DOI: https://doi.org/10.52756/ijerr.2024.v44spl.010 *Int. J. Exp. Res. Rev.*, Vol. 44: 115-120 (2024)

Original Article | Peer Reviewed | Open Access

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in

ISSN 2455-4855

Statistical Analysis and Distribution of Fermat Pseudoprimes Within the Given Interval

Bhawana Fulara[1], Arvind Bhatt[1], Deepak Kumar Sharma[1], Shubham Agarwal[2]*, Geeta Mathpal[1] and Rajesh Mathpal[3]

[1]Department of Mathematics, Uttarakhand Open University, Haldwani-263139, Nainital, India; [2]Department of Mathematics, New Delhi Institute of Management, New Delhi-110062, Delhi, India; [3]Department of Physics, Uttarakhand Open University, Haldwani-263139, Nainital, India

E-mail/Orcid Id:

BF, bhawana.fulara83@gmail.com, https:// orcid.org/0009-0008-0153-2128; *AB,* arvindbhatt@uou.ac.in, https://orcid.org/0000-0001-5010-1510; *DKS,* sharmadeepak0111209@gmail.com, https://orcid.org/0009-0005-9819-2753; *SA,* meshubhamagarwal@gmail.com, https://orcid.org/0000-0001-9205-9904; *GM,* geetaupadhyay001@gmail.com, https://orcid.org/0009-0004-6621-907X; *RM,* rmathpal@uou.ac.in, https://orcid.org/0009-0003-4361-6630

Article History:

Received: 19th June, 2024
Accepted: 20th Oct., 2024
Published: 30th Oct., 2024

Keywords:

Algorithm, analysis, distribution, interval, pseudoprimes.

How to cite this Article:

Bhawana Fulara, Arvind Bhatt, Deepak Kumar Sharma, Shubham Agarwal, Geeta Mathpal and Rajesh Mathpal (2024). Statistical Analysis and Distribution of Fermat Pseudoprimes Within the Given Interval. *International Journal of Experimental Research and Review*, *44*, 115-120.

DOI:
https://doi.org/10.52756/ijerr.2024.v44spl.010

Abstract: Prime numbers are natural numbers that can only be divided by one and the original number. There is more than one of them. Error-correcting codes used in telecommunications are generated using prime numbers. They guarantee automatic message correction both during transmission and reception. Algorithms used in public-key cryptography are built upon primes. They're also employed in the production of pseudorandom numbers. Mathematicians and many other scientific and technological communities have always been fascinated by prime numbers. Additionally, computer engineers can use it to tackle a wide range of real-world problems. The analysis of prime numbers is very important for finding their applications in different fields. The statistical analysis of pseudoprimes within a given interval is carried out in the presented paper and an algorithm of Python program to find the distribution of pseudoprimes has also been generated, which is used to find their distribution with different bases within the given intervals. The data analysis process made use of graphical depiction. The discovery will surely open up new avenues for future number theory study and applications outside of mathematics.

Introduction

A composite number x is referred to as a Fermat pseudoprime to base a (Wagstaff, 2024) for every positive integer a, provided that it divides $a^{x-1} - 1$. The Chinese hypothesis is the fallacious assertion that every number that passes the Fermat primality test for base 2 is prime. 341 is the lowest base-2 Fermat pseudoprime. Since it equals 11•31, it is not a prime, but it does satisfy the Fermat primality test for base 2 because it meets Fermat's little theorem, which states that $2^{340} \equiv 1 \pmod{341}$. When the modifier Fermat is understood, a Fermat pseudoprime is commonly referred to as a pseudoprime.

Sharma et al. (2021) developed a program to locate the multi-reverse primes and determine their distribution, using a novel definition of primes known as multi-reverse primes. Additionally, using multi-reverse primes, a data encryption and decryption technique has been suggested. Sharma et al. (2022a) discovered the correlation between innovative primes and defined them, including the digital super prime, digital multi-reverse prime, and super twin primes. The new primes, known as super primes, were developed by Agarwal et al. (2021). A Java application has also been created to find different primes within the specified range. Pushpa et al. (2021) covered the characteristics and outcomes of numbers as well as various pseudoprime applications in computer applications and cryptography.

The distribution of pseudoprimes is currently an important study issue, but it has been challenging to analyze their distribution over intervals with long ranges because no computer tool has been developed to date. This study aims to analyze the distribution of

*Corresponding Author: meshubhamagarwal@gmail.com

pseudoprimes within a specific interval and create a Python program to ascertain their distribution. Finding the connections between various primes and their uses in many scientific fields would be easier with the current study's help.

Literature review

Somer (1987) established the finite number of d-pseudoprimes. The Fermat test was one of the primality tests provided (Gradini, 2010). The test's algorithm must be coded in Mathematica (6.0 version) in order to be performed. The idea of a pseudoprime is introduced by discussing the applications of Euler's and Fermat's Little Theorems to the tests. Fermat numbers can be used to create an endless number of pseudoprimes and super-pseudoprimes, as demonstrated by Křížek et al. (2002). A key concept in number theory, Fermat's Little Theorem, must be used to define pseudoprimes and super pseudoprimes. It provides a basic feature of primes and serves as the foundation for the majority of primality tests.

He et al. (2022) discussed calculating Fermat's pseudoprimes. In 2018, Parthi et al. studied strong pseudoprimes, a unique class of pseudoprimes on base b that are highly helpful for testing primality. Agarwal et al. (2015) generated the function of primes differently and created a few distributions as well as their uses in cryptography. Agarwal et al. (2023) found a correlation between various primes and developed Java software to find the correlation model. Agarwal et al. (2021) established a new recurrence relation with Fibonacci numbers and created a Java program to detect the distribution of Fibonacci primes and identify the Fibonacci primes inside the specified range. A data encryption and decryption technique based on Fibonacci primes has also been proposed. Compared to the current encryption techniques, the suggested solution offers a high level of protection against an unauthorised excess.

By tabulating all even pseudoprimes up to 10^{16}, Pomerance et al. (2023) demonstrated a recent Ordowski conjecture, The asymptotic density of the set of numbers n that are pseudoprimes to a base that is a suitable divisor of n. Li (1996) obtained the upper bound for even pseudoprimes in an unpublished study. According to Erdos's (1956) conjecture, there are infinite base-a pseudoprimes $n \equiv r \pmod m$. If a, r, and m met these requirements, $P_{a,r,m}(x)$ of base-a pseudoprimes $n \equiv r \pmod m$, $n \leq x$ is $x^{1-o(1)}$ as $x \to \infty$. $S = \{n \in N: \#D(n) > 0\}$ has an asymptotic density, according to the conjecture of (Ordowski, 2021); counts up to 10^8 by A. For sufficiently large x, $C_{r,m}(x) > x^{1/(6 \log \log \log x)}$ if $\gcd(r, m) = 1$. Wright's argument for a considerably weaker bound serves as the foundation for this recent result of the first name (Pomerance, 1981). In this case, $P_{2,r,m}(x)$ is unbounded if $\gcd(r, m) = 1$. Naturally, this finding from Rotkiewicz (1967) is not as strong as the one before it, but it was simpler and more than fifty years earlier.

Sharma et al. (2022b) discovered the relationship between numerous primes and the correlation between them. In 2018, Agarwal et al. produced new methods for number theoretic functions and special numbers that are well-defined within a specified range. They also created flow charts for these numbers and functions. (Zhang, 2007) given ψ'_t for $t \in [13,19]$; and given reasons of K2- and C_3-spsp's $< 10^{36}$ to prove $\psi_t = \psi'_t < \psi''_t$ for $t \geq 12$. ψ_m is the smallest strong pseudoprime to the first m prime bases (Jiang et al., 2014). For $1 \leq m \leq 8$, the precise value of ψ_m is known. Zhang theorized that $\psi_9 = \psi_{10} = \psi_{11} = Q_{11}$ after discovering the 19-decimal-digit number Q_{11} = 3825123056546413051. Jaeschke (1993) defined ψ_k as the lowest strong pseudoprime to all of the first k primes chosen as bases. Also described the underlying facts and methods used to obtain these conclusions, as well as the exact values for ψ_5, ψ_6, ψ_7, and ψ_8 as well as upper bounds for ψ_9, ψ_{10}, and ψ_{11}.

Materials and methods

In the current study, the Python program is used to count the Fermat pseudoprimes in a particular interval. This information is crucial for figuring out the prime pattern and how they relate to one another. Utilizing a Python program, the data was collected, and by creating line graphs in Microsoft Excel, the distribution of Fermat pseudoprimes in various intervals was discovered.

Distribution of pseudoprimes

For every base a > 1, an unlimited number of pseudoprimes exist. Cipolla demonstrated in 1904 how to generate an endless number of pseudoprimes to base a > 1. In that case, n = AB is a pseudoprime to base 'a' and composite (Ribenboim, 1996; Hamahata et al., 2007). For instance, A = 31, B = 11, and n = 341 are pseudoprimes to base 2 if a = 2 and p = 5. Although they are uncommon, there are unlimited Carmichael numbers and strong pseudoprimes to any base larger than 1. There are 245 pseudoprimes below one million, 21853 less than 25•109, and three pseudoprimes to base 2 below 1000. Below this threshold, 2163 Carmichael numbers exist and 4842 strong pseudoprimes base 2.

Program for finding fermat pseudoprimes within the given interval

```
def gcd(p, q):
    while q != 0:
        p, q = q, p % q
```

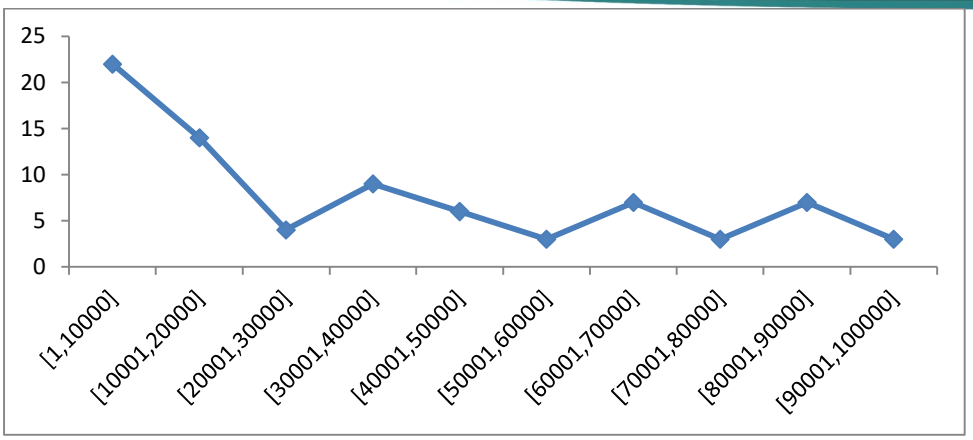

Figure 1. Distribution of Fermat Pseudoprimes with base 2.

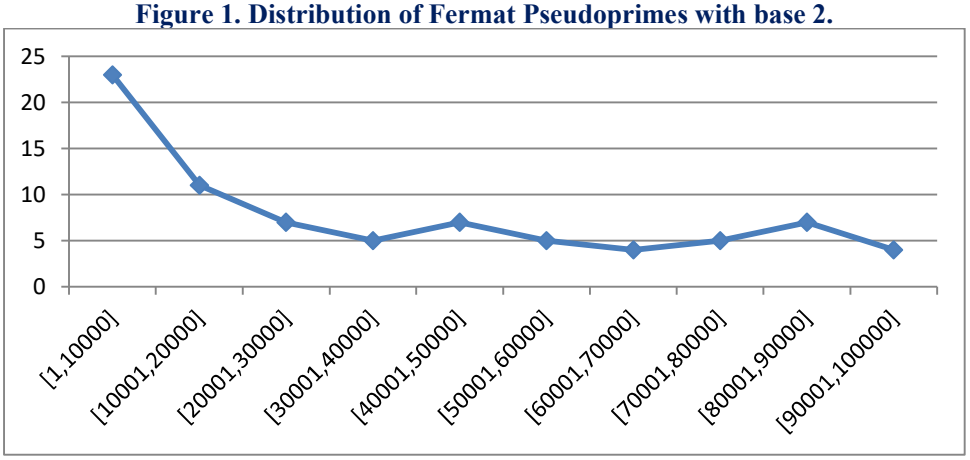

Figure 2. Distribution of Fermat Pseudoprimes with base 3.

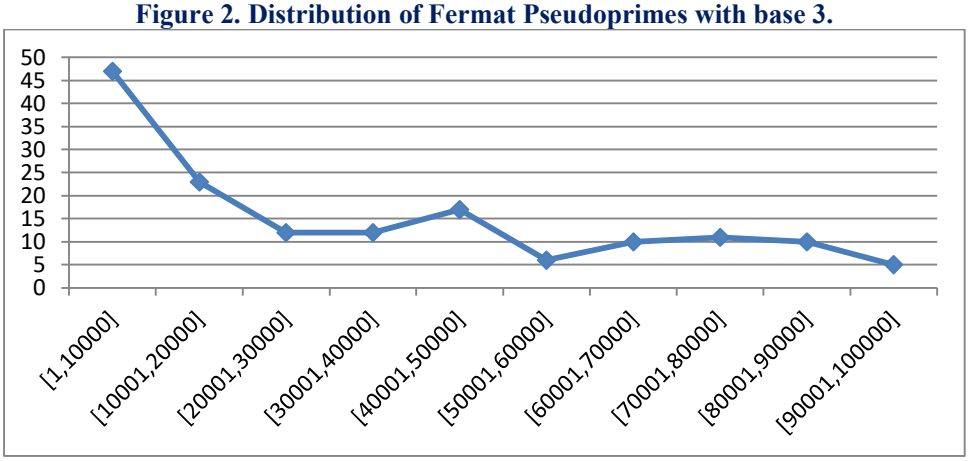

Figure 3. Distribution of Fermat Pseudoprimes with base 4.

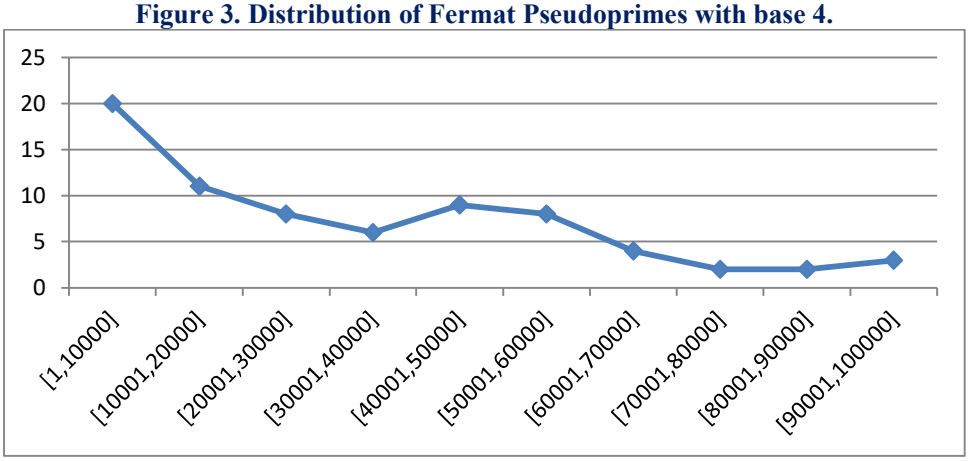

Figure 4. Distribution of Fermat Pseudoprimes with base 5.

DOI: https://doi.org/10.52756/ijerr.2024.v44spl.010

```
    return p
    def is_coprime(x, y):
        return gcd(x, y) == 1
    min=int(input("Min. value of interval = "))
    max=int(input("Max. value of interval ="))
    a=int(input("Base ="))
    pc=0
    for x in range(min,max+1):
        res=(a**(x-1))-1
        cp=is_coprime(x,a)
        count=0
        for i in range(2,x):
            if x%i==0:
             count+=1
        if a>1 and count>=1 and cp==True and res%x==0 :
    print(x, "is Fermat Pseudoprime Number")
            pc=pc+1
    print("Total number of Fermat Pseudoprimes are
    =",pc)
```

Result and Discussion

Table 1 represents the distribution of Fermat pseudoprimes within the given interval. Figure 1 represents the distribution of Fermat Pseudoprimes within different intervals with base 2. Figure 2 represents the distribution of Fermat Pseudoprimes within different intervals with base 3. Figure 3 represents the distribution of Fermat Pseudoprimes within different intervals with base 4. Figure 4 represents the distribution of Fermat Pseudoprimes within different intervals with base 5.

From the analysis, it is clear that out of Fermat pseudoprimes with base 2, 3, 4 and 5, the maximum number of Fermat pseudoprimes with base 4 lies in the intervals [1, 10000], [10001, 20000], [20001, 30000], [30001, 40000], [40001, 50000], [60001, 70000], [70001, 80000], [80001, 90000], [90001, 100000] except the interval [50001, 60000]. The interval [1, 10000] has maximum number of Fermat pseudoprimes with different bases. A minimum of five-base fermat pseudoprimes can be found at the following intervals: [1, 10000], [10001, 20000], [60001, 70000], [70001, 80000], [80001, 90000], and [90001, 100000]. Furthermore, the distribution of Fermat pseudoprimes has no fixed pattern, which strengthens its application in the field of cryptography because it will be challenging for an intruder to quickly identify the pseudoprime utilised in the cryptographic process.

Table 1. Distribution of Fermat pseudoprimes within the given interval.

Interval	No. of Fermat Pseudoprimes (Base 2)	No. of Fermat Pseudoprimes (Base 3)	No. of Fermat Pseudoprimes (Base 4)	No. of Fermat Pseudoprimes (Base 5)
[1,10000]	22	23	47	20
[10001,20000]	14	11	23	11
[20001,30000]	4	7	12	8
[30001,40000]	9	5	12	6
[40001,50000]	6	7	17	9
[50001,60000]	3	5	6	8
[60001,70000]	7	4	10	4
[70001,80000]	3	5	11	2
[80001,90000]	7	7	10	2
[90001,100000]	3	4	5	3

Conclusion

The current work will aid researchers in their investigation of various primes. The suggested Python program will assist researchers in determining the number of Fermat pseudoprimes that lie within the specified intervals with various bases. The finding will undoubtedly expand the possibilities for future number theory research as well as its applications in other domains. Fermat pseudoprimes can also be used in cryptography to generate secure cryptographic algorithms. It can also be used to establish a relationship among different primes.

Acknowledgement

The authors owe their indebtedness to all those researchers and writers whose work has been consulted in the present research.

Conflict of Interest

The current study has no conflicts of interest.

References

Agarwal, A., Agarwal, S., & Singh, B. K. (2021). Analysis of Fibonacci primes & their application in cryptography. *Stochastic Modeling and Applications (SMA), 25(2)*, 73–82. https://doi.org/10.5281/zenodo.13969700

Agarwal, A., Agarwal, S., & Singh, B. K. (2023). Analysis of primes and developing correlation model between them. *Journal of the Maharaja Sayajirao University of Baroda, 57(1)*, 78–82. https://doi.org/10.5281/zenodo.13969833

Agarwal, S., Sharma, D., & Uniyal, A. S. (2021). Formulation & distribution of super primes. *Global and Stochastic Analysis (GSA), 8(2)*, 155–166. https://doi.org/10.5281/zenodo.13969867

Agarwal, S., & Uniyal, A. S. (2015). Multiprimes distribution within a given norms. *International Journal of Applied Mathematical Sciences (JAMS), 8(2)*, 126–132. https://doi.org/10.5281/zenodo.13970797

Agarwal, S., & Uniyal, A. S. (2018). Algorithms for number theoretic functions & special numbers. *International Journal of Research in Engineering, Science and Management (IJRESM), 1(12)*, 112–116. https://doi.org/10.5281/zenodo.13969746

Erdős, P. (1956). On pseudoprimes and Carmichael numbers. *Publ. math. Debrecen, 4*, 201–206.

Gradini, E. (2010). Fermat test and the existence of pseudoprimes. *Visipena Journal, 1(1)*, 37–44. https://doi.org/10.46244/visipena.v1i1.21

Hamahata, Y., & Kokubun, Y. (2007). Cipolla pseudoprimes. *Journal of Integer Sequences, 10*, 1-6. http://eudml.org/doc/54790

He, T. X., Shiue, P. J. S., & Chang, Y. (2022). Computation of Fermat's pseudoprimes (Dedicated to the Memory of Professor Leetsch C. Hsu). *Journal of Discrete Mathematical Sciences and Cryptography, 25(2)*, 335–352. https://doi.org/10.1080/09720529.2019.1662580

Jaeschke, G. (1993). On strong pseudoprimes to several bases. *Mathematics of Computation, 61*, 915–926. https://doi.org/10.1090/S0025-5718-1993-1192971-8

Jiang, Y., & Deng, Y. (2014). Strong pseudoprimes to the first eight prime bases. *Mathematics of Computation, 83*, 2915–2924. https://doi.org/10.1090/S0025-5718-2014-02830-5

Křížek, M., Luca, F., & Somer, L. (2002). Fermat's little theorem, pseudoprimes, and super pseudoprimes. Springer, In *17 Lectures on Fermat Numbers,* pp. 317–338. https://doi.org/10.1007/978-0-387-21850-2_12

Li, S. (1996). On the distribution of even pseudoprimes.

Ordowski, T. (2021). Density of Fermat weak pseudoprimes k to a base d, where d | k and 1 < d < k. Retrieved from http://list.seqfan.eu/pipermail/seqfan/2021-January/073021.html

Parhi, K., & Kumari, P. (2018). Properties of strong pseudoprimes on base b. *International Journal of Creative Research Thoughts, 6(2)*, 1306–1310. Retrieved from http://www.ijcrt.org/papers/IJCRT1813261.pdf

Pomerance, C. (1981). On the distribution of pseudoprimes. *Mathematics of Computation, 37*, 587–593. https://doi.org/10.1090/S0025-5718-1981-0628717-0

Pomerance, C., & Samuel, S. W. (2023). Some thoughts on pseudoprimes. CERIAS Center at Purdue University, 1–11.

Pushpa, A. M., & Subramanian, S. (2021). Study of prime, pseudoprime and applications of pseudoprime. *Turkish Journal of Computer and Mathematics Education, 12(9)*, 934–939. Retrieved from https://turcomat.org/index.php/turkbilmat/article/view/3333

Ribenboim, P. (1996). How Are the Prime Numbers Distributed? In: The New Book of Prime Number Records. Springer, New York, NY. https://doi.org/10.1007/978-1-4612-0759-7_5

Rotkiewicz, A. (1967). On the pseudoprimes of the form ax + b. *Mathematical Proceedings of the Cambridge Philosophical Society, 63(2)*, 389–392. https://doi.org/10.1017/S030500410004130X

Sharma, D., Agarwal, S., & Uniyal, A. S. (2021). Distribution of multi-reverse primes within the given interval & their application in asymmetric cryptographic algorithm. *International Journal of Applied Engineering and Technology, 3(1)*, 29–33. https://doi.org/10.5281/zenodo.13969790

Sharma, D., Agarwal, S., & Uniyal, A. S. (2022a). Neoteric relationship between various primes and their analysis. *Stochastic Modeling and Applications, 26(1)*, 155–162. https://doi.org/10.5281/zenodo.13969806

Sharma, D., Agarwal, S., & Uniyal, A. S. (2022b). Linear regression model for various primes. *Journal of the Maharaja Sayajirao University of Baroda, 56(1)*, 16–23. https://doi.org/10.5281/zenodo.13970738

Somer, L. (1987). On Fermat d-pseudoprimes. In J. M. de Koninck & C. Levesque (Eds.), *Théorie des nombres / Number theory*. De Gruyter, pp. 841–860. https://doi.org/10.1515/9783110852790.841

Wagstaff, S. S., Jr. (2024). Pseudoprimes and Fermat numbers. *Integers: 24*, 1–10. https://doi.org/10.5281/zenodo.10680422

Zhang, Z. (2007). Two kinds of strong pseudoprimes up to 10. *Mathematics of Computation, 76*, 2095–2108. https://doi.org/10.1090/S0025-5718-07-01977-1

How to cite this Article:

Bhawana Fulara, Arvind Bhatt, Deepak Kumar Sharma, Shubham Agarwal, Geeta Mathpal and Rajesh Mathpal (2024). Statistical Analysis and Distribution of Fermat Pseudoprimes Within the Given Interval. *International Journal of Experimental Research and Review*, *44*, 115-120.

DOI : https://doi.org/10.52756/ijerr.2024. v44spl.010