HISTORIC DEVELOPMENT OF PRIME NUMBERS

A THESIS
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
IN THE GRADUATE SCHOOL OF THE
TEXAS WOMAN'S UNIVERSITY

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCES
COLLEGE OF ARTS AND SCIENCES

BY

BRENT RYDER, B.S.

DENTON, TEXAS

MAY 2014

DEDICATION

I dedicate this work to my family and friends without whose support I would not have been able to complete my studies let alone remain as sane as I am upon completion.

ACKNOWLEDGEMENTS

Through the process of writing this thesis I have been helped and encouraged by many. I would especially like to thank my parents for providing a home and the freedom to pursue my academic goals. I would also like to thank my brother Dale and my friends Lawrence, Rita, Chris, and Victor for their support and encouragement to complete this work. I would also like to thank Dr Edwards for all of his understanding and efforts on my behalf. I know how busy good administrators can be and this makes the time he afforded me doubly appreciated.

ABSTRACT

BRENT RYDER

HISTORIC DEVELOPMENT OF PRIME NUMBERS

MAY 2014

The purpose of this thesis is to investigate the history of prime numbers and development of prime number theory. There are three major sections to this thesis, Ancient times, Dark Ages, and Modern times. The ancient time's section has topics on the 'Ishango Bone', 'Rhine Papyrus' with an investigation of Egyptian fractions, and Euclid's Elements where the proof of the existence of an infinite number of primes was first given. The 'Dark Ages' section has topics on non-European mathematicians who worked with prime numbers. The final section covers more modern prime number theory from Gauss, Fermat, Legendre, and Riemann.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

I have always been fascinated with numbers and what can be done with them. I had, of course, been introduced to prime numbers in grade school and investigated them at that time, but my investigations did not produce anything of note. In graduate studies I took a course on elementary number theory taught by Dr. Ellina Grigorieva, I was introduced to number theory and then to prime number theory with Wilson's Theorem and Fermat's little theorem. I was excited by this branch of mathematics and in performing online searches I came across Riemann's Hypothesis and was enthralled with the concept and sought out further information. In order to understand modern concepts of number theory, I decided that I have to learn more about prime numbers through their historic development. .

Prime numbers are important because they are the basic building blocks of all integers. This is known as the Fundamental theorem of Arithmetic, which states that every integer can be broken down into its unique prime number decomposition. As there are an infinite number of primes, it cannot be said that all primes will ever be known. This being said, the proof of Riemann's Hypothesis may allow the direct calculation of any prime number. Being able to calculate any prime would make it possible to determine if a given number is prime or not, aid in the prime decomposition of a given number if not prime and allow the use of very large primes for everyday application.

This work is broken into three chapters, the first covers ancient times and the development of mathematics, the necessary conditions for knowledge of prime numbers, and the first work done with prime numbers. The second chapter covers the ‘Dark Ages’ where virtually no work was done in Europe, but was continued in the other cultures around the world. Lastly, I investigated the more recent work concluding with the Riemann Hypothesis which changed the face of Prime Number Theory.

Riemann’s contemporaries were an enviable group of the greatest mathematicians in the history of mankind. He was a student of Gauss and contemporary of Dirichlet. Other greats such as Fermat, Euler, Legendre, and more made that time in history one of great change and discovery. This research has been very enlightening and inspiring.

CHAPTER II

ANCIENT TIMES

There is evidence that in the time of Neanderthal man, mates were chosen for their mathematical ability. [1] This is not to say they knew math as we do today, but being able to know the difference between more and less is a survival trait and I would surmise that through such natural selection, mathematics became an innate ability. Recent studies have shown that infants are able to subitize, that is to say able to discern up to three objects at a glance, and even understand basic addition and subtraction.[2] I mention this because the basic need for the concept of a prime number is a higher order of math than this, that of division. For division, what is needed is not only subitizing, or counting, numbers or objects, but doing so repeatedly until the original group of objects is sub grouped evenly as many times as is needed. In ancient cultures, the concept of division would not be developed abstractly until a high enough precision in sub dividing a group of objects was required. Based on this observation, it is not likely that the abstract concept of division would have been developed 10,000 to 20,000 years ago which is where we find the first purported instance of prime numbers.

Ishango Bone

The Ishango bone was found in 1960 by Jean de Heinzelin de Braucourt at an archeological dig site in Zaire at a village that had been buried by volcanic fallout. [3]

The bone is about four inches long, has a crystal adhered to one end and has a number of markings carved in it in three lines along the length of the bone. These markings are why this relic is being included because two of the rows of markings are grouped by prime numbers (see images on the next page).

While no conclusive evidence has been forwarded that the bone was indeed a mathematical tool, one column of markings on the Ishango Bone are of all the prime numbers between 10 and 20. Another column has groupings of numbers which could suggest rudimentary multiplication and division problems. There has also been speculation that the bone was just a tally stick or possibly a method of tracking a woman’s menstruation cycle. Many explanations can be made for the markings and I find it apocryphal to formally ascribe any of them with any degree of surety. What is important is that these markings have sparked so much thought and inventiveness which can only forward the sciences in general and mathematics specifically.

Figure 1. Black and white photos of all sides of the Ishango Bone.

From http://www.math.buffalo.edu/mad/Ancient-Africa/ishango.html

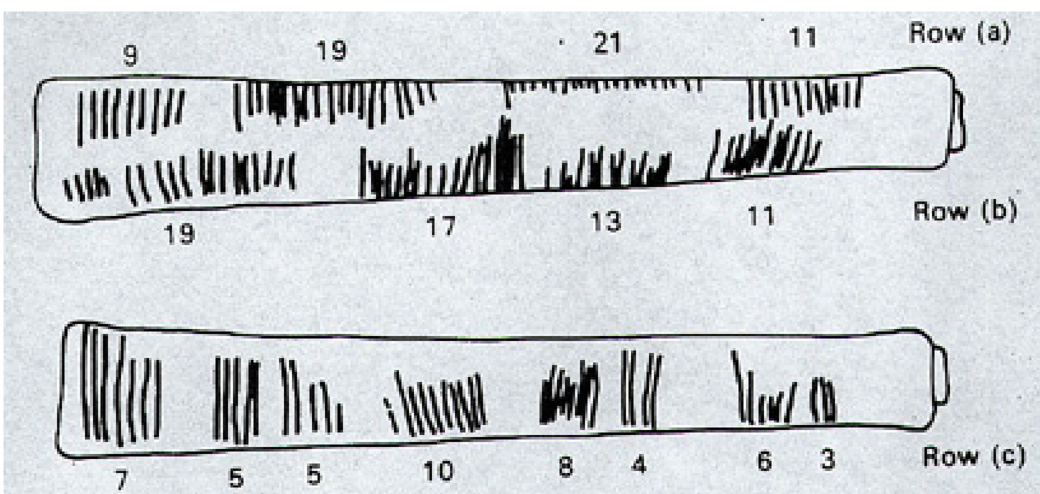


Figure 2. Line drawings of the Ishango Bone showing the grouping of marks.

Plimpton 322

Plimpton 322 refers to catalog item number 322 of the G. A. Plimpton Collection at Columbia University. [4] The item is a mostly intact Babylonian tablet dating from 1900 to 1600 BCE. The remarkable thing about the tablet is that the mathematical markings are said to be of Pythagorean triplets best known in the form $a^2 + b^2 = c^2$ where 'a', 'b', and 'c' are natural numbers. A portion of the left edge of the tablet was broken off so some of the numbers in the first column are missing. The columns also only give 'a' and 'c' from the above equation and mathematicians have inferred the 'b' component. While the argument is compelling, without the missing information or another similar tablet, there will never be certainty in the meaning of this tablet.

What makes Plimpton 322 a part of this thesis is that Pythagorean triplets are 'relatively' prime to each other. That is to say that none of the elements, 'a', 'b', or 'c,' have any common divisor other than one. This is a tenuous link at best to prime numbers. The creator of the tablet would not have called these numbers Pythagorean triplets, "The Old Babylonians knew the Pythagorean Theorem (better called the rule of the right triangle for them since there's no evidence they had a proof; Gillings calls the term "the Pythagorean theorem" a true mumpsimus)." [4]

From http://www.dictionary.reference.com/browse/mumpsimus a mumpsimus is an "adherence to or persistence in an erroneous use of language… out of habit or obstinacy".

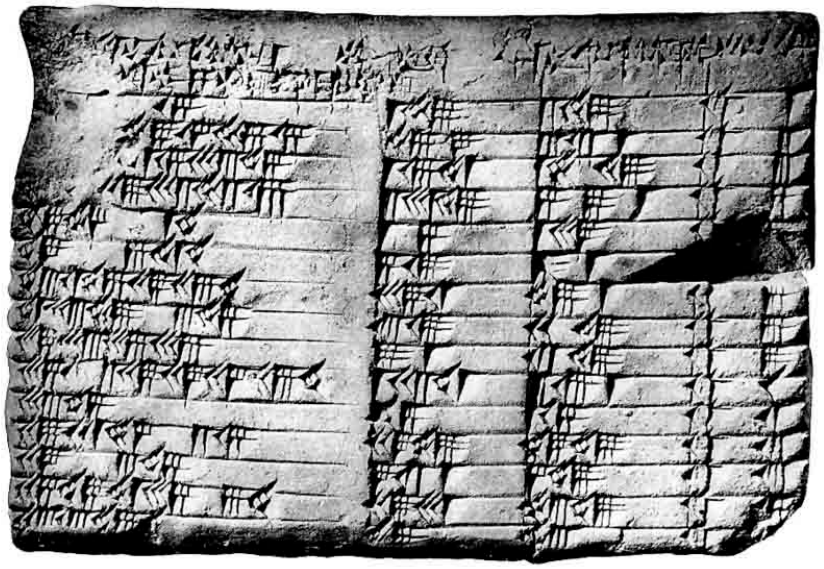


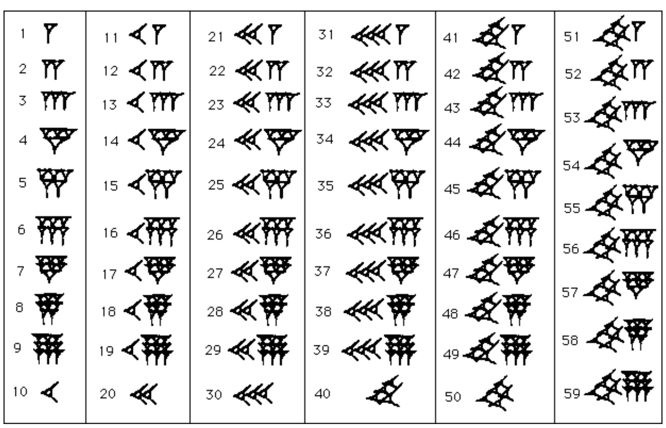
Figure 3. Photo of the Plimpton 322 tablet. From

http://www.historyofinformation.com/expanded.php?category=Mathematics+%2F+Logic

Table 1

Table of Sumerian sexagesimal number system. From

http://www.mathematicsmagazine.com/Articles/TheSumerianMathematicalSystem.php



Rhind Papyrus

The Rhind Papyrus is so named because "In 1858, A. Henry Rhind purchased a partial papyrus in Luxor, Egypt." [5] The papyrus was written by an Egyptian scribe, Ahmes, in about 1650 BCE. Portions of the document seem to have come from an earlier artifact, the Early Mathematical Leather Roll from about 1800 BCE. What makes this a subject of this thesis is that numerical analysis of Ahmes' work in the 2/*n* table show problem solving strategies indicating knowledge of prime numbers. This can be seen in the way the fractions involving prime numbers were handled as opposed to non-prime fractions.

When I first encountered the 2/*n* table reference, I started work on determining a method of converting *2/n*. To this end I struck upon a simple method that can be calculated with the following formula,

$$\frac{2}{p} = \frac{2}{p+1} + \frac{2}{p(p+1)}$$

As an example, for $p = 7$

$$\frac{2}{7} = \frac{2}{7+1} + \frac{2}{7(7+1)} = \frac{2}{8} + \frac{2}{7*8} = \frac{1}{4} + \frac{1}{28}$$

We can derive this easily. Let us assume the denominator of our fraction is composite of two sequential integers:

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1} \tag{1}$$

An example would be:

$$\frac{1}{12} = \frac{1}{3*4} = \frac{1}{3} - \frac{1}{4} = \frac{4}{12} - \frac{3}{12} = \frac{1}{12}$$

This can be extended to non consecutive integers. Let us show that the following formula is also true

$$\frac{1}{n(n+k)} = \frac{1}{k}\left(\frac{1}{n} - \frac{1}{n+k}\right) \tag{2}$$

Using the right-hand side, we find a common denominator and reduce

$$\frac{1}{k}\left(\frac{1}{n} - \frac{1}{n+k}\right) = \frac{1}{k}\left(\frac{n+k-n}{(n)(n+k)}\right) = \frac{1}{n(n+k)}$$

$$\frac{k}{n(n+k)} = \frac{1}{n} - \frac{1}{n+k}$$

$$\frac{1}{n} = \frac{k}{n(n+k)} + \frac{1}{n+k}$$

$$\frac{2}{n} = \frac{2k}{n(n+k)} + \frac{2}{n+k}$$

Let us consider if there are any other values of k, different from k=1, for which the fractions on the right side of the formula

$$\frac{2}{n} = \frac{2k}{n(n+k)} + \frac{2}{n+k} \tag{3}$$

can be reduced and have the numerators 1.

If such is possible, then because n is a prime number, $(n+k)$ must be divisible by 2k, then the following must be true:

$$n + k = 2k \cdot m$$

$$n = k \cdot (2m - 1)$$

The last formula contradicts the condition that n is prime, and it is true only for k=1.

Therefore, the always true formula (3) can explain the Table only for k=1 when it becomes (1). This is in line with the 2/n table and in fact matches the answers in the table until $p > 7$ and then only matches with the 2/n table occasionally. For example for 2/23.

Answers to how the other fractions were obtained can be found in the Works of the 2008 article by Milo Gardner [6], and in the History of Mathematics book by Eves [20].

Table 2

Egyptian 2/n Table, Primes Only, Through 101

$\frac{2}{3}=\frac{1}{2}+\frac{1}{6}$	$\frac{2}{43}=\frac{1}{42}+\frac{1}{86}+\frac{1}{129}+\frac{1}{301}$
$\frac{2}{5}=\frac{1}{3}+\frac{1}{15}$	$\frac{2}{47}=\frac{1}{30}+\frac{1}{141}+\frac{1}{470}$
$\frac{2}{7}=\frac{1}{4}+\frac{1}{28}$	$\frac{2}{53}=\frac{1}{30}+\frac{1}{318}+\frac{1}{795}$
$\frac{2}{9}=\frac{1}{6}+\frac{1}{18}$	$\frac{2}{59}=\frac{1}{36}+\frac{1}{236}+\frac{1}{531}$
$\frac{2}{11}=\frac{1}{6}+\frac{1}{66}$	$\frac{2}{61}=\frac{1}{40}+\frac{1}{244}+\frac{1}{488}+\frac{1}{610}$
$\frac{2}{13}=\frac{1}{8}+\frac{1}{52}+\frac{1}{104}$	$\frac{2}{67}=\frac{1}{40}+\frac{1}{335}+\frac{1}{536}$
$\frac{2}{17}=\frac{1}{12}+\frac{1}{51}+\frac{1}{68}$	$\frac{2}{71}=\frac{1}{40}+\frac{1}{568}+\frac{1}{710}$
$\frac{2}{19}=\frac{1}{12}+\frac{1}{76}+\frac{1}{114}$	$\frac{2}{73}=\frac{1}{60}+\frac{1}{219}+\frac{1}{292}+\frac{1}{365}$
$\frac{2}{23}=\frac{1}{12}+\frac{1}{276}$	$\frac{2}{79}=\frac{1}{60}+\frac{1}{237}+\frac{1}{316}+\frac{1}{790}$
$\frac{2}{29}=\frac{1}{24}+\frac{1}{58}+\frac{1}{174}+\frac{1}{232}$	$\frac{2}{83}=\frac{1}{60}+\frac{1}{332}+\frac{1}{415}+\frac{1}{498}$
$\frac{2}{31}=\frac{1}{20}+\frac{1}{124}+\frac{1}{155}$	$\frac{2}{89}=\frac{1}{60}+\frac{1}{356}+\frac{1}{534}+\frac{1}{890}$
$\frac{2}{37}=\frac{1}{24}+\frac{1}{111}+\frac{1}{296}$	$\frac{2}{97}=\frac{1}{56}+\frac{1}{679}+\frac{1}{776}$
$\frac{2}{41}=\frac{1}{24}+\frac{1}{246}+\frac{1}{328}$	$\frac{2}{101}=\frac{1}{101}+\frac{1}{202}+\frac{1}{303}+\frac{1}{606}$

Euclid (Circa 300 BCE)

The sum total of personal information we have on the greatest geometer in history is that he was born circa 300 BCE, probably trained in Athens and worked in Alexandria. Euclid also wrote on conic sections, perspective, spherical geometry, and number theory. [7] Until the advent of modern geometry in the 20th century, when someone spoke of geometry it was Euclidean Geometry. The first proof of the existence of an infinite number of primes comes from Euclid's Elements [7], book IX, proposition 20, (The references in brackets are to earlier books and propositions within Euclid's Elements):

"Prime numbers are more than any assigned multitude of prime numbers.

Let *A*, *B*, and *C* be the assigned prime numbers.

I say that there are more prime numbers than *A*, *B*, and *C*.

For let the least number measured by *A*, *B*, *C* be taken, [VII, 36]

and let it be *DE*; let the unit *DF* be added to *DE*.

Then *EF* is either prime or not.

First, let it be prime; then the prime numbers *A*, *B*, *C*, *EF* have been found which are more than *A*, *B*, and *C*.

Next, let *EF* not be prime. Therefore it is measured by some prime number. [VII, 31]

Let it be measured by the prime number *G*.

I say that *G* is not the same with any of the numbers *A*, *B*, and *C*.

For, if possible, let it be so.

Now *A*, *B*, *C* measure *DE*, therefore *G* also will measure *DE*

But it also measures *EF*

Therefore *G*, being a number, will measure the remainder, the unit *DF*, which is absurd.

Therefore *G* is not the same with any one of the numbers *A*, *B*, and *C*

And by hypothesis it is prime.

Therefore the prime numbers *A*, *B*, *C*, *G* have been found which are more than the assigned multitude of *A*, *B*, *C*."

I have omitted the image of the line segments from this quote.

To put this into modern terminology: The following statement is true.

Theorem. *There are an infinite number of primes.*

Proof. We will prove this statement by contradiction. Let $(P_1, P_2, P_3, \dots, P_k)$ be all possible prime numbers and let $M = \prod_{n=1}^{k} P_n$ be the least composite number possible of all possible prime numbers.

Let $A = M + 1, then\ A = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$, then A divided by any "known" prime number would give a remainder 1. Thus A is prime. We obtained contradiction. The proof is completed.

If A is prime then there are more primes than are currently known and by extension an infinite number of primes.

Additionally, assume that there are only a finite set of primes and $N = p_k$ is the very last prime number. (For this proof we do not need to list all primes less than N) Consider a product of all natural numbers from 1 to N, called $N!$ (factorial) and add to it one:

$$B = 1 * 2 * 3 * 4 * 5 \cdots * (N-2) * (N-1) * N + 1 = N! + 1$$

Again, when number B is divided by any existing prime less than or equal to N it will leave a remainder of 1. Therefore, $N! + 1$ is a prime and our initial assumption was wrong. Therefore, N is not the largest prime. Moreover, number B will be much greater than A, and of course, much greater than N.

Another proposition from book nine that is of special note is proposition 36, "If as many numbers as we please beginning from an unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the product will be perfect." [7] This is the first reference to perfect numbers which is another application of prime numbers. Perfect numbers are numbers where the sum of the proper divisors of the number equal the number itself. The first one is 6 whose divisors are 1, 2, and 3; and $6 = 3 + 2 + 1$.

The modern translation would be as follows:

Let $P = \sum_{n=0}^{x} 2^x$ where x is the number of iterations necessary to make P a prime number. Then the number $P \times 2^x$ is a perfect number.

In the example given the iterations would be:

First iteration, $2^0 = 1$

Second iteration, $1 + 1 \times 2^1 = 1 + 2 = 3$, which is a prime number

Therefore the perfect number would be $3 \times 2 = 6$ which is the first perfect number.

Third iteration, $3 + 2^2 = 3 + 4 = 7$ which is a prime number

Therefor the second perfect number would be $4 \times 7 = 28$, which is the next perfect number. The divisors of 28 are 1, 2, 4, 7, 14, and their sum is 28.

Eratosthenes (276-195 BCE)

“Eratosthenes was a Greek scholar, chief librarian of the famous library in Alexandria.”[8] He was known as ‘Beta’ and ‘Pentathlos’ because he knew all branches of knowledge well, but none well enough to be first in any. What Eratosthenes is best known for is the “Sieve of Eratosthenes” which is a method of computing primes by elimination. As an example, write down all the numbers from 1 to N. As this is a process of elimination, and knowing 2 is prime, and the only even prime number, the rest of the even numbers are then crossed out. 3 is a prime so cross out every third number after 3. Continue until you have reached a value $x \leq \sqrt{N}$, which is the largest composite value that could be divided into N. The values that have not been crossed out are then prime numbers.

While this is a reliable method of determining primes, it is also time consuming and given to human error especially for large values of N. The method can be converted to an algorithm for a computer to perform which improves reliability so long as the computational time is feasible. What is more important is the ability to use the method for determining the number of primes under a certain value.

The number of primes under a certain value is denoted as $\pi(N)$. The process is started with the first prime, 2, and then built one prime at a time. Define $\lfloor x \rfloor$ as floor function that is the greatest integer not exceeding x. Choosing N=100,

$$100 - \left\lfloor \frac{100}{2} \right\rfloor = 50$$

Next we remove the primes that are a multiple of 3, but then we must add back the composite 3 values. In this case that means all the values that were also cancelled out

$$50 - \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{2 \times 3} \right\rfloor = 50 - 33 + 16 = 33$$

Continuing with removing

$$33 - \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{2 \times 5} \right\rfloor + \left\lfloor \frac{100}{3 \times 5} \right\rfloor - \left\lfloor \frac{100}{2 \times 3 \times 5} \right\rfloor = 33 - 20 + 10 + 6 - 3 = 26$$

$$26 - \left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{2 \times 7} \right\rfloor + \left\lfloor \frac{100}{3 \times 7} \right\rfloor + \left\lfloor \frac{100}{5 \times 7} \right\rfloor - \left\lfloor \frac{100}{2 \times 3 \times 7} \right\rfloor - \left\lfloor \frac{100}{2 \times 5 \times 7} \right\rfloor - \left\lfloor \frac{100}{3 \times 5 \times 7} \right\rfloor$$
$$+ \left\lfloor \frac{100}{2 \times 3 \times 5 \times 7} \right\rfloor = 26 - 14 + 7 + 4 + 2 - 2 - 1 = 22$$

The last step is to add back the primes under $\pi(\sqrt{100})$, which are the primes we have been cancelling out, 2,3,5, and 7. Also, one is added for the number 1 since it is not counted as a prime and was not a part of these calculations. This brings the total to 25. The general form [8] of this process is

$$\pi(N) - \pi(\sqrt{N}) + 1$$
$$= N - \left\lfloor \frac{N}{p_1} \right\rfloor - \left\lfloor \frac{N}{p_2} \right\rfloor - \cdots - \left\lfloor \frac{N}{p_r} \right\rfloor + \left\lfloor \frac{N}{p_1 p_2} \right\rfloor + \left\lfloor \frac{N}{p_1 p_3} \right\rfloor + \cdots + \left\lfloor \frac{N}{p_{r-1} p_r} \right\rfloor$$
$$- \left\lfloor \frac{N}{p_1 p_2 p_3} \right\rfloor - \cdots + \cdots$$

CHAPTER III

THE DARK AGES

The 'Dark Ages' mark a period of restriction in mathematical and scientific research in Europe. This does not mean that there was no research, but what there was must have been done in secret. This is not the case in the rest of the world not under the control of the Catholic Church. Much is owed to the Arabic world for preserving the works of Euclid and the Greeks in general. During the 'Dark Ages' the Arabic mathematicians, as well as mathematicians form other cultures, continued the exploration of mathematics and some few continued to work with prime numbers.

Thabit Ibn Qurra (826 – 901 CE)

The full name of this Arabian mathematician is Al-Sabi Thabit ibn Qurra al-Harrani, and he lived from 826 – 901 CE. I also found other names for Thabit which were all variations and misspellings of this name. During Thabit's life time he translated and edited many documents including editing a translation of Euclid's Elements. Thabit also discovered an equation for amicable numbers.

Amicable numbers are much like the perfect numbers mentioned earlier. The difference is that there are two numbers whose respective divisors sum to the other number. Mathematically, Thabit proved that if $p_1 = 2^{n+1} - 1 + 2^n$, $p_2 = 2^{n+1} - 1 -$

2^{n-1}, and $p_3 = 2^{n+1}(2^{n+1} + 2^{n-2}) - 1$, are three prime numbers greater than 2, then $a_1 = 2^n p_1 p_2$ and $a_2 = 2^n p_3$ are amicable numbers. [9] The proof for this is available in one of Thabit's papers, "*Treatise on the Derivation of the Amicable Numbers in an Easy Way*".

Ibn Al-Haytham (965-1040 CE)

Ibn al-Haytham, known in Europe as Alhazan, has been called the first scientist because of his development and use of the scientific method. He is known for many discoveries in optics and mathematics. When working on the problem of linear congruence, Haytham determined that "if p is any prime number, then the sum $2 \times 3 \times 4 \times \cdots \times (p-1) + 1$ is divisible by p; and if we divide it by any one of the numbers $2, 3, 4, \cdots, (p-1)$, the remainder will always be the unit." [10] In later years this will become known as "Wilson's Theorem" and found more commonly in the modular arithmetic notated form $(p-1)! = -1 (mod\, p)$, which was developed by Gauss in 1796 when he was only 19 years old.

Also found in al-Haytham's work is an attempt to prove the converse of Euclid's perfect number theorem. While the attempt was not successful, it was proven in later years by Euler.

Al-Farisi (Circa 1260-1320 CE)

The full name of this mathematician is Kamal al-Din Abu'l Hasan Muhammad Al-Farisi. [11] Al-Farisi is known for his contribution to the science of optics and numerical analysis. In this later field, Al-Farisi is most known for a refinement to Thabit's equations for amicable numbers. The new formulation for amicable numbers is

For $n > 1$, let $p_n = 3 \times 2^n - 1$ and $q_n = 9 \times 2^{2n-1} - 1$. If p_{n-1}, p_n, and q_n are prime numbers, then $a = 2^n p_{n-1} p_n$ and $b = 2^n q_n$ are amicable numbers.

This new approach included the factorization of numbers into powers of primes which is what is known today as the Fundamental Theorem of Arithmetic.

CHAPTER IV

MODERN TIMES

Once the restriction on mathematical exploration was lifted and the scientific community in general felt they would not be persecuted or excommunicated, there was an explosion in mathematical discovery. Some of this new work involved prime numbers from such great mathematicians as Gauss, Fermat, Euler, and Riemann.

Mersenne (1588-1648 CE)

Marin Mersenne was a monk who felt that science, including mathematics, should be within the reach of the common man. He was an adherent to Ramon Lull's belief that all knowledge can be explained through a few basic truths and with this understanding, the word of God could be explained and believed even by the infidels. Marin carried his belief to the point of corresponding with all of the great minds of his day. His hopes were to be a central point of knowledge of the day. To further this Mersenne also held regular meetings in Paris which eventually led to the foundation of the French Academy of Sciences. [12]

Marin Mersenne is best known for 'Mersenne Primes'. These are prime numbers that follow the expression $2^n - 1$. Mersenne found that if a number is prime and fits this expression, then n is also prime. He also realized the converse is not true as in the case of

$n = 11$ which equals 2047 which is not prime. During his lifetime Mersenne found nine of these primes including $2^{127} - 1$ which is a 36 digit prime.

Fermat (1601-1665 CE)

Often referred to as the greatest amateur mathematician, Pierre Fermat was a prolific mathematician. The only thing Fermat needed to do to be considered a professional mathematician was to actually prove his conjectures instead of forwarding them to the mathematical community for them to prove or disprove. While Fermat did this on occasion, the proofs were never complete. Fermat is known to have shared the development of probability with Pascal, applied the initial concepts of differential calculus before Newton and Leibnitz were born, and developed analytic geometry at the same time as Descartes.

Pierre de Fermat's most important work was in the development of number theory. He defined what a prime was and was not and conjectured that numbers generated by the equation $2^{2^n} + 1$ were primes. This last holds true for $n = 1, 2, 3,$ and 4 but then fails for $n = 5$ and 6. This shows that even great mathematicians can be wrong, but, in Fermat's defense, he never gave a proof of this conjecture. When the equation does hold true, the prime numbers so generated are called "Fermat Primes". An application of these primes comes in the construction of polygons which can be drawn by Euclid's methods. The number of sides of a polygon is either a Fermat Prime or a combination of *different* Fermat Primes. Fermat also conjectured that primes of the form $4n + 1$ is a sum of two squares that can be formed in only one way while primes of the form $4n - 1$ have no solutions of this type. These were later proved to be true by Euler. [13]

The two most famous conjectures of Fermat's were his little theorem and "Fermat's Last Theorem". Fermat's little theorem states that "Given any prime p and any whole number n, the number $n^p - n$ is exactly divisible by p." [12] The modern equivalent of this theorem, using modular notation, is $n^p \equiv n(mod\, p), n \in \boldsymbol{Z}, p \in \boldsymbol{Primes}$. Modular arithmetic is very useful in this instance because it divides p as many times as needed into n^p to give a remainder of n. Dividing both sides of this equation by n gives $n^{p-1} \equiv 1(mod\, p)$.

Fermat's Last Theorem was found as a note in the margin of one of Fermat's books after his death. The Theorem states, "For any integer n (greater than 2), there do not exist any positive integers x, y, and z for which $x^n + y^n = z^n$." [12] Fermat stated in the margin that he had a proof, but that there was not enough room in the margin for it. Fermat did show that $x^4 + y^4 = z^4$ had no positive integer solutions and Euler proved the same for $x^3 + y^3 = z^3$. These are specific proofs and not a general solution. It was not until 1995 that a proof was found by Andrew Wiles.[12]

Euler (1707-1783 CE)

Leonhard (Léonard) Euler was the most prolific mathematician of all time. He is referred to as an "algorist" in that he found algorithms to simplify the calculation of equations. Euler grew up with Jacob Bernoulli as an instructor and his efforts brought him to the attention of Daniel and Nicolaus Bernoulli who became lifelong friends. Leonhard was married twice, had eighteen children, but only 5 survived; was sought after as a national resource by Catherine the Great; and became even more mathematically productive after losing his eyesight completely. [13]

Euler proved Fermat's little theorem in 1736 and in 1760 gave a more general proof of which Fermat's little theorem was a special case. The general case starts with Euler's $\varphi(m)$ function, "When *m* is some integer, we shall consider the problem of finding how many numbers $1, 2, 3, \dots, m-1, m$ are relatively prime to *m*." [8] When *m* is prime, then $\varphi(p) = p - 1$ which should be evident by the definition of a prime number. For the general case, let *p* be some prime dividing *m* and let us first find the number of integers that are not divisible by *p*. These values are multiples of *p*: $p, 2p, \dots, \frac{m}{p}p$. The remaining values that are not divisible by *p* are then $\varphi_p(m) = m - \frac{m}{p} = m\left(1 - \frac{1}{p}\right)$. We repeat this process with other prime(s), i.e. q: $q, 2q, \dots, \frac{m}{q}q$, that divide *m* and compensate for the elements that are in common, i.e. pq: $pq, 2pq, \dots, \frac{m}{pq}pq$, which gives $\frac{m}{q} - \frac{m}{pq} = \frac{m}{q}\left(1 - \frac{1}{p}\right)$. Combining this with our previous result gives

$$\varphi_p(m) = m\left(1-\frac{1}{p}\right) - \frac{m}{q}\left(1-\frac{1}{p}\right) = m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$$

Remembering that by the Fundamental Theorem of Arithmetic,

$$m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$$

where α is the exponent for a given prime divisor, and repeating this process for all primes that divide m we arrive at

$$\varphi_{p_1 \ldots p_t}(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_t}\right)$$

Another way to look at this is to distribute m to give

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right)\cdots\left(p_t^{\alpha_t} - p_t^{\alpha_t - 1}\right)$$

As a side note, this process can be seen as an application of an inductive proof.

Our statement here is that Euler's $\varphi(m)$ function works for all prime decompositions. First we showed that Euler's $\varphi(m)$ function was true for $m = p$, a single prime which could have been 2 as well as any other prime number. Next we assumed it true for $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$. All that is left is to show that the statement holds true for $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_t^{\alpha_t} p_{t+1}^{\alpha_{t+1}}$.

$$\varphi_{p_1 \ldots p_t p_{t+1}}(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_t}\right)$$

$$- \frac{m}{p_{t+1}}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_t}\right)$$

Therefore

$$\varphi_{p_1 \ldots p_t p_{t+1}}(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)\left(1 - \frac{1}{p_{t+1}}\right)$$

This shows that Euler's $\varphi(m)$ function will work for any prime decomposition.

Continuing with the derivation, we now have Euler's Theorem, "For any number a that is relatively prime to m one has the congruence $a^{\varphi(m)} \equiv 1(\bmod m)$." [8] When $\varphi(m)$ is a single prime number with no exponent, then we have Fermat's little theorem, $a^{p-1} \equiv 1(\bmod p)$. With another manipulation, this can also give Wilson's Theorem. There is so much on prime numbers from Euler that I find I have had to choose only a very small representative example. It is estimated that it will take more than 100 volumes to publish all of Euler's work, but before I move on there is one more very important contribution from Euler, Euler's Zeta function. This function showed a deeper connection between arithmetic and multiplication than was hitherto known.

Euler's Zeta function is defined for $s > 1$, where s is any real number, by the infinite sum:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots$$

The infinite sum has a finite answer if s is a real number larger than 1.[14] This is linked to prime numbers in that

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

The process by which this comes about can be seen in a number of the sources I have used. Here is a general outline of the process:

Multiply both sides of Euler's Zeta function by $\frac{1}{2^s}$

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \cdots$$

Subtract this from the original zeta function

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \cdots$$

Just like Eratosthenes Sieve, we have removed all terms with denominators that are multiples of twos from the right hand side. We continue by multiplying through by $\frac{1}{3^s}$

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \cdots$$

And subtract it from the previous equation

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \cdots$$

This process continues infinitely, filtering out one prime and all of its composite forms from the right hand side and multiplying the result to the left hand side. This gives us

$$\prod_p \left(1 - \frac{1}{p^s}\right) \zeta(s) = \prod_p \frac{p^s - 1}{p^s} \zeta(s) = 1$$

Dividing through by the product gives us

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

Combining this with Euler's zeta function

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

This shows a link between the sum of the inverse of all natural numbers to the product of the inverse of $1 - p^{-s}$ of all prime numbers.

Gauss (1777-1855 CE)

Johann Friedrich Carl Gauss was born in Braunschweig, Germany on April 30, 1777. His family was poor and it was only through his mother's efforts that he received an education at all. His father did not want him to be better than him and made this brutally apparent. When Gauss was first able to take a class on mathematics, he astounded his instructor. The instructor, Büttner, went out and bought the best math book available for Gauss with his own money. Gauss promptly breezed through the tome and the instructor said he could teach Gauss nothing more.[13]

Through another serendipitous event, Büttner had an assistant who was mathematically inclined. Johann Martin Bartels worked with Gauss to teach Gauss what he knew and eventually introduced him to influential people. These people led him to Carl Wilhelm Ferdinand, Duke of Braunschweig who paid for the rest of Gauss' education and later career at the University of Göttingen. Gauss published very little during his life and mathematicians are still working out all that he discovered. He was very aptly named the greatest mathematician of the world.[13]

One of the many accomplishments of Gauss was the "…coherent account of complex numbers and to interpret them as labeling points of a plane…" [13] This will be very important in the later work of Riemann. Complex numbers have a real part and what is called an 'imaginary' part. I have emphasized imaginary because the intent was to denote a right angle to the real plane. The intent was not for this to be a mental construct of indeterminate value, but rather a definite location 90 degrees from the working plane(s).

Gauss was very interested in non-Euclidean geometry but would not publish his work in the field for fear of censorship. One of Gauss' students was Bernhard Riemann. When given the choice during Riemann's habilitation, the examination to become a professor, between two topics on mathematics and one on geometry, Gauss chose geometry. The sample lecture that Riemann gave on geometry was one that changed the face of geometry to what we know it today. Riemann's view of geometry even became the basis of Einstein's Theory of General Relativity.

Although Gauss did much work in mathematics, his greatest on the topic of prime numbers was the Prime Number Theorem (PNT). In a letter to Johann Franz Encke, December 1894, Gauss wrote of a recollection from 1792, when he was only 15 that, "…I soon perceived that beneath all of its fluctuations, this frequency is, on average, close to inversely proportional to the logarithm…"[15] In mathematical terms, this is

$$\pi(a) \sim \frac{a}{\ln a}$$

which is the PNT.

The problem with this is that, while it has been proved for a approaching infinity, for lesser values, there is an error factor. I have included a table on the next page to show how this error factor decreases as a increases. It is this error factor that mathematicians such as Legendre, Chebyshev, and Dirichlet endeavored to resolve. To give an idea where these great mathematicians were taking their investigations, I will give some of Legendre's work on the subject in the next section. Also, while Dirichlet was working on this issue, he modified the PNT to a logarithmic integral, $Li(a) = \int_0^a \frac{1}{\log t} dt$. It was this form of the PNT that Jacques Hadamard proved true in 1896.

Table 3

Prime Number Theorem Error Factor Table

a	$\pi(a)$	$\ln a$	$\frac{a}{\ln a}$	% error
1,000	168	6.9077	144.7659	13.8298
1,000,000	78,498	13.8155	72,382.4689	8.4489
1,000,000,000	50,847,534	20.7232	48,255,095.7381	5.0984
1,000,000,000,000	37,607,912,018	27.6310	36,191,234,483.00821	3.7669
1,000,000,000,000,000	29,844,570,422,669	34.5378	28,953,783,970,027.0428	2.9847
1,000,000,000,000,000,000	24,739,954,287,740,860	41.4465	24,127,489,655,338,810.2734	2.4756

Legendre (1752-1833 CE)

Little is known about Adrien-Marie Legendre other than he was born and died in Paris and there is even some conjecture about the location of his birth. Legendre was born to a wealthy family and received the finest education. As he had no need of an income, he taught at College Mazarin with Laplace and otherwise pursued his own researches. The subjects of his research were physics, geometry, mathematics and celestial mechanics.[16]

Legendre did independent work on determining the PNT mentioned earlier not knowing that Gauss had done this already. He went on to do work on the error factor in the PNT. In *Essay on the Theory of Numbers*, Legendre gives the error value as

$$\pi(a) \sim \frac{a}{A \log a + B}$$

for some numbers A and B to be determined. Later he revised this to

$$\pi(a) \sim \frac{a}{\log a - A}$$

where A, for large values of a was close to 1.08366. In one of Gauss' letter to Encke, Gauss refutes the error value while not contributing an answer himself.

Riemann (1826-1866 CE)

Georg Friedrich Bernhardt Riemann was born on September 26th, 1826 in the village of Breselenz, Kingdom of Hanover. His father was a poor Lutheran minister. His mother died before her children had grown up which may have been a blessing to her as only two of her children survived to adulthood. For all the squalor and poor nutrition due to the poverty they lived in, Riemann loved his home and returned to it as often as he could for most of his life.

Riemann was home schooled by his father until he went to the Gymnasium in Hanover, 80 miles away, when he was 14. He was not the best of students as he only focused on what was interesting to him, mathematics. He was also a perfectionist which meant that he would work on his assignments until he was satisfied with them regardless of due dates. Riemann was eventually housed with a teacher who helped him to pass and move on to the University at Göttingen as a theology student where it was believed he would follow his father into the ministry.[15]

When Riemann arrived at the University at Göttingen in 1846 he was not interested in theology. After speaking with his father and gaining his consent, Riemann changed from religion to mathematics as the focus of his studies. Riemann was really excited that Gauss was an instructor at the university. Gauss, on the other hand, hated to teach as he saw it as a waste of time. He attended the linear algebra lectures Gauss gave, but soon found he needed more substance to his studies and transferred to Berlin University. After two years of intense study, Riemann became the mathematician we know of today.

Riemann returned to the University at Göttingen in 1849 to work on his doctorate. After two years he achieved his goal to much acclaim by Gauss. Over the next few years, Riemann made his name and eventually was made a member of the Berlin Academy. This prestigious appointment was also the debut of his most famous work titled "On the Number of Prime Numbers Less Than a Given Quantity". This work was the first time that the Riemann Hypothesis was put before the mathematical community:

All non-trivial zeros of the zeta function have real part one-half.

The zeta function mentioned in the hypothesis is Euler's zeta function, which relates the sum of all natural numbers to the infinite product of prime numbers, but with a very important difference. Riemann conceived of the zeta function in terms of complex numbers. Specifically, by the Riemann Hypothesis, $s = \frac{1}{2} + ai$, where $a \in \boldsymbol{R}$**,** such that $\zeta(s) = 0$. This complex value for s forms a "critical strip" that relates to the distribution of prime numbers. The link between a function and its zeros came from a paper by Jacques Hadamard.[15] What mathematicians have been trying to prove for the past 167 years is that all of these zeros do have real part one half. Showing even one that does not lie on the strip would disprove the hypothesis. "In 1914, the English mathematician G. H. Hardy proved that *an infinitude* of values of *s* satisfy the hypothesis, but an infinity is not enough." [13]

CHAPTER V

CONCLUSION

For the past 23 centuries mathematicians have been working with prime numbers. Sometimes the outcomes of their efforts have been seemingly trivial, like amicable and perfect numbers, while others have great consequences, as in the Riemann Hypothesis. Whether or not the Riemann hypothesis is ever proved, the results of it being true are already being used today.

The proof of Riemann's Hypothesis will mainly affect mathematics itself. There are many conjectures that have been made by other mathematicians to the effect that if the Riemann Hypothesis is proven true, then their conjectures will also be proven. A modern day real use of the proof is in internet security and the use of very large prime numbers to generate encryption keys.

What I find most important is that math builds on itself. First, the concept of division was needed to know anything about prime numbers. Next, the Fundamental Theorem of Arithmetic showed how all numbers could be broken down into prime numbers uniquely which led to proof of there being an infinite number of primes. Knowing that all numbers can be broken into prime numbers led to determining which numbers were prime numbers. This has culminated in the Prime number theory, Riemann's Hypothesis, and the search for a solution to the error factor in the PNT.

In exploring the Riemann Hypothesis, I have found that I will be learning a great deal more in the years that follow. A big part of this will be complex number theory, not to mention real and complex analysis, before I can truly move forward in my research. What I have gathered so far are possible avenues of investigation. Since Gauss and Riemann were both very interested in geometry, there may be some link to a solution through the concept of the complex plane being a plane perpendicular to all n dimensions under consideration: an n+1 dimension. [17, 18] Work on the Twin Prime conjecture may also hold some insight to the resolution of this thorny problem. [19]

As for the error factor, my current thought is that while the distribution of primes may in general have the PNT shape, as well as end equivalent to the PNT, this does not mean that there is not another function overlying the $\pi(a)$ graph. I see this as an oscillating, decreasing, function centered about the $\frac{a}{\ln a}$ function..

BIBLIOGRAPHY

1. Rudman, Peter Strom. *How Mathematics Happened: The First 50,000 Years*. Amherst, NY: Prometheus, 2007. Print.

2. Lakoff, George, and Rafael E. Nunez. *Where Mathematics Comes From: How the Embodied Mind Brings Mathematics into Being*. Ney York: Basic, 2000. Print.

3. De Heinzelin, Jean. "Ishango." *Scientific American* 206.6 (1962): 105-16. Print.

4. Joyce, David E. "PLIMPTON 322." *Plimpton 322 Tablet*. Clark University, Department of Mathematics and Computer Science, 1995. Web. 23 Sept. 2013.

5. Gardner, Milo. "Rhind Papyrus." From *MathWorld*--A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/RhindPapyrus.html

6. Gardner, Milo. "Breaking the RMP 2/n Table." *Breaking the RMP 2/n Table*. Milo Gardner, 21 July 2008. Web. 08 Oct 2013. http://rmprectotable.blogspot.com

7. Euclid, Thomas Little Heath, and Dana Densmore. *Euclid's Elements: All Thirteen Books Complete in One Volume*. Santa Fe, NM: Green Lion, 2003. Print.

8. Ore, Øystein. *Number Theory and Its History*. New York: Dover, 1988. Print.

9. Brentjes, Sonja, and Jan P. Hogendijk. "Notes on Thabit Ibn Qurra and His Rule for Amicable Numbers." *Historia Mathematica* 16.4 (1989): 373-78. Print.

10. Rashed, Roshdi. *The Development of Arabic Mathematics: Between Arithmetic and Algebra*. Dordrecht: Springer Netherlands, 1994. Print.

11. O'Conner, J. J., and E. F. Robertson. "Kamal Al-Din Abu'l Hasan Muhammad Al-Farisi." *Al-Farisi Biography*. University of St Andrews, Scotland, School of Mathematics and Statistics, Nov. 1999. Web. 23 Sept. 2013

12. Wilson, Robin J. *The Great Mathematicians: Unraveling the Mysteries of the Universe*. London: Arcturus, 2011. Print.

13. Bell, E. T. *Men of Mathematics: The Lives and Achievements of the Great Mathematicians from Zeno to Poincaré*. New York: Simon&Schuster, 1986. Print.

14. *Euler's Zeta Function and the Riemann Hypothesis*, Brandy Morrissey and Ann Triplett, Texas Woman's University, December 16 2009

15. Derbyshire, John. *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*. Washington, DC: Joseph Henry, 2003. Print.

16. O'Conner, J. J., and E. F. Robertson. "Adrien-Marie Legendre" *Adrien-Marie Legendre Biography*. University of St Andrews, Scotland, School of Mathematics and Statistics, Jan. 1999. Web. 09 Dec. 2013

17. Connes, Alain. "Trace formula in noncommutative geometry and the zeros of the Riemann zeta function". Cornell University Library, 10 Nov. 1998. Web 04 Apr. 2014

18. Erickson, Carl. "*A Geometric Perspective on the Riemann Zeta Function's Partial Sums*". Stanford University Research Journal. (SURJ) Stanford University, Spring 2005. Web 08 Apr. 2014

19. Granville, Andrew. "*Infinitely many pairs of primes differ by no more than 70 million (and the bounds getting smaller every day)*". Current Events Bulletin, American Mathematical Society. 17 Jan 2014. Print.

20. Eves, Howard Whitley, and Jamie H. Eves. *An introduction to the history of mathematics*. 6th ed. Philadelphia: Saunders College Pub., 1990. Print.