International Journal of Science and Engineering Applications
Volume 6–Issue 12, 360-363, 2017, ISSN:-2319–7560

Symmetry Distribution Law of Prime Numbers on Positive Integers and Related Results

Yibing Qiu
Beijing 100040, China

Abstract: This article presents a new theorem concerning the distribution of prime numbers: Let integer $n \geq 4$, then there exist two distinct odd primes p and q such that $n - p = q - n$. The proof of the theorem is established by using the congruence theory and Fermat's method of infinite descent. Moreover, several results are presented to highlight the significance of the theorem.

Keywords: similarity distribution; odd primes; congruence theory; Chinese remainder theorem; Fermat's method of infinite descent

1. INTRODUCTION

A classical problem in the *Number Theory* is to understand the distribution of prime numbers.

Although, this problem is still fundamentally unsolved, there exist, however, many valuable results including the famous *Bertrand's Postulate* [1]. The theorem states that *there exists at least a prime q such that* $n < q \leq 2n$ *for every integer* $n \geq 1$. This result makes a rough description but gives a strict density lower bound of distribution of primes. From *Bertrand's postulate* we obtain:

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

Furthermore, the smallest element in all odd primes is 3 which is less than every integer $n \geq 4$. Combined with Lemma 1.1, another significant conclusion can be made:

Lemma 1.2. *Let* $n \geq 4$ *be an integer, then there exist two odd primes p and q such that* $3 \leq p < n < q < 2n$.

For any two distinct odd primes p and q, if we count from p to q, the number of the counting must be odd and not less than 3. Assume that it is 2d+1 with $d \geq 1$, then there exists an integer $n \geq 4$ such that $n - p = d$, $q - n = d$, and $n - p = q - n$. Naturally, a proposition can be deduced: for every integer $n \geq 4$, there exist at least two odd primes p and q such that $n - p = q - n$ with $3 \leq p < n < q < 2n$. This means that any two distinct odd primes are symmetrically distributed about an integer $n \geq 4$, and for every integer $n \geq 4$, there exist at least two distinct odd primes that are symmetrically distributed about the integer.

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

Moreover, in positive integers, the above-mentioned proposition along with the following set of propositions presents a significant result in mathematical logic,

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

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

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

(iv) Let $n \geq 5$, 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 by induction. For proposition (iii), this article proposes the necessary and sufficient condition for its validity and applies the *Congruence Theory* and the *Fermat's method of infinite descent* to prove the proposition.

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

$$n - p = q - n. \qquad (1)$$

2. PROOF OF THE THEOREM

Proof. Let $n \geq 4$ be an integer and $p_1, p_2, p_3, \ldots, p_k$ be all odd primes which are less than the integer $n (\geq 4)$. Since $p_1 = 3$, $p_1 < 4 \leq n$, then for $k \geq 1$ in positive integers, 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 $1 \leq i \leq k$. Let $P = \{p_1, p_2, p_3, \ldots, p_k\}$ and $Q = \{q_1, q_2, q_3, \ldots, q_k\}$, where, P and Q be non-empty sets which correspond one-to-one by equation $n - p_i = q_i - n$ for all $1 \leq i \leq k$. If there exist two distinct odd primes p and q such that $n - p = q - n$, then $p \in P$ and $q \in Q$. Since every p_i is odd prime for all $1 \leq i \leq k$ and if there exists at least an odd prime q in Q, then the odd prime q and the odd prime $p \in P$ correspond one-to-one with the q such that $n-p=q-n$. This proves the Theorem. Now the necessary and sufficient condition for the Theorem can be established as: for every integer $n \geq 4$, there exists at least one odd prime q among q_i in the Q for all $1 \leq i \leq k$.

In the following, we prove the necessary and sufficient condition to be tenable and conclude that the Theorem statement is true.

Suppose there exist some integers (≥ 4) such that the necessary and sufficient condition statement does not hold. Let n_0 be the smallest in them, then every q_i in the Q of n_0 is odd composite for all $1 \leq i \leq k$, and we get $\Omega(q_i) \geq 2$ for all $1 \leq i \leq k$. Let u_i be the smallest and v_i be the second odd prime divisors of q_i for all $1 \leq i \leq k$, then $3 \leq u_i \leq v_i$ and $u_i v_i \mid q_i$ for all $1 \leq i \leq k$.

Where $n=n_0$ and we take $P_0=\{p_1,p_2,p_3,\ldots,p_k\}$, $Q_0=\{q_1,q_2,q_3,\ldots,q_k\}$, $U_0=\{u_1,u_2,u_3,\ldots,u_k\}$,

$V_0=\{v_1,v_2,v_3,\ldots,v_k\}$, then there must be $U_0 \subseteq P_0$, $V_0 \subseteq P_0$.

Since $q_i=2n_0-p_i$ for all $1 \leq i \leq k$, then $u_i v_i | q_i \Rightarrow u_i v_i | 2n_0-p_i \Rightarrow 2n_0 \equiv p_i (\mathrm{mod}\ u_i v_i) \Rightarrow$

$2n_0 \equiv p_i (\mathrm{mod}\ u_i)$ for all $1 \leq i \leq k$. Then, we have the system of k congruences

$$x \equiv p_i\ (\mathrm{mod}\ u_i) \qquad \text{for all } 1 \leq i \leq k. \qquad (2)$$

with $2n_0$ as its solution.

Assume $n_0 \equiv r_i (\mathrm{mod}\ u_i)$ and $1 \leq r_i \leq u_i$ for all $1 \leq i \leq k$, then $n_0+n_0 \equiv r_i+r_i\ (\mathrm{mod}\ u_i)$ for all $1 \leq i \leq k$ $\Rightarrow$ $2n_0 \equiv 2r_i\ (\mathrm{mod}\ u_i)$ for all $1 \leq i \leq k$, and $p_i \equiv 2n_0 (\mathrm{mod}\ u_i)$ for all $1 \leq i \leq k$ $\Rightarrow$ $p_i \equiv 2n_0 \equiv 2r_i\ (\mathrm{mod}\ u_i)$ for all $1 \leq i \leq k$.

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

$$x \equiv 2r_i (\mathrm{mod}\ u_i) \qquad \text{for all } 1 \leq i \leq k. \qquad (3)$$

In addition, the system of congruences

$$y \equiv r_i\ (\mathrm{mod}\ u_i) \qquad \text{for all } 1 \leq i \leq k. \qquad (4)$$

has a solution n_0.

To verify, we take $n=4,5,6,7,8$. The Theorem is true, therefore, $n_0>8$, and since $n=n_0$, there exist $k \geq 3$ with $p_k \geq 7$. 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 $p_k<n_0 \leq g<2p_k$, $2p_k>n_0$, and $4p_k>2n_0$. If $p_k \in U_0$, $p_k | q_i$, $q_i \in Q_0$, and since $p_k \geq 7$, and v_i correspond with p_k, we have $v_i \geq p_k \geq 7>4$, $2n_0>q_i>n_0$, then $v_i p_k>4p_k>2n_0>q_i$, $q_i \in Q_0$, which contradicts $v_i p_k \mid q_i$, $q_i \in Q_0$. Hence, 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 $n_0>8$, $k \geq 3$, $p_1=3$, $p_2=5$, $p_3=7$, and $q_i=2n_0-p_i$ for all $1 \leq i \leq k$, then $q_1-q_2=(2n_0-3)-(2n_0-5)=2$, $q_2-q_3=(2n_0-5)-(2n_0-7)=2$, $q_1-q_3=(2n_0-3)-(2n_0-7)=4$, and we get q_1, q_2, q_3 are pairwise relatively prime odd composites, thus u_1, u_2, u_3 are pairwise relatively primes, and u_1, u_2, u_3 are three distinct odd primes.

Assume that there exist $u_h=u_2$ and $u_1,u_3,\ldots,u_h(u_2),\ldots,u_k$ that are pairwise relatively primes in U_0, then there must be $4 \leq h \leq k$, 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, $2n_0 \equiv p_2(\ \mathrm{mod}\ u_h\ )$, $2n_0 \equiv p_h(\ \mathrm{mod}\ u_h\ )$, $2n_0 \equiv p_2 \equiv p_h(\ \mathrm{mod}\ u_h\ )$, $2r_2=2r_h$. Then there exist

$x \equiv p_2(\ \mathrm{mod}\ u_2\ ) \Leftrightarrow x \equiv p_h(\ \mathrm{mod}\ u_h\ )$ in (2), $x \equiv 2r_2(\ \mathrm{mod}\ u_2) \Leftrightarrow x \equiv 2r_h(\ \mathrm{mod}\ u_h\ )$ in (3), and $y \equiv r_2(\ \mathrm{mod}\ u_2) \Leftrightarrow y \equiv r_h(\ \mathrm{mod}\ u_h)$ in (4).

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

$$x \equiv p_1U_1U_1^{-1}+p_3U_3U_3^{-1}+\ldots+p_hU_hU_h^{-1}+\ldots+p_kU_kU_k^{-1}, \qquad (5.1)$$

$$\equiv 2r_1U_1U_1^{-1}+2r_3U_3U_3^{-1}+\ldots+2r_hU_hU_h^{-1}+\ldots+2r_kU_kU_k^{-1}\ (\mathrm{mod}\ u_1u_3\ldots u_h\ldots u_k). \quad (5.2)$$

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

$$y \equiv r_1U_1U_1^{-1}+r_3U_3U_3^{-1}+\ldots+r_hU_hU_h^{-1}+\ldots+r_kU_kU_k^{-1}\ (\mathrm{mod}\ u_1u_3\ldots u_h\ldots u_k), \qquad (6)$$

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 $1 \leq i \leq k$, $i \neq 2$.

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

$$U_iU_i^{-1} \equiv 1(\mathrm{mod}\ u_i) \qquad \text{for all } 1 \leq i \leq k. \qquad (7)$$

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

$$2n_0 \equiv p_1U_1U_1^{-1}+p_3U_3U_3^{-1}+\ldots+p_hU_hU_h^{-1}+\ldots+p_kU_kU_k^{-1}(\mathrm{mod} u_1u_3\ldots u_h\ldots u_k). \qquad (8)$$

Since $2n_0 \equiv p_h \equiv p_2\ (\mathrm{mod}\ u_2)$, $p_h>p_2$, we get $2|p_h-p_2$, $u_2(u_h)|p_h-p_2$.

Let $p_h-p_2=2t$, then $t>0$, $u_2\,(u_h)|2t$, $u_2\,(u_h)|t$, and

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

Then, we have

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

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

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

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

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

Since $u_2|t$, then,

$n_0 \equiv r_1U_1U_1^{-1} + r_2U_2U_2^{-1} + r_3U_3U_3^{-1} + \ldots + r_kU_kU_k^{-1} + u_2 (\mathrm{mod}\ u_2)$. (15)

Assume

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

Then,

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

Moreover,

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

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

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

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

and hence,

$n_1 \equiv r_i (\mathrm{mod}\ u_i)$ for all $1 \le i \le k$. (21)

Since $u_i|q_i$ and $q_i < 2n_0$ for all $1 \le i \le k$, then $u_i \le \sqrt{q_i} < \sqrt{2n_0} < 1.42\sqrt{n_0}$ for all $1 \le i \le k$, $u_2 \le \sqrt{q_2} < \sqrt{2n_0} < 1.42\sqrt{n_0}$. By taking $k \ge h \ge 4$, $n_0 > p_4 (= 11) > 9$, $\sqrt{n_0} > 3$, $n_0 = \sqrt{n_0}\sqrt{n_0} > 3\sqrt{n_0}$, 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 $1 \le i \le k$, and we get $n_0 - u_2 > \sqrt{2n_0} > u_i$ for all $1 \le i \le k$, and hence $n_1 > u_i$ for all $1 \le i \le k$.

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 $1 \le i \le k$. then we have at least three distinct odd primes u_1, u_2, u_3 less than n_1. Let $p_1, p_2, p_3, \ldots, p_s$ be all odd primes which are less than integer n_1, and s not less than 3, then $3 \le s \le k$, $p_3 (= 7) \le p_s \le p_k$, and $n_1 \ge 8$.

Then, we get

$n_1 \equiv r_i (\mathrm{mod}\ u_i)$ for all $1 \le i \le s$, (22)

$2n_1 \equiv 2r_i (\mathrm{mod}\ u_i)$ for all $1 \le i \le s$, (23)

$2n_1 \equiv p_i\ (\mathrm{mod}\ u_i)$ for all $1 \le i \le s$. (24)

From (24) we have, $u_i | 2n_1 - p_i = q_i$ for all $1 \le i \le s$, and $u_i < n_1 < q_i = 2n_1 - p_i$ for all $1 \le i \le s$, which shows $u_i < q_i$ and $u_i | q_i$ for all $1 \le i \le s$. Since $n = n_1 (\ge 8)$, each odd prime p_i which is less than n_1, and every $q_i = 2n_1 - p_i$ such that $n_1 - p_i = q_i - n_1$, be odd composite for all $1 \le i \le s$. Therefore, n_1 also does not make the necessary and sufficient condition statement tenable and $n_1 < n_0$ contradicts the minimality of n_0 which is impossible.

To sum up, there exist no integer $n \ge 4$ for which the necessary and sufficient condition for the Theorem does not hold. Therefore, there must exists at least one odd prime q in the Q of every integer $n \ge 4$. Thus, the necessary and sufficient condition for the Theorem being tenable is proved. This completes the proof of the Theorem. □

3. EQUIVALENT PROPOSITION OF THE THEOREM

Let $n \ge 4$ be an integer, then there exists at least one positive integer d with $1 \le d \le n-3$, such that $n-d$ and $n+d$ are odd primes.

In particular if $d = 1$, then $\{n-1, n+1\}$ be *twin primes*. Then the accurate mathematical

formulas of $d = f(n, p < n, n-p, \ldots, p|n)$ have very important theoretical significance and

practical values.

4. GEOMETRIC SIGNIFICANCE OF THE THEOREM

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

(ii) On real axis, every integer point $n \geq 4$ be the midpoint of the line segment with two distinct odd primes p and q as endpoints.

.

5. THREE COROLLARIES OF THE THEOREM

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

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

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

Proof. From the Theorem, for integer $n \geq 4$ 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 $n \geq 4$ can be written as the arithmetic average of two distinct odd primes.

Moreover, since $3 = (3+3)/2$ and $2 = (2+2)/2$, following results can be deduced:

Every integer $n \geq 3$ can be written as the arithmetic average of two odd primes.

Every integer $n \geq 2$ can be written as the arithmetic average of two primes.

This completes the proof. □

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

Proof. Let $2n \geq 8$ be an even number, then $n \geq 4$ and 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 $n \geq 4$, and $2n\ (\geq 8) = 2 \cdot n\ (\geq 4) = 2 \cdot (p+q)/2 = p + q$, hence:

Every even number $2n \geq 8$ can be written as the sum of two distinct odd primes.

According to the same principle, by the conclusions of the Corollary 5.2, following two results can be found:

Every even number $2n \geq 6$ can be written as the sum of two odd primes.

Every even number $2n \geq 4$, or every even composite, can be written as the sum of two primes.

This completes the proof. □

6. REFERENCES

[1] G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*, 5th ed., Oxford science publications, Oxford, Oxford University press, 1980, XXIIThe series of primes (3), 22.3 Bertrand's postulate and a 'formula' for primes, P.343.

[2] M. B. Nathanson. *Elementary Methods in Number Theory*, Springer-Verlag, Beijing, 2003, Section II, Divisors and Primes in Multiplicative Number Theory, 8 Prime Numbers, 8.4, notes3, P.287.