Goldbach Conjecture: An invitation to Number Theory
by
R. Balasubramanian
Institute of Mathematical Sciences, Chennai
balu@imsc.res.in

Goldbach Conjecture: An invitation to Number Theory
by
R. Balasubramanian
Institute of Mathematical Sciences, Chennai
balu@imsc.res.in

Definition and basic properties of prime numbers

If *n* has no divisor other than 1 and *n*, then *n* is called *prime.*

$$2, 3, 5, 7, 11, 13, \cdots$$

Theorem (1. Euclid)

If p is a prime and p divides ab, then p divides a or p divides b.

Definition and basic properties of prime numbers

If n has no divisor other than 1 and n, then n is called *prime.*

$$2, 3, 5, 7, 11, 13, \cdots$$

Theorem (1. Euclid)

If p is a prime and p divides ab, then p divides a or p divides b.

The interest around 16th century was more on the properties of individual primes.

Definition and basic properties of prime numbers

If n has no divisor other than 1 and n, then n is called *prime.*

$$2, 3, 5, 7, 11, 13, \cdots$$

Theorem (1. Euclid)

If p is a prime and p divides ab, then p divides a or p divides b.

The interest around 16th century was more on the properties of individual primes.Example are

Theorem (2.)

If p does not divide a, then $a^{p-1} - 1$ *is divisible by p.*

Definition and basic properties of prime numbers

If n has no divisor other than 1 and n, then n is called *prime.*

$$2, 3, 5, 7, 11, 13, \cdots$$

Theorem (1. Euclid)

If p is a prime and p divides ab, then p divides a or p divides b.

The interest around 16th century was more on the properties of individual primes.Example are

Theorem (2.)

If p does not divide a, then $a^{p-1} - 1$ is divisible by p.

Before stating other theorem, it is better to introduce a notation (of congruance) due to Gauss.

We say $a \equiv b \pmod{m}$ if the diffrence between a and b is divisible by m.

We say $a \equiv b \pmod{m}$ if the diffrence between a and b is divisible by m.

In the notation, Theorem 2 can be written as

Theorem (3.)

If $a \not\equiv 0 \pmod{p}$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

We say $a \equiv b \pmod{m}$ if the diffrence between a and b is divisible by m.

In the notation, Theorem 2 can be written as

Theorem (3.)

If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

This was generalised by Euler; A special case of Euler's theorem is

Theorem (4.)

If p and q are distinct primes and p and q do not divide a, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

We say $a \equiv b \pmod{m}$ if the diffrence between a and b is divisible by m.

In the notation, Theorem 2 can be written as

Theorem (3.)

If $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

This was generalised by Euler; A special case of Euler's theorem is

Theorem (4.)

If p and q are distinct primes and p and q do not divide a, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Remark

The most popular public key cryptosysten, called RSA (due to Rivest, Shamir and Adleman) is based on Theorem 4.

Some more properties of primes

Theorem (5. Euler)

If $a \not\equiv 0 \pmod{p}$, *then*

$$a^{\frac{p-1}{2}} \begin{cases} \equiv 1 \pmod{p} \text{ if } a \equiv x^2 \pmod{p} \text{ for some } x, \\ \equiv -1 \pmod{p} \text{otherwise.} \end{cases}$$

Some more properties of primes

Theorem (5. Euler)

If $a \not\equiv 0 \pmod{p}$, *then*

$$a^{\frac{p-1}{2}} \begin{cases} \equiv 1 \pmod{p} \text{ if } a \equiv x^2 \pmod{p} \text{ for some } x, \\ \equiv -1 \pmod{p} \text{otherwise.} \end{cases}$$

An important theorem, connecting the behaviour of two primes p and q is quadratic reciprocity law (due to Gauss).

Theorem (Wilson)

$(p-1)! \equiv -1 \pmod{p}$.

Number of primes $= \infty$.

The interest shifted in the late 17th century, when number theorist started studying the distribution of prime numbers.

Number of primes $= \infty$.

The interest shifted in the late 17th century, when number theorist started studying the distribution of prime numbers.We start with

Theorem (6. Euclid)

These are infinitely many prime numbers.

Number of primes $= \infty$.

The interest shifted in the late 17th century, when number theorist started studying the distribution of prime numbers.We start with

Theorem (6. Euclid)

These are infinitely many prime numbers.

The proof, given by Euclid is a “proof from the book”.

Number of primes $= \infty$.

The interest shifted in the late 17th century, when number theorist started studying the distribution of prime numbers.We start with

Theorem (6. Euclid)

These are infinitely many prime numbers.

The proof, given by Euclid is a “proof from the book”.

Proof.

If $p_1, p_2, \cdots p_r$ are the only primes, consider the number

$$N = p_1, p_2, \cdots p_r + 1.$$

Number of primes $= \infty$.

The interest shifted in the late 17th century, when number theorist started studying the distribution of prime numbers.We start with

Theorem (6. Euclid)

These are infinitely many prime numbers.

The proof, given by Euclid is a "proof from the book".

Proof.

If $p_1, p_2, \cdots p_r$ are the only primes, consider the number

$$N = p_1, p_2, \cdots p_r + 1.$$

Since every number has a prime factor, N also has a prime factor and the primes $p_1, p_2, \cdots p_r$ can not be prime factors of N. Hence there exists atleast one more prime. $\square$

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Consider for any real number s,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots + \right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots \right)\cdots$$

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Consider for any real number s,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots + \right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots \right)\cdots$$

When we multiply out, we get terms of the form $\frac{1}{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p^{\alpha_r n})^s}$.

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Consider for any real number s,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots + \right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right)\cdots$$

When we multiply out, we get terms of the form $\frac{1}{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p^{\alpha_r n})^s}$.This means, because of unique factorization, the product is a sum of the elements of the form $\frac{1}{n^s}$ each appearing once.

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Consider for any real number s,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots + \right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots\right)\cdots$$

When we multiply out, we get terms of the form $\frac{1}{\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p^{\alpha_{rn}}\right)^s}$. This means, because of unique factorization, the product is a sum of the elements of the form $\frac{1}{n^s}$ each appearing once. This proves

Theorem (7. Euler's identity)

$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod(1 - \frac{1}{p^s})^{-1}$ $(= \zeta(s))$ *if* $s > 1$.

Euler's proof: Number of primes $= \infty$.

There was no progress on the problem of studying the distribution of primes till the time of Euler. Euler provided a different proof of the fact that there are infinitely many primes.

Consider for any real number s,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots + \right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots \right)\cdots$$

When we multiply out, we get terms of the form $\frac{1}{(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p^{\alpha_r n})^s}$.This means, because of unique factorization, the product is a sum of the elements of the form $\frac{1}{n^s}$ each appearing once. This proves

Theorem (7. Euler's identity)

$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod(1 - \frac{1}{p^s})^{-1}$ $(= \zeta(s))$ *if* $s > 1$.

Euler's proof contd.

We can now deduce Th.6 from Th.7: For example, by putting $s = 2$, we get
$\frac{\pi^2}{6} = \prod_p (1 - \frac{1}{p^2})^{-1}$ and hence it can not be a finite product.

Euler's proof contd.

We can now deduce Th.6 from Th.7: For example, by putting $s = 2$, we get
$\frac{\pi^2}{6} = \prod_p (1 - \frac{1}{p^2})^{-1}$ and hence it can not be a finite product.

Better still: Put $s = 1 + \epsilon$, and $\epsilon \to 0$.
Then

$$\infty = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p}\right)^{-1}$$

and hence it is not a finite product.

Euler's proof contd.

We can now deduce Th.6 from Th.7: For example, by putting $s = 2$, we get
$\frac{\pi^2}{6} = \prod_p (1 - \frac{1}{p^2})^{-1}$ and hence it can not be a finite product.

Better still: Put $s = 1 + \epsilon$, and $\epsilon \to 0$.
Then

$$\infty = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p}\right)^{-1}$$

and hence it is not a finite product.
Incidentally this proves that

$$\sum_p \frac{1}{p} = \infty.$$

Hence there are "more" primes than squares.

Number of primes: Conjectures of Gauss

Now a natural question is: How many primes are there upto N?

$$\pi(N) = \# \text{ of primes up to } N.$$

Number of primes: Conjectures of Gauss

Now a natural question is: How many primes are there upto N?

$$\pi(N) = \# \text{ of primes up to } N.$$

It was conjectured, both on numerical evidences and probablistic considerations, that $\pi(N)$ is around $\frac{N}{\log N}$. (Incidentally, we do not know any exact formula for $\pi(N)$ and we do not even expect to have one).

Number of primes: Conjectures of Gauss

Now a natural question is: How many primes are there upto N?

$$\pi(N) = \# \text{ of primes up to } N.$$

It was conjectured, both on numerical evidences and probablistic considerations, that $\pi(N)$ is around $\frac{N}{\log\ N}$. (Incidentally, we do not know any exact formula for $\pi(N)$ and we do not even expect to have one).

Gauss felt that $\frac{N}{\log N}$ is a good approximation to $\pi(N)$ and $\mathrm{li}(N) = \int_2^N \frac{dt}{\log t}$ is a better approximation.

Number of primes: Conjectures of Gauss

Now a natural question is: How many primes are there upto N?

$$\pi(N) = \# \text{ of primes up to } N.$$

It was conjectured, both on numerical evidences and probablistic considerations, that $\pi(N)$ is around $\frac{N}{\log N}$. (Incidentally, we do not know any exact formula for $\pi(N)$ and we do not even expect to have one).

Gauss felt that $\frac{N}{\log N}$ is a good approximation to $\pi(N)$ and $\mathrm{li}(N) = \int_2^N \frac{dt}{\log t}$ is a better approximation.

(He even postulated that $\pi(N) < \mathrm{li}(N)$ for all N. This was proved false by J.E. Littlewood).

Number of primes: Conjectures of Gauss

Now a natural question is: How many primes are there upto N?

$$\pi(N) = \#\text{ of primes up to } N.$$

It was conjectured, both on numerical evidences and probablistic considerations, that $\pi(N)$ is around $\frac{N}{\log\ N}$. (Incidentally, we do not know any exact formula for $\pi(N)$ and we do not even expect to have one).

Gauss felt that $\frac{N}{\log N}$ is a good approximation to $\pi(N)$ and $\mathrm{li}(N) = \int_2^N \frac{dt}{\log t}$ is a better approximation.
(He even postulated that $\pi(N) < \mathrm{li}(N)$ for all N. This was proved false by J.E. Littlewood).
Since $\mathrm{li}(N)$ is a "difficult" function to handle, one considers

$$\psi(N) = \text{ the primes} p \text{ upto } N \text{ counted with a weight by } \log p.$$

Then $\pi(N) \sim \mathrm{li}(N)$ is same $\psi(N) \sim N$. This statement is called Prime Number Theorem.

Work of Riemann

Riemann initiated a study of Prime Number theorem.

Work of Riemann

Riemann initiated a study of Prime Number theorem.

He started with the Euler's identity (for a complex variables)

- continued $\zeta(s)$ meromorphically throughout the complex plane

Work of Riemann

Riemann initiated a study of Prime Number theorem.

He started with the Euler's identity (for a complex variables)

- continued $\zeta(s)$ meromorphically throughout the complex plane
- and gave a proof of prime number theorem (with a minor gap in the proof).

Work of Riemann

Riemann initiated a study of Prime Number theorem.

He started with the Euler's identity (for a complex variables)

- continued $\zeta(s)$ meromorphically throughout the complex plane
- and gave a proof of prime number theorem (with a minor gap in the proof).

Incidentally this is the only article he work on Prime Number Theory and all the later developments on Prime Number Theory crucially depend on this work.

Work of Riemann

Riemann initiated a study of Prime Number theorem.

He started with the Euler's identity (for a complex variables)

- continued $\zeta(s)$ meromorphically throughout the complex plane
- and gave a proof of prime number theorem (with a minor gap in the proof).

Incidentally this is the only article he work on Prime Number Theory and all the later developments on Prime Number Theory crucially depend on this work.

The minor gap was fixed by Jacques Hadamard and de la Valée Poussin in 1898 - 1899 independently and Prime Number was proved.

Primes in an arithmetic progression

Let $A = (a, a + d, a + 2d, a + 3d, \cdots)$ be an arithmetic progression.

Question

Whether there are infinitely many primes in A?

Primes in an arithmetic progression

Let $A = (a, a + d, a + 2d, a + 3d, \cdots)$ be an arithmetic progression.

Question

Whether there are infinitely many primes in A?

Obvious constraints

- $A = \{9 \pmod{15}\} = (9, 24, 39, 54, 69, \cdots)$. Here every number is divisible by 3 and hence it contains no primes.
- $A = \{3 \pmod{15}\}$ has exactly one prime.

Primes in an arithmetic progression

Let $A = (a, a + d, a + 2d, a + 3d, \cdots)$ be an arithmetic progression.

Question

Whether there are infinitely many primes in A?

Obvious constraints

- $A = \{9 \pmod{15}\} = (9, 24, 39, 54, 69, \cdots)$. Here every number is divisible by 3 and hence it contains no primes.
- $A = \{3 \pmod{15}\}$ has exactly one prime.

If we ignore such exceptions, then every A has infinitely many primes.

Theorem (Dirichlet)

If a and d have no common factors, then $A = \{a \pmod{d}$ *has infinitely many primes.*

Theorem (Dirichlet)

If a and d have no common factors, then $A = \{a \pmod d$ *has infinitely many primes.*

Infact if $d \leq (\log x)^{100}$, then the number of primes $\leq x$, which are in A is around

$$\frac{1}{\phi(d)} \frac{x}{\log\ x},$$

where $\phi(d)$ is the Euler's totient function, defined as the number of integers less than d, having no common factor with d.

Theorem (Dirichlet)

If a and d have no common factors, then $A = \{a \pmod d\}$ has infinitely many primes.

Infact if $d \leq (\log x)^{100}$, then the number of primes $\leq x$, which are in A is around

$$\frac{1}{\phi(d)} \frac{x}{\log\ x},$$

where $\phi(d)$ is the Euler's totient function, defined as the number of integers less than d, having no common factor with d.

The result is proved using the analytic properties of the functions of the following kind.

$$\sum_n \frac{\chi(n)}{n^s},$$

where $\chi : \mathbb{Z} \to \mathbb{C}^*$ is a periodic function with period d and satisfies $\chi(nm) = \chi(n)\chi(m)$.

Additive Number theory

One would like to know whether an integer can be written as a sum of integers of special form and if so, how many summands are needed?

- (Langrange's theorem): Every integer can be written as a sum of atmost 4 squares.

Additive Number theory

One would like to know whether an integer can be written as a sum of integers of special form and if so, how many summands are needed?

- (Langrange's theorem): Every integer can be written as a sum of atmost 4 squares.
  Eg:

$$\begin{aligned} 89 &= 9^2 + 2^2 + 2^2 \\ 103 &= 10^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$

Additive Number theory

One would like to know whether an integer can be written as a sum of integers of special form and if so, how many summands are needed?

- (Langrange's theorem): Every integer can be written as a sum of atmost 4 squares.
  Eg:
  $$\begin{aligned} 89 &= 9^2 + 2^2 + 2^2 \\ 103 &= 10^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$
- (Fermat)(a) If a prime p is of the form $4k + 1$, then it can be written as $a^2 + b^2$.
  (b)If a prime p is of the form $4k + 3$, then it can not be written as $a^2 + b^2$.

One would like to know whether an integer can be written as a sum of integers of special form and if so, how many summands are needed?

- (Langrange's theorem): Every integer can be written as a sum of atmost 4 squares.
  Eg:
  $$\begin{aligned} 89 &= 9^2 + 2^2 + 2^2 \\ 103 &= 10^2 + 1^2 + 1^2 + 1^2 \end{aligned}$$
- (Fermat)(a) If a prime p is of the form $4k+1$, then it can be written as $a^2 + b^2$.
  (b)If a prime p is of the form $4k+3$, then it can not be written as $a^2 + b^2$.

Proof of (b) is easy. First note that every square is of the form $4k$ or $4k+1$. Hence sum of two squares can only be of the form $4k$ or $4k+1$ or $4k+2$.

Theorem

A positive integer n can be written as $x^2 + y^2$*, if and only if*

$$n = 2^a p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} q_1^{2c_1} \cdots q_2^{2c_2} \cdots q_s^{c_s},$$

where p's are primes of the form $4k+1$ *and q's are primes of the form* $4k+3$.

In other words, in the prime factorisation of n, 2 and p can appear to any power. But q's appear only with even power.

Theorem

A positive integer n can be written as $x^2 + y^2$, if and only if

$$n = 2^a p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} q_1^{2c_1} \cdots q_2^{2c_2} \cdots q_s^{c_s},$$

where p's are primes of the form $4k + 1$ and q's are primes of the form $4k + 3$.

In other words, in the prime factorisation of n, 2 and p can appear to any power. But q's appear only with even power.

Theorem

If an integer n is not of the form $4^k(8l + 7)$, then it can be written as $a^2 + b^2 + c^2$.

Goldbach Conjecture

Goldbach's conjecture is an interesting example of a problem in additive number theory, involving prime numbers.

Conjecture

Every even number ≥ 6 *is a sum of two prime numbers;*

$$2n = p_1 + p_2.$$

Goldbach Conjecture

Goldbach's conjecture is an interesting example of a problem in additive number theory, involving prime numbers.

Conjecture

Every even number ≥ 6 *is a sum of two prime numbers;*

$$2n = p_1 + p_2.$$

This conjecture (with a few related conjectures) appeared in a letter by Goldbach to Euler on June 17, 1742.

Goldbach Conjecture

Goldbach's conjecture is an interesting example of a problem in additive number theory, involving prime numbers.

Conjecture

Every even number ≥ 6 *is a sum of two prime numbers;*

$$2n = p_1 + p_2.$$

This conjecture (with a few related conjectures) appeared in a letter by Goldbach to Euler on June 17, 1742.

It seems that this conjecture was observed by Descartes even earlier. Still (as remarked by Erdös), we shall continue to call this Goldbach's conjecture.

Probabilistic evidence

Given any n consider all the solution of the equation

$$2n = a + b \tag{1}$$

with $a, b \geq \frac{n}{2}$. There are n such solution.

Probabilistic evidence

Given any n consider all the solution of the equation

$$2n = a + b \tag{1}$$

with $a, b \geq \frac{n}{2}$. There are n such solution.

The probability that a is prime is around $\frac{1}{\log n}$. Therefore the probabilty that both a and b are primes is around $\frac{1}{\log^2 n}$. Hence there are atleast $c\frac{n}{\log^2 n}$ solutions of (1) with both a and b primes. We need to prove that there is at least one such presentation.

Probabilistic evidence

Given any n consider all the solution of the equation

$$2n = a + b \tag{1}$$

with $a, b \geq \frac{n}{2}$. There are n such solution.

The probability that a is prime is around $\frac{1}{\log n}$. Therefore the probabilty that both a and b are primes is around $\frac{1}{\log^2 n}$. Hence there are atleast $c\frac{n}{\log^2 n}$ solutions of (1) with both a and b primes. We need to prove that there is at least one such presentation.

When we relook at the above argument, one has some misgivings. For example it shows that any odd integer can be also written as a sum of two primes. However sice primes are odd (except for one of them, an oddity), it is not possible that $2N + 1$ can be written as a sum of two primes.

Hardy and Littlewood formulated a conjecure which takes care of local obstructions and in particular gives a number of ways an integer can be written as a sum of two primes.

Numerical evidence

Jean-Marc Deshouillers; te Riele, H.J.J. and Saouter, Y. in 1998 showed that conjecture is true if $n \leq 10^{14}$.

Numerical evidence

Jean-Marc Deshouillers; te Riele, H.J.J. and Saouter, Y. in 1998 showed that conjecture is true if $n \leq 10^{14}$.

Oliveira e Silva in 2008 showed that the conjecture is true if $n \leq 12 \times 10^{17}$.

If $A, B \subset [1, N]$ we set

$$A + B = \{x \in \mathbb{Z} : x = a_1 + b_1 \text{ for some } a_1 \in A, b_1 \in B\}.$$

Methods of attack: Additive combinatorics

If $A, B \subset [1, N]$ we set

$$A + B = \{x \in \mathbb{Z} : x = a_1 + b_1 \text{ for some } a_1 \in A, b_1 \in B\}.$$

Suppose one knows the lower bound for the cardinality of A, B then one can try to get a lower bound for the cardinality of $A + B$; Particularly of one knows that if $r(n)$ is the number of ways of writing n as $a + b$, then $r^2(n)$ is small (at least on average), then $|A + B|$ becomes very large.

Methods of attack: Additive combinatorics

If $A, B \subset [1, N]$ we set

$$A + B = \{x \in \mathbb{Z} : x = a_1 + b_1 \text{ for some } a_1 \in A, b_1 \in B\}.$$

Suppose one knows the lower bound for the cardinality of A, B then one can try to get a lower bound for the cardinality of $A + B$; Particularly of one knows that if $r(n)$ is the number of ways of writing n as $a + b$, then $r^2(n)$ is small (at least on average), then $|A + B|$ becomes very large.

Given $A \subset \mathbb{N}$ we write $A(n)$ to denote the number of elements $a \in A$ with $a \leq n$.

Theorem (Mann)

If $A(n) \geq \alpha n$ and $B(n) \geq \beta n$ then

$$(A + B)(n) \geq (\alpha + \beta)n \ \ \forall n.$$

Given $A \subset \mathbb{N}$ we write $A(n)$ to denote the number of elements $a \in A$ with $a \leq n$.

Theorem (Mann)

If $A(n) \geq \alpha n$ and $B(n) \geq \beta n$ then

$$(A + B)(n) \geq (\alpha + \beta)n \ \ \forall n.$$

Using this Ramaré and Saouter showed that every even integer is a sum of at most 6 primes.

Given $A \subset \mathbb{N}$ we write $A(n)$ to denote the number of elements $a \in A$ with $a \leq n$.

Theorem (Mann)

If $A(n) \geq \alpha n$ and $B(n) \geq \beta n$ then

$$(A + B)(n) \geq (\alpha + \beta)n \ \ \forall n.$$

Using this Ramaré and Saouter showed that every even integer is a sum of at most 6 primes.

Ramaré and Saouter: Every odd inetger upto 1.13×10^{22} is a sum of 3 primes.

Methods of attack: Circle method

So far the best method of attack for Goldbach conjecture seems to be circle method.

This method was developed by Hardy and Ramanujan to get the approximate value of partition function $p(n)$.

The method has been successively used to solve the universal Waring's problem (Hardy-Littlewood, Davenport, Vinogradov, Thanigasalam, Vaughan).

Description of circle method for Goldbach problem

Let $I(N) = \int_0^1 \left(\sum_{p \le N} e^{2\pi i p\alpha} \right)^2 e^{-2\pi i N\alpha} d\alpha = \int_0^1 \sum_{p_1, p_2 \le N} e^{2\pi i (p_1 + p_2 - N)\alpha} d\alpha.$

Description of circle method for Goldbach problem

Let $I(N) = \int_0^1 \left(\sum_{p \le N} e^{2\pi i p \alpha} \right)^2 e^{-2\pi i N \alpha} d\alpha = \int_0^1 \sum_{p_1, p_2 \le N} e^{2\pi i (p_1 + p_2 - N)\alpha} d\alpha.$

Since we have

$$\int_0^1 e^{2\pi i n \alpha} d\alpha = \begin{cases} 0 \text{ if } n \neq 0, \\ 1 \text{ if } n = 0. \end{cases},$$

we have

$$I(N) = \#\{(p_1, p_2) : N = p_1 + p_2\}.$$

Description of circle method for Goldbach problem

Let $I(N) = \int_0^1 \left(\sum_{p \leq N} e^{2\pi i p\alpha} \right)^2 e^{-2\pi i N\alpha} d\alpha = \int_0^1 \sum_{p_1, p_2 \leq N} e^{2\pi i (p_1 + p_2 - N)\alpha} d\alpha.$

Since we have

$$\int_0^1 e^{2\pi i n\alpha} d\alpha = \begin{cases} 0 \text{ if } n \neq 0, \\ 1 \text{ if } n = 0. \end{cases},$$

we have

$$I(N) = \#\{(p_1, p_2) : N = p_1 + p_2\}.$$

The integrand is big when α is very close to a rational number with a small denominator and small otherwise.

Evaluation of the integral in a close neighbourhood of rational numbers with small denominator gives the contribution of the order of $\frac{N}{\log^2 N}$.

If one can prove the rest of the contribution is neglible, one has the result. This method has enabled one to prove.

- (Vinogradov 1937) $2N + 1 = p_1 + p_2 + p_3$ if $N \geq N_0$.

Evaluation of the integral in a close neighbourhood of rational numbers with small denominator gives the contribution of the order of $\frac{N}{\log^2 N}$.

If one can prove the rest of the contribution is neglible, one has the result. This method has enabled one to prove.

- (Vinogradov 1937) $2N + 1 = p_1 + p_2 + p_3$ if $N \geq N_0$.
- (Chen and Wang 1989) The value of N_0 in above theorem may be taken as 10^{43000}.

Evaluation of the integral in a close neighbourhood of rational numbers with small denominator gives the contribution of the order of $\frac{N}{\log^2 N}$.

If one can prove the rest of the contribution is neglible, one has the result. This method has enabled one to prove.

- (Vinogradov 1937) $2N + 1 = p_1 + p_2 + p_3$ if $N \geq N_0$.
- (Chen and Wang 1989) The value of N_0 in above theorem may be taken as 10^{43000}.
- (Deshouillers, Effinger, Riele, Zinoviev 1997) Assuming Generalised Riemann Hypothesis (GRH) we may take $N_0 = 3$

Evaluation of the integral in a close neighbourhood of rational numbers with small denominator gives the contribution of the order of $\frac{N}{\log^2 N}$.

If one can prove the rest of the contribution is neglible, one has the result. This method has enabled one to prove.

- (Vinogradov 1937) $2N + 1 = p_1 + p_2 + p_3$ if $N \geq N_0$.
- (Chen and Wang 1989) The value of N_0 in above theorem may be taken as 10^{43000}.
- (Deshouillers, Effinger, Riele, Zinoviev 1997) Assuming Generalised Riemann Hypothesis (GRH) we may take $N_0 = 3$

Ramaré and Saouter established that every odd integer upto 1.13×10^{22} is a sum of three primes.

Using “Sieve methods” Chen established that $2N = p_1 + n$, where p_1 is prime and n has atmost 2 prime factors.

Using “Sieve methods” Chen established that $2N = p_1 + n$, where p_1 is prime and n has atmost 2 prime factors.

K. Ramachandra showed that given a sufficiently large x, any interval $[x, x + x^{7/12}]$ contains an even integer which can be written as a sum of two primes.

Using "Sieve methods" Chen established that $2N = p_1 + n$, where p_1 is prime and n has atmost 2 prime factors.

K. Ramachandra showed that given a sufficiently large x, any interval $[x, x + x^{7/12}]$ contains an even integer which can be written as a sum of two primes.

Montgomery and Vaughan showed that the number of even natural numbers which are $\leq x$ and can not be written as a sum of two primes is at most x^{1-c}, where $c > 0$ is an absolute constant.