A Method for Solving Legendre's Conjecture

Hashem Sazegar

Department of Mathematics, Azad University of Mashhad, Mashhad, Iran

E-mail: h.sazegar@gmail.com

Received: September 29, 2011 Accepted: October 31, 2011 Published: February 1, 2012

doi:10.5539/jmr.v4n1p121 URL: http://dx.doi.org/10.5539/jmr.v4n1p121

Abstract

Legendre's conjecture states that there is a prime number between n^2 and $(n + 1)^2$ for every positive integer n. In this paper we prove that every composite number between n^2 and $(n + 1)^2$ can be written $u^2 - v^2$ or $u^2 - v^2 + u - v$ that $u > 0$ and $v \geq 0$. Using these result as well as induction and residues $(modq)$ we prove Legendre's conjecture.

Keywords: Bertrand-Chebyshev theorem, Landau's problems, Goldbach's conjecture, Twin prime, Ramanujan proof

1. Introduction

Bertrand's postulate state for every positive integer n, there is always at least one prime p, such that $n < p < 2n$. This was first proved by Chebyshev in 1850 which is why postulate is also called the Bertrand-chebyshev theorem. Ramanujan gave a simple proof by using the properties of gamma function, which resulted in concept of Ramunajan primes (Ramanujan, 1919, p. 181-182). In 1932 Erdos published a simple proof using the Chebyshev's function and properties of binomial coefficient (Erdos, 1932, p. 194-198). Legendre's conjecture states that there is a prime between n^2 and $(n + 1)^2$ for every positive integer n, which is one of the four Landau's problems. The rest of these four basic problems are:

(i) Twin prime conjecture: there are infinitely many primes p such that $p + 2$ is a prime.

(ii) Goldbach's conjecture: every even integer $n > 2$ can be written as the sum of two primes.

(iii) Are there infinitely many primes p such that $p - 1$ is a perfect square?

problems *(i),(ii),(iii)* are open till date.

In this paper we state one proof for Legendre's conjecture.

Theorem *There is at least a prime between n^2 and $(n + 1)^2$.*

We prove it by induction that if there is at least a prime between all squares less than $(x-1)^2$, then there is a prime between $(x - 1)^2$ and x^2, that x is a large positive integer. Assume that this is not hold, i.e all numbers in interval $(x - 1)^2$ and x^2 are composite and we reach to a contradiction.

To proceed to this proof, firstly we use the following Lemmas and Definitions.

2. Lemmas and Definitions

In this section, we present several lemmas and definitions which are used in the proof of our main theorem. In this article we prove that every composite numbers, $x^2 - j$ that $1 \leq j \leq 2x - 2$, between $(x - 1)^2$ and x^2 can be written $u^2 - v^2$ or $u^2 - v^2 + u - v = (u + 1/2)^2 - (v + 1/2)^2 = u_1^2 - v_1^2$ that $u > 0$ and $v \geq 0$ and $u - v = u_1 - v_1 = q$, where q is a prime number.

Lemma 2.1 *All prime factors q where $2 \leq q \leq x$ are Appeared in numbers between $(x - 1)^2$ and x^2.*

Proof: According to Algorithm division, $x^2 - j = qs + f$ in which $0 \leq f \leq q - 1$, $1 \leq j \leq x - 1$ and $2 \leq q \leq x$, then $1 \leq j + f \leq 2x - 2$.

Lemma 2.2 *Every composite number between $(x - 1)^2$ and x^2 can be written to $u^2 - v^2$ or $u^2 - v^2 + u - v$ where $u > 0$ and $v \geq 0$.*

Proof: For simplicity we call the composite numbers $x^2 - j$ as T hereafter. If T is not prime, then:

$$T = qf,\ (q < x)$$

q is a prime number and f is a positive integer. Later we show that every composite number between $(x - 1)^2$ and x^2 has a prime factor like q so that $q < x$.

$$f = q + w$$

If w is an even number so $w = 2v$ otherwise $w = 2v + 1$, so:

$$T = q^2 + 2qv$$

Or

$$T = q^2 + 2qv + q$$

Substituting q by $u - v$, we will have

$$q = u - v$$

So

$$T = u^2 - v^2$$

Or

$$T = u^2 - v^2 + u - v$$

Definition 1 If $T = u^2 - v^2$ so $T = q(u + v)$, we assume that $u + v = 2x - q + A$, A is an integer.

Definition 2 If $T = u^2 - v^2 + u - v = (u - v)(u + v + 1) = u_1^2 - v_1^2$, in which, $q = (u + 1/2) - (v + 1/2) = u_1 - v_1$ so $T = q(u_1 + v_1)$, we assume that $u_1 + v_1 = 2x - q + A$, A is an integer, $u_1 = u + 1/2$ and $v_1 = v + 1/2$.

Lemma 2.3 If $(x - m)^2 - j = q(u' + v') = q(2(x - m) - q + A')$ and $(x - m - 1)^2 - j_2 = p$, where p is prime, A' is an integer and $m > 1$ should be defined earlier in the paper.

Notice: According to the hypothesis of induction there is at least a prime between all squares less than $(x - 1)^2$.
If $q = 1$, then

$$-j_1 + j_2 - A' + p = 0,\ 1 \le j_1 \le 2x - 2m - 2 \text{ and } 1 \le j_2 \le 2x - 2m - 4$$

Proof: we consider two equation as

$$(x - m)^2 - j = q(u' + v') = q(2(x - m) - q + A') \text{ and } (x - m - 1)^2 - j_2 = p$$

So we have

$$(2x - 2m - 1) - j + j_2 = q(2x - 2m - q + A') - p$$

Then

$$2x(q - 1) - (q^2 - 1) + A'(q - 1) - 2m(q - 1) = -j + j_2 - A' + p$$

For $(x - m)^2 - j$ to be the prime number in a specific $j = j_1$, $1 \le j_1 \le 2x - 2m - 2$, q should be equal to 1.
So

$$-j_1 + j_2 - A' + p = 0$$

Lemma 2.4 *Assume that $x^2 - j' = q(2x - q - A_1)$ and $(x - m - 1)^2 - j_2 = p$, in which p is prime, and also $1 \le j' \le 2x - 2$, A_1 is an integer, then:*

$$2(m + 1)x - (m + 1)^2 - j' + j_2 = 2xq - q^2 + A_1 q - p$$

Lemma 2.5 *If l to be the number of $2 \le q < x$ are in $x^2 - j' = tq$ that $1 \le j' \le 2x - 2$ so $l < x - 1$ or $l < \frac{x-1}{q}$, for all $3 \le q < x$.*

Proof: If $q = 2$, we put $j' = i + 2l$ $(i \ge l)$, so $i + 2l \le 2x - 2$, then $l < x - 1$, but if $q \ge 3$, we put $j' = i + 2ql$ $(i \ge l)$, so $i + 2ql \le 2x - 2$, then $l < \frac{x-1}{q}$, in this case l is the number of $q \ge 3$ that $x^2 - j' = tq$ is odd.

Lemma 2.6 *If f to be the number of $p > x$ are in $x^2 - j' = t_1 p$ that these numbers are odd and $1 \le j' \le 2x - 2$.*
So

$$f \le \frac{2x - 2}{9} \cdot \frac{1}{2}$$

Or

$$f \le \frac{x - 1}{3} \cdot \frac{1 - 1/9}{5}$$

Or

$$f \le \frac{x - 1}{3} \cdot \frac{1 - 1/9 - 1/15}{7}$$

.

.

.

we continue this method to reach $1 - 1/9 - 1/15 - ... = 0$.

Proof: If $p > x$ and $x^2 - j' = t_1 p$ to be odd, since $1 \leq j' \leq 2x - 2$, so $(x-1)^2/q \leq p \leq x^2/q$, in which $3 \leq q < x$. Since the distance of between two primes should be at least 2, so $(x-1)^2/q - 2 \leq p - 2 = p' \leq x^2/q - 2$, p' is prime number, but $(x-1)^2/q - 4 \leq p - 4 = w \leq x^2/q - 4$, w is not prime.

If $q = 3$, the number of such p is:

$$f \leq \frac{2x-2}{6} \cdot \frac{2}{3} \cdot \frac{1}{2}$$

but since $p > x$, only one $p > x$ could be in $x^2 - j' = t_1 p$, so for $q = 5$, $f \leq \frac{x-1}{3} \cdot \frac{1-1/9}{5}$. For $q = 7$, $f \leq \frac{x-1}{3} \cdot \frac{1-1/9-1/15}{7}$, we continue this method to reach, $1 - 1/9 - 1/15 - ... = 0$.

3. The Proof of Main Theorem

Theorem T*here is at least a prime between* $(x-1)^2$ *and* x^2.

Proof: Let we have at least a prime between all squares less than $(x-1)^2$. By induction, we prove that, we have a prime between $(x-1)^2$ and x^2. Assume that this is not true, so we can write $x^2 - j' = lq$, i.e all numbers in interval $(x-1)^2$ and x^2 are not primes. Since $1 \leq j' \leq 2x-2$ so according to (Hardy & Wright, 1964) there is a prime factor like q that for any composite number in interval$(x-1)^2$ and x^2. $q \leq \sqrt{x^2-1} < x$.

Note: If a number in interval $(x-1)^2$ and x^2 like T is not prime so T has a prime factor like q that $q \leq \sqrt{x^2-1} < x$. In this section we assume that $j'' = -j_2 + h$ that $0 \leq h < q$ and $1 \leq j'' \leq 2x - 2$, notice that for each number $x^2 - j'$, there is a corresponding divisor q. Now we start to prove main theorem: concluding from lemma 2.3, $-j_1 + j_2 - A' + p = 0$, we can rewrite below equations:

$$-A' + p - 2(m+1)x + (m+1)^2 = -b + q_j t_j + j_1 + j_2$$

$$-A' + p - 2(m+1)x + (m+1)^2 = -(b+1) + q_v t_v + j_1 + j_2$$

$$.$$

$$.$$

$$.$$

$$-A' + p - 2(m+1)x + (m+1)^2 = 0 + q_i t_1 + j_1 + j_2$$

$$-A' + p - 2(m+1)x + (m+1)^2 = 1 + q_f t_2 + j_1 + j_2$$

$$-A' + p - 2(m+1)x + (m+1)^2 = 2 + q_s t_3 + j_1 + j_2$$

$$.$$

$$.$$

$$.$$

$$-A' + p - 2(m+1)x + (m+1)^2 = a + q_u t_a + j_1 + j_2$$

a, b will be determined later.

By substituting the above equations into $-j_1 + j_2 - A' + p = 0$, we have:

$$-j_2 + b - (j_2 + 2(m+1)x - (m+1)^2) \equiv 0 \pmod{q_j}$$

$$-j_2 + (b+1) - (j_2 + 2(m+1)x - (m+1)^2) \equiv 0 \pmod{q_v}$$

$$.$$

$$.$$

$$.$$

$$-j_2 - a - (j_2 + 2(m+1)x - (m+1)^2) \equiv 0 \pmod{q_u}$$

We assume that $j'' = -j_2 + h$, in which $-b \leq h \leq a$.
So

$$j'' - (j_2 + 2(m+1)x - (m+1)^2) \equiv 0 \pmod{q} \text{ that } 2 \leq q < x$$

According to lemma 2.4, if we substitute the above results into equation:

$$2(m+1)x-(m+1)^2-j'+j_2=2xq-q^2+A_1q-p$$

Then

$$j''-j'\equiv 2xq-q^2+A_1q-p \pmod q \text{ that } 2\le q<x$$

But we should have $j'\neq j''+qt$, otherwise $q\mid p$, and this is a contradiction unless $q=1$, but we determine m such that $p>x$, so $q\neq p$.

We mention again that $j'\not\equiv j'' \pmod q$ and $j'=1,2,...,2x-2$ sincej_2 is a number between $(x-m-2)^2$ and $(x-m-1)^2$, then, $1\le j_2\le 2x-2m-4$.

If x is even, we put $m=\frac{x}{2}$;

If x is odd, we put $m=\frac{x+1}{2}$.

So in $j''=-j_2+h$, that $-b\le h\le a$, we determine a,b such that j'' is all numbers between 1 to $2x-2$, or $j''=1,2,...,2x-2$. But from $j''-j'\equiv 2xq-q^2+A_1q-p \pmod q$, we have $x^2-j''\equiv p \pmod q$, that $j'=1,2,...,2x-2$ and $j'\not\equiv j'' \pmod q$, since x^2-p is between two squares and according to induction, there is a positive integer like k, such that, $x^2-p-k=p_2\equiv o \pmod{q_u}$, so $q_u\mid p_2$, Pei's Prime and this is a contradiction unless $q=1$. If for a j'', $|q_lt_s|$ is a prime, for example $|q_lt_s|=p_1$, so for a j'', $x^2-j''=p+p_1$, then for all j'', that $1\le j''\le 2x-2$, $x^2-j''=p+p_1$ or $x^2-j''=p+qt$.

Now we use the above results to reach a contradiction, we use odd statements so:

$$(x^2-1or2)...(x^2-(2x-3)\text{ or}(2x-2))=(p+3t_1)(p+5t_2)...(p+qt_1)(p+p_1)(p+p'_1)...$$

but $(x-m-1)^2-j_2=p$, we assume that $m=x/2$ so $1\le j_2\le x-4$, if x is even and $m=(x+1)/2$ so $1\le j_2\le x-5$, if x is odd.

Hence $p>(x-3)^2/4$, but $x^2-j''=p+qt>4p$ and also $x^2-j''=p+p_1>4p$.

According to lemmas 2.5 and 2.6, we have:

$$(x^2-1or2)...(x^2-(2x-3)or(2x-2))<3^{\frac{x-1}{3}}\times\ldots\times q_a^{\frac{x-1}{q_a}}\times\frac{x^2}{3}^{\frac{x-1}{9}}\times\frac{x^2}{5}^{\frac{(x-1)(1-1/9)}{3\times5}}\times\ldots$$

We continue to reach $1-1/9-1/15-...-1/q_a=0$ that $q_a<w\ll\ x$, w is a positive large integer and q_a is a prime number. Hence we have:

$$(x-1)log(4p)<log(x^2-1or2)+...+log(x^2-(2x-3)or(2x-2))<$$

$$(x-1)\sum_{3\le q<w}\frac{logq}{q}+(x-1)(1/9+(1-1/9)/3\times5+(1-1/9-1/15)/3\times7+...+0)logx^2$$

So by refer to (Hardy & Wright, 1964), $\sum_{3\le q<w}\frac{logq}{q}<logw+c$, that c is positive constant number, so:

$$(x-1)log(4p)<(x-1)logw+(x-1)c+0.8(x-1)logx^2$$

Then for a large x, $(x-1)log(4p)<1.7(x-1)logx$ or $p<x^{1.7}/4$ and this is a contradiction, because $p>(x-3)^2/4$.

For example, assume that $x=10$, then $m=5$, so $(10-5)^2-2=23$ and $(10-5-1)^2-3=13$, so $j_1=2$, $p=13$, $j_2=3$, since $-j_1+j_2-A'+p=0$, then$A'=14$. But $-j_2+h-(j_2+2(m+1)x-(m+1)^2)\equiv 0 \pmod{q_j}$, since $j''=-j_2+h$, then $j''=-3+h$, so, if we put $h=4,5,...,21$, we have all numbers between 10^2 and 9^2.

References

G. H. Hardy, & E. M. Wright. (1964). *An introduction to the theory of numbers*. Oxford .

M. EI Bachraoui. (2006). Prime in the interval $[2n,3n]$. *International Journal of Contemporary Mathematical Sciences*, 1(3), 617-621.

P. Erdos, & J. Suranyi. (2003). Topics in the theory of numbers. undergraduate texts in mathematics. Springer Verlag.

P. Erdos. (1932). Beweis eines satzes von tschebyschef. Acta Litt. Univ. Sci., Szeged, Sect. Math., 5, 194-198.

Richard K. Guy. (2004). *Unsolved problem in number theory*. Springer.

Shiva Kintali. (2008). A Generalization of Erdos's Proof of Bertrand-Chebyshev Theorem. http://www.cs.princeton.edu/ kintali.

S. Ramanujan. (1919). A proof of Bertrand, S. Postulate. *Journal of the Indian Mathematical Society, 11*, 181-182.