Why Primes?

Shanta Laishram

Professor of Mathematics & Head
Stat Math Unit, Indian Statistical Institute
New Delhi, India

http://www.isid.ac.in/∼shanta
shanta@isid.ac.in, shantalaishram@gmail.com

IIIT Delhi

November 25, 2023

Is it a prime?

- Which one of the following number(s) is a prime?

$$((((((((((2^3 + 2)^3 + 30)^3 + 6)^3 + 80)^3 + 12)^3 + 450)^3 + 894)^3 + 3636)^3 + 70756)^3 + 97220$$

Is it a prime?

- Which one of the following number(s) is a prime?

$$((((((((((2^3+2)^3+30)^3+6)^3+80)^3+12)^3+450)^3 + 894)^3+3636)^3+70756)^3+97220$$

or

$$((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3 + 894)^3+3636)^3+70756)^3+97220$$

Is it a prime?

- Which one of the following number(s) is a prime?

$$((((((((((2^3+2)^3+30)^3+6)^3+80)^3+12)^3+450)^3 + 894)^3+3636)^3+70756)^3+97220$$

or

$$((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3 + 894)^3+3636)^3+70756)^3+97220$$

- Both of them have 20,562 decimal digits.

What is a prime?

- **Prime Number**: An positive integer $p > 1$ is called a prime number if its only positive divisors (factors) are 1 and p itself.

What is a prime?

- **Prime Number**: An positive integer $p > 1$ is called a prime number if its only positive divisors (factors) are 1 and p itself.
- $2, 3, 5, 7, 11, 13, \ldots$ are primes.

What is a prime?

- **Prime Number**: An positive integer $p > 1$ is called a prime number if its only positive divisors (factors) are 1 and p itself.
- $2, 3, 5, 7, 11, 13, \ldots$ are primes.
- Primes are building blocks of numbers, hence important.

What is a prime?

- **Prime Number**: An positive integer $p > 1$ is called a prime number if its only positive divisors (factors) are 1 and p itself.
- $2, 3, 5, 7, 11, 13, \ldots$ are primes.
- Primes are building blocks of numbers, hence important.
- The set of primes is infinite and they are mysterious.
- A positive integer $n > 1$ is composite if it is not a prime.
- $4, 6, 8, 9, 10, \ldots$ are composites.

What is a prime?

- **Prime Number**: An positive integer $p > 1$ is called a prime number if its only positive divisors (factors) are 1 and p itself.
- $2, 3, 5, 7, 11, 13, \ldots$ are primes.
- Primes are building blocks of numbers, hence important.
- The set of primes is infinite and they are mysterious.
- A positive integer $n > 1$ is composite if it is not a prime.
- $4, 6, 8, 9, 10, \ldots$ are composites.
- Is 1 a prime or a composite?

Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.

Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.
- Hence every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $p_1 < p_2 < \cdots < p_r$ are primes and $a_1, a_2, \cdots, a_r$ are non negative integers.

Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.
- Hence every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $p_1 < p_2 < \cdots < p_r$ are primes and $a_1, a_2, \cdots, a_r$ are non negative integers.
- For example $100 = 2^2 \cdot 5^2$.

Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.
- Hence every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

  where $p_1 < p_2 < \cdots < p_r$ are primes and $a_1, a_2, \cdots, a_r$ are non negative integers.
- For example $100 = 2^2 \cdot 5^2$.
- 1 is neither a prime nor a composite else Fundamental Theorem will be violated.

Fundamental Theorem of Arithmetic

- Every positive integer $n > 1$ can be written as product of primes and it is unique upto order of primes.
- Hence every $n \in \mathbb{N}$ can be written uniquely in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

  where $p_1 < p_2 < \cdots < p_r$ are primes and $a_1, a_2, \cdots, a_r$ are non negative integers.
- For example $100 = 2^2 \cdot 5^2$.
- 1 is neither a prime nor a composite else Fundamental Theorem will be violated.
- Every $n > 1$ has a prime divisor.

Fundamental Theorem of Arithmetic

- A positive integer n is called *squarefree* if n is not divisible by a square of a prime number. In that case, $n = p_1 p_2 \cdots p_r$.
- $1, 2, 3, 6, 10$ are squarefree. $45 = 5 \cdot 3^2$ is not squarefree.
- Every positive integer $n > 1$ can be written uniquely as product of a square and a squarefree, i.e., $n = ab^2$ with a squarefree. Here a is called the squarefree part of n.

Fundamental Theorem of Arithmetic

- A positive integer n is called *squarefree* if n is not divisible by a square of a prime number. In that case, $n = p_1 p_2 \cdots p_r$.
- $1, 2, 3, 6, 10$ are squarefree. $45 = 5 \cdot 3^2$ is not squarefree.
- Every positive integer $n > 1$ can be written uniquely as product of a square and a squarefree, i.e., $n = ab^2$ with a squarefree. Here a is called the squarefree part of n.
- For squares, the squarefree part is 1.
- In fact 1 is considered empty product of primes and is both square and squarefree.
- Given any set of r primes, there are exactly 2^r squarefree positive integers whose prime factors belong to the set.

Theorem 1.

The set of primes is infinite.

Proof.

- Suppose there are finitely many primes $p_1, p_2, \cdots, p_r$. Then are are 2^r squarefree positive integers.

Euclid's Theorem: Proof of Erdős

Theorem 1.

The set of primes is infinite.

Proof.

- Suppose there are finitely many primes $p_1, p_2, \cdots, p_r$. Then are are 2^r squarefree positive integers.
- Let $N = 2^{2r} + 1$. Every $1 < n \leq N$ can be written uniquely as $n = ab^2$ with a squarefree and $b \leq \sqrt{n} \leq \sqrt{N}$.
- Here the number of choices of b is at most $\sqrt{N}$ and there are 2^r choices of a.
- Hence there are at most $2^r\sqrt{N}$ choices of ab^2.
- Thus $N \leq 2^r\sqrt{N}$ implying $\sqrt{N} \leq 2^r$ or $N \leq 2^{2r}$.
- This is a contradiction.

□

Prime Counting Function

- Let $\pi(X) := \#\{primes \ \leq x\}$ be the prime counting function.
- $\pi(1) = 0, \pi(10) = 4, \pi(100) = 25$ etc.
- If $r = \pi(N)$, the above proof implies $N \leq 2^r \sqrt{N}$ or $\pi(N) = r \geq \log N/(2 \log 2)$.
- **Prime Number Theorem:**

$$\pi(N) \sim \frac{N}{\log N} \quad \text{i.e.,} \quad \lim_{N \to \infty} \frac{\pi(N) \log N}{N} = 1.$$

- Hence for a given N, a number $n < N$ is a prime with probability $\frac{1}{\log N}$.

Carl Friedrich Gauss, Disquisitiones Arithmeticae, 1801

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the mind will never penetrate.

No branch of number theory is more saturated with mystery and elegance than the study of prime numbers.

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)
- **Wilson's Theorem**: p is prime if and only if p divides $(p-1)! + 1$.

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)
- **Wilson's Theorem**: p is prime if and only if p divides $(p-1)! + 1$.
- **Fermat's Little Theorem**: If p is prime and a is any integer, then $a^p - a$ is divisible by p.

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)
- **Wilson's Theorem**: p is prime if and only if p divides $(p-1)!+1$.
- **Fermat's Little Theorem**: If p is prime and a is any integer, then $a^p - a$ is divisible by p.
- **Bertrand's postulate**: For $n > 1$, there is always a prime p with $n < p < 2n$.

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)
- **Wilson's Theorem**: p is prime if and only if p divides $(p-1)!+1$.
- **Fermat's Little Theorem**: If p is prime and a is any integer, then $a^p - a$ is divisible by p.
- **Bertrand's postulate**: For $n > 1$, there is always a prime p with $n < p < 2n$.
- Richert(1948): Each natural number $n \geq 7$ can be expressed as sum of distinct primes.

Some properties of Primes

- All prime numbers except 2 and 5 end in 1, 3, 7 or 9. (2 divide numbers ending in 0, 2, 4, 6 or 8 and 5 divides numbers ending in 0 or 5.)
- **Wilson's Theorem**: p is prime if and only if p divides $(p-1)!+1$.
- **Fermat's Little Theorem**: If p is prime and a is any integer, then $a^p - a$ is divisible by p.
- **Bertrand's postulate**: For $n > 1$, there is always a prime p with $n < p < 2n$.
- Richert(1948): Each natural number $n \geq 7$ can be expressed as sum of distinct primes.
- **Copeland-Erdős constant** $0.23571113171923293137414\ldots$, obtained by writing all primes is known to be an irrational number.

- **Mersenne Primes**: Primes of the form $2^n - 1$ with n prime.
- $3 = 2^2 - 1, 7 = 2^3 - 1, 31 = 2^5 - 1, 8191 = 2^{13} - 1$ are first few Mersenne primes.
- Conjecturally: There are infinitely many Mersenne primes.
- Largest known: 24862048 digit prime, $2^{82589933} - 1$, discovered in 2018.

Factorial/Primorial Primes

- **Primorial Primes**: Primes of the form $p_1 p_2 \cdots p_r + 1$.
- $3 = 2+1, 7 = 2 \cdot 3 + 1, 31 = 2 \cdot 3 \cdot 5 + 1, 211 = 2 \cdot 3 \cdot 5 \cdot 7 + 1$ are first Primorial primes.
- Conjecturally: There are infinitely many Primorial primes.
- Largest known: 1+product of primes ≤ 3267113, discovered in 2021

Factorial/Primorial Primes

- **Primorial Primes**: Primes of the form $p_1 p_2 \cdots p_r + 1$.
- $3 = 2 + 1, 7 = 2 \cdot 3 + 1, 31 = 2 \cdot 3 \cdot 5 + 1, 211 = 2 \cdot 3 \cdot 5 \cdot 7 + 1$ are first Primorial primes.
- Conjecturally: There are infinitely many Primorial primes.
- Largest known: 1+product of primes ≤ 3267113, discovered in 2021
- **Factorial Primes**: Primes of the form $n! + 1$.
- $2 = 1! + 1, 3 = 2! + 1, 7 = 3! + 1, 39916801 = 11! + 1$ are first few factorial primes.
- Conjecturally: There are infinitely many Factorial primes.
- Largest known: $422429! + 1$, discovered in 2022.

Sophie Germain Primes

- **Sophie Germain Primes**: Odd primes p such that $2p + 1$ is also prime.
- $7 = 2 \cdot 3 + 1, 11 = 2 \cdot 5 + 1, 23 = 2 \cdot 11, 47 = 2 \cdot 23 + 1$ give first few Sophie Germain Primes.
- Connected to **Fermat's Last Theorem**: The equation $x^n + y^n = z^n$ has no non-trivial integer solutions if $n > 2$; proved first for n divisible by Sophie Germain primes.
- Conjecturally: There are infinitely many Sophie Germain Primes.
- Largest known: $2618163404417 \cdot 2^{1290000} - 1$, discovered in 2016.

Primes of the form $n^2 + 1$ and Fermat Primes

- Conjecture: Infinitely many primes of the form $n^2 + 1$.

Primes of the form $n^2 + 1$ and Fermat Primes

- Conjecture: Infinitely many primes of the form $n^2 + 1$.
- **Fermat Primes**: Primes of the form $\mathbb{F}_n = 22^n + 1$.
- $\mathbb{F}_1 = 5, \mathbb{F}_2 = 17, \mathbb{F}_3 = 257$ and $\mathbb{F}_4 = 65537$ are primes.
- Conjecture: For $n > 4$, $\mathbb{F}_n$ is composite.

Digitally delicate primes or weakly prime number

- **Digitally delicate prime**: Primes which become composite if any of the digits is replaced by a digit.
- Also called **Weakly prime numbers**.
- Erdős: Infinitely many weakly prime numbers.
- Smallest: 294001
- Largest known: 1000 digit weakly prime

$$\frac{17(10^{1000}-1)}{99}+21686652.$$

- Tao: A positive proportion of primes are digically delicate for all bases.

Twin Primes

- **Twin Primes**: Primes p such that $p+2$ is also prime.
- $(p, p+2)$ is called a Twin prime pair in such case. .
- $(3,5),(5,7),(11,13),(17,19),(41,43)$ are first few twin prime pairs.
- Largest known: $2996863034895 \cdot 2^{1290000} \pm 1$ which has 388342 decimal digits, discovered in 2016.
- Conjecturally: There are infinitely many twin prime pairs.

Twin Primes

- **Twin Primes**: Primes p such that $p + 2$ is also prime.
- $(p, p + 2)$ is called a Twin prime pair in such case. .
- $(3, 5), (5, 7), (11, 13), (17, 19), (41, 43)$ are first few twin prime pairs.
- Largest known: $2996863034895 \cdot 2^{1290000} \pm 1$ which has 388342 decimal digits, discovered in 2016.
- Conjecturally: There are infinitely many twin prime pairs.
- **Cousin Primes**: Primes pairs of the form $(p, p + 4)$.
- Conjecture: Given $n \geq 1$, there are infinitely many prime pairs of the form $(p, p + 2n)$.

Goldbach Conjecture

- **Goldbach Conjecture:** Every even integer $n > 4$ is sum of two odd primes!
- Verified for all $n \leq 4 \times 10^{18}$.

Goldbach Conjecture

- **Goldbach Conjecture:** Every even integer $n > 4$ is sum of two odd primes!
- Verified for all $n \leq 4 \times 10^{18}$.
- **Vinogradov's Theorem:** Every sufficiently large odd integer is a sum of three prime numbers.
- Sufficiently large was larger than 10^{1346}.
- Helfgott: Confirmed for all odd integers.

Prime Gaps

- Consecutive primes differ by at least 2.
- Let $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$ be sequences of primes.
- **Question**: How large can be the gaps $p_{n+1} - p_n$?
- Goldbach: $p_{n+1} - p_n < p_n$ for all n.
- Riemann Hypothesis: $p_{n+1} - p_n \ll p_n^{\frac{1}{2}}$.
- Grimm's Conjecture: $p_{n+1} - p_n \ll p_n^{0.46}$.

Prime Matching

24	25	26	27	28
2	5	13	3	7

Prime Matching

24	25	26	27	28
2	5	13	3	7

90	91	92	93	94	95	96
5	7 or 13	23	31	47	19	2 or 3

2018	2019	2020	2021	2022	2023	2024	2025	2026
1009	673	101	47	337	17	23	5	1013

Grimm's Conjecture

- For n, k such that $n+1, n+2, \ldots, n+k$ are consecutive composite numbers, there are distinct primes $p_1, p_2, \ldots, p_k$ such that $p_1|(n+1), p_2|(n+2), \ldots p_k|(n+k)$.

Grimm's Conjecture

- For n, k such that $n+1, n+2, \ldots, n+k$ are consecutive composite numbers, there are distinct primes $p_1, p_2, \ldots, p_k$ such that $p_1|(n+1), p_2|(n+2), \ldots p_k|(n+k)$.
- This is the famous *Grimm's Conjecture*, considered quite difficult to prove.
- Verified for all n and k with $n \leq 10^{12}$.
- It implies *Legendre Conjecture*: Given n, there is a prime between n^2 and $(n+1)^2$.
- In fact it implies, there is a prime between n and $n + n^{.46}$ for n sufficiently large, which is a result better than that given by *Riemann Hypothesis*, the *Holy Grail of Number Theory, if not for the whole of mathematics*.

Riemann Hypothesis

- For $s = \sigma + it \in \mathbb{C}$ with $\sigma > 1$, define the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

- This function can be analytically continued to whole of $\mathbb{C}$. The resulting function is called *Riemann Zeta Function*, denoted by $\zeta(s)$.

Riemann Hypothesis

- For $s = \sigma + it \in \mathbb{C}$ with $\sigma > 1$, define the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

- This function can be analytically continued to whole of $\mathbb{C}$. The resulting function is called *Riemann Zeta Function*, denoted by $\zeta(s)$.
- The Riemann zeta function satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s)$$

where Γ is the Gamma function.

Riemann Hypothesis

- For $s = \sigma + it \in \mathbb{C}$ with $\sigma > 1$, define the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

- This function can be analytically continued to whole of $\mathbb{C}$. The resulting function is called *Riemann Zeta Function*, denoted by $\zeta(s)$.
- The Riemann zeta function satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

where Γ is the Gamma function.
- The functional equation shows that the Riemann zeta function has zeros at $-2, -4, \ldots$ which are called the trivial zeros. Other zeros are called *non-trivial zeros* and such zeros s satisfy $0 \leq \Re(s) \leq 1$.

Riemann Hypothesis

- The \$1000000 question is: If $s = \sigma + it \in \mathbb{C}$ is a non trivial zero, then $\Re(s) = \frac{1}{2}$.

Riemann Hypothesis

- The \$1000000 question is: If $s = \sigma + it \in \mathbb{C}$ is a non trivial zero, then $\Re(s) = \frac{1}{2}$.
- This a very powerful conjecture and it has lots of implications in Number Theory and other areas of mathematics.

Riemann Hypothesis

- The \$1000000 question is: If $s = \sigma + it \in \mathbb{C}$ is a non trivial zero, then $\Re(s) = \frac{1}{2}$.
- This a very powerful conjecture and it has lots of implications in Number Theory and other areas of mathematics.
- In fact showing that $\zeta(1 + it) \neq 0$ implies the *Prime Number Theorem*: The number of primes upto x is around $\frac{x}{\log x}$ when $x \to \infty$.

Primitive Prime Divisors

- Given a sequence of integers $a_0, a_1, \cdots$, we say that p is a *primitive prime divisor* of a_n if $p | a_n$ but $p \nmid a_m$ for $m < n$ and $a_m \neq 0$.

Primitive Prime Divisors

- Given a sequence of integers $a_0, a_1, \cdots$, we say that p is a *primitive prime divisor* of a_n if $p|a_n$ but $p \nmid a_m$ for $m < n$ and $a_m \neq 0$.
- *Fibonacci Sequence F_n:* is defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$.
- $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \cdots$ are first few terms of the sequence.

Primitive Prime Divisors

- Given a sequence of integers $a_0, a_1, \cdots$, we say that p is a *primitive prime divisor* of a_n if $p|a_n$ but $p \nmid a_m$ for $m < n$ and $a_m \neq 0$.
- *Fibonacci Sequence* F_n*:* is defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$.
- $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \cdots$ are first few terms of the sequence.
- It is an important question to show (F_n) contains infinitely many primes.

Primitive Prime Divisors

- Given a sequence of integers $a_0, a_1, \cdots$, we say that p is a *primitive prime divisor* of a_n if $p | a_n$ but $p \nmid a_m$ for $m < n$ and $a_m \neq 0$.
- *Fibonacci Sequence F_n:* is defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$.
- $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \cdots$ are first few terms of the sequence.
- It is an important question to show (F_n) contains infinitely many primes.
- However after 144, there exist primitive prime divisors of F_n for each n which is a very powerful result.
- It also gives another proof(more difficult) of infinitude of primes.

An example

From the factorization of

$$F_{210} = 2^3 \times 5 \times 11 \times 13 \times 29 \times 31 \times 61 \times 71 \times 211 \times 421$$
$$911 \times 21211 \times 141961 \times 767131 \times 8288823481$$

guess a primitive prime factor of F_{210}!

An example

$$
\begin{aligned}
F_{105} &= 2 \times 5 \times 13 \times 61 \times 421 \times 141961 \times 8288823481 \\
F_{70} &= 5 \times 11 \times 13 \times 29 \times 71 \times 911 \times 141961 \\
F_{42} &= 2^3 \times 13 \times 29 \times 211 \times 421 \\
F_{30} &= 2^3 \times 5 \times 11 \times 31 \times 61.
\end{aligned}
$$

From

$$
\begin{aligned}
F_{210} =& 2^3 \times 5 \times 11 \times 13 \times 29 \times 31 \times 61 \times 71 \times 211 \times 421 \\
& 911 \times \underline{21211} \times 141961 \times \underline{767131} \times 8288823481,
\end{aligned}
$$

the primitive divisors of F_{210} are 21211 and 767131.

Fibonacci as product of Factorials

Theorem 2.

The largest solution of the equation

$$F_n = m_1!m_2!\cdots m_k!$$

with $2 \leq m_1 \leq m_2 \leq \cdots \leq m_k$ *is* $F_{12} = 3!4! = (2!)^2 3!$.

Fibonacci as product of Factorials

Theorem 2.

The largest solution of the equation

$$F_n = m_1!m_2!\cdots m_k!$$

with $2 \le m_1 \le m_2 \le \cdots \le m_k$ *is* $F_{12} = 3!4! = (2!)^2 3!$.

Proof.

Let $n > 12$. Then F_n has a primitive divisor $p \equiv \pm 1 \pmod{n}$ so that $p \ge n-1$. Also $p | m_k$ so that $m_k \ge p \ge (n-1)$. Hence

$$\alpha^{n-1} \ge \frac{\alpha^n - \beta^n}{\alpha - \beta} = F_n \ge m_k! \ge (n-1)! > \left(\frac{n-1}{e}\right)^{n-1}$$

where $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$ and using $t! > (t/e)^t$. This gives $12 \le n-1 \le e\alpha$ which is a contradiction. □

Radical and abc

- Given n, the radical of n is given by $R(n) = \prod_{p|n} p$ and put $R(1) = 1$.
- $R(100) = 2 \cdot 5 = 10$ and $R(81) = 3$.

Radical and abc

- Given n, the radical of n is given by $R(n) = \prod_{p|n} p$ and put $R(1) = 1$.
- $R(100) = 2 \cdot 5 = 10$ and $R(81) = 3$.
- **Oesterle-Masser** or **abc Conjecture**: Given $\epsilon > 0$, there is a constant κ_ϵ, depending only on abc, such that for any pairwise coprime positive integers a, b, c with $a + b = c$, we have

$$c < \kappa_\epsilon \left(\prod_{p|abc} p \right)^{1+\epsilon}.$$

Radical and abc

- Given n, the radical of n is given by $R(n) = \prod_{p|n} p$ and put $R(1) = 1$.
- $R(100) = 2 \cdot 5 = 10$ and $R(81) = 3$.
- **Oesterle-Masser** or **abc Conjecture**: Given $\epsilon > 0$, there is a constant κ_ϵ, depending only on abc, such that for any pairwise coprime positive integers a, b, c with $a + b = c$, we have

$$c < \kappa_\epsilon \left(\prod_{p|abc} p \right)^{1+\epsilon}.$$

- Considered one of the most difficult problems in Number theory, it has lots of interesting and important consequences, including Fermat's Last Theorem.

Primes in arithmetic progression

- Green-Tao: Sequence of primes contain arbitrarily long arithmetic progressions.
- That is, given n, there are n primes in an arithmetic progression.
- Largest known AP of primes: 27 primes in AP, discovered in 2019:

$$224584605939537911 + 81292139 \cdot 23m$$

for $m = 0, 1, 2, \cdots, 26$.

Primes dividing a product of consecutive integers

- Well-known: A product of $k \geq 1$ consecutive positive integers is divisible by $k!$.
- One of the combinatorial proofs is given by the fact that the binomial coefficient $\binom{n}{k} \in \mathbb{Z}$.

$$ {}^{n}C_k = \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}. $$

- Each prime $p \leq k$ divides a product of $k \geq 1$ consecutive positive integers.
- We can ask if there is a prime $> k$ dividing a product of k consecutive positive integers.

A result of Sylvester-Erdős

- Theorem of Sylvester-Erdős: *A product of k consecutive integers each of which exceeds k is divisible by a prime greater than k*. In other words,

$$P((n+1)(n+2)\cdots(n+k)) > k \quad \text{when} \quad n \geq k.$$

- Here $P(m)$ stands for the largest prime divisor of m with the convention $P(1) = 1$.
- This implies *Bertrand's Postulate*: Taking $n = k$ gives a prime p with $k < p < 2k$.
- Shorey-Tijdeman: For $n \geq 1, d > 1, k \geq 3$ with $\gcd(n, d) = 1$,

$$P(n(n+d)(n+2d)\cdots(n+(k-1)d)) > k \quad \text{for} \quad (n, d, k) \neq (2, 7, 3).$$

A result of Sylvester-Erdős

- Theorem of Sylvester-Erdős: *A product of k consecutive integers each of which exceeds k is divisible by a prime greater than k*. In other words,

$$P((n+1)(n+2)\cdots(n+k)) > k \quad \text{when} \quad n \geq k.$$

- Here $P(m)$ stands for the largest prime divisor of m with the convention $P(1) = 1$.
- This implies *Bertrand's Postulate*: Taking $n = k$ gives a prime p with $k < p < 2k$.
- Shorey-Tijdeman: For $n \geq 1, d > 1, k \geq 3$ with $\gcd(n, d) = 1$,

$$P(n(n+d)(n+2d)\cdots(n+(k-1)d)) > k \quad \text{for} \quad (n, d, k) \neq (2, 7, 3).$$

Prime divisor of an AP

- Conjecture: For positive integers $n, d, k \geq 4$ with $\gcd(n, d) = 1$ and $n \geq dk$,

$$P(n(n+d)(n+2d)\cdots(n+(k-1)d)) > \frac{dk}{200}$$

except for finitely many (n, d, k).

Prime divisor of an AP

- Conjecture: For positive integers $n, d, k \geq 4$ with $\gcd(n, d) = 1$ and $n \geq dk$,

$$P(n(n+d)(n+2d)\cdots(n+(k-1)d)) > \frac{dk}{200}$$

  except for finitely many (n, d, k).
- Considered a difficult problem, verified for all $k \leq 400$ and it has many interesting consequences.

Prime divisor of an AP

- Conjecture: For positive integers $n, d, k \geq 4$ with $\gcd(n, d) = 1$ and $n \geq dk$,

$$P(n(n+d)(n+2d)\cdots(n+(k-1)d)) > \frac{dk}{200}$$

  except for finitely many (n, d, k).
- Considered a difficult problem, verified for all $k \leq 400$ and it has many interesting consequences.
- Implication: A product of four or consecutive terms of an arithmetic progression is never a square.

Primes and Irreducibility of polynomials

- Primes play an important role in showing irreducibility of polynomials.
- Well known Eisenstein's Criterion: Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_x + a_0 \in \mathbb{Z}[X].$$

If there is a prime p such that $p|a_i$ for $0 \leq i < n, p \nmid a_n$ and $p^{\nmid} a_0$, then $f(x)$ is irreducible.

Primes and Irreducibility of polynomials

- Primes play an important role in showing irreducibility of polynomials.
- Well known Eisenstein's Criterion: Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_x + a_0 \in \mathbb{Z}[X].$$

  If there is a prime p such that $p|a_i$ for $0 \leq i < n, p \nmid a_n$ and $p^{\nmid} a_0$, then $f(x)$ is irreducible.
- Use of $p-$adic Newton polygons and Sylvester's Theorem imply:

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

  is irreducible for all n.

Primes and Irreducibility of polynomials

- Primes play an important role in showing irreducibility of polynomials.
- Well known Eisenstein's Criterion: Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_x + a_0 \in \mathbb{Z}[X].$$

  If there is a prime p such that $p | a_i$ for $0 \leq i < n, p \nmid a_n$ and $p^{\nmid} a_0$, then $f(x)$ is irreducible.
- Use of $p-$adic Newton polygons and Sylvester's Theorem imply:

$$E_n(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

  is irreducible for all n.
- In fact, primes also play an important role in computing Galois groups for a large infinite family of polynomials.

Check if it is a prime?

- 101: Easy

Check if it is a prime?

- 101: Easy
- 65537: Still managable!

Check if it is a prime?

- 101: Easy
- 65537: Still managable!
- $2^{123456789} - 1$:

Check if it is a prime?

- 101: Easy
- 65537: Still managable!
- $2^{123456789} - 1$: Still easy since $7 = 2^3 - 1$ is a factor!

Check if it is a prime?

- 101: Easy
- 65537: Still managable!
- $2^{123456789} - 1$: Still easy since $7 = 2^3 - 1$ is a factor!
- $2^{13466917} - 1$:

Check if it is a prime?

- 101: Easy
- 65537: Still managable!
- $2^{123456789} - 1$: Still easy since $7 = 2^3 - 1$ is a factor!
- $2^{13466917} - 1$: Quite Difficult!

Top Ten Largest Known Primes

Prime	Number of Digits	Year
$2^{82589933} - 1$	24862048	2018
$2^{77232917} - 1$	23249425	2018
$2^{74207281} - 1$	22338618	2016
$2^{57885161} - 1$	17425170	2013
$2^{43112609} - 1$	12978189	2008
$2^{42643801} - 1$	12837064	2009
$\Phi_3(-516693^{1048576})$	1981518	2023
$\Phi_3(-465859^{1048576})$	11887192	2023
$2^{37156667} - 1$	11185272	2008
$2^{32582657} - 1$	9808358	2006

Awards for finding large primes

- The Electronic Frontier Foundation (EFF) is offering prizes for finding large primes.

Awards for finding large primes

- The Electronic Frontier Foundation (EFF) is offering prizes for finding large primes.
- Offered a prize of US Dollar $100,000$ (Rs 4500000 approx. that time) to GIMPS and the UCLA mathematics department for discovering a 13 million digit prime number in August 2008.

Awards for finding large primes

- The Electronic Frontier Foundation (EFF) is offering prizes for finding large primes.
- Offered a prize of US Dollar $100,000$ (Rs 4500000 approx. that time) to GIMPS and the UCLA mathematics department for discovering a 13 million digit prime number in August 2008.
- Will offer US Dollar $150,000$ (Rs 10500000 approx) for prime with 100 million digits and US Dollar $250,000$(approx. Rs 1.75 Crore) for prime with 1 billion digits.

Awards for finding large primes

- The Electronic Frontier Foundation (EFF) is offering prizes for finding large primes.
- Offered a prize of US Dollar $100,000$ (Rs 4500000 approx. that time) to GIMPS and the UCLA mathematics department for discovering a 13 million digit prime number in August 2008.
- Will offer US Dollar $150,000$ (Rs 10500000 approx) for prime with 100 million digits and US Dollar $250,000$(approx. Rs 1.75 Crore) for prime with 1 billion digits.
- Paid US Dollar $50,000$ for prime with 1 million digits.

Awards for finding large primes

- The Electronic Frontier Foundation (EFF) is offering prizes for finding large primes.
- Offered a prize of US Dollar $100,000$ (Rs 4500000 approx. that time) to GIMPS and the UCLA mathematics department for discovering a 13 million digit prime number in August 2008.
- Will offer US Dollar $150,000$ (Rs 10500000 approx) for prime with 100 million digits and US Dollar $250,000$(approx. Rs 1.75 Crore) for prime with 1 billion digits.
- Paid US Dollar $50,000$ for prime with 1 million digits.
- RSA Factoring Challenge offered prizes up to US Dollar $200,000$ for factoring numbers which is product of two primes.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.
- Checking the divisibility by all the primes upto $\sqrt{n}$ will take a lot of time and is not efficient.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.
- Checking the divisibility by all the primes upto $\sqrt{n}$ will take a lot of time and is not efficient.
- *The Rabin-Miller Primality testing Algorithm* is one of the fastest probabilistic and widely used algorithm for checking primes.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.
- Checking the divisibility by all the primes upto $\sqrt{n}$ will take a lot of time and is not efficient.
- *The Rabin-Miller Primality testing Algorithm* is one of the fastest probabilistic and widely used algorithm for checking primes. But it is not deterministic.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.
- Checking the divisibility by all the primes upto $\sqrt{n}$ will take a lot of time and is not efficient.
- *The Rabin-Miller Primality testing Algorithm* is one of the fastest probabilistic and widely used algorithm for checking primes. But it is not deterministic.
- Elliptic Curve Primality proving is deterministic but polynomial time.

Some facts

- If n is not a prime, it is divisible by a prime $p \leq \sqrt{n}$.
- That is the basis of *Sieve of Erasthosnes* which we learnt in school.
- Checking the divisibility by all the primes upto $\sqrt{n}$ will take a lot of time and is not efficient.
- *The Rabin-Miller Primality testing Algorithm* is one of the fastest probabilistic and widely used algorithm for checking primes. But it is not deterministic.
- Elliptic Curve Primality proving is deterministic but polynomial time.
- *AKS* Algorithm is the only known polynomial time deterministic algorithm.

Primality Testing Algorithms

- Rabin Miller Primality Test: Fast but not deterministic
- AKS Algorithm: Polynomial time deterministic algorithm
- Elliptic Curve Primality Testing: deterministic.

A large prime

- $(((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!

A large prime

- $((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!
- 20,562 decimal digits.

A large prime

- $((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!
- 20,562 decimal digits.
- Primality was proved using fastECPP on several networks of workstations, was suggested as a challenge for primality proving.

A large prime

- $((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!
- 20,562 decimal digits.
- Primality was proved using fastECPP on several networks of workstations, was suggested as a challenge for primality proving.
- Started on 32-bit machines (Sep-Oct 2005), finished on nine 64-bit bi-processors (Feb-June 2006).

A large prime

- $(((((((((2^3 + 3)^3 + 30)^3 + 6)^3 + 80)^3 + 12)^3 + 450)^3 + 894)^3 + 3636)^3 + 70756)^3 + 97220$ is prime!
- 20,562 decimal digits.
- Primality was proved using fastECPP on several networks of workstations, was suggested as a challenge for primality proving.
- Started on 32-bit machines (Sep-Oct 2005), finished on nine 64-bit bi-processors (Feb-June 2006).
- 1st phase: 1900 days (396 for sqrt; 384 for Cornacchia; 1353 for PRP tests)

A large prime

- $((((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!
- 20,562 decimal digits.
- Primality was proved using fastECPP on several networks of workstations, was suggested as a challenge for primality proving.
- Started on 32-bit machines (Sep-Oct 2005), finished on nine 64-bit bi-processors (Feb-June 2006).
- 1st phase: 1900 days (396 for sqrt; 384 for Cornacchia; 1353 for PRP tests)
- 2nd phase: 319 days (8 days for building all H_D's; 277 for solving H_D mod p)

A large prime

- $(((((((((2^3+3)^3+30)^3+6)^3+80)^3+12)^3+450)^3+894)^3+3636)^3+70756)^3+97220$ is prime!
- 20,562 decimal digits.
- Primality was proved using fastECPP on several networks of workstations, was suggested as a challenge for primality proving.
- Started on 32-bit machines (Sep-Oct 2005), finished on nine 64-bit bi-processors (Feb-June 2006).
- 1st phase: 1900 days (396 for sqrt; 384 for Cornacchia; 1353 for PRP tests)
- 2nd phase: 319 days (8 days for building all H_D's; 277 for solving H_D mod p)
- Cumulated timings are given w.r.t. AMD Opteron(tm) Processor 250 at 2.39 GHz.

Miller-Rabin Primality testing Algorithm

- Let n be an odd composite number and suppose that $a^{n-1} \equiv 1$ modulo n.
- Write $n - 1 = 2^s m$ with m odd.

Miller-Rabin Primality testing Algorithm

- Let n be an odd composite number and suppose that $a^{n-1} \equiv 1$ modulo n.
- Write $n - 1 = 2^s m$ with m odd.
- Define $b_j \equiv a^{2^j m} (\text{mod } n)$ for each $j = 0, 1, 2, \ldots, s$.
- $a^{n-1} \equiv 1$ implies $b_s = 1$.
- If $b_0 = 1$, then $b_j = 1$ for each j.

- Let n be an odd composite number and suppose that $a^{n-1} \equiv 1$ modulo n.
- Write $n-1 = 2^s m$ with m odd.
- Define $b_j \equiv a^{2^j m} \pmod{n}$ for each $j = 0, 1, 2, \ldots, s$.
- $a^{n-1} \equiv 1$ implies $b_s = 1$.
- If $b_0 = 1$, then $b_j = 1$ for each j.
- If $b_0 \neq 1$, then there exists a unique j with $b_j \neq 1$ and $b_{j+1} = 1$.

Miller-Rabin Primality testing Algorithm

- Let n be an odd composite number and suppose that $a^{n-1} \equiv 1$ modulo n.
- Write $n - 1 = 2^s m$ with m odd.
- Define $b_j \equiv a^{2^j m} (\text{mod } n)$ for each $j = 0, 1, 2, \ldots, s$.
- $a^{n-1} \equiv 1$ implies $b_s = 1$.
- If $b_0 = 1$, then $b_j = 1$ for each j.
- If $b_0 \neq 1$, then there exists a unique j with $b_j \neq 1$ and $b_{j+1} = 1$.
- If $b_j \neq -1$, then it is a non-trivial square roots of 1 and hence n is composite.

Lemma 3.

Suppose p is an odd prime. Let $p-1 = 2^k m$ *where m is odd. Let* $1 < a < p$. *Either*

$$a^m \equiv 1 (p)$$

or one of

$$a^m, a^{2m}, a^{2^2 m}, a^{2^3 m}, \cdots, a^{2^{k-1} m}$$

is congruent to $-1(p)$.

Rabin-Miller Primality testing Algorithm

- Fix the number t of iterations.
- Write $n - 1 = 2^s m$ with m odd.
- For $i = 1, 2, \ldots, t$: Choose a random integer $a \in \{2, 3, \ldots, n-1\}$ and compute $b_0 \equiv a^m$ modulo n.
- If $b_0 \neq 1$, compute $b_0, b_1 \equiv b_0^2, b_2 \equiv b_1^2, \cdots, b_j$ with $j \leq s - 2, b_{j+1} = 1$ modulo n.
- If $b_j \neq -1$ modulo n, return n *is composite*.
- If $b_{s-1} \equiv -1$ modulo n, return n *is composite*.
- Else n is prime.

Rabin-Miller Primality testing Algorithm

- Fix the number t of iterations.
- Write $n-1=2^s m$ with m odd.
- For $i=1,2,\ldots,t$: Choose a random integer $a\in\{2,3,\ldots,n-1\}$ and compute $b_0\equiv a^m$ modulo n.
- If $b_0\neq 1$, compute $b_0, b_1\equiv b_0^2, b_2\equiv b_1^2,\cdots,b_j$ with $j\leq s-2, b_{j+1}=1$ modulo n.
- If $b_j\neq -1$ modulo n, return *n is composite*.
- If $b_{s-1}\equiv -1$ modulo n, return *n is composite*.
- Else n is prime.
- The probability of a composite n declared as a prime is not more than $\frac{1}{4^t}$ since the fraction of bases in $\mathbb{Z}_n$ for which n is a strong pseudoprime is at most $1/4$.

Rabin-Miller Primality testing Algorithm

- Fix the number t of iterations.
- Write $n - 1 = 2^s m$ with m odd.
- For $i = 1, 2, \ldots, t$: Choose a random integer $a \in \{2, 3, \ldots, n-1\}$ and compute $b_0 \equiv a^m$ modulo n.
- If $b_0 \neq 1$, compute $b_0, b_1 \equiv b_0^2, b_2 \equiv b_1^2, \cdots, b_j$ with $j \leq s-2, b_{j+1} = 1$ modulo n.
- If $b_j \neq -1$ modulo n, return *n is composite*.
- If $b_{s-1} \equiv -1$ modulo n, return *n is composite*.
- Else n is prime.
- The probability of a composite n declared as a prime is not more than $\frac{1}{4^t}$ since the fraction of bases in $\mathbb{Z}_n$ for which n is a strong pseudoprime is at most $1/4$.
- Choosing t appropriately, we can reduce the error probability to a very low value.
- Running time is $O((\log n)^3)$.

Agarwal-kayal-Saxena(AKS) Algorithm

- It is the only known polynomial time deterministic algorithm.

Agarwal-kayal-Saxena(AKS) Algorithm

- It is the only known polynomial time deterministic algorithm.
- Works on the the fact that n is a prime if and only $n|\binom{n}{k}$ for each $1 \leq k \leq n-1$.

Agarwal-kayal-Saxena(AKS) Algorithm

- It is the only known polynomial time deterministic algorithm.
- Works on the the fact that n is a prime if and only $n | \binom{n}{k}$ for each $1 \leq k \leq n-1$.

AKS Algorithm

- For any prime number p we let
$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$
denote the $p-$th cyclotomic polynomial.
- Let ζ_p be a zero of $\Phi_p(x)$ and let $\mathbb{Z}[\zeta_p]$ denote the ring generated by ζ_p over $\mathbb{Z}$.
- For any $n \in \mathbb{Z}$ we write $\mathbb{Z}[\zeta_p]/(n)$ for the residue ring $\mathbb{Z}[\zeta_p]$ modulo the ideal (n) generated by n. For $n \neq 0$, this is a finite ring.

Basis for AKS Algorithm

Lemma 4.

Let n be an odd positive integer and let r be a prime number. Suppose that

1. *n is not divisible by any of the primes r;*
2. *the order of $n (mod\ r)$ is at least $(\log n/\log 2)^2$;*
3. *for every $0 \leq j < r$ we have $(\zeta_r + j)^n = \zeta_r^n + j$ in $\mathbb{Z}[\zeta_p]/(n)$.*

Then n is a prime power.

AKS Algorithm

- Let $n > 1$ be an odd integer.
- First check that n is not a proper power of an integer.
- By successively trying $r = 2, 3, \ldots,$ determine the smallest prime r not dividing n nor any of the numbers $n^i - 1$ for $1 \leq i \leq (\log n / \log 2)^2$.
- For $0 \leq j < r - 1$ check that $(\zeta_r + j)^n = \zeta_r^n + j$ in $\mathbb{Z}[\zeta_p]/(n)$.
- If the number n does not pass the tests, it is composite. If it passes them, it is a prime.

Proof of Correctness

- If n is prime, it passes the tests by Fermat's little theorem.

Proof of Correctness

- If n is prime, it passes the tests by Fermat's little theorem.
- Conversely suppose that n passes the tests.
- We check the conditions of Lemma.

Proof of Correctness

- If n is prime, it passes the tests by Fermat's little theorem.
- Conversely suppose that n passes the tests.
- We check the conditions of Lemma.
- By the definition of r , the number n has no prime divisors $\leq r$.
- Since r does not divide any of the $n^i - 1$ for $1 \leq i \leq (\log n / \log 2)^2$, the order of n modulo r exceeds $(\log n / \log 2)^2$.
- This shows that the second condition of Lemma is satisfied.
- Since test (3) has been passed successfully, the third condition is satisfied.
- We deduce that n is a prime power. Since n passed the first test, it is therefore prime.

Can you factor as product of primes?

- 77: Easy

Can you factor as product of primes?

- 77: Easy
- 11639 : Still managable!

Can you factor as product of primes?

- 77: Easy
- 11639 : Still managable! $= 103 \cdot 113$

What about the prime factors of this number RSA-240?

1246203667817187840658350446081065904348
2037465167880575481878888328966680118821
0855036039570272508747509864768438458621
0548655379702539305718912176843182863628
4694840530161441643046806687569941524699
318570418303051254959437 1372159029236099

RSA Factoring Challenge

- RSA Laboratories which designs protocols for RSA cryptosystem has a set of numbers(which is a product of two large primes) and challenges everyone to factor it.

RSA Factoring Challenge

- RSA Laboratories which designs protocols for RSA cryptosystem has a set of numbers(which is a product of two large primes) and challenges everyone to factor it.
- There are prizes ranging from US Dollars 1000 to 10000.

RSA Factoring Challenge

- RSA Laboratories which designs protocols for RSA cryptosystem has a set of numbers(which is a product of two large primes) and challenges everyone to factor it.
- There are prizes ranging from US Dollars 1000 to 10000.
- A research team led by Emmanuel Thomé at France's National Institute for Computer Science and Applied Mathematics(INRIA) successfully factored RSA-240 in December 2019.
- Other members in the team included Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger and Paul Zimmermann.

The 795 bits number RSA−240

1246203667817187840658350446081065904348
2037465167880575481878888328966680118821
0855036039570272508747509864768438458621
0548655379702539305718912176843182863628
4694840530161441643046806687569941524699
318570418303051254959437 1372159029236099

The 795 bits number RSA−240

1246203667817187840658350446081065904348
2037465167880575481878888328966680118821
0855036039570272508747509864768438458621
0548655379702539305718912176843182863628
4694840530161441643046806687569941524699
318570418303051254959437 137215902923609

and factors are

5094359522858399145550510235808437141326
4838202411147318666029652182120646974670
0620316443478873837606252372049619334517

and

2446242088383181505678131390240028966538
0209257893140145204122133655847709517815
5258218897735030590669041302045908071447.

RSA-240

- The CPU time spent amounts to approximately 900 core-years on a 2.1 GHz Intel Xeon Gold 6130 CPU.
- RSA-240 sieving: 800 physical core-years
- RSA-240 matrix: 100 physical core-years
- In fact, record Factoring done along with another record of a Discrete Logarithm of the same size at the same time with a total computation time of roughly 4000 core-years
- Worked with an open source software, CADO-NFS, used to implement the Number Field Sieve.
- CADO-NFS comprises 300,000 lines of code written in C and C++.

Factoring Algorithms

- Elliptic Curve Factoring Method
- Number Field Sieve
- Pollard-ρ factoring method

Fermat's Factoring Method

- Can you factor $N = 13199$?

Fermat's Factoring Method

- Can you factor $N = 13199$?
- We will use a very simple idea to factor N.

Fermat's Factoring Method

- Can you factor $N = 13199$?
- We will use a very simple idea to factor N.
- If $N = a^2 - b^2$ and $a - b \neq 1$, then $N = (a-b)(a+b)$.

Fermat's Factoring Method: $N = 13199$

m	$m^2 - N$		m	$m^2 - N$
115	26		124	2117
116	257		125	2426
117	490		126	2677
118	725		127	2930
119	962		128	3185
120	1201		129	3442
121	1442		130	3701
122	1685		131	3962
123	1930		132	$4225 = 65^2$

$$N = 132^2 - 65^2 = (132 - 65)(132 + 65) = 67 \cdot 197$$

Applications

- Public Key Cryptography algorithms and Internet Security

Applications

- Public Key Cryptography algorithms and Internet Security
- Used for hash tables and pseudorandom number generators.

Applications

- Public Key Cryptography algorithms and Internet Security
- Used for hash tables and pseudorandom number generators.
- Some rotor machines were designed with a different number of pins on each rotor, with the number of pins on any one rotor either prime, or coprime to the number of pins on any other rotor. This helped generate the full cycle of possible rotor positions before repeating any position.

The basis of the RSA Cryptosystem is Euler's Theorem.

Theorem 5.

Let a and n be positive integers such that $gcd(a, n) = 1$. *Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where $\varphi(n) = \#\{i : 1 \leq i < n,\ \gcd(a, n) = 1\}$.
Here $i \equiv j (mod\ n)$ *means* $n | (i - j)$.

The basis of the RSA Cryptosystem is Euler's Theorem.

Theorem 5.

Let a and n be positive integers such that gcd$(a, n) = 1$*. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where $\varphi(n) = \#\{i : 1 \leq i < n,\ \gcd(a, n) = 1\}$*.*
Here $i \equiv j(\text{mod } n)$ *means* $n|(i - j)$*.*

In particular, for a prime p and any integer a, we have

$$p|(a^{p-1} - 1)$$

which is **Fermat's Little Theorem.**

Helen Spalding: Let Us Now Praise Prime Numbers

Let us now praise prime numbers
With our fathers who begat us:
The power, the peculiar glory of prime numbers
Is that nothing begat them,
No ancestors, no factors,
Adams among the multiplied generations.

None can foretell their coming.
Among the ordinal numbers
They do not reserve their seats, arrive unexpected.
Along the lines of cardinals
They rise like surprising pontiffs,
Each absolute, inscrutable, self-elected.

In the beginning where chaos
Ends and zero resolves,
They crowd the foreground prodigal as forest,
But middle distance thins them,
Far distance to infinity
Yields them rare as unreturning comets.

O prime improbable numbers,
Long may formula-hunters
Steam in abstraction, waste to skeleton patience:
Stay non-conformist, nuisance,
Phenomena irreducible
To system, sequence, pattern or explanation.

$$
\begin{aligned}
7 \times 17^2 + 1 = \quad & 813258173412030282336987549031 \\
& - 813258173412030282336987547007.
\end{aligned}
$$