

**The Distribution of Primes Ending in 1, 3, 7, and 9.**

**with Consideration of Their Primitive Roots**



**By: Matthew Myers, Brandon Hopper, and Rossoul Parsons. UNCA Higher Education Prison Program Participants. This presentation was prepared for STAT 185, taught by Professor Bahls.**

**Abstract**

All primes < 1,416,360 – excluding two and five (108,244 primes) – and multiple groupings of them, were arranged by various value ranges and prime counts. A TI-89 calculator with custom programming and Microsoft Excel Macros was used to test, gather, sort, and count primes. After the data was collected, several different statistical methods were applied to analyze the information, and locate exceptional outliers and patterns. Primes are evenly distributed by their last digit (1,3,7,9) when ignoring their primitive root, as is predicted by the Dirichlet prime number theorem. It was determined that the distribution of primitive roots is not always random, but does follow rules, which means it has some structure. Based upon the results of our distribution testing, we believe that primes which end in 1 are the most difficult to calculate a primitive root for. It is suggested that more testing of larger lists of prime numbers, numerous larger primitive root values, and different moduli be completed before cryptographers attempt to apply the discoveries made in this report.

**The Distribution of Primes Ending in 1, 3, 7, and 9 with Consideration of Their Primitive Roots.**

**INTRODUCTION**

While people who are not interested in number theory may believe that exploring prime numbers is a useless endeavor, prominent mathematicians throughout history such as Carl Friedrich Gauss viewed it as one of the most important and useful exercises in arithmetic.1(p.13)Anyone who wants to maintain their privacy online, unintentionally utilizes prime numbers with public key cryptography. School children are taught about primes and factors, but not primitive roots; which some key exchange systems, like the Dippie-Hellman scheme, use.2(p.8) New computer processor units are also tested by utilizing prime number and primitive root computations. This has caught microchip design errors in the past, and prevented the mass production of defective hardware.

A prime number is a number that is greater than 1 and not divisible by any other integer than one and itself. Any number greater than 1 that is not a prime number is considered to be a composite number. The number 1 is neither prime nor composite. Sometime after 600 BC, Pythagoras and his disciples were the first to rigorously separate integers by their mathematical properties: even numbers (2,4,6,8…) odd numbers (1,3,5,7…) prime numbers (2,3,5,7…) composite numbers, polygonal numbers, etc.3(p. 1,2) There are many other classifications of numbers that have been developed since that time – such as perfect numbers, Mersenne numbers, Fermat numbers, irrational numbers, and transcendental numbers (to name just a few) but those are not our focus for this project.

The Prime Number Theorem, conjectured by Gauss and Legendre in the 1790s and proved by Hadamard and De La Vallee in 1896, states that the Quantity Q of primes not exceeding x approaches x/loge(x): Q(x) ~ . This means primes become increasingly rare.

Here is a brief table of this function and its comparison with x/loge , where loge(x) is the natural logarithm of x.

|  |  |  |  |
| --- | --- | --- | --- |
| x | Q(x) | x/loge(x) | Q(x)÷x/loge(x) |
| 10 | 4 | 4.3 | 0.93 |
| 102 | 25 | 21.7 | 1.15 |
| 103 | 168 | 144.8 | 1.16 |
| 104 | 1,229 | 1,086 | 1.13 |
| 105 | 9,592 | 8,686 | 1.10 |
| 106 | 78,498 | 72,382 | 1.08 |
| 107 | 664,579 | 620,420 | 1.07 |
| 108 | 5761,455 | 5,428,681 | 1.06 |
| 109 | 50,847,534 | 48,254,942 | 1.05 |
| 1010 | 455,052,511 | 434,294,482 | 1.048 |

Every prime number has at least one primitive root, most have several.4(p.131) A primitive root of a prime number p, is a number N such that Np-1/p has a remainder of 1, but for no lower power of N does this equation hold true. For every p this has the result of generating the list of all numbers between N and p-1 as every integer exponential power is cycled through. We know from Dickson6(p.197) that "E. de Jonquieres proved that the product of an even number of primitive roots of a prime p is never a primitive root...", so combinations such as 2, 3, and 6 as primitive roots do not have to be tested. This is useful in advanced mathematics that the three of us have become intrigued by. Our goal was to test Stewarts statement that, “there seems to be no really simple way of finding a primitive root for large values of p”. 4(p.131)

**METHODOLOGY**

We began gathering data using a TI-89 calculator running custom written functions to efficiently determine primitive roots for primes and their distributions. When laptops were made available to our class, we verified the collected data for the first 10,000 primes (excluding 2 and 5) using a brute force method to prevent miscalculation. After this confirmation of good programming code, we continued our data collection process for the remainder of primes in the studies range. We generated our list of primes by using a modified version of the procedure known as “The sieve of Eratosthenes”. In our method, where all numbers up to N are recorded, then multiples of each prime < are eliminated5(p.4) we first listed all of the candidate numbers (3,7,11,13,17, and all primes > 17 that are not divisible by a prime <19) between one and 1,416,360 then removed all multiples of each prime above our starting point, up to 1190 (the square root of 1,416,360) which left us with just prime numbers. 1,416,360 was chosen as the upper limit due to practicality and =100,000 when x = 1,416,360. We utilized Microsoft Excel and its Macro editor to complete the computations of all primes and primitive roots within our aforementioned parameters.

Though conducting brute force solving on the laptop was quicker than the efficient code on the TI-89, we still faced limitations. Due to the absence of internet access to validate Microsoft Office, we were unable to access Excel for a period of time, until “tech support” found time in their busy schedule to assist us.

We used the following programming code in Microsoft Excel’s MACRO Editor to test by brute force for primitive roots because VBA does not have the functioning capacity to test for primality or factoring numbers.:

Function TEST\_ROOT (Prime, Root)

TEST\_ROOT=0

VC = Root

VD = Prime – 1

For VF = 1 To VD

VC = VC \* Root

VC = VC – Int (VC / Prime) \* Prime

If VC = 1 Then Exit For

Next

If VF = VD – 1 Then TEST\_ROOT = 1

End Function

**FINDINGS**

As predicted by Dirichlet’s theorem on arithmetic progressions7(p.3)the distribution of primes ending in 1,3,7, and 9 are randomly equivalent.

Once primitive roots are taken into consideration, randomness is reduced. Many people have shown that primes of certain forms have certain primitive roots.6(p.184-199) This demonstrates structure. Our analysis showed that 5 is not a primitive root for any prime ending in 1 or 9 that is less than 1,416,433. If a prime ends in 3 or 7, then we are 95% confident that 5 is its primitive root between 78.3% and 79.0% of the time. The proportion of primes ending in 1,3,7, and 9 are affected by what primitive root we group them by, but not the range of primes counted. See appendix A for further data concerning alternate groupings. Primes ending in 1 are underrepresented for the primitive roots of 2,3,5,7, and their combinations.

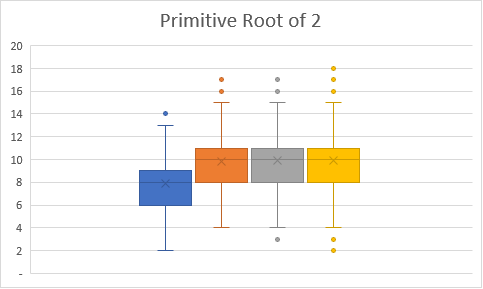


The above data summary shows values taken from a data set of 1,000 groups of 100 primes. The Chi-Square Test values near 0 show that we do not expect the distribution among prime endings to be random, unlike when primitive roots are not considered which has a value near 1.



The above data summary shows when 5 is a primitive root of a prime, we found no primes ending in 1 or 9 in any of the 1,000 groups of 100 primes. While all the Chi-Square Test values are high enough to infer random distributions of primes ending in 3 and 7, it would be interesting to see if the value for primes with primitive roots of 7 stays comparatively low at 0.1817 with a larger data set of primes.

The graph below shows the boxplots generated from distribution coubts of 1,000 groups of 100 primes.



Ending in 1, 3, 7, and 9

Primes ending in 1, 3, 7, and 9

It is our hope that these results will inspire further research that may prove that 5 is never a primitive root of any prime ending in 1 or 9. From the primitive roots we used, it appears that primes ending in 1 are the hardest to compute a primitive root for. Further testing of other primitive root values is needed before cryptographers can take advantage of this preliminary research.

**References**

1. Ribenboim, P. The Book of Prime Number Records. New York (NY): Springer-Verlag; 1988
2. Primitive Root Modul n. Wikipedia; c2016 [updated 2016 December 20; accessed 2017

February 8]. <https://en.wikipedia.org/wiki/Primitive_root_modulo_n>.

1. Apostol, TM. Introduction to Analytical Number Theory. New York (NY): Springer Science

+ Business Media, Inc; 1976.

1. Stewart, B.M. Theory of Numbers, Second Edition. New York (NY): The Macmillan

Company; 1964.

1. Hardy, G.H. & Wright, E.M. An Introduction to the Theory of Numbers. Fifth Edition. New

York (NY): Oxford University Press; 1998.

1. Dickson, L.E. History of the Theory of Numbers: Vol. 1. Divisibility and Primality. New

York (NY): G.E. Sterchert 7 Co.; 1934

1. Dirichlet’s Theorem on Arithmetic Progressions. Wikipedia; c2018 [updated 2018 Dec 27;

accessed 2019 Mar 7]. <https://en.wikipedia.org/wiki/Dirichlet%27s_theorem-on->

arithmetic\_progressions.