Probabilistic Fermat's Primality test and Deterministic Primes in P (AKS algorithm)

Dr. Animesh Chaturvedi

Assistant Professor: **IIIT Dharwad**

Young Researcher: **Heidelberg Laureate Forum** and **Pingala Interaction in Computing**

Young Scientist: **Lindau Nobel Laureate Meetings**

Postdoc: **King's College London** & **The Alan Turing Institute**

PhD: **IIT Indore** MTech: **IIITDM Jabalpur**

Basics on Prime number

- A **prime number** (or a prime) is a natural number greater than 1 that is not a product of two smaller natural numbers.
- A natural number greater than 1 that is not prime is called a **composite number.**
- For example,
  - 5 is prime because the only ways of writing it as a product, 1×5 or 5×1, involve 5 itself.
  - 4 is composite because it is a product (2×2) in which both numbers are smaller than 4.
- The first 25 prime numbers (all the prime numbers less than 100) are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97
- Primes are used in several routines in information technology,
  - such as public-key cryptography, which relies on the difficulty of factoring large numbers into their prime factors.

https://en.wikipedia.org/wiki/Prime_number
https://en.wikipedia.org/wiki/Prime_(disambiguation)

Probabilistic Fermat Primality Test

Fermat primality test

- aks Fermat's little theorem
- Fermat's little theorem is the basis for the Fermat primality test and is one of the fundamental results of elementary number theory.
- The theorem is named after Pierre de Fermat, who stated it in 1640. It is called the "little theorem" to distinguish it from Fermat's Last Theorem.
- We can pick random integers ***a*** not divisible by ***p*** and see whether the equality holds. If the equality does not hold for value of ***a***, then ***p*** is composite. This congruence is unlikely to hold for random ***a*** if ***p*** is composite.

$$1 < a < p - 1$$

- If the congruency ≅ does hold for one or more values of ***a***, then we say that ***p*** is **probably prime**.

$$a^p \equiv a \pmod{p}$$

https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

Fermat primality test

- For large p, the exhaustive search is hard for primality test, thus use Fermat primality test
- If p is a prime number,
  then for any integer a, the number $a^p - a$ is an integer multiple of p.
- In the notation of modular arithmetic, this is expressed as $a^p \equiv a \pmod{p}$
  - if $a = 2$ and $p = 7$,
    then $2^7 = 128 \equiv 2 \pmod{7}$ ➔ $128 - 2 = 126 = 7 \times 18$ is multiple of 7.
- To test whether p is prime,
  - if p is prime and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$
  - this means, if a is not divisible by p, $a^{p-1} - 1$ is an integer multiple of p
  - if $a = 2$ and $p = 7$,
    then $2^{7-1} = 2^6 = 64 \equiv 1 \pmod{7}$ ➔ $64 - 1 = 63 = 7 \times 9$ is multiple of 7.

https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

Fermat primality test

- Any ***a*** such that when ***n*** is composite is known as a Fermat liar. In this case ***n*** is called Fermat pseudoprime to base ***a***.
- Suppose we wish to determine whether n = 221 is prime. Randomly pick **1 < a < 220**, say a = 38.

$$a^{n-1} = 38^{220} \equiv 1 \pmod{221}$$

- Either 221 is prime, or 38 is a Fermat liar, so we take another ***a***, say 24:

$$a^{n-1} = 24^{220} \equiv 81 \not\equiv 1 \pmod{221}$$

- So 221 is composite and 38 was indeed Fermat liar. Furthermore, 24 is Fermat witness for the compositeness of 221.

https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

Fermat primality test to AKS algorithm

- Many primality tests are known that work only for numbers with certain properties.
- For example,
  - the Lucas–Lehmer test works only for Mersenne numbers (a Mersenne prime is prime number that is one less than a power of two), the prime numbers of form $M_p = 2^p - 1$ for some prime p
  - while Pépin's test can be applied to Fermat numbers $F_n = 2^{2^n} + 1$
- AKS algorithm is a generalization to polynomials of Fermat's little theorem.
- The AKS algorithm can be used to verify the primality of any given number.

https://en.wikipedia.org/wiki/AKS_primality_test

PRIMES is in P
(A hope for NP problems in P)

PRIMES is in P

- In 2002, it was shown that the problem of determining if a number is prime is in P.
- AKS (Agrawal–Kayal–Saxena) primality test,
  - famous research of IIT Kanpur, and
  - authors received the 2006 Gödel Prize and the 2006 Fulkerson Prize
- AKS primality test:
  - "an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite"

Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. "PRIMES is in P." *Annals of mathematics* (2004): 781-793.
https://en.wikipedia.org/wiki/AKS_primality_test

PRIMES is in P

- The key idea is to find the coefficient of x^i in $((x + a)^n - (x^n + a))$
  - if all coefficients are multiple of n, then n is prime
  - else composite number
- We work out it for $a = -1$.
  - What are the coefficient of x^i in $((x - 1)^n - (x^n - 1))$?

```
Input:  integer n > 1.
1.  If (n = a^b for a ∈ N and b > 1), output COMPOSITE.
2.  Find the smallest r such that o_r(n) > log^2 n.
3.  If 1 < (a,n) < n for some a ≤ r, output COMPOSITE.
4.  If n ≤ r, output PRIME.^1
5.  For a = 1 to ⌊sqrt(φ(r)) log n⌋ do
        if ((X + a)^n ≠ X^n + a (mod X^r − 1, n)), output COMPOSITE;
6.  Output PRIME;
```

Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. "PRIMES is in P." *Annals of mathematics* (2004): 781-793.
https://en.wikipedia.org/wiki/AKS_primality_test

Pascal Triangle

- Coefficients of $(x - 1)^n$
  - $(x - 1)^0 = 1$
  - $(x - 1)^1 = x - 1$
  - $(x - 1)^2 = (x^2 - 2x + 1)$
  - $(x - 1)^3 = x^3 - 3x^2 + 3x - 1$
  - $(x - 1)^4 = x^4 - 4x^3 + 6x^2 - 4x + 1$
  - $(x - 1)^5 = x^5 - 5x^4 + 10x^3 - 10x + 1$
  - and so on…

1																	
1	1																
1	2	1															
1	3	3	1														
1	4	6	4	1													
1	5	10	10	5	1												
1	6	15	20	15	6	1											
1	7	21	35	35	21	7	1										
1	8	28	56	70	56	28	8	1									
1	9	36	84	126	126	84	36	9	1								
1	10	45	120	210	252	210	120	45	10	1							
1	11	55	165	330	462	462	330	165	55	11	1						
1	12	66	220	495	792	924	792	495	220	66	12	1					
1	13	78	286	715	1287	1716	1716	1287	715	286	78	13	1				
1	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1			
1	15	105	455	1365	3003	5005	6435	6435	5005	3003	1365	455	105	15	1		
1	16	120	560	1820	4368	8008	11440	12870	11440	8008	4368	1820	560	120	16	1	
1	17	136	680	2380	6188	12376	19448	24310	24310	19448	12376	6188	2380	680	136	17	1

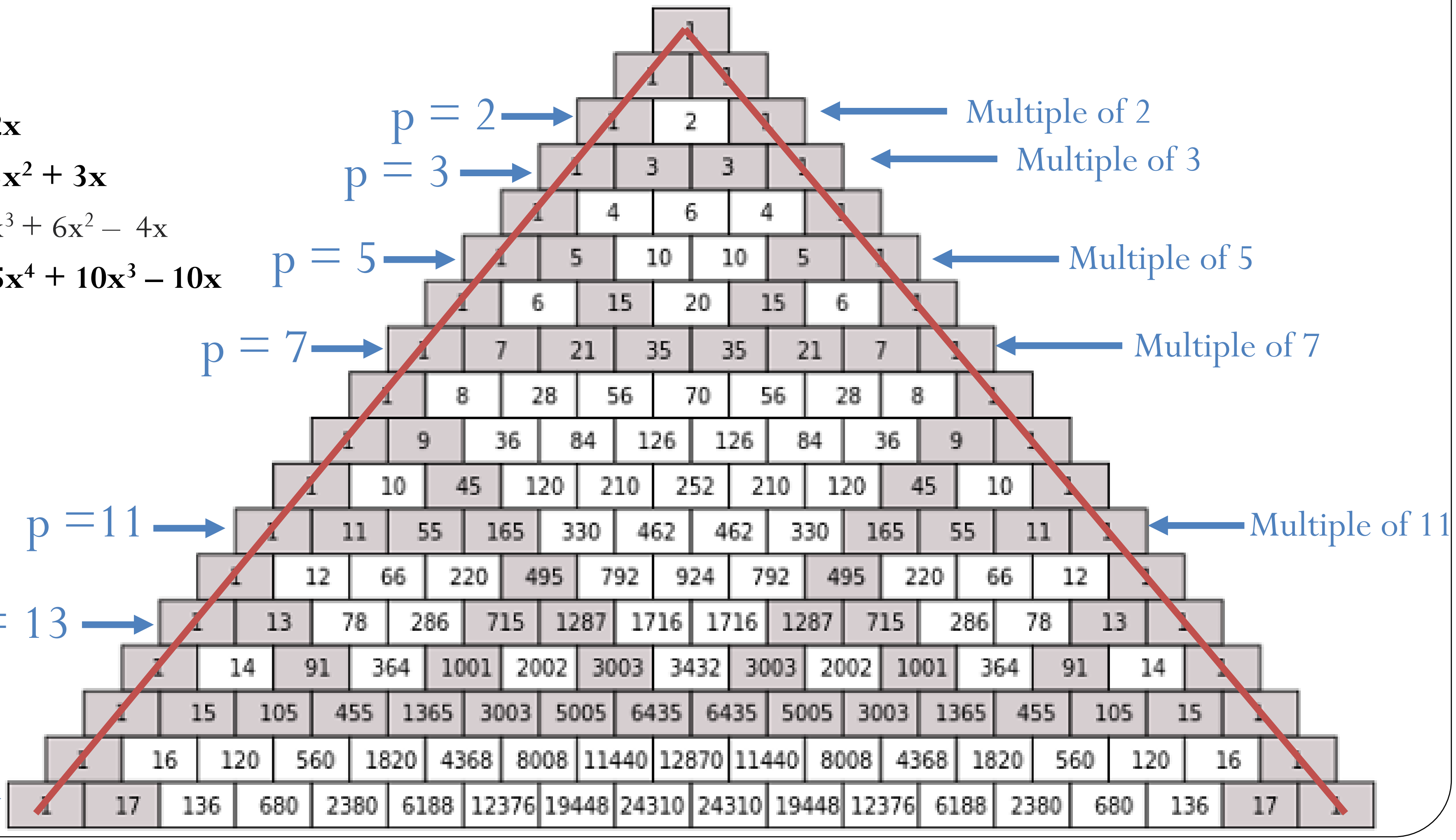
Pascal triangle trace back to Piṅgala

- The formal theory of Sanskrit meters formulated by Piṅgala in the 2nd century B.C.E. Halāyudha's construction of Pascal's triangle traces to Piṅgala.
- Piṅgala's calculation of the binomial coefficients, use of repeated partial sums of sequences and the formula for summing a geometric series became an integral part of Indian mathematics.
- Around 300 Sutras, proposed "**Meru Prastara**" now known as Pascal Triangle
- Meru means pyramid, Prastara means spreading "Pyramid Spreading"
- Pascal triangle construction can be traced to back to Piṅgala
- Pascal triangle is fixed 2D structure, **Meru Prastara** is generalized N-D structure

A HISTORY OF PIṄGALA'S COMBINATORICS, JAYANT SHAH Northeastern University, Boston, Mass,
https://web.northeastern.edu/shah/papers/Pingala.pdf
https://archive.org/details/ChhandaSutra-Pingala https://archive.org/details/halyudhaskavira00hellgoog

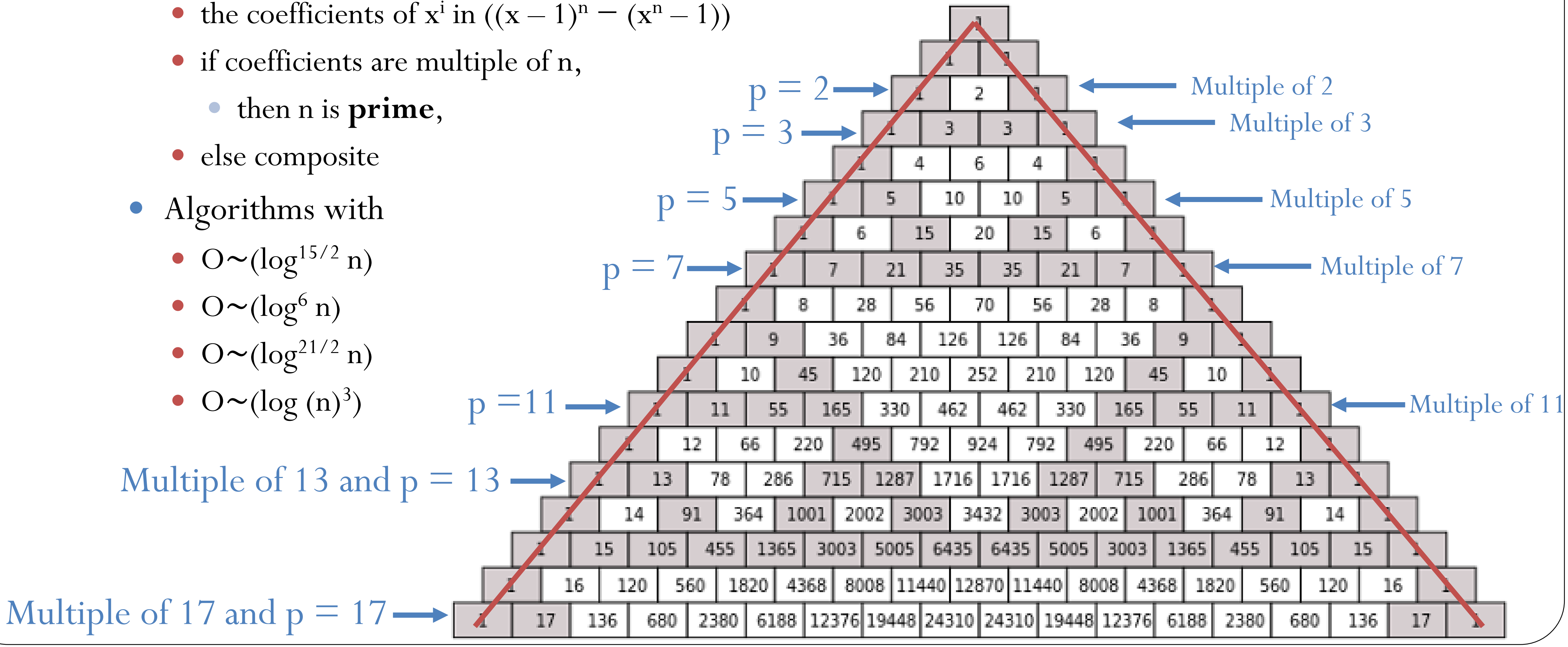
Prime and Pascals Triangle (Meru Prastara)

- Coefficients of $(x - 1)^n - (x^n - 1)$
  - $(x - 1)^0 - (x - 1) =$ ---
  - $(x - 1)^1 - (x^1 - 1) =$ ---
  - $\mathbf{(x - 1)^2 - (x^2 - 1) = - 2x}$
  - $\mathbf{(x - 1)^3 - (x^3 - 1) = - 3x^2 + 3x}$
  - $(x - 1)^4 - (x^4 - 1) = - 4x^3 + 6x^2 - 4x$
  - $\mathbf{(x - 1)^5 - (x^5 - 1) = - 5x^4 + 10x^3 - 10x}$
  - and so on…



Prime and Pascals Triangle (Meru Prastara)

- It is possible to write a polynomial time algorithm to find
  - the coefficients of x^i in $((x - 1)^n - (x^n - 1))$
  - if coefficients are multiple of n,
    - then n is **prime**,
  - else composite
- Algorithms with
  - $O\sim(\log^{15/2} n)$
  - $O\sim(\log^6 n)$
  - $O\sim(\log^{21/2} n)$
  - $O\sim(\log (n)^3)$



More on Prime number

- Fast methods for primality test are available for Mersenne numbers $M_p = 2^p - 1$.
- As of December 2018, the largest known prime number is a Mersenne prime with 24,862,048 decimal digits.
- In 1975, Vaughan Pratt showed that there existed a certificate for primality that was checkable in polynomial time, and thus that PRIMES was in NP.
- It was long suspected but not proven that primality could be solved in polynomial time.
- AKS primality test finally settled this long-standing question and placed PRIMES in P

https://en.wikipedia.org/wiki/Prime_number
https://en.wikipedia.org/wiki/Prime_(disambiguation)
https://en.wikipedia.org/wiki/Primality_test

Millennium Problems

Millennium Problems

- The Millennium Prize Problems are seven problems in mathematics that were stated by the Clay Mathematics Institute on May 24, 2000.
- One of 7 Millennium Problems for which Clay Math Institute awards \$1,000,000 i.e., US\$1 million prize
- One-million dollar (*) question: $P = NP$?
- almost all researchers think $P \neq NP$

https://www.claymath.org/millennium-problems
https://www.claymath.org/millennium-problems/millennium-prize-problems
https://en.wikipedia.org/wiki/Millennium_Prize_Problems

Millennium Problems

- Yang–Mills and Mass Gap
- Riemann Hypothesis
- P vs NP Problem: If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.
- Navier–Stokes Equation
- Hodge Conjecture
- Poincaré Conjecture
- Birch and Swinnerton-Dyer Conjecture

https://www.claymath.org/millennium-problems

Millennium Problems

- To date, the only Millennium Prize problem to have been solved is the Poincaré conjecture,
- A century passed between its formulation in 1904 by Henri Poincaré and its solution by Grigoriy Perelman, announced in preprints posted on ArXiv.org in 2002 and 2003.
- Grigoriy Perelman is the Russian mathematician.
- He declined the prize money.
- Perelman was selected to receive the Fields Medal for his solution, but he declined the award.

https://www.claymath.org/millennium-problems/poincar%C3%A9-conjecture
https://en.wikipedia.org/wiki/Millennium_Prize_Problems

References

- https://en.wikipedia.org/wiki/Prime_number
- https://en.wikipedia.org/wiki/Prime_(disambiguation)
- https://en.wikipedia.org/wiki/Primality_test
- https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
- https://en.wikipedia.org/wiki/AKS_primality_test
- Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. "PRIMES is in P." Annals of Mathematics (2004): 781-793.
- https://en.wikipedia.org/wiki/AKS_primality_test
- A HISTORY OF PIṄGALA'S COMBINATORICS, JAYANT SHAH Northeastern University, Boston, Mass, https://web.northeastern.edu/shah/papers/Pingala.pdf
- https://archive.org/details/ChhandaSutra-Pingala
- https://archive.org/details/halyudhaskavira00hellgoog
- https://www.claymath.org/millennium-problems
- https://www.claymath.org/millennium-problems/millennium-prize-problems
- https://en.wikipedia.org/wiki/Millennium_Prize_Problems

תודה רבה
Hebrew

Ευχαριστώ
Greek

Danke
German

Спасибо
Russian

धन्यवादः
Sanskrit

Merci
French

ধন্যবাদ
Bangla

நன்றி
Tamil

شكرا
Arabic

ಧನ್ಯವಾದಗಳು
Kannada

Thank You
English

നന്ദി
Malayalam

多謝
Traditional Chinese

Grazie
Italian

ధన్యవాదాలు
Telugu

આભાર
Gujarati

ਧੰਨਵਾਦ
Punjabi

धन्यवाद
Hindi & Marathi

多谢
Simplified Chinese

Gracias
Spanish

https://sites.google.com/site/animeshchaturvedi07

Obrigado
Portuguese

ありがとうございました
Japanese

ขอบคุณ
Thai

감사합니다
Korean