Prime Numbers and Their Digital Roots

Samidha Bhosale

Undergraduate, Electronics and Telecommunication Engineering, Ramrao Adik Institute of Technology, Mumbai, India

---***---

Abstract - *Prime numbers have remained a matter of interest in the mathematical, scientific as well as technical community. Prime numbers follow an enigmatic pattern that is still unknown to date but holds great importance. Prime numbers are building blocks of numbers as atoms are of molecules therefore it is necessary to understand their properties and solve the pattern. This paper shows one such property which is how prime numbers can have specific digital roots only. It further proves this case by using the properties of digital roots. Large numbers are time-consuming to check for primality. In this paper, two simple algorithms are created to find if the number is composite or probable prime before having it checked for primality using existing primality tests, and further distribution of digital roots among different types of prime numbers are shown using pie charts obtained from python programs.*

Key Words: **Prime numbers, Digital Roots, Twin primes, Mersenne primes, Factorial primes, Primorial primes, Sophie Germain primes.**

1. INTRODUCTION

Any whole number greater than one whose only factor is one and itself is called a prime number. A factor of a number is an integer that can be divided into another integer.

For p to be prime,

(i) p > 1
(ii) p has only two positive divisors 1 and p itself.

The first few prime numbers are 2,3,5,7,11,13,17,19. $2^{82589933}-1$ is the largest prime number found to date. It is a Mersenne prime containing 24,862,048 digits. This prime number was found in 2018 by Patrick Laroche with a computer voluntarily involved in the Great Internet Mersenne Prime Search. There are 78498 prime numbers from 1 to 1 million. 70435 prime numbers from 1 million to 2 million. 67883 prime numbers from 2 million to 3 million. The density of prime numbers decreases as they get larger. This is called the asymptotic distribution of primes among the positive integers, and it is described in the Prime Number Theorem (PNT). Based on ideas introduced by the German mathematician Bernhard Riemann, Jacques Hadamard and Charles Jean de la Vallée Poussin proved this theorem in 1896.

In the prime number theorem,

For some real number x, π(x) is a prime function. This is a function defined as the number of primes less than or equal to x.

By PNT, the limit of the quotient is one when π(x) is divided by x/log(x) as x rises without bound.

$$\lim_{x\to\infty} \frac{\pi(x)}{\left[\frac{x}{\log(x)}\right]} = 1,$$

Therefore x/log(x) is a good approximation to π(x) with some relative error. The relative error approaches 0 because x tends to rise without limit.

$$\pi(x) \sim \frac{x}{\log x}.$$

1.1 History of Prime numbers

Prime numbers have been subjected to study and research for thousands of years. The Rhind Mathematical Papyrus of around 1550 BC, named after the Scottish antiquary Alexander Henry Rhind, contains expansions of Egyptian fractions of various forms for prime and composite numbers. The explicit study of prime numbers first came from ancient Greek mathematics. The Greek mathematician Euclid proved in his book "Elements" published around 300 BC that there are infinitely many prime numbers. "Every integer greater than one is either prime or can be represented as a product of primes." Was a hypothesis that was later proved by Euclid. This theorem is called the Fundamental Theorem of Arithmetic also known as the Unique Factorization Theorem. It can be explained in another way as Primes are the building blocks of positive integers: every positive integer is a product of primes in one and only one way. For example, 150 can be written as the product of prime numbers 2,3, and 5 as $150=2*5^2*3$. Other great minds of the world such as Littlewood, Riemann, Gauss, Hilbert, and Harvey later contributed to the study of prime numbers.

2 Types of Prime numbers

There are 76 types of prime numbers. The largest known types of prime numbers are Twin primes, Mersenne primes, Factorial/Primorial primes, and Sophie Germain primes.

2.1 Twin Primes

A Twin prime is a prime that is in the form of either 2 less or 2 more than another prime. It has a prime space of 2. A number N is a twin prime if N-1 or N+1 is also a prime number. Each twin is of the form (6N-1,6N+1) except (3,5). (3,5) is the smallest pair of twin primes. It is unknown whether the largest twin prime pair exists, or if there are infinitely many twin primes. This unsolved conjecture is known as the twin prime conjecture. The largest known twin prime pair to date is $(2996863034895*2^{1290000}-1, 2996863034895*2^{1290000}+1)$

2.2 Mersenne's Primes

When a prime is in the form of one is less than a power of two (2^n–1), it is called a Mersenne prime. Mersenne prime numbers are named after the French polymath Marin Mersenne. He studied them in the early 17th century. 2^p-1 is a Mersenne prime if both p and 2^p-1 are prime. As Mersenne numbers are easier to check for primality, many of the largest known prime numbers are Mersenne primes. A total of 51 Mersenne primes have been found so far. The smallest Mersenne prime is 3 having a form of 2^2-1. The largest known Mersenne prime is $2^{82589933}$– 1.

2.3 Factorial prime numbers

The product of the first n given numbers is called a factorial (n!). When a prime number is in the form of n! ± 1 where n! is a factorial of n, it is called a factorial prime.

$$n! = \prod_{i=1}^{n} i.$$

The smallest factorial prime number is 2. It can be expressed in two factorial forms 0! + 1 for n=0 or 1! + 1 for n=1 second is 3 which can be expressed as 2! + 1 for n=2. The first few factorial primes are 2, 3, 5, 7, 23, and 719. The largest known factorial prime so far is 422429! + 1 for n=422429.

2.4 Primorial primes

A primorial (#) is the same as a factorial but here the product of the first n prime numbers is considered. When a prime number is in the form of p_n#±1, where p_n# is the primorial of p_n, the prime number is called a primorial prime.

$$p_n\# = \prod_{k=1}^{n} p_k$$

The smallest primorial prime is 2 same as the smallest factorial prime. It is expressed as 0# + 1 for n=0. The first few primorial primes are 2, 3, 5, 7, 29, 31, and 211. The largest primorial prime known to date is 3267113#-1 for n=3267113.

2.5 Sophie Germain Primes

If both n and 2n+1 are primes, then the prime n is a Sophie Germain prime and the prime 2n+1 associated with it is called a safe prime. French mathematician Sophie Germain used these types of prime numbers to prove the first case of Fermat's last theorem hence they were named after her. It is unknown if there are infinitely many Sophie Germain primes. The smallest Sophie Germain prime number is 2 because, for n=2, 2n+1=5 is also a prime number, which concludes that 5 is a safe prime number. The first few Sophie Germain primes are 2, 3, 5, 11, 23, 29, and 41. The largest known Sophie Germain prime to date is 2618163402417×21290000 – 1.

3. Types of primality tests

A primality test is a test to determine whether a given number is prime or not. There are two types of primality tests which are deterministic and probabilistic. Deterministic tests are used to determine whether a number is prime or not with absolute certainty. Although probabilistic tests are much faster than deterministic tests, they can potentially identify a composite number as prime. First, probability tests are performed to filter out composite numbers. Numbers that pass probability tests are therefore called probable primes. Deterministic tests are then performed on these probable primes. Deterministic tests accurately identify the true primes from the probable primes. The remaining numbers are called pseudoprimes because they are composite numbers falsely identified as primes.

3.1 Trial Division

The simplest test for primality is the trial division test. In trial division, to check whether a number N is prime or not, divide it by all primes between 2 and the square root of N. If a number N is divisible by any of these primes, it is a composite number otherwise, it is a prime number. For numbers, up to thirty digits trial division and Sieve of Eratosthenes are most suitable.

3.2 Sieve of Eratosthenes

In the Sieve of Eratosthenes, we take the number N (N>1) and then create a list of all integers less than or equal to N, then we cross out the multiples of all prime numbers less than or equal to the square root of N, the numbers we are left with are prime numbers.

These tests are accurate and efficient for small numbers, but time-consuming for large numbers. Primality tests exist for large numbers, such as the Fermat primality test and the Miller–Rabin primality test.

3.3 Fermat's primality test

In a letter to Fre'nicle on October 18, 1640, the French mathematician Pierre de Fermat stated a theorem later known as Fermat's Little Theorem. It is an algorithm that checks whether a number is prime or not, with only a 0.002% chance of identifying a composite number as prime. This algorithm was first discovered by the ancient Chinese. According to it, the following congruence holds for a prime number p and a coprime integer a:

$a^{p}-1 \equiv 1(\text{mod } p)$

To test whether a number p is prime, we choose a random integer a that is not divisible by p.

a is chosen from 1<a<p-1 as the congruence stated above also holds if p is odd and $a^{p}-1 \equiv -1(\text{mod } p)$.

if the congruence doesn't hold then it is a composite number otherwise, the numbers are called probable primes. Among these probable primes, the composite numbers for which the equation holds are called Fermat's liar or Fermat's pseudoprime with base a.

3.4 Miller–Rabin primality test

In 1976, Mathematician and theologian Gary Miller discovered this test as deterministic, but its credibility depends on the extended Riemann hypothesis which is unproven to date. Later in 1980, Mathematician and computer scientist Michael O. Rabin worked on it and modified it as an absolute probabilistic test. This test states that for p to be a strong probable prime following congruences should hold.

1. $a^{d} \equiv 1(\text{mod } p)$
2. $a^{(2^{\wedge}r)\cdot d} \equiv -1(\text{mod } p)$ for some $0 \le r < s$

Here, p is an odd integer greater than 2 written in the $2^{s}\cdot d + 1$ form where both s and d are positive integers and d has to be odd. Integer a is called a base. It should lie in between 0 and p. A random base a is chosen to test p for probability, if p is in fact composite then it has lesser chances of being a strong pseudoprime as congruences do not hold for multiple bases. The strong probable primes found are further tested using deterministic tests.

4. Digital root

In mathematics, the value obtained by summing the digits of a number is called the digit sum of that number whereas the value obtained through an iterative process of summing digits of a number until it becomes a single digit is called the digital root of that number. For example, the digit sum of 5667 is 5+6+6+7=24 and the digital root is 2+4=6.

4.1 The digital root of multiples of 3

The digital root of multiples of 3 can only be 3,6, or 9. Proof of the theorem lies in the divisibility rule of 3 which says a number is divisible by 3 if its digit sum is a multiple of 3. If we consider n as a number and n1 as its digit sum, then for n to be divisible by 3, n1 must be a multiple of 3. In the same way for n1 to be divisible by 3, the digit sum of n1 must be a multiple of 3. If we continue the same process repeatedly until it becomes a single digit, we will be left with either 3,6, or 9 as they are the only single-digit multiples of 3. Hence for any multiple of 3, The digit root will always be 3,6, or 9.

For example, consider the number n=8481 which is also a Fermat pseudoprime.

For 8481 to be divisible by 3, The addition of its digits, 8+4+8+1=21 must be a multiple of 3

In this case, 21 is a multiple of 3. Further for 21 to be divisible by 3,

The addition of its digits, 2+1=3 must be a multiple of 3.

In this way, any number having 3,6 or 9 as its digital root is a multiple of 3 therefore a composite number.

Further to prove the divisibility by 3 theorem, we will be considering X as a number that can be written in the following form.

$X=a_0+a_1\times10+a_2\times10^2+a_3\times10^3...+a_n\times10^n$
X can be rearranged and written as,
$X= a_0+a_1\times(9+1) +a_2\times(99+1)+ a_3\times(999+1)...+a_n\times(9...9$ (9 occurs n times))
$X= a_0+9\times a_1+ a_1+99\times a_2+ a_2+ 999\times a_3+ a_3...+9...9$ (9 occurs n times) $\times a_{n+} a_n$
$X=\mathbf{9\times a_1+99\times a_2+999\times a_3+9...9}$ **(9 occurs n times)** $\mathbf{\times a_n}+a_0+a_1+a_2+a_3...+a_n$

In the above equation, coefficients of a_n are always 9 repeated n times in the highlighted part of the equation so it can be concluded that the highlighted part of the equation will always be divisible by 3 as 9 repeated n times is a multiple of 3. Hence proved that for X to be divisible by 3 the remaining part of the equation $(a_0+a_1+a_2+a_3...+a_n)$ which is equal to the addition of all the digits of X must be a multiple of 3.

4.2 The digital root of multiples of 9

When any number is multiplied by 9 its digital root will always be 9. Proof of this statement lies in the divisibility rule of 9 which says for any number to be divisible by 9, the digital sum of that number must be divisible by 9. Similar to the proof of divisibility by 3, The highlighted part of a number $X=\mathbf{9\times a_1+99\times a_2+999\times a_3+9...9}$ **(9 occurs n times)**

$\times a_n+a_0+a_1+a_2+a_3...+a_n$ will always be divisible by 9 as 9 repeated n times is a multiple of 3. Hence proved that for X to be divisible by 9, The addition of digits of X ($a_0+a_1+a_2+a_3...+a_n$) must be divisible by 9.

Also similar to the digital root of 3, The only single-digit multiple of 9 is 9 itself. Therefore, any number having a digital root as 9 is multiples of 9, and hence it is a composite number.

5. Application of digital root as a feasible probabilistic test

Prime numbers are mysterious. Apart from their numerous applications, they only get harder to find as they get larger. Using this probabilistic test, any smaller or larger non-prime numbers can be filtered out in a very less time before proceeding with other probabilistic tests or deterministic tests. This test states that for a number p to be prime, its digital root can only be 1,2,4,5,7,8. If the digital root is 3,6 or 9 then the number is certainly composite and should not be further tested.

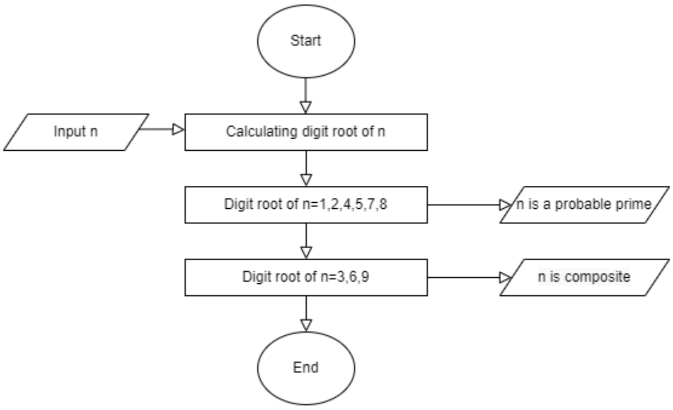


Fig-1 Algorithm of the probabilistic test using digital roots

5.1 Finding digital roots of numbers in the form of $2^n \pm 1$

For 2^n-1, the digital root repeats itself for n>6 as per the table given below.

Number (2^n -1)			Digital root	Remainder x=n%6
2^1-1	1	1	1	1
2^2-1	3	3	3	2
2^3-1	7	7	7	3
2^4-1	15	1+5=6	6	4
2^5-1	31	3+1=4	4	5
2^6-1	63	6+3=9	9	0

Table-1 Digital roots of 2^n-1 as per the remainder obtained

For the equation n≡ x (mod 6),

Consider n as the exponent of 2 and x as the remainder when n is divided by 6.

Any number greater than 0, when divided by 6, will give a remainder in the range from 0 to 5.

When the division results in the remainder x=1 then the digital root of the number will be 1.

Similarly, When the division results in the remainder x=2 then the digital root of the number will be 3.

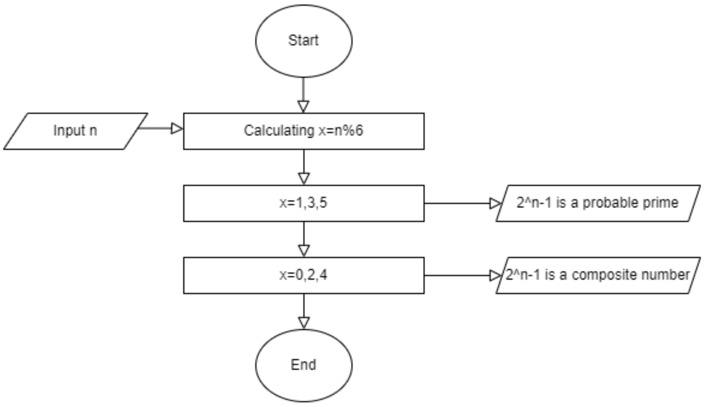


Fig-2 Algorithm for finding digital roots of 2^n-1

Similar to 2^n-1, the digital root repeats itself for n>6 for 2^n+1 as well.
The remainders when n is divided by 6 and the resulting digital root for 2^n+1 are given in the table below.

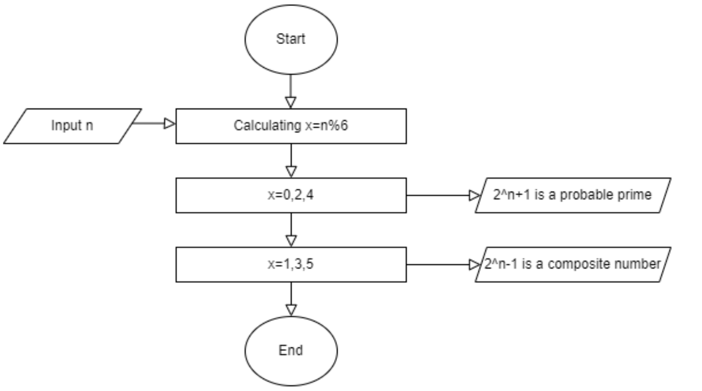


Fig-3 Algorithm for finding digital roots of 2^n-1

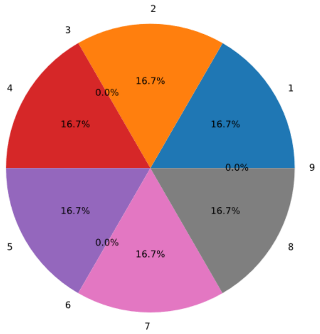
Number (2^n +1)			Digital root	Remainder x=(n%6)
2^1+1	3	3	3	1
2^2+1	5	5	5	2
2^3+1	9	9	9	3
2^4+1	17	1+7=8	8	4
2^5+1	33	3+3=6	6	5
2^6+1	65	6+5=11(1+1=2)	2	0

Table-2 Digital roots of 2^n+1 as per the remainder obtained

6. Prime numbers and their digital roots with graphical representation using python programs.

6.1 Prime numbers from 2 to 2^{26}

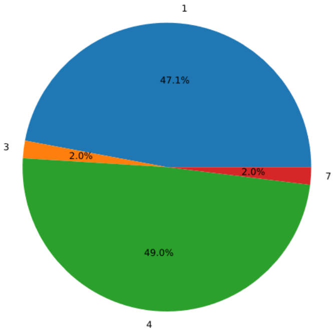
These prime numbers were obtained using the sympy python library and their digital roots were calculated with the help of the math python library. The digital roots of these numbers are almost equally distributed among 1,2,4,5,7,8.



Piechart Ditribution of Digital Roots of Prime Numbers from 2 to 2^26

6.2 Mersenne's Primes

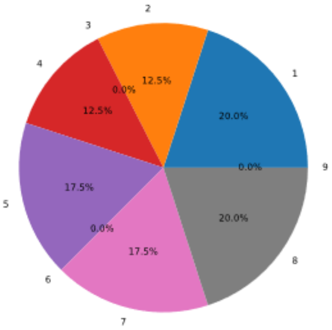
Mersenne's primes are in the form of 2^n-1 therefore the digital roots of these primes can be calculated directly using Fig 2 and Table 1.



Piechart Distribution of Digital roots of Mersennes primes

6.3 Twin Primes

If the digital root of twin prime P is n then the digital root of P+2 will be n+2 except if n=8 then the digital root of P+2 will be 1. The following pie chart represents the distribution of digital roots among the 20 largest twin prime pairs.



Piechart Ditribution of Digital Roots of 20 largest Twin Primes

6.4 Factorial Primes

When any number is multiplied by 9, its digital root is always equal to 9. The factorial primes are in the form of n! ±1. As n! is the multiplication of all the numbers from 1 to n, n! will always include 9 in its multiplication for all the numbers greater than 8. Therefore, the digital root of all the factorial primes where n>8 is 1 for n! + 1 or 8 for n! -1. For factorial primes where n<8 will have 3 in the multiplication of n!. As mentioned earlier multiples of 3 can have digital roots 3,6, or 9 only. Therefore, the digital root of the factorial primes where n<8 is 4,7,1 for n! +1 or 2,5,8 for n! -1.

6.5 Primorial Primes

Like Factorial primes, All Primorial Primes are in the form of p#±1 where p# is the multiplication of all the prime numbers from 1 to p. p# will always have 3 in its multiplication therefore p# is a multiple of 3 hence primorial primes can have digital roots of 4,7,1 for n! + 1 or 2,5,8 for n! -1.

7. Applications of prime numbers

The various applied uses of prime numbers justify the importance and time focused on understanding and learning their properties.

In cryptography, the RSA algorithm created by Ron Rivest, Adi Shamir, and Len Adleman makes extensive use of prime numbers to create public and private keys that are to be used for the encryption and decryption of any message. It is easy to multiply two large prime numbers and produce a very large composite number, but it is extremely time-consuming to do the reverse of that process rigorously. No algorithm exists to date to make this prime factorization easier because of this prime numbers are used to do monetary transactions and to protect data. Prime numbers are also used to define the color intensity of the pixels on computer screens.

In nature, Scientists discovered that Cicada insects also known as Periodical Cicadas use a predator-prey model to increase their survival rate. They do so by only leaving their burrows in the intervals of prime numbers such as 7,13, or 17 years. To understand this model, we can consider a predator of the life cycle of 6 years and Cicada of the life cycle of 17 years. If Cicadas hide underground away from their predators for 16 years and come out to feed and mate the next year, then around 2 generations of the predator are deprived of feeding on Cicadas and hence resulting in the reduction of their population. In 1963, mathematician Stanisław Ulam demonstrated how arranging prime numbers in a certain way produces a spiral that resembles patterns already existing in nature such as the rose's petals.

8. CONCLUSIONS

The importance of prime numbers is scientifically verified and as the applications of prime numbers are irrefutably needed, it is necessary to learn as much as we can about them. This paper gives insight into how prime numbers can have specific digital roots only and how they are distributed among them. It is also included how digital roots of larger numbers can be found directly in a matter of few seconds and how prime numbers with certain digital roots can be discarded directly without having to check for primality.

REFERENCES

[1] G.H. Hardy and E.M Wright, An Introduction to the Theory of numbers, Oxford press

[2] "Survey on prime numbers" by A.R.C.De Vas Gunasekara, A.A.C.A.Jayathilake and A.A.I.Perera

[3] Ghannam, T. (2012) The Mystery of Numbers: Revealed through Their Digital Roots. 2nd Edition, Create Space Publications, Seattle.

[4] "A Dynamical Systems Proof of Fermat's Little Theorem", Kevin Iga, Mathematics magazine, Vol. 76, No. 1. (Feb 2003)

[5] "Prime numbers and their analysis" by Mit Patel, Alok M. Patel, R.B.Gandhi.

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

[7] "PRIMES is in P" by Manindra Agrawal Neeraj Kayal Nitin Saxena.

[8] http://mathworld.wolfram.com/PrimeNumberTheorem.html

[9] "Finding prime numbers" by Jovan Jovancevic

[10] https://primes.utm.edu/primes/

[11] https://brilliant.org/wiki/digital-root/

[12] "On Some Properties of Digital Roots" by Ilhan M. Izmirli