Proof of Goldbach's Conjecture

"Any even integer greater than 2 can be written as the sum of two primes."

C. Pokorski

May 26, 2024

Abstract

This document proposes a proof of the Goldbach conjecture (1742). The approach consists of reformulating the conjecture to make it more accessible and exploiting the properties of prime numbers and their relationship to integers through their decompositions.

Intermediate Lemmas

Lemma 1. Let n be a composite positive integer and P be the set of prime numbers less than or equal to $n/2$. Then P contains all the prime factors of n, including $n/2$ if n is even.

Proof. Let n be a composite positive integer. By the prime factorization theorem, n can be uniquely factored into a product of primes:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers.

Suppose there is a prime factor p_i of n that is not in P. Then $p_i > n/2$.

If $p_i > n/2$, then p_i must be the largest prime factor of n. This means that the product of the other prime factors (if any) must be less than or equal to $n/2$, because $n = p_i \cdot (\text{product of other factors})$.

However, $p_i \cdot (\text{product of other factors}) \leq p_i \cdot (n/p_i) = n$ implies that the other factors must be less than or equal to $n/p_i \leq n/2$. This is a contradiction because $p_i > n/2$.

So all prime factors of n must be in P, including $n/2$ if n is even. □

Lemma 2. Let n be a composite positive integer and p a prime such that $n-p$ is also composite. Then n and $n-p$ share at least one prime factor distinct from p.

Proof. Let n be a composite positive integer and p a prime such that $n-p$ is also composite.

Since $n - p$ is composite, it has at least one prime factor q distinct from p.
Since q divides $n - p$, there exists an integer k such that $n - p = qk$.
We then have $n = p + qk$. Since q divides qk, q must also divide n.
Therefore, q is a prime factor of n distinct from p.
Thus, n and $n - p$ share at least one prime factor distinct from p. □

Lemma 3. Let n be a composite positive integer and P a set of primes such that for each prime factor q of n, there exists a $p \in P$ such that $\gcd(n, n - p)$ includes q as a factor. Then the product $\prod_{p \in P} \gcd(n, n-p)$ covers all the prime factors of n exactly once.

Proof. To prove this lemma, we need to show that for each prime factor q of n, there exists exactly one $p \in P$ such that q is a factor of $\gcd(n, n - p)$.

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime factorization of n, where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers.

By hypothesis, for each prime factor $q_i = p_i$ of n, there exists a $p \in P$ such that $\gcd(n, n - p) \neq 1$. This means p_i must divide $\gcd(n, n - p)$.

Suppose there are two distinct primes p and p' in P such that p_i divides both $\gcd(n, n - p)$ and $\gcd(n, n - p')$. This would imply:

$$p_i \mid (n - p) \quad \text{and} \quad p_i \mid (n - p')$$

Consequently, p_i must divide the difference:

$$(n - p) - (n - p') = p' - p$$

Since p and p' are distinct primes, $p' - p$ is not divisible by any prime factor of n unless $p' - p = 0$, which contradicts $p \neq p'$. Therefore, for each prime factor p_i of n, there can be at most one $p \in P$ such that p_i divides $\gcd(n, n - p)$.

We have established that each prime factor p_i of n corresponds to exactly one $p \in P$ where $p_i \mid \gcd(n, n - p)$. Therefore, the product $\prod_{p \in P} \gcd(n, n - p)$ will include all prime factors of n exactly once. □

Lemma 4. The following two conjectures are equivalent:

- Goldbach's Conjecture: Any even number greater than 2 can be expressed as the sum of two primes.
- Reformulation: For any even number n greater than 2, there exists at least one prime p such that $n - p$ is also prime.

Proof. **Direction: From "Goldbach's Conjecture" to "Reformulation"**

Suppose Goldbach's conjecture is true. Then, for any even number n greater than 2, there exist prime numbers p and q such that $n = p+q$. Let $q = n-p$. By definition of p and q as prime numbers, $n - p$ is prime since it's simply q under another designation. So, for every even n and every choice of p, if $p + q = n$ with q prime, then $n - p$ is also prime. This shows that if Goldbach's conjecture is true, then so is the reformulation.

Direction: From "Reformulation" to "Goldbach's Conjecture"

Conversely, suppose the reformulation is true. This means that for any even number n greater than 2, we can find a prime number p such that $n-p$ is also prime; let's denote this second prime by q. Then $n = p + (n-p) = p + q$, where p and q are primes. This shows that if the reformulation is true, then so is Goldbach's conjecture. □

Main Theorem

Theorem 1. For any even number n greater than 2, there exists at least one prime number p such that $n-p$ is also a prime number.

Proof. We will use a proof by contradiction.

Assume for contradiction that there exists an even number n greater than 2 such that for every prime number $p \leq n/2$, $n-p$ is composite.

Prime Set P: Let P be the set of all primes $p \leq n/2$. By our assumption, for each $p \in P$, $n-p$ is composite.

Shared Prime Factors: By Lemma 2, for each $p \in P$, n and $n-p$ share at least one prime factor distinct from p.

Prime Factorization of n: Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime factorization of n, where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers.

Coverage by P: Since P contains all primes less than or equal to $n/2$ and by Lemma 1, P includes all prime factors of n.

Multiplication of gcd **Values:** For each $p \in P$, consider the $\gcd(n, n-p)$. Since $n-p$ is composite, $\gcd(n, n-p)$ must be greater than 1 and must include a prime factor of n.

Contradiction: Now consider $\prod_{p \in P} \gcd(n, n-p)$. This product should cover all the prime factors of n exactly once because each $\gcd(n, n-p)$ will introduce at least one prime factor of n. However, if $n-p$ is composite for all $p \in P$, then the prime factors of n would need to repeatedly appear in the gcd terms across different $p \in P$.

This scenario cannot occur because it would require the number of distinct prime factors of n to be greater than the number of primes $\leq n/2$, which contradicts the fixed number of prime factors of n.

Therefore, our initial assumption is false. Hence, there must be at least one prime p such that $n-p$ is also prime for any even number n greater than 2. □

Information

Document version: 1.2, May 2024
Contact: cpokorski.fr@gmail.com