ViJaiPraTap – A Probable Prime Number for Cryptography

Vishwas Raval
Associate Professor & Head, DST, SNSS, Central University of Gujarat, Kundhela, Vadodara-391107

Prashant Chauhan
Programmer, Computer Centre
The M S University of Baroda
Vadodara-390001

Jainam Shah & Tapashree
Computer Science Graduate (2017-2021)

ABSTRACT

A probable prime is a number that, based on a certain probabilistic test, is likely but not certain to be prime. Probable primes are frequently used in cryptography and computer science, where large primes are essential but verifying primality can be time-consuming. This paper gives Mersenne's probable prime number of 79209 digits and how it has been generated, its properties, and their main applications.

General Terms

Cryptography, Cyber Security, Prime Number

Keywords

Probable prime, PRP, Mersenne's prime, security, cryptography

1. WHAT IS PROBABLE PRIME?

A probable prime is a number that passes a specific probabilistic test designed to assess whether it's prime. If it passes the test, it's probably prime, though there is a small chance it's composite (not prime). A probable prime isn't definitively confirmed as prime but has a very high likelihood of being prime based on the test used. There are few tests which are carried out to prove if a number is probable prime or not.

1.1 Fermat Test

Uses Fermat's Little Theorem to check for "Fermat pseudoprimes," numbers that appear prime under this theorem but aren't.

1.2 Miller-Rabin Test

One of the most popular tests for large primes. It's a probabilistic algorithm, so by repeating the test, you can reduce the likelihood of error, making it a "strong probable prime test."

1.3 Solovay-Strassen Primality Test

Another probabilistic test for primality that's less commonly used but similarly effective.

Of the probable prime numbers, Mersenne's prime number is another way of finding if a given large number is probable prime or not.

Mersenne numbers are numbers of the form 2^n - 1, where n is a prime number. A Mersenne prime is a Mersenne number that is also a prime number. It is called a Mersenne prime if it is truly prime, is a number in the form: [1]

$$M_p = 2^p - 1 \text{ where p is itself a prime number.}$$

For example, if p=3, then:

$$M_3 = 2^3 - 1 = 7$$

which is indeed a prime number. For some values of p, M_p is prime, making it a Mersenne prime. When it's not yet verified as prime but is expected to be, it's referred to as a probable prime.

Some other examples of Mersenne primes include:

- p=2: $M_2=3$
- p=3: $M_3=7$
- p=5: $M_5=31$
- p=7: $M_7=127$

The Lucas-Lehmer test is commonly used to verify if a Mersenne number is prime for any given p.

Mersenne primes are of interest to mathematicians because they are related to perfect numbers, which are numbers that are equal to the sum of their proper divisors. For example, the first perfect number is 6, which is equal to 1 + 2 + 3. The second perfect number is 28, which is equal to 1 + 2 + 4 + 7 + 14.

As of 2024, there are 52 known Mersenne primes. The largest known Mersenne prime is 2^82,589,933 - 1, which has 24,862,048 digits. It was discovered in December 2018 by the Great Internet Mersenne Prime Search (GIMPS) project. [1]

Mersenne primes are also used in cryptography. For example, the RSA cryptosystem, which is used to secure internet communications, uses large prime numbers. Mersenne primes are particularly well-suited for this purpose because they are very large and difficult to factor.

Here are some of the properties of Mersenne primes:

- All Mersenne primes are of the form $2^n - 1$, where n is a prime number.
- The only even Mersenne prime is 2.
- All Mersenne primes are of the form 4k + 1 or 8k + 1, where k is an integer.
- There are no known Mersenne primes of the form $2^n - 1$, where n is a Fermat number.
- The largest known Mersenne prime is 2^82,589,933 - 1, which has 24,862,048 digits. [5]
- Mersenne primes are a fascinating topic in number theory, and they continue to be an active area of research.

The following section explains the experimental setup and process of how Mersenne's prime number has been generated on various systems.

2. EXPERIMENTAL SET UP

Data Parallelism has been used to find probable prime in less time. However, various computer systems and software have been used for time checking and experiments.

2.1 On Personal computer(4-cores) using Prime95 Software

Prime95 is a freeware application developed by George Woltman [2]. It's primarily used for two purposes:

2.1.1 Participating in the Great Internet Mersenne Prime Search (GIMPS)

GIMPS is a volunteer computing project dedicated to finding Mersenne primes, which are prime numbers of the form 2^p - 1, where p is also a prime number. Prime95 is the official client for GIMPS, allowing you to contribute your computer's idle processing power to the search for these elusive primes.

2.1.2 Stress Testing Computer Hardware

Prime95 is a popular tool for overclockers and hardware enthusiasts to test the stability of their systems. By running Prime95, you can push your CPU and memory to their limits, helping to identify potential stability issues before they cause problems.

2.1.3 Key Features of Prime95

Mersenne Prime Search: It can perform primality tests on Mersenne numbers. Stress Testing: It can stress-test your CPU and memory, helping to identify overclocking stability issues. User-Friendly Interface: It has a simple and intuitive interface, making it easy to use. Cross-Platform Compatibility: It runs on Windows, Linux, macOS, and FreeBSD.

On the personal computer, laptop of quad cores, using Prime95 software, it took 25 days to complete the iterations. The following figure shows the iterations.

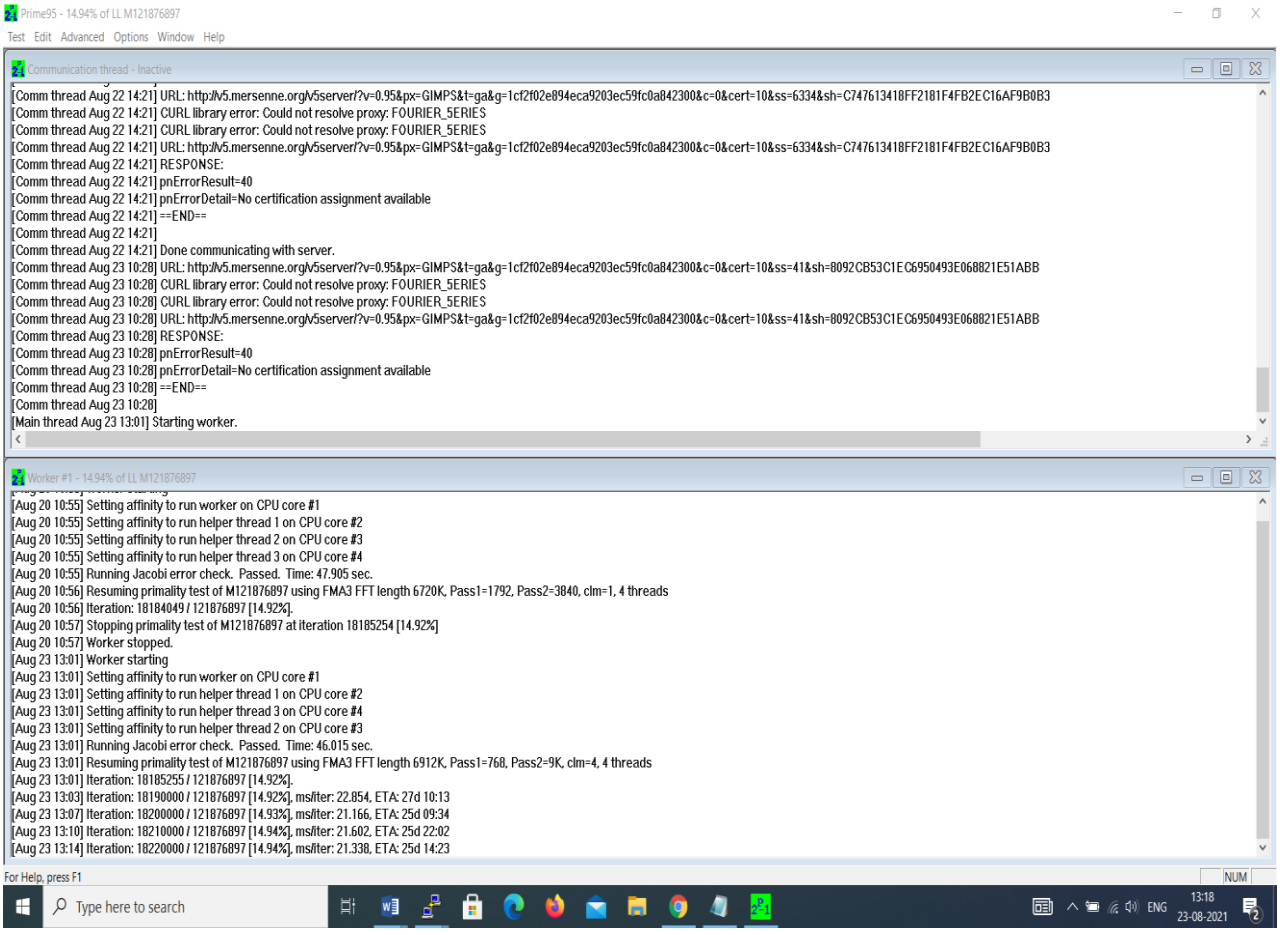

Fig 1: Iterations on Personal Computer

2.2 OpenPFGW Software

OpenPFGW is software designed to perform primality tests on numbers of specific forms [3]. It's a powerful tool for number theory enthusiasts and researchers, allowing them to explore the world of prime numbers. The key features are as under:

2.2.1 PRP and Primality Tests

It can perform both probabilistic (PRP) and deterministic primality tests.

2.2.2 Specific Number Forms

It is optimized for testing numbers of specific forms, making it efficient for certain types of prime number searches.

2.2.3 x86 Hardware Compatibility

It runs on most x86 hardware, including Windows, Linux, and macOS.

2.2.4 Open Source

It is an open-source project, allowing for community contributions and modifications.

It took 83 seconds to complete the test using data parallelism by creating 5 instances. The following figure 2 shows the iterations of OpenPGFW software.

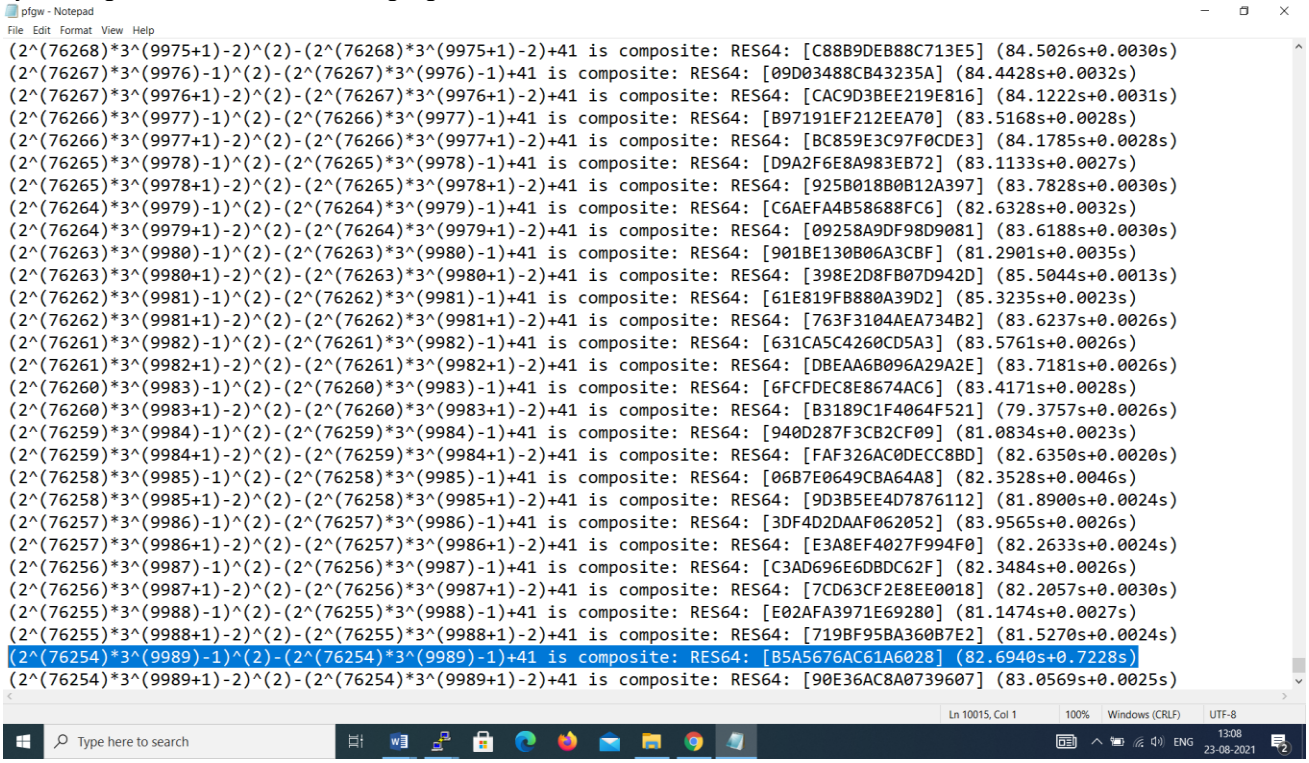

Fig 2: OpenPGFW Software

2.3 Param Shawak – Super Computer

The Param Shawak supercomputer is having following configurations. [4]

Table 1. Technical Specifications of PARAM Shavak

Processor	2 X Intel Xeon Scalable Processors with minimum 18 Cores each of minimum 2.2 GHz Clock Speed with Max. capacity of 10.4 Tera-FLOPS
RAM	96 GB ECC (8GBX12) DDR4 2400 MHz
HDD	4 X 4TB SATA – 3.5" 7200 RPM with Hardware RAID Controller (1GB Cache)
Graphics	Nvidia Quadro P400
Network	Two 1GbE network port
Accelerator	2X16 PCI-E Gen3 Slots for GPU/Co-processors
OS	RHEL
Accelerator Card	1 X NVIDIA GP100
Other Built-in Applications	• ONAMA – A set of Library for HPC in the disciplines like Computer Science, Mechanical, Civil, Electrical, Electronics, Chemical • CHReME – An HPC Resource Management Engine • Intel Software Development Suite

This took only 33 seconds and 1,54,951 iterations to evaluate and find out the probable prime of 79209 digits. The number has been named as ViJaiPraTap. Following figure shows the experiment screenshot of Param Shawak.

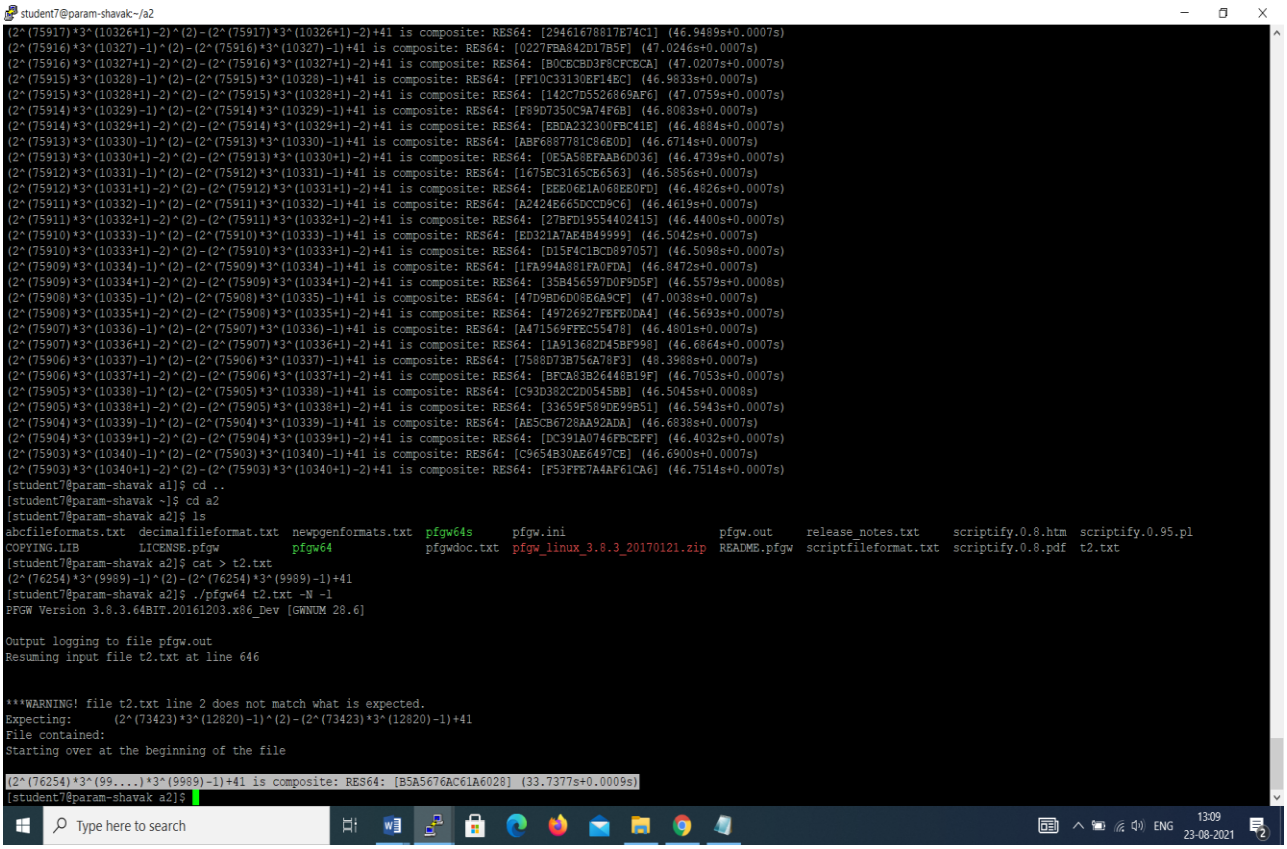

Fig 3: Execution on Param Shawak

3. APPLICATIONS OF PROBABLE PRIME

Probable prime has various applications. Following are the applications of Probable prime numbers.

3.1 Cryptography

Probable primes are essential in public-key cryptography, especially in algorithms like RSA and ECC (Elliptic Curve Cryptography). Generating large, guaranteed primes is computationally expensive, but by using probable primes, algorithms can securely generate numbers that are highly likely to be prime, which is typically sufficient.

3.1.1 RSA Cryptosystem

RSA relies on the multiplication of two large probable prime numbers to create a public key and a private key. Breaking the encryption involves factoring the product of these primes, which is nearly impossible for large numbers.

3.1.2 Digital Signatures and Key Exchange

In systems like Diffie-Hellman and DSA (Digital Signature Algorithm), probable primes are used to generate secure public keys.

3.2 Hash Functions and Pseudo-Random Number Generators (PRNGs)

Probable primes are often used in designing hash functions and PRNGs because they help produce large and unique numbers efficiently, which adds unpredictability to the generated sequences.

3.3 Randomized Algorithms

In computer science, certain algorithms require the generation of large primes for tasks like hashing or data shuffling. Probable primes help ensure these algorithms run efficiently without needing full prime verification.

3.4 Error-Resistant Data Transmission (Coding Theory)

In coding theory, probable primes can be used to build error-correcting codes by generating large fields of numbers. This approach helps ensure that data sent over unreliable networks can be decoded accurately, even if some bits are lost or corrupted.

4. REFERENCES

[1] https://www.mersenne.org/

[2] https://www.mersenne.org/download/

[3] https://sourceforge.net/projects/openpfgw/

[4] https://cdac.in/index.aspx?id=hpc_ss_param_shavak

[5] http://www.primenumbers.net/prptop/topdisc.php