Proof of Legendre's conjecture

Kouji Takaki

February 16th, 2021
Abstract
By a consideration of this research, since we found that at least one prime number exists between \( n^2 \) and \( n(n + 1) \) when \( n \geq 3 \), we have obtained a conclusion that Legendre's conjecture is true.

Contents

1. Introduction
   This is the conjecture that there is a prime number always between \( n^2 \) and \( (n + 1)^2 \) for arbitrary positive integer \( n \). It was set up by the French mathematician Adrien-Marie Legendre. (Quoted from Wikipedia)

2. Proof
   Let \( n \) and \( p \) be positive integers. If Legendre's conjecture is true, there is at least one prime number \( p \) satisfying the following inequalities.
   \[
   n^2 < p < (n + 1)^2 \quad (n \geq 1) \quad \ldots (1)
   \]
   I. When \( n < 3 \)
   The inequalities (1) hold when \( n = 1 \) since there are prime numbers 2 and 3 between 1 and 4. In the same way, the inequalities hold when \( n = 2 \) since there are prime numbers 5 and 7.

   II. When \( n \geq 3 \)
   Suppose that \( p \) satisfies the following inequalities,
   \[
   n^2 < p < n(n + 1) \quad \ldots (2)
   \]
   Let \( q \) be a positive integer. If any \( p \) is a composite number and has prime factors, the largest possible factor of \( p \) in the range of the inequalities (2) is \( n(n + 1)/2 - 1 \) and \( p \) must be divided by \( q \) from \( n + 2 \) to \( (n^2 + n - 2)/2 \) since \( n \) and \( n + 1 \) cannot divide \( p \) and the product of two factors between 2 and \( n - 1 \) cannot be \( p \).
\[
\begin{align*}
n + 1 < q < n(n + 1)/2 \ldots (3)
\end{align*}
\]
We will consider the case where \( p \) is divisible by \( q \) satisfying the inequalities above. Let \( r \) be a positive integer and the quotient when \( p \) is divided. \( r \) must be satisfied the following inequalities.

\[
1 < r < n \ldots (4)
\]
If it is assumed that \( p \) are all composite numbers in the range of the inequalities (2), \( p \) must be divided by \( q \) in the inequalities (3). When \( p \) is a composite number, one \( p \) corresponds to some combinations of \( q \) and \( r \). \( q \) has a one-to-one correspondence with \( p \) since the minimum number of \( q \), \( n + 2 \) is greater than the number of \( p \) satisfying the inequalities (2), \( n - 1 \) and \( r \) has a one-to-many correspondence with \( p \).

We need to apply a rule to select the relations from \( p \) to \( r \) and consider the case when \( n = 9 \).

When \( p = 82 \), \((q, r) = (41, 2)\)
When \( p = 84 \), \((q, r) = (42, 2), (28, 3), (21, 4), (14, 6), (12, 7)\)
When \( p = 85 \), \((q, r) = (17, 5)\)
When \( p = 86 \), \((q, r) = (43, 2)\)
When \( p = 87 \), \((q, r) = (29, 3)\)
When \( p = 88 \), \((q, r) = (44, 2), (22, 4), (11, 8)\)
Define \([p, r]\) as a relation from \( p \) to \( r \). We will select the relations between \( p \) and \( r \) so that there are all one-to-one correspondences. At first the relations are selected by \( r \) which are multiples of 2 for each \( p \). \([82,2]\) is sorted out when \( p = 82 \). Then \([84,4]\) is sorted out since \( r = 2 \) has been selected. When \( p = 86 \), there is one combination \((q, r) = (43,2)\) and \( r = 2 \) has been taken from. In this case, we consider to use the factor 2 of 6 and think that there is a relation \([86,6]\). Then \([88,8]\) is sorted out. Next, we select the relation by 3 multiples \( r \) and \([87,3]\) is sorted out.

When \( r \) is a composite number we skip the number since we have already taken from the relations by a multiple of the prime factor of \( r \). Next, we select the relations by multiples of prime numbers greater than or equal to 5.

Let \( a(n, r) \) and \( b(n, r) \) be integers and \( a(n, r) \) be the number of \( r \) multiples in the range of the inequalities (2) and \( b(n, r) \) be that in the range of the inequalities (4). The following inequalities hold:

\[
a(n, r) \leq b(n, r) + 1
\]
When \( n = 8 \), \( a(8,5) = 2 \), \( b(8,5) = 1 \) and \( a(8,5) > b(8,5) \) hold.

When \( p = 65 \), \( (q,r) = (13,5) \)
When \( p = 66 \), \( (q,r) = (33,2),(22,3),(11,6) \)
When \( p = 68 \), \( (q,r) = (34,2),(17,4) \)
When \( p = 69 \), \( (q,r) = (23,3) \)
When \( p = 70 \), \( (q,r) = (35,2),(14,5),(10,7) \)

In this case, \([65,5]\) can be selected since \([70,6]\) has already sorted out when \( r = 2 \).

Let \( s \) be a prime number less than \( r \). In the case of \( a(n,r) > b(n,r) \), the actual increase in the number of relations between \( p \) and \( r \) is less than or equal to \( b(n,r) \) at the time of making the selection because one of the \( s \) adjacent multiples of \( r \) is a multiple of \( s \) and the relations have already been selected by \( s \) multiples. The value of \( s \) can be considered 2 or 3 since \( a(n,s) = b(n,s) \) holds as follows.

Let \( m \) be an integer.

\[ a(2m,2) = \text{floor}((2m)^2) - \text{floor}(2m) = m - 1 \]
\[ b(2m,2) = \text{floor}(2m) = m - 1 \]

\[ a(2m+1,2) = \text{floor}(((2m+1)^2) - (2m+1) = m \]
\[ b(2m+1,2) = \text{floor}(2m+1) = m \]

Therefore, \( a(n,2) = b(n,2) \) holds when \( n \geq 3 \).

\[ a(3m,3) = \text{floor}(((3m)^2) - (3m) = m - 1 \]
\[ b(3m,3) = \text{floor}(3m) = m - 1 \]

\[ a(3m+1,3) = \text{floor}(((3m+1)^2) - (3m+1) = m \]
\[ b(3m+1,3) = \text{floor}(3m+1) = m \]

\[ a(3m+2,3) = \text{floor}(((3m+2)^2) - (3m+2) = m \]
\[ b(3m+2,3) = \text{floor}(3m+2) = m \]

Therefore, \( a(n,3) = b(n,3) \) holds when \( n \geq 3 \).

From the above, the prime number \( r \) with \( a(n,r) > b(n,r) \) satisfies \( r \geq 5 \).

We will consider the case when \( n = 17 \).

When \( n = 17 \), \( a(17,5) = 4 \), \( b(17,5) = 3 \) and \( a(17,5) > b(17,5) \) hold.
When $p = 290$, $(q, r) = (145, 2), (58, 5), (29, 10)$
When $p = 291$, $(q, r) = (97, 3)$
When $p = 292$, $(q, r) = (146, 2), (73, 4)$
When $p = 294$, $(q, r) = (147, 2), (98, 3), (49, 6), (42, 7), (21, 14)$
When $p = 295$, $(q, r) = (59, 5)$
When $p = 296$, $(q, r) = (148, 2), (74, 4), (37, 8)$
When $p = 297$, $(q, r) = (99, 3), (33, 9), (27, 11)$
When $p = 298$, $(q, r) = (149, 2)$
When $p = 299$, $(q, r) = (23, 13)$
When $p = 300$, $(q, r) = (150, 2), (100, 3), (75, 4), (60, 5), (50, 6), (30, 10), (25, 12), (20, 15)$
When $p = 301$, $(q, r) = (43, 7)$
When $p = 302$, $(q, r) = (151, 2)$
When $p = 303$, $(q, r) = (101, 3)$
When $p = 304$, $(q, r) = (152, 2), (76, 4), (38, 8), (19, 16)$
When $p = 305$, $(q, r) = (61, 5)$

In the beginning, we select the relations $[290, 2], [292, 4], [294, 6], [296, 8], [298, 10], [300, 12], [302, 14]$ and $[304, 16]$ when $r = 2$. Then we select $[291, 3], [297, 9]$ and $[303, 15]$ when $r = 3$. When $r = 5$, we should select the relations in the case of $p = 295$ and $p = 305$. However, there is only 5 for $r$ which corresponds to $p$ since 10 and 15 have already been taken from. With this method, we cannot select the one-to-one relations between $p$ and $r$.

And so we will change the rules as follows. We select relations by multiples of the prime numbers in descending order. When $a(n, r) > b(n, r)$ holds, a composite number $p$ can be skipped since one of the relations can later be selected by multiples of a prime number less than $r$. When $n = 17$, the relations are selected as follows.

When $r = 13$, $[299, 13]$
When $r = 11$, $[297, 11]$
When $r = 7$, $[294, 7], [301, 14]$
When $r = 5$, $[290, 5], [295, 10], [305, 15]$
When $r = 3$, $[291, 3], [300, 6], [303, 9]$
When $r = 2$, $[292, 2], [296, 4], [298, 8], [302, 12], [304, 16]$

The minimum $n$ when there exists $r$ with $a(n, r) > b(n, r)$ is 7 and the minimum $r$ where $a(n, r) > b(n, r)$ holds is 5. Therefore, if we select the relations this way, one-to-one correspondence with all composite numbers $p$ can be set for $r$, for all $n$ in the range of $n \geq 3$. 

4
However, it becomes a contradiction since the number of \( p \) in the inequalities (2), \( n - 1 \) is greater than the number of \( r \) in the inequalities (4), \( n - 2 \) and it does not become a one-to-one correspondence between \( p \) and \( r \). Therefore, the assumption that \( p \) are all composite numbers in the range is false and there is at least one prime number in the range of the inequalities (2) when \( n \geq 3 \). From the above I and II, it is proved that Legendre’s conjecture is true. (Q.E.D.)

3. Complement
Oppermann’s conjecture states that, for every integer \( x > 1 \), there is at least one prime number between \( x(x - 1) \) and \( x^2 \), and at least another prime between \( x^2 \) and \( x(x + 1) \). It is named after Danish mathematician Ludvig Oppermann, who announced it in an unpublished lecture in March 1877. (Quoted from Wikipedia)

\[
x(x + 1) < p < x(x + 2)
\]

Considering an integer \( p \) satisfying these inequalities, because \( a(x, r) \leq b(x, r) + 1 \) holds and the minimum \( x \) where there exists \( r \) with \( a(x, r) > b(x, r) \) is 9 and the minimum \( r \) where \( a(x, r) > b(x, r) \) holds is 7, we found that at least one prime number between \( x(x + 1) \) and \( (x + 1)^2 \) when \( x \geq 3 \) in the same way as this proof. Therefore, we conclude that Oppermann’s conjecture is true.

4. Acknowledgement
We would like to thank my family members who sustained a research environment and mathematicians who reviewed these studies.

5. References
Hiroyuki Kojima, "The world is made of prime numbers" Kodakawa Shoten, (2017)
Fumio Sairaiji·Kenichi Shimizu, "A story that prime is playing" Kodansha, (2015)
The Free Encyclopedia Wikipedia