Goldbach's Conjecture

Ritvi Singh D/O Mr. Jasveer Singh
Student of B.Sc (Final year),
Govt. R.D. Girls College
Bharatpur, Rajasthan, India

Goldbach's conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states:
Every even integer greater than 2 can be expressed as sum of two primes

Proof: We can prove above conjecture with the help of mathematical induction
Let P(n) be the statement that “every even integer greater than 2 can be expressed as sum of two primes”
i.e. every number of form 2n, n≥2 can be expressed as sum of two primes

We have,
P(2) = 2(2) = 4 = 2 + 2
⇒ 4 can be expressed as sum of two primes (2 and 2)
⇒ P(2) is true
Let P(m) be true then
P(m) = 2m = P₁ + P₂  ......................(i)
Where P₁ and P₂ are primes
Now, we shall show that P(m+1) is true
For which we have to show that 2(m+1) can be expressed as sum of two primes
We have,
P(m+1) = 2(m+1) = 2m + 2
⇒ 2(m+1) = P₁ + P₂ + 2  ......................(ii)
In order to show that 2(m+1) is sum of two primes we need to prove that either of the following possibility holds true:
• Since P₁ is prime so it is sufficient to prove that (P₂+2) is prime
• (P₁+1) and (P₂+2) both are prime
• If both the above possibilities do not holds good then we can show that if P₃ is any prime less (or greater) than P₁ then there exist a prime P₄ such that P₃ + P₄ = 2(m+1)

Now using equation (ii)
2(m+1) = P₁ + P₂ + 2
\[
\frac{2}{a} \left( m \right) = \frac{P₁}{a} + \frac{P₂+2}{a}  \]
Where a is any arbitrary number less than 2(m+1)
Since, 2(m+1)>each term of R.H.S
⇒ factors of any term of RHS if exists will be smaller than 2(m+1)
Now there are two types of numbers smaller than 2(m+1):
• Numbers which divides 2(m+1)
• Numbers which do not divides 2(m+1)

Thus there arises following two cases:
• a is any arbitrary number which divides 2(m+1)
• a is any arbitrary number which do not divides 2(m+1)

Case – 1: when a is any arbitrary number which divides 2(m+1)
Suppose a divides 2(m+1), q times then
\[
\frac{2}{a} \left( m \right) = q  \]
......................(iv)
Where \( q \) is any natural number

Now, \( P_1 \) is prime

\[ \Rightarrow a \text{ do not divide } P_1 \]

Suppose \( a \) divides \( P_1 \) \( u \) times and leaves \( r_1 \) as remainder then,

\[ P_1 = ua + r_1 \]

\[ \frac{P_1}{a} = \frac{ua + r_1}{a} \] ........................ (v)

Substituting value of equation (iv) and (v) in (iii)

\[ qa = \frac{ua + r_1}{a} + P_2 + 2 \]

\[ qa = ua + r_1 + P_2 + 2 \]

\[ (q-u)a - r_1 = P_2 + 2 \]

\[ (q-u)a + r = P_2 + 2 \]

\[ Z_a + r = P_2 + 2 \] ........................ (vi)

Where \( z = (q-u-1) \)

And \( r = a - r_1 \)

Then by division algorithm we can say that \( (P_2 + 2) \) is not divided by \( a \) if \( z \) is whole number and \( r < a \)

Now, we will prove that \( z \) is whole number

Clearly,

\[ 2(m+1) > P_1 > 0 \]

\[ \Rightarrow \frac{qa}{a} > \frac{ua + r_1}{a} \]

\[ \Rightarrow (q-u) > \frac{r_1}{a} \]

Also, \( r_1 < a \)

\[ \Rightarrow \frac{r_1}{a} < 1 \]

\[ \Rightarrow (q-u) > 1 \]

\[ \Rightarrow (q-u-1) \geq 0 \] ................................. (vii)

Also, \( q, u, 1 \) all are whole numbers so their difference will also be a whole number

Thus, \( z = (q-u-1) \) is whole number..........................(viii)

Again, \( r = (a - r_1) \)

Where \( 0 < r_1 < a \)

\[ \Rightarrow a - r_1 < a \]

\[ \Rightarrow r < a \] .............................. (ix)

Thus from equation (vi), (viii) and (ix) we can say that \( a(P_2 + 2) \) is not divided by \( a \)

Note : (Here \( a \neq 1 \). As,

\[ (P_2 + 2) = za + r \] where \( 0 < r < a \)

Now if \( a = 1 \) \( \Rightarrow r = 0 \)

\[ \Rightarrow P_2 + 2 = za \]

\[ \Rightarrow P_2 + 2 \] is divided by \( a \)

Result of case I : \( (P_2 + 2) \) is not divided by any number (other than 1) which divides \( 2(m+1) \)

Case II :When \( a \) is any arbitrary number which do not divides \( 2(m+1) \)

Since \( a \) do not divides \( 2(m+1) \) then by division algorithm we can say that

\[ 2(m+1) = sa + r_2 \] ...........................(x)

Where \( s \) is any whole number

And \( r_2 < a \)

Again \( P_1 \) is prime thus \( P_1 \) is not divided by \( a \)

Thus, \( P_1 = ta + r_3 \) ............................... (xi)
Where \( t \) is any whole number
And \( r_4 \leq a \)
Now, substituting values from equation (x) and (xi) in equation (iii) we get,
\[
\frac{sa + r_2}{a} = \frac{ta + r_3}{a} + \frac{P_2 + 2}{a} \\
\Rightarrow \frac{(s-t)a + (r_2 - r_3)}{a} = \frac{P_2 + 2}{a} \\
\Rightarrow \frac{(s-t) + \frac{r_2 - r_3}{a}}{a} = \frac{P_2 + 2}{a} \\
\Rightarrow (s-t)a + (r_2 - r_3) = P_2 + 2 \\
\Rightarrow wa + r_4 = P_2 + 2 \\
\Rightarrow wa + r_4 = P_2 + 2 \\
\]
........................................(xii)

Since \( s \) and \( t \) are whole numbers this implies \((s-t)=w\) is also a whole number
Now there arises following two cases

1. **If \( w=0 \) then** ,
\[
0(a) + (r_2 - r_3) = P_2 + 2 \\
r_2 - r_3 = P_2 + 2 \\
\]
Also,
\[
0 < r_2, r_3 < a \\
\Rightarrow -a < r_2 - r_3 < a \\
\Rightarrow -a < r_4 < a \\
\]
Now on the basis of nature of \( r_4 \) there arises following conditions:

- **\(-a < r_4 < 0\)**
  In this case equation (xiii) implies \( P_2 + 2 \) is negative integer but we know that \( P_2 + 2 \) is positive
  Hence, if \( w=0 \) then \( r_4 \) will never be less than zero .

- **\( r_4 = 0 \)**
  This is also not possible because if \( r_4 = 0 \) then from equation (xiii) \( P_2 + 2 = 0 \) but \( P_2 + 2 \) is positive. Hence \( r_4 \) will never be zero when \( w=0 \)

- **\( 0 < r_4 < a \)**
  In this case by equation (xiii) we can say that
  \[
r_4 = \frac{P_2 + 2}{a} \\
\]
  Since \( r_4 < a \)
  \[
0 < \frac{r_4}{a} < 1 \\
0 < \frac{P_2 + 2}{a} < 1 \\
\]
  \( P_2 + 2 \) is not divided by \( a \) \( \Rightarrow \frac{P_2 + 2}{a} \) is a fraction smaller than 1

**Result:** In this case \( 2(m+1) \) can be expressed as sum of two primes \( P_1 \) and \( P_2 + 2 \)

2. **If \( w>0 \)**
Now there arises following conditions on the basis of nature of \( r_4 \)

- **\(-a < r_4 < 0\)**
  Now in this condition we need to check whether \( P_2 + 2 \) is divided by \( a \) or not
  From equation (xii)
  \[
wa + r_4 = P_2 + 2 \\
wa + a + r_4 = P_2 + 2 \\
(w-1)a + (a+r_4) = P_2 + 2 \\
\]

DOI: 10.9790/5728-12060113117  www.iosrjournals.org  115 | Page
(w-1)a+r_5=P_2+2
Since w≥1
⇒(w-1)≥0
Hence, (w-1) is whole number ............(xiii)
Also,
-a<r_4<0 
-a+a<r_4+a<0+a
0<r_5<a ............. (xiv)
Thus, from equation (xiii) and (xiv) we can say that (P_2+2) is not divided by a

Thus in this case 2(m+1) can be expressed as sum of two primes P_1 and (P_2+2)
• 0<r_7<\ a
Again from equation (xii)
w_5a+r_7=P_2+2
Where w is whole number
And r_7<\ a
Then clearly from division algorithm we can say P_2+2 is not divided by a

Result: In this case 2(m+1) can be expressed as sum of two primes P_1 and (P_2+2)
• r_7=0

Since r_7 and r_5 are not zero this implies r_4 will be zero only and only if r_2 = r_3
Then in this case equation (xii) becomes
(s-t)a=P_2+2 
If (s-t)=1
⇒a=P_2+2 
⇒P_2+2 is divided by itself
Also (s-t)≠1 then from equation (xii) we can say that P_2+2 is not prime. But it does not mean that 2(m+1) cannot be expressed as sum of two primes as now also we have two more possibilities as told in starting of proof

[Which were 2. possibility: 2(m+1) is sum (P_1+1) and (P_2+1) then we will show that P_1+1 and (P_2+1) are primes
3. possibility: 2(m+1) is sum of P_3 and P_4 where P_3 is an prime less(or greater) than P_1 and P_4 is any natural number and then we will prove that P_4 is also prime]
Now we will check whether the second possibility holds true
2(m+1)=(P_1+1)+(P_2+1)
Now we will prove that (P_1+1) and (P_2+1) both are prime
But, we know that all prime numbers except 2 are odd
Also P_2 and P_2 both are prime
⇒P_1 and P_2 both are odd
⇒ (P_1+1) and (P_2+1) are even
⇒(P_1+1) and (P_2+1) can be prime only and only if (P_1+1) and (P_2+1) both are separately equal to 2
Thus this possibility holds true only and only if 2(m+1)=(P_1+1)+(P_2+1)
\[2(m+1)=2\]
\[2(m+1)=4\]
Now we will check whether our last possibility holds true or not. For which let us consider a prime P_3 and a
natural number P_4 such that P_3 + P_4= 2(m+1)............ (xv)
Since P_3 is prime, hence it will not be divided by any a(other than 1 and itself)
Thus we can write P_3 = va +r_6 (using division algorithm)........... (xvi)
Also 2(m+1) = sa +r_2............... (xvii)
(as we have taken the case that 2(m+1) is not divided by a)
Now substituting value of P_3 and 2(m+1) in equation (xv) we get
\[sa+ r_2=va+r_6+P_4\]
\[(s-v)a+(r_2-r_6)=P_4\]
w_5a + r_7 = P_4
Again there arises following three conditions on the basis of nature of r_7
• a<r_7<0
• 0<r_7<\ a
• r_7=0

DOI: 10.9790/5728-120601113117  www.iosrjournals.org  116 | Page
Again for first two conditions we can prove \( P_4 \) is prime in similar manner as we have proved for \( P_2 + 2 \)

But, if \( r_5 = 0 \) then,

\[
(r_2 - r_6) = 0
\]

Since \( r_2 \) and \( r_6 \) are not zero

\[
\Rightarrow r_2 = r_6
\]

Where \( r_6 \) is remainder when \( P_3 \) is divided by \( a \)

But, \( r_5 = r_3 \)

Where \( r_3 \) is remainder when \( P_1 \) is divided by \( a \)

\[
\Rightarrow r_3 = r_6
\]

Now we will repeat above process finite number of times then we will definitely get a prime \( P_n \) which when divided by \( a \) leaves a remainder \( r_n \) such that \( r_2 \neq r_6 \)

Because if \( r_2 = r_6 \) then it means that on dividing each prime number by arbitrary \( a \) we get same remainder but it is not possible.

If it would have been possible then difference between any two prime numbers will be multiple of \( a \) but we know that prime numbers do not follow any such law. For example 5, 13 and 23 are primes but difference between any two is not divided by arbitrary \( a \) as

\[
13 - 5 = 8
\]

\[
23 - 13 = 10
\]

But there exist no arbitrary \( a \) which divides both 8 and 10

**Note:** Here \( a \neq 2 \) as we have taken the case that \( a \) do not divides \( 2(m+1) \)

Hence we can say that we can obtain a prime \( P_n \) such that \( 2(m+1) = P_n + P_{n+1} \)

And \( 2(m+1) \) and \( P_n \) when divided by \( a \) do not leaves same remainder

i.e. \( r_2 \neq r_6 \) where \( r_2 \) is remainder when \( 2(m+1) \) is divided by \( a \)

And \( r_6 \) is remainder when \( P_n \) is divided by \( a \)

\[
\frac{2(m+1)}{a} = \frac{P_n + P_{n+1}}{a}
\]

\[
\Rightarrow \frac{2a + r_2}{a} = \frac{xa + r_n}{a} + \frac{1}{a}
\]

\[
\Rightarrow \frac{r_2 - r_n}{a} = \frac{P_n + 1}{a}
\]

(\( s - x \))\( a + \frac{r_2 - r_n}{a} = \frac{P_n + 1}{a} \)

Now, there arise only two cases which are as under:

- (s-x)=0 \quad \text{In this case} P_{n+1} \text{ will be prime we can prove it in similar manner as we have proved for } P_2 + 2
- (s-x)\#0 \quad \text{then again there arises two conditions}

1. \( 0 < r_2 - r_n < a \)
2. \(-a < r_2 - r_n < 0\)

In both cases we can prove that \( P_{n+1} \) is prime in similar manner as we have proved for \( P_2 + 2 \)

\text{[here (iii) condition } r_2 - r_n = 0 \text{ do not appears as } r_2 \neq r_n \text{ also } r_2, r_n \neq 0)\]

Hence we can say that in this condition also \( 2(m+1) \) can be expressed as sum of two primes

Combining results of case I and results of all the conditions of case II we can say that in each and every condition we can express \( 2(m+1) \) as a sum of two primes

Hence \( P(m+1) \) is also true

Thus by principle of mathematical induction we can prove that every even integer greater than two can be expressed as sum of two primes