A proof of Bertrand's postulate, Journal of the Indian Mathematical Society 11: 181–182, 1919