The Chinese Remainder Theorem • Goldbach’s Conjecture

(A) • Hardy-Littewood’s Conjecture (A)

Tong Xin Ping
txp1313abc @ hotmail.com

Abstract: \( N = p_i + (N-p_i) = p_+ + (N-p) \). \( \text{①} \) If \( p \) is congruent to \( N \) modulo \( p_i \), Then \( (N-p) \) is a composite integer. When \( i = 1, 2, \ldots, r \), if \( p \) and \( N \) are incongruent modulo \( p_i \), Then \( p \) and \( (N-p) \) are solutions of Goldbach’s Conjecture (A); \( \text{②} \) By Chinese Remainder Theorem we can calculate the primes and solutions of Goldbach’s Conjecture (A) with different system of congruence; \( \text{③} \) The \( (N-p) \) must have solution of Goldbach’s Conjecture (A), The number of solutions of Goldbach’s Conjecture (A) is increasing as \( N \rightarrow \infty \), and finding unknown particulars for Hardy-Littewood’s Conjecture (A).

Key words: congruent, Chinese Remainder Theorem, Goldbach’s Conjecture (A), Hardy-Littewood’s Conjecture (A).

“Every even positive integer greater than 2 can be written as the sum of two primes.” This conjecture was stated by Christion Goldbach in a letter to Leonhard Euler in 1742.

Let \( p_i < \sqrt{N} \), \( \sqrt{N} < p < N \). We have \( N = p_i + (N-p_i) = p_+ + (N-p) \). \( \text{①} \) If \( p \) is congruent to \( N \) modulo \( p_i \), then \( (N-p) \) is a composite integer, (See Theorem 1.) When \( i = 1, 2, \ldots, r \), if \( p \) and \( N \) are incongruent modulo \( p_i \), Then \( p \) and \( (N-p) \) are solutions of Goldbach’s Conjecture (A); (See Theorem 2.) \( \text{②} \) By Chinese Remainder Theorem, we can calculate the primes and solutions of Goldbach’s Conjecture (A) with different system of congruence (3), (5). (See Theorem 3, 4.) \( \text{③} \) The \( (N-p) \) must have solution of Goldbach’s Conjecture (A), (See Theorem 5.) The number of solutions of Goldbach’s Conjecture (A) is increasing as \( N \rightarrow \infty \), (See Theorem 6.) and finding unknown particulars for Hardy-Littewood’s Conjecture (A); (See Theorem 6.)

1. Term, Terminology, Symbol.

\( N \) — Even positive integers. Let \( 2 \leq p_i \leq p_r \leq \sqrt{N} < p_{r+1} < N < p_{r+1}^2 < p_1 p_2 \ldots p_r \).

\( p_i, p_r, p_{r+1} \) — Prime number. \( i = 1, 2, 3, \ldots, r \). \( r = \lceil \sqrt{N} \rceil \).

\( 1 \) \( w_r = p_i p_2 \ldots p_r = \prod_{2 \leq p \leq \sqrt{N}} p \).

\( p \) — Prime number. \( p_{r+1} \leq p < (N - p_r + 1) \). We have \( (N - p) > p_r \). Every \( p \) can be written as \( p = p(a_i) + n p_i \). \( 1 \leq p(a_i) \leq p_i - 1 \).

Let \( f_i(a_i) = 1, 2, \ldots, (p_i - 1) \).

\( p \) — All \( p \). We have \( p = f_i(a_i) + n p_i \). \( f_i(a_i) = 1, 2, \ldots, (p_i - 1) \).

Let \( N = p_i + (N-p_i) = p_+ + (N-p) \). When \( N = 98, 126, 128, \ldots \) The \( (N-p_i) \)-composite integers. We prove that \( (N-p) \) must have prime.

Lemma 1. If \( r \geq 4 \), Then \( N < p_1^2 < p_1 p_2 \ldots p_r = w_r \).

When \( r < 4 \), we can finding \( p_1 p_2 \ldots p_r < N \). Therefore, This paper studies \( r \geq 4 \), \( N \geq 50 \).

\( N(a_i) \) — Remainder that divided \( N \) by \( p_i \). We have \( N = N(a_i) + n p_i \). \( 0 \leq N(a_i) \leq p_i - 1 \).
N(a)_r — A group of systematic remainders that divided N by p_1, p_2,..., p_r. N(a)_r = N(a_1), N(a_2),..., N(a_r). For example, N=90, r=4, 90(a_1)=90(a_1), 90(a_2),..., 90(a_4) =0, 0, 0, 6.

f_2(a)_i — Take N(a)_i out of f_1(a)_i, we can obtain f_2(a)_i. 1. When p_i | N, N(a)_i=0 using f_2(a)_i, the number of element of f_2(a)_i is (p_r−1); 2. When (p_i, N)=1, 0<N(a)_i≤p_r−1. f_1(a)_i =1, 2,...,(p_r−1). The N(a)_i is one element of f_1(a)_i. The number of element of f_2(a)_i is (p_r−2).

N(1,1)_i — The number of solutions of Goldbach’s Conjecture (A) lying in the interval (0, p_r+1) and (N−p_r−1, N).

N(1,1)_r — The number of solutions of Goldbach’s Conjecture (A) lying in the interval (p_r+1, N−p_r−1).

N(1,1) = r≤(N) — The number of solutions of Goldbach’s Conjecture (A) lying in the interval (0,N). N(1,1) = N(1,1)_r + 2 N(1,1)_i.


Theorem 1. If N is congruent to p modulo p_i, Then the (N−p) is a composite integer.

Proof. N≡p(mod p_i), p_i | (N−p), We have (N−p)=kp_i. (k≥1.) As before, (N−p) > p_r, k>1, Then (N−p) is composite integer. Theorem 1 is proved.

Theorem 2. If i=1, 2, 3,..., r. N and p are incongruent modulo p_1, p_2,..., p_r. Then p and (N−p) are solutions of Goldbach’s Conjecture (A).

Proof. i=1, 2, 3,..., r. N and p are incongruent modulo p_1, p_2,..., p_r. In other words, the (N−p) is not divisible by any prime not exceeding $\sqrt{N}$. The (N−p) is a prime. The p and (N−p) are solutions of Goldbach’s Conjecture (A). Theorem 2 is proved.


Lemma 2. The Chinese Remainder Theorem. Let m_1, m_2, ..., m_r be pairwise relatively prime positive integers. Then the system of congruences

(2) \[ x \equiv a_1 \pmod{m_1}, \]
\[ x \equiv a_2 \pmod{m_2}, \]
\[ \vdots \]
\[ x \equiv a_r \pmod{m_r}, \]

has a unique solution modulo \(M=m_1m_2...m_r\).

Theorem 3. The \(u\) is number of solutions of system of congruences (3). When \(y<N\), the \(y\) is a prime.

(3) \[ y \equiv f_1(a_1) \pmod{p_1} \]
\[ y \equiv f_1(a_2) \pmod{p_2} \]
\[ \vdots \]
\[ y \equiv f_1(a_r) \pmod{p_r} \]
\[ u=(p_1−1)(p_2−1)...(p_r−1)= \prod_{2 \leq p \leq \sqrt{N}} (p−1) \]

Proof. The \(f_1(a_1)=1\), The number of elements of \(f_1(a_1)\) is \((p_r−1)\);

The \(f_1(a_2)=1, 2\). The number of elements of \(f_1(a_2)\) is \((p_2−1)\); ...

The \(f_1(a_r)=1, 2,..., (p_r−1)\). The number of elements of \(f_1(a_r)\) is \((p_r−1)\).
When \(i=1,2,\ldots, r\) we taking one element of the \(f_i(a_i)\), We can obtain different system of congruences (3), The number of the different system of congruences (3) is \((p_1-1)(p_2-1)\cdots(p_r-1)=u\).

By (3), if \(y< N\), the \(y\) is not divisible by any prime not exceeding \(\sqrt{N}\). The \(y\) is a prime. Theorem 3 is proved.

**Theorem 4.** The \(v\) is number of solutions of system of congruences (5). When \((p_r+1)<y<(N-p_r-1)\), the \(y\) and \((N-y)\) are solutions of Goldbach's Conjecture (A).

\[
y = f_2(a_1) \pmod{p_1}
y = f_2(a_2) \pmod{p_2}
\vdots
y = f_2(a_i) \pmod{p_i}
\]

\[
(6) \quad v = \prod_{3 \leq p \leq \sqrt{N}} (p-2) \prod_{2 \leq p \leq \sqrt{N}} (p-1) = \prod_{3 \leq p \leq \sqrt{N}} (p-2) \prod_{2 \leq p \leq \sqrt{N}} \frac{p-1}{p-2} \quad \text{(get rid of } p_1-1=1_{\text{, }})\]

*Proof.* When \((N, p_i)=1\), The number of elements of \(f_2(a_i)\) is \((p_i-2)\); When \((N, p_i)= p_i\), The number of elements of \(f_2(a_i)\) is \((p_i-1)\). (When \(p_i>2\), We have \((p_i-1)=(p_i-2) \frac{p_i-1}{p_i-2}\).)

When \(i=1,2,\ldots, r\) we taking one element of the \(f_2(a_i)\), We can obtain different system of congruences (5), The number of the different system of congruences (5) is multiply \(\prod(p_i-2)\prod(p_i-1)\). (See 6.)

By (5), if \((p_r+1)<y<(N-p_r-1)\), ① Because \(f_2(a_i)\neq 0\), by Theorem 3, the \(y\) is a prime; ② Because \(f_2(a_i)\neq N(a_i)\), \(N\) and \(y\) are incongruent modulo \(p_1, p_2, \ldots, p_r\). By Theorem 2, the \((N-y)\) is a prime. The \(y\) and \((N-y)\) are solutions of Goldbach's Conjecture (A). Theorem 4 is proved.

### 4. The Proof of Goldbach's Conjecture (A).

**Theorem 5.** \((N-p)\) must have prime.

*Proof.* \((N-p)\geq p_r\), Suppose \((N-p)=\text{composite integer}=h_p(h_r>1)\) We have \(p=N-h_p=N(p_i)+np_r\) \(h_p=N(p_i)+(n-h)p_i\). The \(p=N(p_i)+(n-h)p_i\) are in contradiction with \(p=f_1(a_i)+np_r\). (The \(N(p_i)\) is one of the \(f_1(a_i)\).) The contradiction shows, that there are some primes in \((N-p)\). Theorem 5 is proved.

**Lemma 3.** \(\pi(N) = \varepsilon N \prod_{2 \leq p \leq \sqrt{N}} \frac{p-1}{p}\)

*Proof.* The \(\pi(N)\) and \(u\) are number of positive integer that are not divisible by any prime not exceeding \(\sqrt{N}\).

Noticing \(\pi(N) \neq \frac{u}{w_r}\), we have \(\pi(N) = \varepsilon \frac{u}{w_r}\), and \(\pi(N) = \varepsilon \frac{N \cdot u}{w_r}\). Lemma 3 is proved.

**Theorem 6.** The number of solutions of Goldbach's Conjecture (A) is increasing as \(N \to \infty\).

*Proof.* By Lemma 3, we have
\[
1 = \prod_{p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \prod_{p \leq \sqrt{N}} \frac{p-1}{p} \frac{p-1}{p} \times \prod_{2 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1}
\]

\[
= \prod_{p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N} \times \prod_{p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1}
\]

\[
= 4 \prod_{p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{3 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{3 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{3 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{3 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

\[
= \prod_{3 \leq p \leq \sqrt{N}} \frac{p}{p-1} \frac{p}{p-1} \times \frac{1}{\varepsilon} \frac{\pi(N)}{N} \frac{1}{\varepsilon} \frac{\pi(N)}{N}
\]

The \(N(1,1)\) and \(v\) are number of positive integer that are not divisible by any prime not exceeding \(\sqrt{N}\). Added to this, these positive integer and \(N\) are incongruent modulo \(p_i\).

Noticing \(\frac{N(1,1)}{N} \neq \frac{v}{w_r}\). We have \(\frac{N(1,1)}{N} = \psi \frac{v}{w_r}\), and have (7).

(7) \(N(1,1) = \psi \frac{v}{w_r} N\)

\[
= \psi \frac{N}{2} \prod_{3 \leq p \leq \sqrt{N}} \frac{p-2}{p} \prod_{3 \leq p \leq \sqrt{N}} \frac{p-1}{p-2} \times 1
\]

\[
= \psi \frac{2\pi(N)\pi(N)}{\varepsilon N} \prod_{3 \leq p \leq \sqrt{N}} \frac{p-2}{p-1} \frac{p}{p-1} \prod_{3 \leq p \leq \sqrt{N}} \frac{p-1}{p-2}
\]

\[
= \psi \frac{2\pi(N)\pi(N)}{\varepsilon N} \prod_{3 \leq p \leq \sqrt{N}} (1 - \frac{1}{(p-1)^2}) \prod_{3 \leq p \leq \sqrt{N}} \frac{p-1}{p-2}
\]

The \[\frac{2\pi(N)\pi(N)}{\varepsilon N} \prod_{3 \leq p \leq \sqrt{N}} (1 - \frac{1}{(p-1)^2}) \prod_{3 \leq p \leq \sqrt{N}} \frac{p-1}{p-2} (= r_2(N))\]. It is Hardy-Littlewood’s Conjecture (A). The (7) is increasing as \(N \to \infty\). Theorem 6 is proved.

The \(\varepsilon\) and \(\psi\) are some unknown particulars for Hardy-Littlewood’s Conjecture (A).

5. Discussion.

This Goldbach’s Conjecture (A) the proof.

If \(N \to \infty\), proof \(\frac{\psi}{\varepsilon} \to 1\), Then Hardy-Littlewood’s Conjecture (A) is proved.

The others particulars of Hardy-Littlewood’s Conjecture (A) is still under discussion.

Reference material: