Mumbai Math Circle
TIFR and St. Xavier's College
email: mumbaimathcircle (at) protonmail.com
Current Webpage: www.math.tifr.res.in/~ amitava/MMC

Prime Numbers:

What are prime numbers?

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

Prime Numbers:

What are prime numbers?

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

How to check if a number is prime or not a prime ?

Prime Numbers:

What are prime numbers?

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

How to check if a number is prime or not a prime ?
How many prime numbers are there?

There are infinitely many prime numbers !

There are infinitely many prime numbers !
How to show this?
Euclid's Argument:

Euclid A Greek mathematician, often referred to as the “founder of geometry”.
He was active in Alexandria during the reign of Ptolemy I (323–283 BC). His Elements is one of the most influential works in the history of mathematics for more than 2000 years.

Euclid A Greek mathematician, often referred to as the "founder of geometry".
He was active in Alexandria during the reign of Ptolemy I (323–283 BC). His Elements is one of the most influential works in the history of mathematics for more than 2000 years.

"Euclid replied there is no royal road to geometry."

Let $L = \{p_1, p_2, \ldots, p_k\}$ be a list of primes.

Let $L = \{p_1, p_2, \ldots, p_k\}$ be a list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

Let $L = \{p_1, p_2, \ldots, p_k\}$ be a list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.

Let $L = \{p_1, p_2, \ldots, p_k\}$ be a list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.
This implies either N is a prime itself or it is divisible by a prime not in the list.

Let $L = \{p_1, p_2, \ldots, p_k\}$ be a list of primes.

$$N = p_1 p_2 p_3 \ldots p_k + 1$$

This number cannot be divided by any or the primes in the list L.
This implies either N is a prime itself or it is divisible by a prime not in the list.
This implies there is at least 1 more prime.

Fermat number

For $n = \{0, 1, 2, \ldots\}$

$$F(n) := 2^{2^n} + 1$$

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$$

Fermat number

For $n = \{0, 1, 2, \ldots\}$

$$F(n) := 2^{2^n} + 1$$

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, \ldots$$

Fermat conjectured that all Fermat numbers are prime.

Leonhard Euler in 1732 showed that

$$F(5) = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

Euler proved that every factor of $F(n)$ must have the form $k2^{n+1} + 1$.

Leonhard Euler in 1732 showed that

$$F(5) = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

Euler proved that every factor of $F(n)$ must have the form $k2^{n+1} + 1$.

Exercise: Prove it.

Pierre de Fermat (1607 1665)

He is best known for his Fermat's principle for light propagation and his Fermat's Last Theorem in number theory.

$$a^n + b^n = c^n$$

Any two Fermat numbers are relatively prime.
It means $gcd\ (F(i), F(j)) = 1$ if $i \neq j$.

Any two Fermat numbers are relatively prime.
It means $gcd\ (F(i), F(j)) = 1$ if $i \neq j$.
$gcd\ (a, b) = gcd\ (b, a) = gcd\ (a - b, b)$ if $a > b$

Observe that

$$(F(0) \times F(1) \times \cdots \times F(n-1)) \times F(n) = F(n+1) - 2$$

Proof:

$$\begin{aligned}
(\prod_{k=0}^{n-1} F(k)) \times F(n) &= (F(n) - 2) \times F(n) \\
&= (2^{2^n} - 1)(2^{2^n} + 1) \\
&= 2^{2^{n+1}} - 1
\end{aligned}$$

Observe that

$$(F(0) \times F(1) \times \cdots \times F(n-1)) \times F(n) = F(n+1) - 2$$

Proof:

$$\begin{aligned}(\prod_{k=0}^{n-1} F(k)) \times F(n) &= (F(n) - 2) \times F(n) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= 2^{2^{n+1}} - 1\end{aligned}$$

Suppose $n > m$, then

$$gcd\ (F(m), F(n)) = gcd\ (F(m), 2) = 1$$

Observe that

$$(F(0) \times F(1) \times \cdots \times F(n-1)) \times F(n) = F(n+1) - 2$$

Proof:

$$\begin{aligned} (\prod_{k=0}^{n-1} F(k)) \times F(n) &= (F(n) - 2) \times F(n) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= 2^{2^{n+1}} - 1 \end{aligned}$$

Suppose $n > m$, then

$$gcd\ (F(m), F(n)) = gcd\ (F(m), 2) = 1$$

Thus, every $F(n)$ is a prime or it has a new prime factor.

Exercise: Consider the number $2^p - 1$ where p is a prime. Show that all its prime factors are greater than p.
Exercise: Consider any polynomial $P(x)$. Show that the sequence $P(0), P(1), \ldots$ cannot be only prime numbers.

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

$$\text{What about } 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots =?$$

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

What about $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots =?$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \to \infty$$

Proof: We consider a simpler and smaller sum

$$1+\frac{1}{2}+(\frac{1}{4}+\frac{1}{4})+(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8})+(\frac{1}{16}+\cdots)+(\frac{1}{32}+\cdots)\cdots()\cdots$$

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

$$\text{What about } 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = ?$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \to \infty$$

Proof: We consider a simpler and smaller sum

$$1 + \frac{1}{2} + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}) + (\frac{1}{16} + \cdots) + (\frac{1}{32} + \cdots) \cdots () \cdots$$

$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \cdots \to \infty$$

What about prime numbers ?

What about prime numbers ?

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots =?$$

We give a proof by Erdös.

Paul Erdös (Hungarian: 1913 –1996)
Erds published around 1,500 mathematical papers during his lifetime.

Suppose

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots = M$$

(p_i's are in increasing order) Then there must be a k such that

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$$

Suppose

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots = M$$

(p_i's are in increasing order) Then there must be a k such that

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$$

Let $P_s = p_1, p_2, \ldots, p_k$ be called small primes and
$P_b := p_{k+1}, p_{k+2}, \ldots$ be called big primes.

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p}_i < \frac{N}{2}$$

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p_i} < \frac{N}{2}$$

Let N_b be the number of integers $\leq N$ that is divisible by at least one big prime.
Let N_s be the number of integers $\leq N$, that are divisible by only small primes.
Clearly $N_b + N_s = N$.

For any natural number N we must have

$$\sum_{i=k+1}^{\infty} \frac{N}{p_{\ i}} < \frac{N}{2}$$

Let N_b be the number of integers $\leq N$ that is divisible by at least one big prime.
Let N_s be the number of integers $\leq N$, that are divisible by only small primes.
Clearly $N_b + N_s = N$.
We will show that for a suitable N, $N_s + N_b < N$, a contradiction.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.
Total number of choices for squared part is at most $\sqrt{N}$.
This implies $N_s \leq 2^k \sqrt{N}$.

$$N_b \leq \sum_{i>k} \left\lfloor \frac{N}{p}_i \right\rfloor < \frac{N}{2}$$

To estimate N_s, write $n < N$ as $n = ab^2$. a squarefree part and a squared part.
Total choices number of for square free part is at most 2^k.
Total number of choices for squared part is at most $\sqrt{N}$.
This implies $N_s \leq 2^k\sqrt{N}$.
For contradiction find N such that $2^k\sqrt{N} < \frac{N}{2}$.

Issai Schur (1875–1941) was a Russian mathematician who worked in Germany. He was a student of the great group theorist Frobenius. Schur worked in various areas and proved many deep results in representation theory.

Issai Schur (1875–1941) was a Russian mathematician who worked in Germany. He was a student of the great group theorist Frobenius. Schur worked in various areas and proved many deep results in representation theory.

Let $P(x)$ be a non-constant polynomial with integer coefficients. Then $\{P(i) : i \in \mathbb{N}\}$ has infinitely many prime divisors.
(see Lemma 3 in https://mast.queensu.ca/~murty/poly2.pdf)

Christian Elsholtz: Prime divisors of thin sequences, Amer. Math. Monthly 119 (2012), 331–333

Let $S := \{s_1, s_2, \ldots\} \subset \mathbb{Z}$ be a sequence of integers such that

1. No integer appears more than c times.
2. S has subexponential growth i.e. $|s_n| < 2^{2^{f(n)}}$ where $\frac{f(n)}{\log_2 n} \to 0$. $(f : \mathbb{N} \to \mathbb{R})$

Christian Elsholtz: Prime divisors of thin sequences, Amer. Math. Monthly 119 (2012), 331–333

Let $S := \{s_1, s_2, \ldots\} \subset \mathbb{Z}$ be a sequence of integers such that

1. No integer appears more than c times.
2. S has subexponential growth i.e. $|s_n| < 2^{2^{f(n)}}$ where $\frac{f(n)}{\log_2 n} \to 0$. ($f : \mathbb{N} \to \mathbb{R}$)

Theorem: If a set S is "almost" injective and of sub-exponential growth (the above two conditions) then the set of prime numbers P_S that divide a member of S is infinite.

The two conditions are clearly required. Suppose the first condition does not hold. Then consider the sequence $S := \{2, 4, 4, 8, 8, 8, 8, 16, \ldots\}$.

The two conditions are clearly required. Suppose the first condition does not hold. Then consider the sequence $S := \{2, 4, 4, 8, 8, 8, 8, 16, \dots\}$.

If the second condition does not hold then the sequence $\{2^i 3^j\}$, $i, j \in \mathbb{N}$ arranged in increasing order has $\frac{f(n)}{\log_2 n} \sim \frac{1}{2}$

Without loss of generality assume $f(n)$ is increasing.

Without loss of generality assume $f(n)$ is increasing.
Otherwise redefine it as $g(n) := \max_{i \leq n} f(n)$.
Suppose $P_S = \{p_1, p_2, \dots, p_k\}$.
Then $s_n = \epsilon_n p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where $\epsilon_n = \{-1, 0, +1\}$ and $\alpha_i \geq 0$
This implies

$$2^{\alpha_1 + \alpha_2 + \cdots \alpha_k} \leq |s_n| \leq 2^{2^{f(n)}}$$

for $s(n) \neq 0$.

$$\Rightarrow 0 \leq \alpha_i \leq \alpha_1 + \alpha_2 + \cdots \alpha_k \leq 2^{f(n)} \text{ for } 1 \leq i \leq k$$

.

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \leq (2^{f(N)} + 1)^k \leq 2^{(f(N)+1)k}.$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\log_2(N-c) - \log_2(2c) \leq k(f(N)+1) \text{ for all } N.$$

$$\#\{|s(n)| \neq 0 \text{ and } n \leq N\} \geq \frac{N-c}{2c}$$

$$\frac{N-c}{2c} \leq 2^{k(f(N)+1)}$$

$$\log_2(N-c) - \log_2(2c) \leq k(f(N)+1) \text{ for all } N.$$

Divide both sides by $\log_2 N$. Then LHS goes to 1 and RHS goes to 0.

$$\frac{\log_2(N-c)}{\log_2 N} \to 1 \text{ as } N \to \infty$$

and

$$\frac{f(N)}{\log_2 N} \to 0 \text{ as } N \to \infty.$$

$$\frac{\log_2(N-c)}{\log_2 N} \to 1 \text{ as } N \to \infty$$

and

$$\frac{f(N)}{\log_2 N} \to 0 \text{ as } N \to \infty.$$

This is a contradiction.

Frustenberg's proof: (Mercer's note)
Notation: All integers congruent to $r \mod m$ is denoted by $r + m\mathbb{Z}$ and they are called AP.
Example:

$$3 + 11\mathbb{Z} = \{\dots, -30, -19, -8, 3, 14, 25, 36, \dots\}$$

For $m > 1$, set of integers not divisible (ND) by m are as

$$(1 + m\mathbb{Z}) \cup \cdots \cup ((m-1) + m\mathbb{Z}).$$

Assertion 1: Intersection of two AP's is either empty or infinite.

Assertion 1: Intersection of two AP's is either empty or infinite.
Assertion 2: Finite intersection of finite unions of sets is also a finite union of finite intersections of sets.
Example:

$$(A \cup B \cup C) \cap (D \cup E) \cap (F \cup G) = (A \cap D \cap F) \cup () \cup \dots$$

Proof: If $p_1, p_2, \dots, p_k$ is the set of all primes then

$$\{-1, 1\} = ND(p_1) \cap ND(p_2) \dots \cap ND(p_k)$$

RHS is either empty or infinite!