SYMMETRY DISTRIBUTION LAW OF PRIME NUMBERS ON POSITIVE INTEGERS AND RELATED RESULTS

Yibing Qiu

Room607, 12th floor, 3rd block, Zhao Feng Yuan Section, Feng Tai District,

Beijing 100040, P.R .CHINA

yibing.qiu@hotmail.com

Abstract

This article puts forward a new theorem concerns the distribution of prime numbers: *Let integer* $n \geqslant 4$, *there exist two distinct odd primes p and q such that* $n - p = q - n$. Proves the theorem establish applied the *Congruence theory* and the *Fermat's method of infinite descent*. With the application of the theorem, reaches several results.

Keywords.: Exist two distinct odd prime numbers p and q; Such that $n - p = q - n$; Integer $n \geqslant 4$; One necessary and sufficient condition; Chinese remainder theorem; Fermat's method of infinite descent

1. Introduction

One classical problem in *Number Theory* is to understand the distribution of prime numbers, although this problem is still fundamentally unsolved, we have know many valuable results, and a famous in them is *Bertrand's Postulate*[1], the theorem states that *there exists at least a prime q such that* $n < q \leqslant 2n$ *for every integer* $n \geqslant 1$.It makes a rough description but gives a strict density lower pound of prime numbers distribution. By the theorem, we obtain:

Lemma 1.1. *Let integer* $n \geqslant 4$*, there exists at least an odd prime q such that* $n < q < 2n$.

And for the smallest element in all odd primes is 3 that be less than every integer $n \geqslant 4$, combined with Lemma1.1, another deep conclusion reaches:

Lemma1.2.*Let integer* $n \geqslant 4$,*there exist two odd primes p and q such that* $3 \leqslant p < n < q < 2n$.

As for the any given two distinct odd primes p and q, if we count from p to q, the number of the counting must be an odd and not less than 3, assume it equals 2d+1 with $d \geqslant 1$, thus, there must exists an integer $n \geqslant 4$ such that $n - p = d$; $q - n = d$, and $n - p = q - n$. Naturally, a proposition can be brings: for every integer $n \geqslant 4$, there must exist at least two odd primes p and q such that $n - p = q - n$ with $3 \leqslant p < n < q < 2n$. The proposition statement means that any two distinct odd primes are symmetrically distributed to an integer $n \geqslant 4$; and for every integer $n \geqslant 4$, there must exist at least two distinct odd primes are symmetrically distributed to the integer.

Since $n - p = q - n \Leftrightarrow n = (p + q)/2$, if the proposition statement is true, as a result, the completeness which contains in the proposition statement, establishes a clear quantity relationship between every integer $n \geqslant 4$ to two distinct odd primes p and q, that every integer $n \geqslant 4$ can be written as the arithmetic average of two distinct odd primes p and q.

Moreover, in positive integers, the proposition with the following three others is a set of propositions, that contains symmetrical and progressive significance in mathematical logic,

(i) Let $n \geqslant 2$, there exist two distinct odd numbers a_1 and a_2 such that $n - a_1 = a_2 - n$.

(ii) Let $n \geqslant 3$, there exist two distinct even numbers b_1 and b_2 such that $n - b_1 = b_2 - n$.

(iii) Let $n \geqslant 4$, there exist two distinct odd primes $c_1(p)$ and $c_2(q)$ such that $n - c_1 = c_2 - n$.

(iv) Let $n \geqslant 5$, there exist two distinct even composites d_1 and d_2 such that $n - d_1 = d_2 - n$.

The propositions (i), (ii) and (iv), can be proved establish by induction, with regard to the (iii), in this article, proposes the necessary and sufficient condition for the proposition be able to set up, and proves the condition being tenable applied the *Congruence Theory* and the *Fermat's method of infinite descent*, then get the proposition statement is true.

Theorem. *Let integer* $n \geqslant 4$, *there exist two distinct odd primes p and q such that*

$$n - p = q - n. \tag{1}$$

2. Proof of the Theorem

Proof. Let integer $n \geqslant 4$,and $p_1, p_2, p_3, \ldots, p_k$ be all odd primes which less than integer $n(\geqslant 4)$, since $p_1 = 3$, $p_1 < 4 \leqslant n$, then $k \geqslant 1$, in positive integers, we have, there always exist k odd integers $q_1, q_2, q_3, \ldots, q_k$ and $n < q_k < \ldots < q_2 < q_1 < 2n$, such that $n - p_i = q_i - n$ and $q_i = 2n - p_i$ for all $1 \leqslant i \leqslant k$. Let $P = \{p_1, p_2, p_3, \ldots, p_k\}$ and $Q = \{q_1, q_2, q_3, \ldots, q_k\}$, P and Q all be non-empty set, which corresponding with one-to-one by equation $n - p_i = q_i - n$ for all $1 \leqslant i \leqslant k$. If there exist two distinct odd primes p and q such that $n - p = q - n$, then $p \in P$ and $q \in Q$. Because every p_i be odd prime for all $1 \leqslant i \leqslant k$, if there exists at least an odd prime q in Q, then odd prime q and another odd prime p among P, which corresponding with the q one-to-one such that $n - p = q - n$, the Theorem will be set up. Then we get the necessary and sufficient condition for the Theorem can be establish is: for every integer $n \geqslant 4$, there must exists at least one odd prime q among q_i in the Q for all $1 \leqslant i \leqslant k$.

The following part to prove the necessary and sufficient condition statement being tenable, and conclude the Theorem statement is true.

Should proof by contradiction is applied. Suppose there exist some integers ($\geqslant 4$) makes the necessary and sufficient condition statement cannot tenable, n_0 is the smallest in them, then every q_i in the Q of n_0 be odd composite for all $1 \leqslant i \leqslant k$. we get $\Omega(q_i) \geqslant 2$ for all $1 \leqslant i \leqslant k$. Let u_i be the smallest and v_i be the second odd prime divisors of q_i for all $1 \leqslant i \leqslant k$, then $3 \leqslant u_i \leqslant v_i$ and $u_i v_i \mid q_i$ for all $1 \leqslant i \leqslant k$.

Where $n = n_0$, we sign $P_0 = \{p_1, p_2, p_3, \ldots, p_k\}$, $Q_0 = \{q_1, q_2, q_3, \ldots, q_k\}$, $U_0 = \{u_1, u_2, u_3, \ldots, u_k\}$, $V_0 = \{v_1, v_2, v_3, \ldots, v_k\}$, and there must be $U_0 \subseteq P_0$, $V_0 \subseteq P_0$.

Since $q_i = 2n_0 - p_i$ for all $1 \leqslant i \leqslant k$, then $u_i v_i \mid q_i \Rightarrow u_i v_i \mid 2n_0 - p_i \Rightarrow 2n_0 \equiv p_i (\text{mod } u_i v_i) \Rightarrow 2n_0 \equiv p_i (\text{mod } u_i)$ for all $1 \leqslant i \leqslant k$. Then we have the system of k congruences

$$x \equiv p_i \pmod{u_i} \qquad \text{for all } 1 \leqslant i \leqslant k. \tag{2}$$

Be solvable and $2n_0$ is a solution to the system of congruences.

Assume $n_0 \equiv r_i \pmod{u_i}$ and $1 \leqslant r_i \leqslant u_i$ for all $1 \leqslant i \leqslant k$, then $n_0 + n_0 \equiv r_i + r_i \pmod{u_i}$ for all $1 \leqslant i \leqslant k \Rightarrow 2n_0 \equiv 2r_i \pmod{u_i}$ for all $1 \leqslant i \leqslant k$, and $p_i \equiv 2n_0 \pmod{u_i}$ for all $1 \leqslant i \leqslant k \Rightarrow p_i \equiv 2n_0 \equiv 2r_i \pmod{u_i}$ for all $1 \leqslant i \leqslant k$.

Then we have the system of congruences (2) is equivalent to the system of congruences

$$x \equiv 2r_i \pmod{u_i} \qquad \text{for all } 1 \leqslant i \leqslant k. \tag{3}$$

In addition, the system of congruences

$$y \equiv r_i \pmod{u_i} \qquad \text{for all } 1 \leqslant i \leqslant k. \tag{4}$$

Be also solvable and n_0 is a solution to the system of congruences.

By verifying , we have, where $n = 4, 5,6,7,8,$ the Theorem is true, therefore, $n_0 > 8$, then where $n = n_0$, there $k \geqslant 3$, $p_k \geqslant 7$. moreover, by *Bertrand's Postulate*, we know there exists at least an odd prime g such that $p_k < g < 2p_k$, and n_0 must be such that $p_k < n_0 \leqslant g < 2p_k$, $2p_k > n_0$, $4p_k > 2n_0$, if $p_k \in U_0$, $p_k \mid q_i$, $q_i \in Q_0$, since $p_k \geqslant 7$, about the v_i which corresponding with p_k, we have $v_i \geqslant p_k \geqslant 7 > 4$, $2n_0 > q_i > n_0$, then $v_i p_k > 4p_k > 2n_0 > q_i$, $q_i \in Q_0$, which contradicts $v_i p_k \mid q_i$, $q_i \in Q_0$. So we get $p_k \notin U_0$, and $\{u_1,u_2,u_3,\ldots,u_k\} \subseteq \{p_1,p_2,p_3,\ldots, p_{k-1}\}$, by *Pigeonhole Principle*, we know, there exist at least two of the same elements in U_0.

Since $n_0 > 8$, $k \geqslant 3$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, and $q_i = 2n_0 - p_i$ for all $1 \leqslant i \leqslant k$, then $q_1 - q_2 = (2n_0 - 3) - (2n_0 - 5) = 2$, $q_2 - q_3 = (2n_0 - 5) - (2n_0 - 7) = 2$, $q_1 - q_3 = (2n_0 - 3) - (2n_0 - 7) = 4$, we get q_1, q_2, q_3 are pairwise relatively prime odd composites, thus u_1, u_2, u_3 are pairwise relatively prime, and u_1, u_2, u_3 are three distinct odd primes.

Assume there exist $u_h = u_2$ and $u_1,u_3,\ldots,u_h\,(u_2),\ldots,u_k$ are pairwise relatively prime in U_0, then there must be $4 \leqslant h \leqslant k$, and $u_1u_3\ldots u_h(u_2)\ldots u_k = [u_1,u_2,u_3,\ldots,u_h,\ldots,u_k]$. In addition, we have, $2n_0 \equiv p_2 \pmod{u_h}$, $2n_0 \equiv p_h \pmod{u_h}$, $2n_0 \equiv p_2 \equiv p_h \pmod{u_h}$, $2r_2 = 2r_h$. Then there be $x \equiv p_2 \pmod{u_2} \Leftrightarrow x \equiv p_h \pmod{u_h}$ in (2), $x \equiv 2r_2 \pmod{u_2} \Leftrightarrow x \equiv 2r_h \pmod{u_h}$ in (3), and $y \equiv r_2 \pmod{u_2} \Leftrightarrow y \equiv r_h \pmod{u_h}$ in (4).

By the *Chinese Remainder Theorem*, we get the set of all solutions to the system of congruences (2) or (3) is:

$$x \equiv p_1U_1U_1^{-1} + p_3U_3U_3^{-1} + \ldots + p_hU_hU_h^{-1} + \ldots + p_kU_kU_k^{-1} \tag{5.1}$$

$$\equiv 2r_1U_1U_1^{-1} + 2r_3U_3U_3^{-1} + \ldots + 2r_hU_hU_h^{-1} + \ldots + 2r_kU_kU_k^{-1} \pmod{u_1u_3\ldots u_h\ldots u_k} \tag{5.2}$$

In addition, the set of all solutions to the system of congruences (4) is:

$$y \equiv r_1U_1U_1^{-1} + r_3U_3U_3^{-1} + \ldots + r_hU_hU_h^{-1} + \ldots + r_kU_kU_k^{-1} \pmod{u_1u_3\ldots u_h\ldots u_k} \tag{6}$$

where $u_1u_3\ldots u_h\ldots u_k = [u_1,u_2,u_3,\ldots,u_h,\ldots,u_k] = u_i U_i$ for all $1 \leqslant i \leqslant k$, $i \neq 2$.

And U_i^{-1} is a unique integer such that

$$U_i U_i^{-1} \equiv 1 (\bmod u_i) \qquad \text{for all } 1 \leqslant i \leqslant k. \tag{7}$$

By $2n_0$ is a solution to the system of congruences (2) or (3), then

$$2n_0 \equiv p_1U_1U_1^{-1} + p_3U_3U_3^{-1} + \ldots + p_hU_hU_h^{-1} + \ldots + p_kU_kU_k^{-1} (\bmod u_1u_3\ldots u_h\ldots u_k) \tag{8}$$

Since $2n_0 \equiv p_h \equiv p_2 (\bmod u_2)$, $p_h > p_2$, we get $2 \mid p_h - p_2$, $u_2(u_h) \mid p_h - p_2$.
Let $p_h - p_2 = 2t$, then $t > 0$, $u_2 (u_h) \mid 2t$, $u_2 (u_h) \mid t$, and

$$U_hU_h^{-1} = U_2U_2^{-1}, \quad p_hU_hU_h^{-1} = (p_2 + 2t)U_2U_2^{-1} = p_2U_2U_2^{-1} + 2tU_2U_2^{-1} \tag{9}$$

Then we have

$$2n_0 \equiv p_1U_1U_1^{-1} + p_2U_2U_2^{-1} + 2tU_2U_2^{-1} + p_3U_3U_3^{-1} + \ldots + p_kU_kU_k^{-1} (\bmod u_1u_3\ldots u_h\ldots u_k) \tag{10}$$

$$2n_0 \equiv 2r_1U_1U_1^{-1} + 2r_2U_2U_2^{-1} + 2r_3U_3U_3^{-1} + \ldots + 2r_kU_kU_k^{-1} + 2tU_2U_2^{-1} (\bmod u_1u_2u_3\ldots u_k) \tag{11}$$

$$n_0 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} + tU_2U_2^{-1} (\bmod u_1u_2u_3\ldots u_k) \tag{12}$$

$$n_0 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} + tU_2U_2^{-1} (\bmod u_2) \tag{13}$$

$$n_0 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} + t (\bmod u_2) \tag{14}$$

since $u_2 \mid t$, then

$$n_0 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} + u_2 (\bmod u_2) \tag{15}$$

Assume

$$n_0 = r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_k U_kU_k^{-1} + u_2 \tag{16}$$

Then

$$n_0 - u_2 = r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} \tag{17}$$

Moreover

$$n_0 - u_2 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} (\bmod u_1u_2u_3\ldots u_k) \tag{18}$$

Let $n_1 = n_0 - u_2$, then we have

$$n_1 = r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} \tag{19}$$

$$n_1 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} (\bmod u_1u_2u_3\ldots u_k) \tag{20}$$

and there be $$n_1 \equiv r_i (\bmod u_i) \qquad \text{for all } 1 \leqslant i \leqslant k \tag{21}$$

Since $u_i \mid q_i$ and $q_i < 2n_0$ for all $1 \leqslant i \leqslant k$, then $u_i \leqslant \sqrt{q_i} < \sqrt{2n_0} < 1.42\sqrt{n_0}$ for all $1 \leqslant i \leqslant k$, $u_2 \leqslant \sqrt{q_2} < \sqrt{2n_0} < 1.42\sqrt{n_0}$. by $k \geqslant h \geqslant 4$, $n_0 > p_4 (= 11) > 9$, $\sqrt{n_0} > 3$,

$n_0=\sqrt{n_0}\sqrt{n_0}>3\sqrt{n_0}$, then $n_0-u_2>n_0-1.42\sqrt{n_0}$, $n_0-1.42\sqrt{n_0}>3\sqrt{n_0}-1.42\sqrt{n_0}=1.58\sqrt{n_0}>\sqrt{2n_0}>u_i$ for all $1\leqslant i\leqslant k$, we get $n_0-u_2>\sqrt{2n_0}>u_i$ for all $1\leqslant i\leqslant k$, and there be $n_1>u_i$ for all $1\leqslant i\leqslant k$.

As we know, there exist at least three distinct odd primes u_1,u_2 and u_3 in U_0, and $n_1>u_i$ for all $1\leqslant i\leqslant k$, we have, there exist at least three distinct odd primes u_1,u_2,u_3 be less than n_1. Let $p_1, p_2, p_3,\ldots,p_s$ be all odd primes which less than integer n_1, then s not less than three, so there be $3\leqslant s\leqslant k$, $p_3\,(=7)\leqslant p_s\leqslant p_k$, and $n_1\geqslant 8$.

Then we get

$$n_1\equiv r_i (\mathrm{mod}\ u_i) \qquad \text{for all } 1\leqslant i\leqslant s \tag{22}$$

$$2n_1\equiv 2r_i (\mathrm{mod}\ u_i) \qquad \text{for all } 1\leqslant i\leqslant s \tag{23}$$

$$2n_1\equiv p_i (\mathrm{mod}\ u_i) \qquad \text{for all } 1\leqslant i\leqslant s \tag{24}$$

by (24), we have, $u_i \mid 2n_1-p_i=q_i$ for all $1\leqslant i\leqslant s$, and $u_i<n_1<q_i=2n_1-p_i$ for all $1\leqslant i\leqslant s$, it shows $u_i<q_i$ and $u_i \mid q_i$ for all $1\leqslant i\leqslant s$. then, where $n=n_1(\geqslant 8)$, for each odd prime p_i which less than n_1, every $q_i=2n_1-p_i$ such that $n_1-p_i=q_i-n_1$ be odd composite for all $1\leqslant i\leqslant s$. Therefore, n_1 also makes the necessary and sufficient condition statement cannot tenable, and $n_1<n_0$, which contradicts the minimality of n_0, it is impossible.

To sum up, we must have, there being no any one integer $n\geqslant 4$ makes the necessary and sufficient condition for the Theorem cannot tenable, therefore, we get that there must exists at least one odd prime q in the Q of every one integer $n\geqslant 4$. Thus, the necessary and sufficient condition for the Theorem being tenable has proved, and we get the Theorem statement is true. This completes the proof of the Theorem. □

3. An Equivalent Proposition of the Theorem. *Let integer $n\geqslant 4$, there must exists at least one positive integer d with $1\leqslant d\leqslant n-3$, makes n - d and n + d being odd primes.*

In particular, if $d=1$, then $\{n-1, n+1\}$ be *twin primes*. So the accurate mathematical formulas of $d=f(n, p<n, n-p, \cdots, p|n)$ have very important theoretical significance and practical values.

4. The Geometric Significance of the Theorem

(i) On real axis, there must exist two distinct odd prime points p and q be symmetrically distributed to every integer point $n\geqslant 4$.

(ii) On real axis, every integer point $n\geqslant 4$ be the midpoint of the line segment that with two distinct odd prime points p and q for endpoints.

5. Three Corollaries of the Theorem

Corollary 5.1. *Let integer* $n \geqslant 4$, *and* $p_1, p_2, \ldots, p_k$ *be all odd primes which less than n, then the equation* $n - p_i = x_i - n$ *has no solution, which every* x_i *be odd composite for all* $1 \leqslant i \leqslant k$.

Proof. The proof of the Corollary 5.1 is the same as the proof of the Theorem. □

Corollary 5.2. *Every integer* $n \geqslant 2$ *can be written as the arithmetic average of two primes.*

Proof. By the Theorem , if integer $n \geqslant 4$, there exist two distinct odd primes p and q such that $n - p = q - n$, and $n - p = q - n \Leftrightarrow n = (p + q)/2$, then we get: Every integer $n \geqslant 4$ can be written as the arithmetic average of two distinct odd primes.

Moreover, there being $3 = (3 + 3)/2$ and $2 = (2 + 2)/2$, the further results can be reached:
Every integer $n \geqslant 3$ can be written as the arithmetic average of two odd primes.
Every integer $n \geqslant 2$ can be written as the arithmetic average of two primes.
This completes the proof . □

Corollary 5.3. (*Goldbach conjecture* [2]) *Every even number* $2n \geqslant 4$ *can be written as the sum of two primes.*

Proof. Let even number $2n \geqslant 8$, then $n \geqslant 4$, by the results in the proof of the Corollary 5.2, there exist two distinct odd primes p and q such that $n = (p + q)/2$ for every integer $n \geqslant 4$, and $2n\ (\geqslant 8) = 2 \cdot n\ (\geqslant 4) = 2 \cdot (p + q)/2 = p + q$, one result reached:
Every even number $2n \geqslant 8$ can be written as the sum of two distinct odd primes.

According to the same principle, by the conclusions of the Corollary 5.2, two results can be getting:
Every even number $2n \geqslant 6$ can be written as the sum of two odd primes .
Every even number $2n \geqslant 4$,or every even composite can be written as the sum of two primes.
This completes the proof. □

References

[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Number*, Fifth Edition, Oxford Science Publications, Oxford University Press, Oxford, 1980.

[2] M. B. Nathanson. *Elementary Methods in Number Theory*, Springer--Verlag, Beijing, 2003.