Unterschrift des Betreuers

TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

D I P L O M A R B E I T

Prime Numbers
–
The DNA of Mathematics

Thema

Ausgeführt am Institut für

Analysis und Scientific Computing

der Technischen Universität Wien

unter der Anleitung von

Ao.Univ.Prof. Dr.phil. Rudolf Taschner

durch

Daniela Schwendinger

Name

Kehlermähder 22A, 6850 Dornbirn

Anschrift

Datum

Unterschrift (Studentin)

TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

D I P L O M A R B E I T

Prime Numbers
–
The DNA of Mathematics

Ausgeführt am Institut für

Analysis und Scientific Computing

der Technischen Universität Wien

unter der Anleitung von

Ao.Univ.Prof. Dr.phil. Rudolf Taschner

durch

Daniela Schwendinger

Wien, September 2012

Herzlicher Dank gebührt in erster Linie meinen Eltern (Hildegard und Anton Schwendinger), ohne deren Beistand und finanzielle Mithilfe ich dieses Studium niemals beginnen und mit der vorliegenden Diplomarbeit abschließen hätte können. Weiters möchte ich auch allen anderen danken die mich während dieser Zeit begleitet und unterstützt haben, insbesondere meinen Geschwistern (Eva und Matthias) und meinem Freund (Manuel).

Es ist mir ein besonderes Anliegen an dieser Stelle auch Herrn Prof. Taschner zu danken, der mich während des Schreibens dieser Arbeit hilfreich betreut, mir zugleich aber auch entscheidende Freiheiten in deren Gestaltung gewährt hat.

Table of Contents

1. Introduction

1, 2, 3, 4, 5, 6, 7, 8, 9, 10… counting is one of the main parts of mathematics and most certainly the first which appeared in history. Most people know that there is a difference between even (2, 4, 6, 8, 10…) and odd (1, 3, 5, 7, 9…) numbers. But what do the numbers 2, 3, 5, 7… have in common and why are they so significant for mathematics?

Prime numbers are the DNA of mathematics. Every number consists of primes and can be decomposed into primes in a unique way. Thus one assumes rightly that there has been an enormous amount of studies to investigate and understand prime numbers. Nevertheless, they are still one of the greatest mysteries in mathematics.

This paper deals with the mysteries and secrets of prime numbers and is divided into four main parts. The first part offers a brief history of the numerous achievements concerning prime numbers. This is followed by a second more mathematical part which states the different definitions of prime numbers and proves their most important characteristics, such as the fundamental theorem of arithmetic.

However, the most fascinating attribute of prime numbers, their distribution, is still hidden behind a veil of mere approximations and an, as it seems, unprovable hypothesis. In the last two sections of this paper one experiences the whole way from the proof of infinitely many prime numbers and the first unsure consideration of their distribution to the still unproven but vitally important Riemann hypothesis.

2. History of Prime Numbers

This chapter gives a short overview of the historical discovery of prime numbers and their properties. It starts with the very early discoveries of the ancient Greeks and ends with the RSA algorithm, which is nowadays very important in electronic commerce. In between, it mentions the most important mathematicians and their achievements with regard to prime numbers, such as Euclid, Eratosthenes, Fermat, Mersenne, Euler, Gauss, Legendre, Riemann, etc.

2.1. Ancient Greek (500-200 BC)

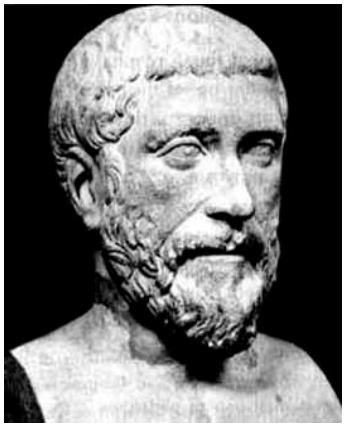

Image 1: Pythagoras of Samos (about 569 BC in Samos – about 475 BC)

Ancient Greek mathematicians were the first who studied prime numbers and their properties extensively. Especially the mathematicians of Pythagoras' school were interested in number theory and their mystical properties. They already proved that every number is either a prime number or can be decomposed into prime numbers. They argued that if there were such numbers which are neither prime numbers nor decomposable into prime numbers, then there would also exist a smallest one, which will be called N. Since this N is no prime number, there have to exist two smaller numbers A and B which when multiplied with each other result in N. Due to the fact that A and B are smaller than N, they have to be either prime numbers themselves or decomposable into prime numbers. This argument shows that N itself can be written as a product of primes, which is a contradiction to the definition of N. Therefore, the first argument is wrong and such numbers do not exist. This is one of the first proofs which bases its arguments on a contradiction[1][2].

[1] du Sautay 2004, pp. 51-52
[2] O'Connor & Robertson 2009

About 300 BC, Euclid wrote the most influential book at that time, called *Elements*, in which, amongst other things, he proved several important results about prime numbers. In Book IX, proposition 20, he proved that there exist infinitely many prime numbers[3]. The complete proof is stated in section 4.1.1. In the *Elements*, Euclid also gave a proof of the fundamental theorem of arithmetic which says that every integer can be written as a unique product of prime numbers [4]. The proof of existence of such a prime factorization was already mentioned earlier in this section. The proof of uniqueness is more challenging and will be stated in section 3.2.

Image 2: Euclid of Alexandria (about 325 BC – about 265 BC in Alexandria)

Another famous ancient Greek mathematician was Eratosthenes. He is credited with being the first who discovered that there is an easy algorithm to find all primes up to a given number N. In order to do so, one has to write down all the numbers up to N. Afterwards, one has to take the first prime number and cross out every multiple of this number. Thereafter, one does the same thing with the next number which is not crossed out, thus, the next prime number. In the 13th century, it was found out that one only has to cross out all multiples up to the number $\sqrt{N}$ since at least one prime factor of all composite numbers up to N does not exceed $\sqrt{N}$.[5]

Image 3: Eratosthenes of Cyrene (276 BC – 194 BC)

2.2. Middle Ages

During the so called Dark Ages, there is a long gap in the history of primes. Nearly everything that the Greeks had discovered about the prime numbers fell into oblivion during the Roman times[6].

[3] Euclid 2003, pp. 204-205
[4] Euclid 2003, p. 199
[5] Harman 2007, p. 4
[6] Kerkhoff, Krycki & Stuckenholz 1998

2.3. Modern Age

Image 4: Pierre de Fermat (1601 Beaumont de Lomage – 1665 Castres)

It took the mathematics until the renaissance to recover from the Dark Ages. At the beginning of the 17th century, Pierre de Fermat made a new important discovery. He proved the speculation of Albert Girard that every prime number of the form $4n + 1$ can be written as the sum of two squares in a unique way. He also argued that if p is a prime number and if a is an integer, then $a^p \equiv a\,(mod\,p)$. In particular, if p does not divide a, then $a^{p-1} \equiv 1\,(mod\,p)$. This argument is known as Fermat's little theorem and Euler published the first proof of it[7]. This theorem will be proved in section 3.3. Fermat's little theorem is the basis for several later discovered results in Number Theory, especially for methods of checking whether a number is prime or not. Some of these methods are still used today. Another well known discovery of Fermat are Fermat Numbers, which are of the form $2^{2^n} + 1$. Fermat believed that all of his numbers are primes and he verified it for $n = 1,2,3,4$ but he could not prove it on the whole. It took a hundred years until Euler could show that the Fermat Number $2^{2^5} + 1 = 4294967297$ is not prime because it is divisible by 641 [8] [9].

Image 5: Marin Mersenne (1588 Oizé in Maine – 1648 Paris)

Fermat corresponded with the French monk Marin Mersenne and told him about his numbers. Encouraged by Fermat's discoveries, Mersenne studied numbers of the form $2^n - 1$, which are therefore called Mersenne Numbers. These numbers are composite unless n is prime. Nevertheless, not all numbers of the form $2^n - 1$ are prime even if n is a prime number (for example $2^{11} - 1 = 2047 = 23 * 89$). Mersenne argued that these numbers are prime as long as n is one of the following prime numbers:

[7] Ribenboim 1996, p. 22
[8] du Sautoy 2004, p. 56
[9] O'Connor & Robertson 2009

$2, 3, 5, 7, 13, 19, 31, 67, 127, 257$, which is nowadays known to be wrong. At the end of the 19th century, Édouard Lucas managed to show that Mersenne's list misses the numbers 61, 89, and 107 and due to the help of computers we know today that $2^{257} - 1$ is no prime number[10]. Nevertheless, Mersenne Numbers are far more effective in finding large prime numbers than Fermat Numbers and provided the largest known primes for many years[11].

In 1772, Euler discovered that the equation $x^2 + x + 41$ produces prime numbers when fed with numbers $n = 0, \dots 39$. Moreover, he ascertained that also with $q = 2, 3, 5, 11, 17$ the equation $x^2 + x + q$ generates prime numbers for $x = 0, \dots, q - 2$.[12] Euler also showed that the infinite series $1/2 + 1/3 + 1/5 + 1/7 + 1/11 + \cdots$ formed by summing the reciprocals of the prime numbers is divergent[11].

Image 6: Leonhard Euler (1707 Basel – 1783 St. Petersburg)

Another famous mathematician, who lived at the turn of the 18th century, was Carl Friedrich Gauss. Gauss invented a calculating machine which worked like a clock, the so called modulo calculator. This new way of calculating was very important for later prime discoveries[13]. Both Gauss and the French mathematician Adrian-Marie Legendre independently conjectured that for a number N the number of primes not exceeding N is about $\frac{N}{\log(N)}$. Gauss as well as Legendre improved this estimate of the number of primes, but in different ways[14]. It took a whole century until

Image 7: Johann Carl Friedrich Gauss (1777 Brunswick – 1855 Göttingen)

[10] du Sautoy 2004, p. 58, 253
[11] O'Connor & Robertson 2009
[12] du Sautoy 2004, pp. 62-63
[13] du Sautoy 2004, pp. 33-34
[14] du Sautoy 2004, pp. 67-68, 73-76

Jacques Hadamard and, simultaneously, Charles de la Vallée-Poussin were able to prove the Prime Number Theorem[15]. This theorem will be discussed in more detail in section 4.3.

A famous student of Gauss was Bernhard Riemann, who studied mathematics at the University of Göttingen[16]. Gauss supervised Riemann's dissertation and had a great influence on his work with prime numbers[17]. Riemann defined the zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, which had already appeared in Euler's work, for complex numbers $s \neq 1$. He suspected that all zeros in the critical strip, consisting of the nonreal complex numbers s with $0 \leq Re(s) \leq 1$, have the real part $\frac{1}{2}$. This conjecture is known as the famous Riemann hypothesis and is until now unproved[18]. It is one of only three still unsolved Hilbert's problems, a list of 23 problems in mathematics published in 1900[19]. More about Riemann and his hypothesis can be found in section 5.

Image 8: Georg Friedrich Bernhard Riemann (1826 Breselenz – 1866 Selasca)

2.4. Computer Era

Due to the increasing need to send secret messages in the 20th century (bank transfers, secret diplomatic information, etc.), there has been a great focus on developing safe methods of coding messages. The idea of a public key crypto-system was introduced by Whitfield Diffie and Martin E. Hellman in 1976[20]. Until then, the decoding und encoding keys were identical, which made this system very vulnerable because no matter how complex the coding scheme might be, there were at least two parties which had to know the keys. In 1977, on the basis of Diffie's and Hellman's work, Roland Linn Rivest, Adi Shamir, and Leonard Adleman have

[15] du Sautoy 2004, p. 135
[16] du Sautoy 2004, p. 84
[17] du Sautoy 2004, p. 95
[18] Ribenboim 1996, pp. 221-223
[19] Yandell 2001, p. 385
[20] Ribenboim 1996, p. 173

invented a very effective public key crypto-system, called the RSA-system. In this new crypto-system the encryption and decryption keys are distinct. It is theoretically possible to figure out the decryption key from the encryption key but it is “computationally infeasible”[21]. The benefits of a public key crypto-system compared to a traditional crypto-system are the public key, its simplicity and, nevertheless, the high difficulty in cracking it. The concept of the RSA-system is based on the extreme difficulty of prime factorization. This system is still widely used and especially important in electronic commerce[22].

[21] Bressoud 1989, p. 43
[22] Ribenboim 1996, p. 173

3. Definition and Characteristics of Prime Numbers

In this part of the paper, the definition and important attributes of prime numbers are stated. Moreover, the fundamental theorem of arithmetic will be proved in three ways, one of them being Euclid's proof. This part also includes the proof of Fermat's little theorem. At the end, it is proved that there exist arbitrarily big gaps in the prime number sequence before it comes to the part of the prime number estimate.

3.1. Definition of Prime Numbers

The most common definition of primes is the following:

Definition 3.1: *An integer $p > 1$ is called prime number or prime if there exists no divisor d of p with $1 < d < p$. Every integer $a > 1$ which is no prime number is called composite*[23].

An important characteristic of prime numbers is the theorem of Euclid:

Theorem 3.1: *If p is a prime number and $p \mid ab$, then $p \mid a$ or $p \mid b$. In general: If $p \mid a_1 a_2 \dots a_n$, then p is a divisor of at least one a_i*[24].

Proof: In order to proof this theorem one needs the definition of the greatest common divisor and two lemmas.

Definition 3.2: *Let a and b be integers. The greatest common divisor of a and b is the largest positive integer which divides both a and b. It will be denoted by $\gcd(a, b)$* [25].

Lemma 3.1: *For any positive integers a and b, there exists a unique pair (q, r) of nonnegative integers such that*

$$b = aq + r, \quad \text{with} \quad r < a.$$

[23] Niven, Zuckerman 1972, p. 15
[24] Niven, Zuckerman 1972, p. 19
[25] Bressoud 1989, p.6

In this case q is called the quotient and r the remainder[26].

Proof of lemma 3.1: Since $a > 1$, there exist positive integers n such that

$$na > b \text{ (for example } n = b).$$

Let q be the least positive integer for which

$$(q + 1)a > b.$$

Hence,

$$qa \leq b.$$

Let $r = b - qa$. It follows that

$$b = aq + r, \quad \text{with} \quad 0 \leq r < a.$$

To prove the uniqueness, one assumes that $b = aq' + r'$, where q' and r' are also nonnegative integers and $0 \leq r' < a$. Then

$$aq + r = aq' + r',$$

which implies that

$$a(q - q') = r' - r$$

and, thus,

$$a|r' - r.$$

Hence,

$$|r' - r| \geq a \text{ or } |r' - r| = 0.$$

Since $0 \leq r, r' < a$, it follows that

$$|r' - r| < a$$

and, therefore,

[26] Andreescu, Andrica 2009, pp. 3-4

$$|r' - r| = 0,$$

implying

$$r' = r \text{ and, consequently, } q' = q^{27}.$$ □

Lemma 3.2: *Let a and b be integers and let $g = \gcd(a, b)$. Then there exist integers m and n such that*

$$g = m * a + n * b^{28}.$$

Proof of lemma 3.2: Assuming that a and b are positive, one can apply lemma 3.1, which leads to

$$a = q_1 b + r_1, \qquad \text{with} \quad 0 \leq r_1 < b.$$

If $r_1 = 0$ then b divides a and $b = \gcd(a, b)$. One can than choose $m = 0$ and $n = 1$. If not, one can divide b by r_1:

$$b = q_2 r_1 + r_2, \qquad \text{with} \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, one stops here. If not, one has to continue by dividing r_1 by r_2:

$$r_1 = q_3 r_2 + r_3, \qquad \text{with} \quad 0 \leq r_3 < r_2.$$

This process is continued until the remainder is 0, which has to happen since the remainders are always nonnegative and each remainder is strictly smaller than the previous one. These are the last two equations:

$$r_{k-2} = q_k r_{k-1} + r_k, \quad \text{with} \quad 0 \leq r_k < r_{k-1},$$

$$r_{k-1} = q_{k+1} r_k + 0.$$

The greatest common divisor of a and b is the last non-zero remainder, r_k. To see this, one must work back up the whole list of equations. By the last equation, one can see that r_k divides r_{k-1}. By the second last equation, one can see that r_k also divides

[27] Andreescu, Andrica 2009, p. 4
[28] Bressoud 1989, p.6

r_{k-2} because r_k divides r_k and r_{k-1}. One continues this all the way to the third equation. By the third equation, one can see that r_k divides r_1 because r_k divides r_3 and r_2. By the second equation, one can see that r_k also divides b. And finally, by the first equation, one can see that r_k also divides a. Hence, r_k is a common divisor of a and b.

To show that r_k is the largest divisor, let d be any other common divisor of a and b. By the first equation, one can see that d divides r_1 because d divides both a and b. Continuing down the list, one sees that d must divide all the remainders $r_1, r_2, r_3, \dots, r_k$ and, therefore, $d \leq r_k$.

One can now use these equations to find the m and n from lemma 3.2. By the first equation, r_1 can be written as

$$r_1 = 1a + (-q_1)b.$$

By making this substitution for r_1 in the second equation, r_2 can be written as

$$r_2 = b - q_2 r_1$$

$$= b - q_2(a - q_1 b)$$

$$= -q_2 a + (1 + q_1 q_2)b.$$

Continuing down the list of equations, each remainder $r_i$can be written as an integer times a plus an integer times b and this proves lemma 3.2. □

Sequel to the proof of theorem 3.1: Let p be a prime number and $p|ab$. If $p|a$, the theorem is proved. If not, than $\gcd(p, a) = 1$ because p is prime and, thus, 1 is besides p the only other integer which divides p. According to lemma 3.2, one can find two integers n and m such that

$$1 = mp + na.$$

Multiplying both sides by b, one gets

$$b = mpb + nab.$$

Since $p|ab$ and $p|p$, it divides both summands on the right side and, thus, divides their sum, which is b. Hence, if p does not divide a, it must divide b. □

3.2. Fundamental Theorem of Arithmetic

Theorem 3.2: *The fundamental theorem of arithmetic says that every integer greater than* 1 *can be written as a unique product of prime numbers except for the ordering of the factors*[29]*.*

The existence of a prime factorization has already been proved in the section "Ancient Greek". To prove the uniqueness of such a factorization one uses an indirect approach.

1st proof: Assuming that there exists a natural number n with two different prime factorizations, one can omit the prime numbers which appear in both factorizations and gets

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

with $p_i \neq q_j$ for every $i = 1, \dots, r$ and every $j = 1, \dots, s$. This is not possible because $p_1 \mid q_1 q_2 \dots q_s$ and due to theorem 3.1 p_1 has to be a divisor of at least one of the q_j with $j = 1, \dots s$ and because p_1 and every q_j are prime numbers, this means that p_1 has to be identical with at least one of the q_j with $j = 1, \dots s$[30]. □

2nd proof: Assuming that the theorem is not true, there exists a smallest natural number n with more than one prime factorization.

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \quad \text{with } s, r > 1$$

None of the prime numbers $p_1, p_2, \dots, p_r$ is identical with any of the prime numbers $q_1, q_2, \dots, q_s$. Otherwise one could omit the identical prime number $p_i = q_j$ and get two different factorizations of the natural number $\frac{n}{p_i}$, which is a contradiction to the

[29] Niven, Zuckerman 1972, p. 19
[30] Niven; Zuckerman 1972, pp. 19-20

assumption that n is the smallest natural number with more than one prime factorization.

It is easy to see that

$$(q_1 - p_1)q_2q_3 \dots q_s = p_1(p_2p_3 \dots p_r - q_2q_3 \dots q_s)$$

because

$$q_1q_2 \dots q_s - p_1q_2q_3 \dots q_s = p_1p_2 \dots p_r - p_1q_2q_3 \dots q_s$$

And, hence,

$$(q_1 - p_1)q_2q_3 \dots q_s = p_1(p_2p_3 \dots p_r - q_2q_3 \dots q_s).$$

Without loss of generality it can be implied that $p_1 < q_1$. Let

$$N = (q_1 - p_1)q_2q_3 \dots q_s = p_1(p_2p_3 \dots p_r - q_2q_3 \dots q_s).$$

Apparently, $N < n$ and, thus, factorable in a unique way.

However, $p_1 \nmid (q_1 - p_1)$ and, hence, one gets two factorizations of N with one containing p_1 and the other one not containing p_1. This is a contradiction because $N < n$ and, therefore, not factorable in different ways[31]. □

In the following proof, the word “measure” will be used in the sense of “divide” just like Euclid did.

Euclid’s proof: If a is the least number to be measured by b, c, and d, Euclid claims that a cannot be measured by any other prime number than b, c, and d. Assuming that e measures a and e is not identical with b, c or d, there has to exist an f which multiplied with e results in a and, therefore, also measures a. According to proposition 30 in book VII, b, c and d have to measure either e or f because they are prime numbers and they measure the product of e and f. Since e is also a prime number and not identical with b, c or d, they have to measure f. This would be a

[31] Niven; Zuckerman 1972, pp. 20-21

contradiction to the argument at the beginning because f is smaller than a, but according to the definition of a, a is the least number which can be measured by b, c, and d. Consequently, no prime number besides b, c, and d can measure a [32] [33].

3.3. Fermat's Little Theorem

Theorem 3.3: *Fermat's little theorem says that if p is a prime number and if a is an integer, then $a^p \equiv a\ (mod\ p)$. In particular, if p does not divide a then $a^{p-1} \equiv 1\ (mod\ p)$*[34].

Proof: This theorem can easily be proved by induction on a.

Basis $a = 1$:

$$1^p = 1 \equiv 1\ (mod\ p)$$

Induction step: Assuming that for an arbitrary integer a,

$$a^p \equiv a\ (mod\ p)\ \text{(induction hypothesis)}.$$

Now it needs to be proved that $(a+1)^p \equiv a + 1\ (mod\ p)$[35].

To be able to prove this, one needs the binomial theorem, which says that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

$$\text{with } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$ [36].

Furthermore, one needs the following lemma.

Lemma 3.1: *If p is a prime number,*

[32] Euclid 2003, pp. 199-200
[33] du Sautoy 2004, p. 53
[34] Ribenboim 1996, p. 22
[35] Ribenboim 1996, p. 22
[36] Kraft; Bürger; Unfried; Götz 2006, p.31

$$(x+y)^p \equiv x^p + y^p \ (mod\ p).$$

Proof of lemma 3.1: According to the binomial theorem

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k.$$

For $0 < k < p$, $\binom{p}{k}$ is divisible by p because neither of the terms in the denominator includes a factor of p and, therefore,

$$\binom{p}{k} \equiv 0 \ (mod\ p) \text{ for } 0 < k < p.$$

Thus, one only has to consider $\binom{p}{0}$ and $\binom{p}{p}$, which are both by definition 1.

This leads to

$$(x+y)^p \equiv \binom{p}{0} x^{p-0} y^0 + \binom{p}{p} x^{p-p} y^p \ (mod\ p)$$

$$\equiv x^p + y^p (mod\ p).$$ □

Sequel to the proof of theorem 3.3: By the lemma one has

$$(a+1)^p \equiv a^p + 1^p \ (mod\ p).$$

Using the inductive hypothesis this becomes

$$(a+1)^p \equiv a + 1 \ (mod\ p)^{37}.$$

Finally, one has to show that if p does not divide a then

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

It has already been shown that $a^p \equiv a \ (mod\ p)$. Since a is not divisible by p, a has a multiplicative inverse $mod\ p$. Thus, multiplying each side with the multiplicative inverse of $a \ (mod\ )p$ one obtains

$$a^{p-1} \equiv 1 \ (mod\ p).$$ □

[37] Ribenboim 1996, p. 22

3.4. Arbitrarily Big Gaps in the Prime Number Sequence

First of all, the gap between prime numbers has to be defined because there are two different standard definitions. In this paper, gap stands for the number of composites between two sequenced prime numbers and not for the difference of the two primes.

For example the gap between 23 and 29 is 5 $(24, 25, 26, 27, 28)$ and not $29 - 23 = 6$.

Theorem 3.3: *There exist arbitrarily big gaps in the prime number sequence. That means for any natural number k exist k consecutive composites*[38]*.*

Proof: To generate a sequence of k composites, one has to build the following numbers:

$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k, (k+1)! + k + 1$$

Each of these is a composite, because at least j is a divisor of $(k+1)! + j$ with $2 \leq j \leq k + 1$[39]. □

3.5. Twin Primes

Definition 5.1: *If p and $p + 2$ are prime numbers, they are called twin primes*[40].

For Clement's characterization of twin primes one needs Wilson's theorem, which is a corollary of Fermat's little theorem.

Theorem 5.1.: *Wilson's theorem sates that $p > 1$ is a prime number, if and only if*

$$(p-1)! \equiv -1 \ (mod\ p)$$[41].

Proof: It is obvious that for any component number $n > 1$

$$(n-1)! \equiv 0 \ (mod\ n).$$

[38] Niven; Zuckerman 1972, p. 22
[39] Niven; Zuckerman 1972, p. 22
[40] Ribenboim 1996, p. 259
[41] Ribenboim 1996, p. 25

If p is a prime number, then the integers $1, 2, 3, \ldots, p-1$ are relatively prime to p. Therefore, for each of these integers a exists an integer b so that $a * b \equiv 1\ (mod\ p)$. Moreover, this b is unique $mod\ p$ and since p is prime, $a \equiv b\ (mod\ p)$ if and only if $a = 1$ or $a = p - 1$. If one omits 1 and $p - 1$, the other integers can be grouped into pairs whose product is $1\ mod\ p$.

Thus,

$$2 * 3 * 4 * \ldots * (p-2) \equiv 1(mod\ p)$$

or more simply

$$(p-2)! \equiv 1\ (mod\ p).$$

Multiplying this equality by $p - 1$ one gets

$$(p-1)! \equiv p - 1\ (mod\ p) \equiv -1\ (mod\ p)^{42}.$$

□

In 1949, twin primes have been characterized by Clement as follows:

Theorem 5.2: *Let $n \geq 2$. The integers n and $n + 2$ form a pair of twin primes if and only if*

$$4[(n-1)! + 1] + n \equiv 0\ [mod\ n(n+2)]^{43}.$$

Proof: First, one has to show that if the congruence is satisfied, n and $n + 2$ are prime numbers. It can be seen that $n \neq 2,4$ and

$$(n-1)! + 1 \equiv 0\ (mod\ n).$$

According to Wilson's theorem n is a prime. Moreover,

$$4(n-1)! + 2 \equiv 0\ (mod\ n+2).$$

Multiplying this equation by $n(n+1)$ one obtains

$$4[(n+1)! + 1] + 2n^2 + 2n - 4 \equiv 0\ (mod\ n+2)$$

[42] http://primes.utm.edu/notes/proofs/Wilsons.html
[43] Ribenboim 1996, p. 259

hence

$$4[(n+1)!+1]+(n+2)(2n-2)\equiv 0\ (mod\ n+2).$$

Since $(n+2)(2n-2)$ is a multiple of $n+2$, it can be omitted. Thus, by Wilson's theorem $n+2$ is prime too.

Now, one has to show the other direction, i.e. if n and $n+2$ are primes, the congruence has to be satisfied. Since n and $n+2$ are prime number, $n \neq 2$ and

$$(n-1)!+1\equiv 0\ (mod\ n),$$

$$(n+1)!+1\equiv 0\ (mod\ n+2).$$

Because $n(n+1)=(n+2)(n-1)+2$, it follows that

$$2(n-1)!+1=k(n+2),$$

where k is an integer.

Due to Wilson's theorem, one knows that $(n-1)!\equiv -1\ (mod\ n)$. Thus,

$$2k+1\equiv 0\ (mod\ n)$$

and substituting

$$4(n-1)!+2\equiv -(n+2)[mod\ n(n+2)].$$

Therefore,

$$4[(n-1)!+1]+n\equiv 0\ [mod\ n(n+2)]^{44}.$$ □

[44] Ribenboim 1996, pp. 259 - 260

4. Prime Number Estimate

4.1. There Exist Infinitely Many Prime Numbers

Already the ancient Greeks knew that the list of primes has no end. Euclid was the first who published this proposition in his book *The Elements.* This section will include three of the most famous proofs of this theorem.

4.1.1. Euclid's Proof

Euclid's proof: Suppose that a, b, and c are all the existing prime numbers. Let $P = abc$, the smallest number divisible by a, b and c. Now we look at $P + 1$ and let p be a prime dividing $P + 1$. Hence, p cannot be identical with a, b or c, otherwise it would divide $P + 1 - P = 1$, which is impossible. Therefore, p is another prime and a, b and c cannot be all the existing primes[45] [46].

4.1.2. Goldbach's Proof

Christian Goldbach used a very simple idea to prove that there exist infinitely many prime numbers. He just had to find an infinite sequence of natural numbers $a_1, a_2, a_3, \ldots$ greater than 1, which are pairwise relatively prime. Relatively prime is equivalent to their greatest common divisor being 1. Let p_1 be a prime dividing a_1, p_2 a prime dividing a_2 and so forth, then $p_1, p_2, p_3, \ldots$ is a infinite sequence of different prime numbers. In 1730, Goldbach wrote Euler a letter with his proof using Fermat numbers as infinite sequence of natural numbers. He had to show that the Fermat numbers $F_n = 2^{2^n} + 1$ (for $n \geq 0$) are pairwise relatively prime.

Goldbach's proof: First, it needs to be shown that $F_m - 2 = F_0 F_1 \ldots F_{m-1}$, which is easiest seen by induction on m.

Basis $m = 1$:

$$F_1 - 2 = 2^{2^1} + 1 - 2 = 3 = 2^{2^0} + 1 = F_0$$

Induction step: Assuming that for an arbitrary natural number m,

[45] Euclid 2003, pp. 204-205
[46] Ribenboim 1996, p. 3

$$F_m - 2 = F_0 F_1 \dots F_{m-1}$$ (inductive hypothesis).

It is sufficient to prove that $F_{m+1} - 2 = F_0 F_1 \dots F_m$:

$$F_{m+1} - 2 = 2^{2^{m+1}} - 1 = (2^{2^m} - 1)\left(2^{2^m} + 1\right) = (F_m - 2)(F_m)$$

Using the inductive hypothesis this becomes

$$F_{m+1} - 2 = F_0 F_1 \dots F_{m-1} F_m.$$

Now, it can be seen that if $n < m$, F_n divides $F_m - 2$. If F_n and F_m were not relatively prime, there would exist a prime p which would divide both of them. According to the above proved, p would also divide $F_m - 2$ and F_m, hence also the difference $F_m - (F_m - 2) = 2$, which is not possible because F_m is odd[47]. □

4.1.3. Euler's Proof

The reason for the importance of Euler's Proof of the infinitude of prime numbers is the fact that it has led to one of the most important developments concerning the Prime Number Theorem, which will be described in a section 5.1.

Before one can start with Euler's Proof, one needs the following lemma.

Lemma 4.1.: *If* $|r| < 1$ *then*

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1-r}$$[48].

Proof of lemma 4.1.: Starting with the finite sum

$$\sum_{k=0}^{n} r^k = 1 + r + r^2 + \cdots + r^{n-1} + r^n$$

one can then obtain the limit $n \to \infty$.

By multiplying both sides with r one obtains

[47] Ribenboim 1996, pp. 4-5
[48] Weisstein

$$r\sum_{k=0}^{n} r^k = r + r^2 + r^3 + \cdots + r^n + r^{n+1}$$

and subtracting this from the original equation, one thus has

$$(1-r)\sum_{k=0}^{n} r^k = (1 + r + r^2 + \cdots + r^{n-1} + r^n) - (r + r^2 + r^3 + \cdots + r^n + r^{n+1})$$

$$= 1 - r^{n+1}.$$

Hence, it follows that

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1-r}.$$

For $|r| < 1$, the sum converges as $n \to \infty$ and, thus,

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1-r}$$ [49].

□

Euler's proof: Assuming that $p_1, p_2, \ldots, p_n$ are all the existing primes. Due to lemma 4.1., for each $i = 1, \ldots, n$,

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \frac{1}{p_i}}.$$

Multiplying these n equalities, one obtains

$$\prod_{i=1}^{n}\left(\sum_{k=0}^{\infty} \frac{1}{p_i^k}\right) = \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}}.$$

On the left-hand side every product of prime numbers appears exactly once in the denominator. Due to the fundamental theorem of arithmetic, asserting that every integer can be written as a unique product of prime numbers, the term on the left-

[49] Weisstein

hand side is equal to the sum over the inverses of all natural numbers, the harmonic series. Therefore, the left-hand side is infinite, whereas the right-hand side is clearly finite, which is absurd. Hence, there exist infinitely many prime numbers[50]. □

4.2. Initial Considerations About the Growth of $\pi(x)$

The various proofs of the infinitude of prime numbers are hardly constructive and do not give any indication of how to generate the $n-th$ prime number. Furthermore, the proofs do not indicate the amount of prime numbers less than any given number N. Therefore, this section now offers a detailed analysis of the growth of $\pi(x)$, the so called prime counting function, which is defined as the number of primes p between 1 and x [51].

As mentioned in the section above, Euclid proved that there exist infinitely many prime numbers and, therefore,

$$\lim_{n\to\infty} \pi(x) = \infty$$

Varying Euclid's proof a little bit, it says that if there existed only a finite number of primes $p_1, p_2, p_3, \dots, p_n$, one of them would be able to divide $p_1 p_2\, p_3 \dots p_n - 1$ and this is not possible. Consequently, there has to exist a p_m $(m > n)$, which is a divisor of $p_1 p_2\, p_3 \dots p_n - 1$, and, thus, not greater than $p_1 p_2\, p_3 \dots p_n$. Arranging the primes according to their size, one can prove that

$$p_{n+1} \leq 2^{2^n}.$$

Proof: This can easily be seen by induction on n:

Basis $n = 1$:

$$p_1 = 2 = 2^{2^0}.$$

Hence

[50] Ribenboim 1996, pp. 6-7
[51] Ribenboim 1996, p. 213

$$p_1 \leq 2^{2^0}$$

Induction step: If for any natural number $\leq n$,

$$p_n \leq 2^{2^{n-1}} \text{ (inductive hypothesis)}$$

then

$$p_{n+1} \leq p_1 p_2\, p_3 \ldots p_n \leq 2^{2^0} * 2^{2^1} * \ldots * 2^{2^{n-1}} = 2^{2^0+2^1+\cdots+2^{n-1}} \leq 2^{2^n}$$ □

If n denotes the greatest number with

$$2^{2^{n-1}} \leq x, \qquad (x \leq 2)$$

it follows that

$$\pi(x) \geq n \geq 1 + \left[\frac{1}{\log 2} * \log\left(\frac{\log x}{\log 2}\right)\right].$$

The right-hand side increases at least proportional to $\log\log x$. Consequently, Euclid implicitly proved that

$$\pi(x) \geq c * \log\log x, \qquad (c > 0)^{52}.$$

Although not fitting chronologically but with regard to contents, this section will now focus on Dressler's considerations about the growth of $\pi(x)$. On the basis of a method of Erdös, Dressler argued as follows. Every square-free number $n \leq x$ is at most divisible by $p_1, p_2, \ldots, p_k$ $(k = \pi(x))$. Therefore, n can be written as

$$n = \prod_{i=1}^{\pi(x)} p_i^{vi}$$

in a unique way with v_i only taking the values 0 and 1. According to the probability theory, there are at most $2^{\pi(x)}$ square-free numbers. Since the asymptotic density of square-free numbers is $\frac{6}{\pi^2}$, it can be said that

$$c_1 x \leq 2^{\pi(x)}$$

[52] Hlawka; Schoißengeier; Taschner 1986, p. 99

for a positive absolute term $c_1 < \frac{6}{\pi^2}$ and x being sufficiently large. Hence,

$$\pi(x) \geq c * \log x$$

with $c = \log c_1 / \log 2$ [53].

Euler managed to show that "the primes are not so sparse as the squares". To demonstrate this, he first illustrated that the sum of the inverses of the prime numbers is divergent:

$$\sum_{p=1}^{\infty} \frac{1}{p} = \infty$$

Proof: Let N be an arbitrary positive integer. As we already know, one can write each integer $n \leq N$ as a product of primes p, $p \leq n \leq N$, in a unique way. Moreover, for every prime p,

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}.$$

With the same argument as in Euler's proof of the existence of infinitely many prime numbers, it follows that

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \leq N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}}.$$

However,

$$\log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} = - \sum_{p \leq N} \log \left(1 - \frac{1}{p} \right),$$

and for each prime p individually,

$$- \log \left(1 - \frac{1}{p} \right) = \sum_{m=1}^{\infty} \frac{1}{m p^m} \leq \frac{1}{p} + \frac{1}{p^2} \left(\sum_{h=0}^{\infty} \frac{1}{p^h} \right)$$

[53] Hlawka; Schoißengeier; Taschner 1986, p. 100

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

$$< \frac{1}{p} + \frac{1}{(p-1)^{2.}}$$

Therefore,

$$\log \sum_{n=1}^{N} \frac{1}{n} \leq \log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \frac{1}{(p-1)^2} \leq \sum_{p} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

One knows that the series $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent. Moreover, since N is arbitrary and the harmonic series is divergent, it follows that $\log \sum_{n=1}^{\infty} \frac{1}{n} = \infty$ and thus the series $\sum_{p} \frac{1}{p}$ is divergent.

Because the series $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is convergent, but the series $\sum_{p} \frac{1}{p}$ is divergent, one can see that the squares are not as plentifully distributed as the prime numbers[54]. □

4.3. Prime Number Theorem

Definition 4.1: *Two positive real valued functions $f(x)$ and $g(x)$ defined for $x \geq x_0 > 0$ are asymptotically equal, noted $f(x) \sim g(x)$, if $lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$.*

Theorem 4.1: *The Prime Number Theorem states that the prime counting function $\pi(x)$ is asymptotically equal to $\frac{x}{log\, x}$.*

4.3.1. Gauss's Assumption

In 1792, at the age of 15, Gauss started to engage himself in the prime counting function $\pi(x)$. A year earlier he had got a book with a logarithm table in it and a prime number table in the appendix as a present and this might have been the trigger for

[54] Ribenboim 1996, pp. 215-217

his breakthrough in the determination of the order of magnitude of $\pi(x)$. Gauss tried to diagnose how many prime numbers do exist between 1 and an arbitrary number[55].

Table 1[56] Connection between the amount of prime numbers and the decimal power.

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
10^2	25	4,0
10^3	168	6,0
10^4	1229	8,1
10^5	9 592	10,4
10^6	78 498	12,7
10^7	664 579	15,0
10^8	5 761 455	17,4
10^9	50 847 534	19,7
10^{10}	455 052 512	22,0

For a sufficiently large x, $x/\pi(x)$ increases 2,3 when one goes from a power of 10 to the next. 2,3 is approximately $\log 10$ with the basis e. The table, which Gauss made at the age of 15, led him to believe that for the numbers 1 to x, nearly every $x \log x$ number is a prime number[57] [58]. This means that the probability of a number between 1 and x being a prime number is approximately $\log x$. Therefore, $\pi(x)$ is asymptotically equal to $x/\log x$ Nevertheless, if one compares the graph of $\pi(x)$ with the graph of $x/\log x$, the function $x/\log x$ qualitatively mirrors the behavior of $\pi(x)$ but does not completely agree with it[59].

[55] du Sautoy 2004, pp. 64 - 66
[56] Hlawka; Schoißengeier; Taschner 1986, p. 100
[57] Hlawka; Schoißengeier; Taschner 1986, p. 100
[58] du Sautoy 2004, pp. 66-68
[59] Zagier 1975, pp. 9-10

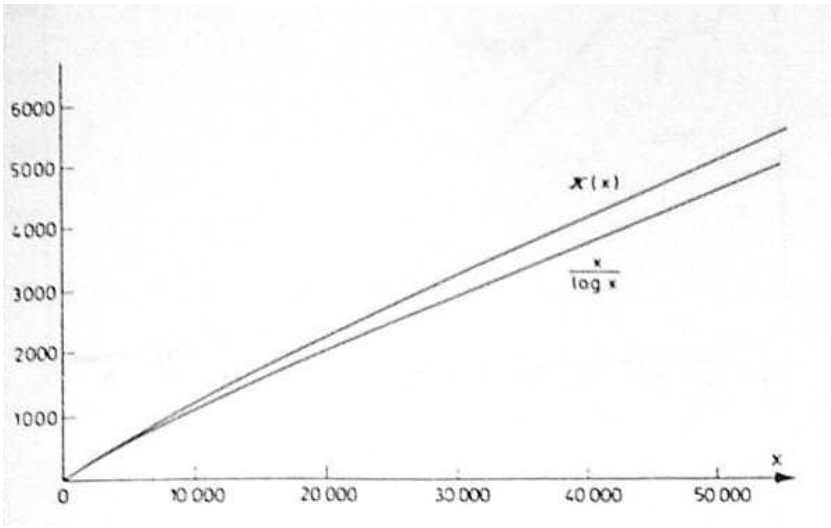

Figure 1: Comparison of the graph $\pi(x)$ with the approximate graph $\frac{x}{\log x}$.

4.3.2. Legendre's Improvements

Adrien-Marie Legendre was 25 years older than Gauss. Legendre lived in a wealthy family, but during the French revolution he lost all his money and he had to do mathematics for a living. He was very fascinated by number theory. In 1798, six years after Gauss, he discovered the connection between the prime counting function and the logarithm. A big fight for the rights of this discovery began but some years later it could be proved that Gauss had made this detection long before Legendre. Nevertheless, Legendre managed to improve Gauss conjecture to

$$\frac{x}{\log x - 1{,}08366}.$$

He inserted a little adjustment to be even closer to the real prime counting function[60].

4.3.3. Gauss's Logarithmic Integral Li(N)

Gauss managed to show that

$$\frac{x}{\log x} \sim Li\ x$$

and, therefore,

$$Li\ x \sim \pi(x).$$

[60] du Sautoy 2004, pp. 72-74

He defined the integral logarithm as Cauchy principal value logarithm

$$Li\ x = \int_0^x \frac{dt}{\log t} = \lim_{\epsilon \to 0} \left(\int_0^{1-\epsilon} + \int_{1+\epsilon}^{x} \right) \frac{dt}{\log t}.$$

Using the l' Hôpital's rule one can show the asymptotic equality of $Li\ x$ and (x) :

$$\lim_{x\to\infty} \frac{Li\ x}{\frac{x}{\log x}} = \lim_{x\to\infty} \frac{\frac{1}{\log x}}{\frac{1}{\log x} - \frac{1}{\log^2 x}} = 1.$$

Thus,

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

Gauss assumed that $\pi(x)$ gets better described by $Li\ x$ than by $\frac{x}{\log x}$, which seems to get confirmed by the following table[61].

Table 2[62] Comparison of the two approximation $Li(x)$ and $\frac{x}{\log x}$ with $\pi(x)$.

$\boldsymbol{x}$	$\boldsymbol{\pi(x)}$	$\boldsymbol{li\ x - \pi(x)}$	$\boldsymbol{\frac{x}{\log x} - \pi(x)}$
10^1	4	2,2	0,3
10^2	25	5,1	-3,3
10^3	168	10	-23
10^4	1 229	17	-143
10^5	9 592	38	-906
10^6	78 498	130	-6 116

[61] Hlawka; Schoißengeier; Taschner 1986, p. 101
[62] Ribenboim 1996, p. 237

10^7	664 579	339	-44 158
10^8	5 761 455	754	-332 774
10^9	50 847 534	1 701	-2 592 592
10^{10}	455 052 512	3 104	-20 785 030

4.3.4. Riemann's Contribution to the Prime Number Theorem

Riemann not only counted the prime numbers as primes but also the powers of primes. More precisely he counted the square of a prime as half a prime, the cube of a prime as a third prime, etc. He then claimed that the probability for a large number x to be a prime number is even closer to $x/\log x$. This leads to the approximation

$$\pi(x) + \frac{1}{2}\pi\left(\sqrt{x}\right) + \frac{1}{3}\pi\left(\sqrt[3]{x}\right) + \frac{1}{4}\pi\left(\sqrt[4]{x}\right) + \cdots \approx Li(x)$$

or, equivalently

$$\pi(x) \approx Li(x) - \frac{1}{2}Li\left(\sqrt{x}\right) - \frac{1}{3}Li\left(\sqrt[3]{x}\right) - \frac{1}{4}Li\left(\sqrt[4]{x}\right) - \cdots$$

In honor of Riemann, the right side of this function is called $R(x)$. Riemann's approximation provides an amazingly good approximation to $\pi(x)$ as can be seen in the following table[63].

Table 3[64] Riemann's approximation $R(x)$ compared with $\pi(x)$.

$\boldsymbol{x}$	$\boldsymbol{\pi(x)}$	$\boldsymbol{R(x)}$
100,000,000	5,761,455	5,761,552
200,000,000	11,078,937	11,078,090
300,000,000	16,252,325	16,252,355
400,000,000	21,336,326	21,336,185

[63] Zagier 1975, p. 10
[64] Zagier 1975, p. 10

500,000,000	26,355,867	26,355,517
600,000,000	31,324,703	31,324,622
700,000,000	36,252,931	36,252,719
800,000,000	41,146,179	41,146,248
900,000,000	46,009,215	46,009,949
1,000,000,000	50,847,534	50,847,455

Unlike Gauss and Legendre, who obtained their approximations only empirically, Riemann discovered his function $R(x)$ by theoretical considerations. Nevertheless, he never managed to prove the Prime Number Theorem. The first two who accomplished to prove it were Jacques Hadamard in 1896 and, independently, Charles-Jean de la Vallée Poussin. Both their proofs where based on Riemann's work[65].

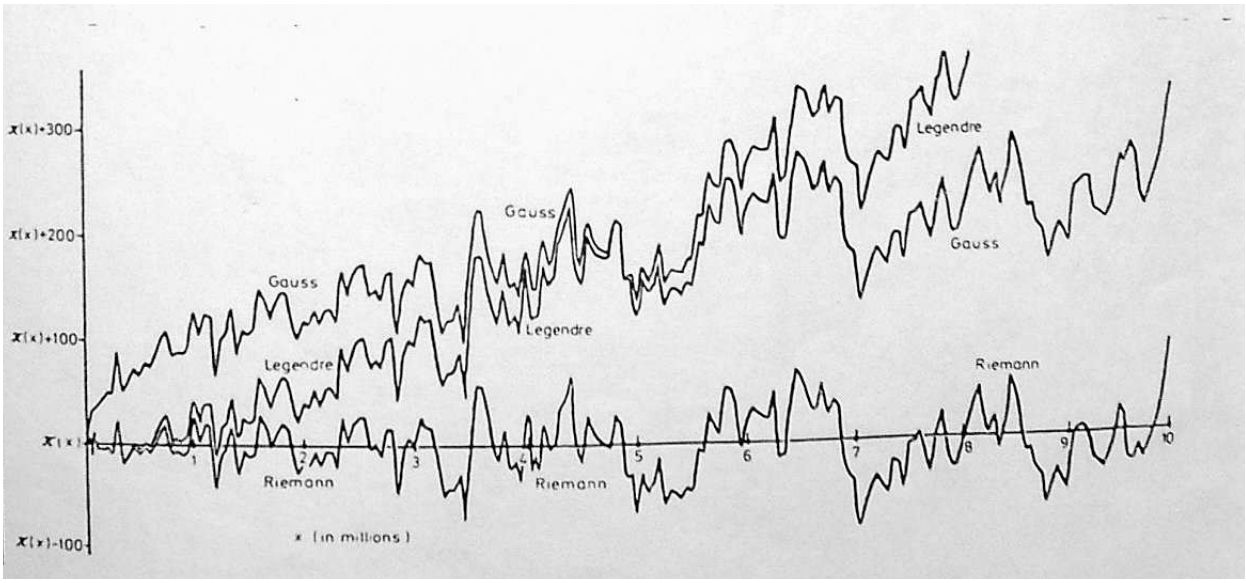

Figure 2: Comparison of the function $\pi(x)$ with the approximations of Gauss, Legendre and Riemann up to 10 million only illustrating the differences between them.

Since the four functions ($\pi(x)$ and the approximations of Gauss, Legendre and Riemann) lie so close together that one would not be able to distinguish them with the naked eye, the illustration only depicts the differences between them. It can be observed that for a small number x Legendre's approximation is significantly better

[65] Zagier 1975, p. 11

than Gauss's $Li(x)$. Nevertheless, after 5 million Gauss's approximation is better and it can be proved that $Li(x)$ stays better when x grows. Regarding Fig. 2, it can easily be noticed that at least in this interval Riemann's function describes $\pi(x)$ the best because it is always smaller than $Li(x)$. However, Littlewood proved that there actually do exist numbers where $\pi(x)$ becomes larger than $Li(x)$, although no such numbers have been found. Skewes managed to prove that there exist at least one such number which is smaller than $10^{10^{10^{34}}}$ [66].

4.4. Chebyshev's Theorem

Around 1850, Chebyshev nearly managed to prove the prime number theorem[67].

He conjectured the following theorem and made great progress in the determination of the order of magnitude of $\pi(x)$.

Theorem 4.2: *There exist two positive absolute terms c_1 and c_2, so that for a sufficiently large x*

$$c_1 * \frac{x}{log\, x} < \pi(x) < c_2 * \frac{x}{log\, x}$$ [68] [69].

Chebyshev proved this for $c_1 = 0{,}89$ and $c_2 = 1{,}11$ [70]. However, in this paper it will only be shown for $c_1 = \frac{2}{3}$ and $c_2 = 1{,}7$.

Proof: At first, one has to prove that

$$\pi(x) < 1{,}7\frac{x}{\log x}$$

by induction on x.

Basis $x = 2$:

[66] Zagier 1975, pp. 12-13
[67] Hlawka; Schoißengeier; Taschner 1986, p. 101
[68] Hlawka, Schoißengeier; Taschner 1986, p. 101
[69] Niven, Zuckerman 1972, p. 240
[70] Zagier 1975, p. 13

$$\pi(2) = 1 < 1{,}7\frac{2}{\log 2} \approx 11{,}3$$

According to Zagier, this inequality is even true for $x < 1200$ [71].

Induction step: Assuming that for any natural number $x < n$ the inequality has been proved. Since

$$2^{2n} = (1+1)^{2n}$$

and according to the binomial theorem

$$(1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n-1} + \binom{2n}{2n},$$

the middle binomial coefficient $\binom{2n}{n}$ is at most 2^{2n}.

Moreover,

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(2n) * (2n-1) * \ldots * 2 * 1}{(n * (n-1) * \ldots * 2 * 1)^2}.$$

It can be seen that $\binom{2n}{n}$ is divisible by every prime number between n and $2n$, because every prime p smaller than $2n$ appears in the numerator but no prime bigger than n can appear in the denominator. Thus,

$$\prod_{n<p\leq 2n} p \mid \binom{2n}{n}.$$

Since this product has $\pi(2n) - \pi(n)$ factors, each bigger than n, it follows that

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p\leq 2n} p \leq \binom{2n}{n} < 2^{2n}.$$

Taking logarithms, one gets

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n} < 1{,}39\frac{n}{\log n}.$$

[71] Zagier 1975, p.13

According to the induction hypothesis, the inequality is valid for n,

$$\pi(n) < 1{,}7\frac{n}{\log n}.$$

Adding this relation, one gets

$$\pi(2n) - 1{,}7\frac{n}{\log n} < \pi(2n) - \pi(n) < 1{,}39\frac{n}{\log n}$$

and, thus,

$$\pi(2n) < 3{,}09\frac{n}{\log n} < 1{,}7\frac{2n}{\log 2n} \qquad (n > 1200)$$

Therefore, the inequality is also true for $2n$. Since

$$\pi(2n+1) \leq \pi(2n) + 1$$

it follows

$$\pi(2n+1) < 3{,}09\frac{n}{\log n} + 1 \leq 1{,}7\frac{2n+1}{\log(2n+1)} \qquad (n > 1200).$$

Hence, the inequality is also true for $2n+1$ completing the induction[72].

To prove the other direction, namely $\frac{2}{3}\frac{n}{\log n} < \pi(n)$, one needs the following lemma.

Lemma 4.1: *Let p be a prime number and p^{v_p} is the largest power of p dividing $\binom{n}{k}$, then*

$$p^{v_p} \leq n\ ^{73}.$$

Lemma 4.1 can be proved by using the formula of the power of p dividing $n!$, which says that if n is a nonnegative integer and p is a prime, the exponent (N) of the highest power of p that divides $n!$ is equal to

[72] Zagier 1975, pp. 13-14
[73] Zagier 1975, p. 14

$$N = \sum_{i=1}^{\infty} \frac{n}{p^i}$$ [74] [75].

Corollary 4.1: *Every binomial coefficient* $\binom{n}{k}$ *satisfies*

$$\binom{n}{k} = \prod_{p \le n} p^{v_p} \le n^{\pi(n)}$$ [76].

Sequel to the proof of theorem 4.2:

Using the inequality of corollary 4.1, one gets

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \le (n+1) * n^{\pi(n)}$$

and taking the logarithms of it

$$n \log 2 \le \log(n+1) + \pi(n) \log n,$$

hence,

$$\pi(n) \ge \frac{n \log 2}{\log n} - \frac{\log(n+1)}{\log n} > \frac{2}{3} \frac{n}{\log n} \qquad (n > 200)$$ [77]

□

Chebychev nearly managed to prove the Prime Number Theorem. He already knew that if the function $\pi(x)$ is asymptotic to some $c\frac{x}{\log x}$, c has to be 1. However, the real difficulty in proving the prime number theory is to show that $\lim_{x\to\infty} \pi(x)/(x/\log x)$ exists at all. Although Chebychev made great progress in the field of prime numbers, the world of mathematics had to wait another 46 years until Hadamard and de la Vallée Poussin independently proved the Prime Number Theorem in 1896[78].

[74] Zagier 1975, p. 14
[75] Sato, p.20
[76] Zagier 1975, p. 14
[77] Zagier 1975, p. 14
[78] Crandall, Pomerance 2005, p. 10

5. Riemann and the Zeta Function

Bernhard Riemann was born in 1826 in Hannover. He studied mathematics at the University of Göttingen and also at the Berlin University. In 1851, Riemann submitted his Ph.D thesis, which was supervised by Gauss. It is said that Gauss had a great influence on Riemann and his interest in number theory[79].

In 1859, Riemann was elected to become a member of the Berlin Acadamy at the early age of 32. This was a great honor for such a young mathematician. Since it was common at such occasions to report to the Academy on their most recent research, Riemann presented his work *On the Number of Prime Numbers Less Than a Given Quantity*[80]*.* In this paper, Riemann investigated the zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which had already been examined by Euler. However, Riemann considered the zeta function as a complex function instead of a real one[81]. He suspected that all non-trivial zeros of the zeta function have real part $\frac{1}{2}$, but did not prove it[82]. He just remarked:

> "Certainly one would wish for a stricter proof here; I have meanwhile temporarily put aside the search for this after some fleeting futile attempts, as it appears unnecessary for the next objective of my investigation."[83]

This casual guess of Riemann is now known as the Riemann hypothesis and is one of the most important unsolved problems in mathematics. More about the fascination of the Riemann hypothesis is stated in section 5.3.

So far, there has not been an obvious reason for mentioning the zeta function in a paper about prime numbers. Why is the Riemann hypothesis always associated with prime numbers?

---

[79] O'Connor & Robertson 1998
[80] Derbyshire 2003, p. ix
[81] O'Connor & Robertson 1998
[82] Derbyshire 2003, p. xi
[83] Riemann 1859, p. 4

The following two sections are going to answer this question and reveal the connection between the zeta function and the prime numbers.

5.1. Relation to Prime Numbers

The connection with prime numbers had already been noticed earlier by Euler. By proving the following theorem he managed to express the zeta function as a product over prime numbers only[84].

Theorem 5.1: *If* $s > 1$ *then*

$$\zeta(s) = \prod_{p \in P} (1 - p^{-s})^{-1},$$

with P *being the set of primes*[85]*.*

Proof: This proof starts with the zeta function and slowly converts it into the above mentioned product. First, one has to apply the sieve of Eratosthenes to the zeta function. By multiplying both sides with $\frac{1}{2^s}$, one gets

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{10^s} + \cdots$$

and by subtracting the result from the original zeta function, it becomes

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots$$

It can be seen, that the subtraction eliminated all the even-numbered terms from the infinite sum. Continuing this with $\frac{1}{3^s}$, one gets

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \frac{1}{33^s} + \cdots$$

and again subtracting it from the expression before

[84] Hardy & Wright 1979, p. 246
[85] Crandall & Pomerance 2005, p. 34

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{13^s}+\frac{1}{17^s}+\cdots$$

Thus, all the multiples of three terms were eliminated from the infinite sum. By repeating this process infinitely often (for every prime number), one receives the following equation

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

and written in a closed form, one obtains

$$\zeta(s)\prod_{p\in P}\left(1-\frac{1}{p^s}\right)=1.$$

This is equivalent to

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

or avoiding fractions

$$\zeta(s)=\prod_{p\in P}(1-p^{-s})^{-1}\ ^{86}.$$

□

The attentive reader might have noticed that this theorem is somehow similar to Euler's proof of the existence of infinitely many prime numbers. Actually, this theorem leads directly to Euler's proof.

Proof: By rewriting the left side of theorem 5.1, one gets the expression

$$\sum_{n=1}^{\infty}n^{-s}=\prod_{p\in P}(1-p^{-1})^{-1}.$$

[86] Derbyshire 2003, pp. 102-105

Both sides are infinite sums. If the prime numbers ended, the product on the right side of the equation would end as well. Therefore, it would work out to a finite number, regardless of the value of s. However, when $s = 1$, the left hand side is the harmonic series, which is known to add up to infinity. And this is a contradiction. Therefore, the number of primes must be infinite[87]. □

Consequently, one can see that the connection between the zeta function and the prime numbers has already been established with Euler's proof in section 4.1.2.

5.2. Connection between $\pi(x)$ and ζ Function

Since the Riemann hypothesis and the connection between $\pi(x)$ and ζ function is highly complicated, this section is going to be more explanatory than the previous ones and the focus is not so much on exact mathematical proofs but on conveying the topic in an understandable way.

First of all, the function $\pi(x)$ needs to be defined more precisely with some adjustments in order that the following arguments are correct.

Definition 5.1.: *The prime counting function $\pi(x)$ is defined as following:*

$$\pi(x) = \begin{cases} number\ of\ primes\ smaller\ than\ x, & if\ x\ is\ no\ prime \\ number\ of\ primes\ smaller\ than\ x\ plus\ \frac{1}{2}, & if\ x\ is\ prime \end{cases}$$ [88].

This definition is illustrated by Fig. 3. One can see that every time x reaches a prime number the function $\pi(x)$ jumps up one half. The domain of this function consists of all the non negative numbers.

[87] Derbyshire 2003, p. 105
[88] Derbyshire 2003, p. 297

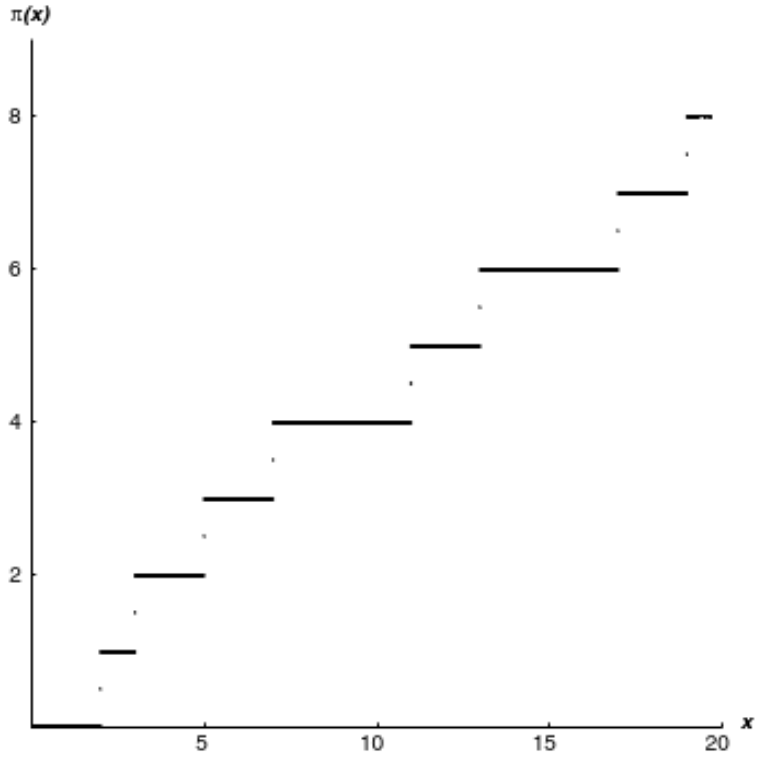

Figure 3: The prime counting function for $0 \leq x \leq 20$.

The next function, which is going to be introduced, will be called J function following Harold Edwards although Riemann referred to it as the f function. Since f is nowadays mostly used to refer to any generic function, it would be unusual to use f to refer to a specific one[89].

Definition 5.2: *For any non negative number x, J is defined as*

$$J(x) = \sum_{n=1}^{\infty} \frac{1}{n} \pi\left(\sqrt[n]{x}\right) = \pi(x) + \frac{1}{2}\pi\left(\sqrt{x}\right) + \frac{1}{3}\pi\left(\sqrt[3]{x}\right) + \frac{1}{4}\pi\left(\sqrt[4]{x}\right) + \cdots$$ [90]

Although this function seems to be infinite, it is actually a finite sum, since the prime counting function $\pi(x)$ is zero for every $x < 2$ [91]. Fig. 4 depicts the J function up to 100.

[89] Derbyshire 2003, p. 298
[90] Derbyshire 2003, p. 299
[91] Derbyshire 2003, p. 299

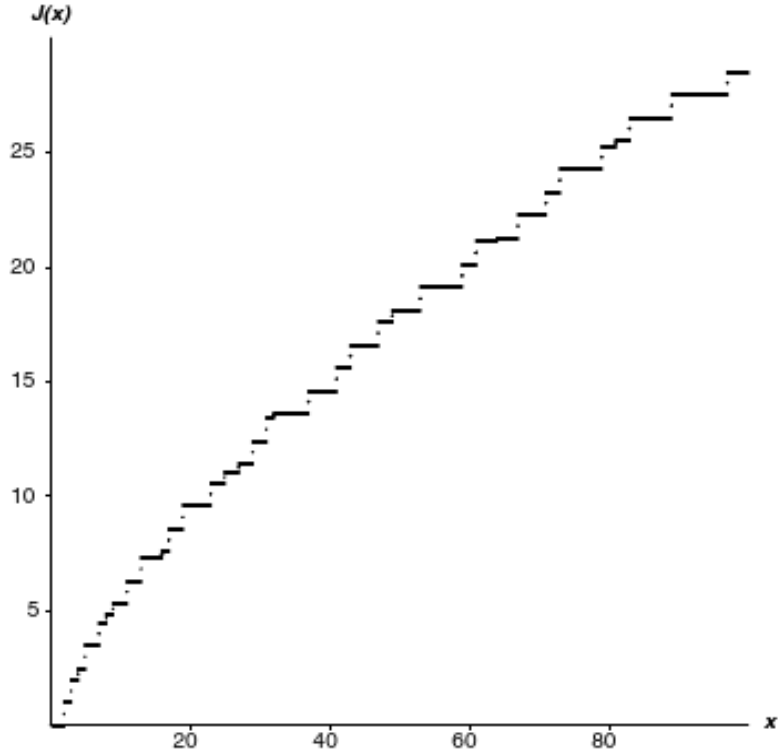

Figure 4: The $J(x)$ function for $0 \leq x \leq 100$.

The next step is now the inversion of this relationship and, therefore, one needs the Möbius function and the Möbius inversion.

Definition 5.3: *The Möbius function $\mu(n)$is defined as follows:*

(i) $\mu(1) = 1$,

(ii) $\mu(n) = 0$ *if n has a squared factor,*

(iii) $\mu(p_1 p_2 \dots p_k) = (-1)^k$ *if all the primes $p_1, p_2, \dots, p_k$ are different*[92].

For a better understanding of the Möbius function and its relationship with the zeta function, one has to take a closer look at the reciprocal of the zeta function. Due to theorem 5.1

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

$$= \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{6^s}\right)\left(1 - \frac{1}{7^s}\right)\dots$$

[92] Hardy & Wright 1979, p. 234

Every term in this expression which is not equal to 1 is a number between 0 and $-\frac{1}{2}$. By multiplying an infinite of them, the result would be no bigger than $\left(-\frac{1}{2}\right)^{\infty}$, which is zero. Thus, if one wants to multiply out this parenthesis, one must only look at the products with a finite number of terms not equal to 1. By doing so one receives the following expression.

$$\frac{1}{\zeta(s)} = 1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \frac{1}{7^s} + \frac{1}{10^s} - \frac{1}{11^s} - \frac{1}{13^s} + \frac{1}{14^s} \dots$$

It can be seen that this expression includes every natural number that is the product of an odd number of different primes prefixed by a minus sign and every natural number that is the product of an even number of different primes prefixed by a plus sign. The only numbers missing are those which have a squared factor and this is exactly the definition of the Möbius function. Thus, one can express the zeta function in terms of the Möbius function.

$$\frac{1}{\zeta(s)} = \sum_{n=0}^{\infty} \frac{\mu(n)}{n^s}$$ [93]

Theorem 5.2: *The Möbius inversion says that if f is any arithmetic function, and g is the arithmetic function defined by*

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

And vice versa, if g is any arithmetic function, and f is the arithmetic function defined by

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

[93] Derbyshire 2003, pp. 247-250

then

$$g(n) = \sum_{d|n} f(d)$$ [94].

Proof: In order to be able to prove the Möbius inversion, one needs the following lemmas and definitions.

Lemma 5.1: *The Möbius function $\mu(n)$ is multiplicative (more precisely: an arithmetic function $f(n)$ is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$), and*

$$\sum_{d|n} \mu(d) \begin{cases} = 1 & if\ n = 1, \\ = 0 & if\ n > 1 \end{cases}$$ [95].

Proof of lemma 5.1: The multiplicativity follows immediately from the definition of $\mu(n)$, because if $(m,n) = 1$ and both are square free integers with k and l prime factors, respectively, then the product mn is also square free with $k + l$ factors. Thus,

$$\mu(m)\mu(n) = (-1)^k(-1)^l = (-1)^{k+l} = \mu(mn).$$

The second part of lemma 5.1 is slightly more difficult to prove. If $n = 1$,

$$\sum_{d|n} \mu(d) = \mu(1) = 1.$$

For $n > 1$, let

$$n = {p_1}^{r_1}{p_2}^{r_2} \dots {p_k}^{r_k}$$

be the prime factorization of n with $r_1, r_2, \dots, r_k \geq 1$. Consequently, the largest square free divisor of n, namely the radical of n, is

$$rad(n) = p_1 p_2 \dots p_{k.}$$

This is the product of all the different prime numbers dividing n. Let $m = rad(n)$. If d divides n and $\mu(d) \neq 0$, it follows that d is square free and, thus, d must also divide m. Therefore,

---

[94] Nathanson 2000, pp. 218-219
[95] Nathanson 2000, p. 217

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d)$$

Since m is the product of k different primes, it follows that there are exactly $\binom{k}{i}$ divisors of m which consist of i distinct primes. Consequently, the number of divisors d of m such that $\omega(d) = i$ ($\omega(d)$ being defined as the number of distinct prime divisors of d) is $\binom{k}{i}$. Hence,

$$\sum_{d|m} \mu(d) = \sum_{i=0}^{k} \sum_{\substack{d|m \\ \omega(d)=i}} \mu(d)$$

$$= \sum_{i=0}^{k} \sum_{\substack{d|m \\ \omega(d)=i}} (-1)^i$$

$$= \sum_{i=0}^{k} \binom{k}{i} (-1)^i$$

and according to the binomial theorem

$$= (1-1)^k$$

$$= 0$$ [96].

Definition 5.4: *The Dirichlet convolution $f * g$ is defined by*

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{dd'=n} f(d) g(d'),$$

where the sum is over all positive divisors d of n[97]*.*

Definition 5.5: *The arithmetic function $\delta(n)$ is defined by*

$$\delta(n) = \begin{cases} 1 & if\ n = 1, \\ 0 & if\ n > 1, \end{cases}$$

[96] Nathanson 2000, pp. 217-218
[97] Nathanson 2000, p. 201

the zero function $0(n)$ *by*

$$0(n) = 0,$$

and the function $1(n)$ *by*

$$1(n) = 1$$

for all n[98].

Lemma 5.2: *The Dirichlet convolution is commutative and associative, that is,*

$$f * g = g * f$$

and

$$(f * g) * h = f * (g * h)$$

for all arithmetic functions $f, g,$ *and* h[99]*.*

Proof of lemma 5.2: To prove this lemma, one has to use mere elementary calculations. It is

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right) f(d) = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = (g * f)(n),$$

which proves the commutativity of the Dirichlet convolution. Moreover,

$$\big((f * g) * h\big)(n) = \sum_{d|n} (f * g)(d) h\left(\frac{n}{d}\right)$$

$$= \sum_{dm=n} (f * g)(d) h(m)$$

$$= \sum_{dm=n} \sum_{k|d} f(k) g\left(\frac{d}{k}\right) h(m)$$

[98] Nathanson 2000, p. 201 and 218
[99] Nathanson 2000, p. 202

$$= \sum_{dm=n} \sum_{kl=d} f(k)g(l)h(m)$$

$$= \sum_{klm=n} f(k)g(l)h(m)$$

$$= \sum_{k|n} f(k) \sum_{lm=n/k} g(l)h(m)$$

$$= \sum_{k|n} f(k) \sum_{l|(n/k)} g(l)h\left(\frac{n}{kl}\right)$$

$$= \sum_{k|n} f(k)(g * h)\left(\frac{n}{k}\right)$$

$$= \big(f * (g * h)\big)(n)$$

and, thus, the Dirichlet convolution is also associative[100]. □

With the use of straightforward calculations, one can even prove that the set of all complex-valued arithmetic functions is a commutative ring, with addition defined by point wise sum and multiplication defined by the Dirichlet convolution. The additive identity is $0(n)$, whereas the multiplicative identity is $\delta(n)$[101]. However, this is not needed for the Möbius inversion and, therefore, not proved in this paper.

By using the Dirichlet convolution and by defining the arithmetic function $1(n)$ by $1(n) = 1$ for all n, one can reformulate lemma 5.1 as follows:

$$\mu * 1 = \delta$$

and, thus, the Möbius function is a unit with inverse 1[102].

Sequel to the proof of theorem 5.2: If one uses lemma 5.1 and 5.2, the Möbius inversion is easy to prove. Using the Dirichlet convolution, the definition

[100] Nathanson 2000, p. 202
[101] Nathanson 2000, p. 202
[102] Nathanson 2000, p. 218

$$g(n) = \sum_{d|n} f(d)$$

is equivalent to

$$g = f * 1.$$

Moreover,

$$g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * \delta$$

and

$$(f * \delta)(n) = (\delta * f)(n) = \sum_{d|n} \delta(d) f\left(\frac{n}{d}\right) = \delta(1) f\left(\frac{n}{1}\right) = f(n),$$

hence,

$$g * \mu = f$$

and by applying the definition of the Dirichlet convolution, one gets

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

To prove the other direction, one uses the same arguments.

The definition

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

is equivalent to

$$f = g * \mu.$$

Furthermore,

$$f * 1 = (g * \mu) * 1 = g * (\mu * 1) = g * \delta = g$$

and again by applying the definition of the Dirichlet convolution, one obtains

$$g(n) = \sum_{d|n} f(d)1\left(\frac{n}{d}\right)$$

and due to the definition of the function $1(n)$ for all n, this gives

$$g(n) = \sum_{d|n} f(d)^{103}.$$

Now with the help of the Möbius inversion, one can express the prime counting function $\pi(x)$ in terms of the J function.

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} J\left(\sqrt[n]{x}\right)$$

This is again a finite sum, since $J(x) = 0$ for every $x < 2$. The most important fact is that Riemann managed to express $J(x)$ in terms of $\zeta(x)$.

According to theorem 5.1,

$$\zeta(s) = \prod_{p \in P} (1 - p^{-s})^{-1}.$$

By taking the logarithm, one gets

$$\log \zeta(s) = \sum_{p \in P} -\log(1 - p^{-s})\ ^{104}.$$

McLaurin's infinite series for $\log(1 - x)$ says that if $-1 \leq x < 1$, it follows that

$$\log(1 - x) = \sum_{n=1}^{\infty} -\frac{x^n}{n}\ ^{105}.$$

Therefore, as long as s is positive one can apply McLaurin's infinite series for $\log(1 - x)$. Hence,

[103] Nathanson 2000, p. 219
[104] Derbyshire 2003, pp. 302-304
[105] Derbyshire 2003, pp. 148-149

$$\log \zeta(s) = \sum_{p \in P} \sum_{n=1}^{\infty} \frac{1}{np^{ns}}$$

$$= \frac{1}{2^s} + \frac{1}{2 * 2^{2s}} + \frac{1}{3 * 2^{3s}} + \frac{1}{4 * 2^{4s}} + \cdots$$

$$+ \frac{1}{3^s} + \frac{1}{2 * 3^{2s}} + \frac{1}{3 * 3^{3s}} + \frac{1}{4 * 3^{4s}} + \cdots$$

$$+ \frac{1}{5^s} + \frac{1}{2 * 5^{2s}} + \frac{1}{3 * 5^{3s}} + \frac{1}{4 * 5^{4s}} + \cdots$$

$$+ \cdots$$

In order to be able to establish the connection with the J function, one has to look at the integral of $J(x)$ [106].

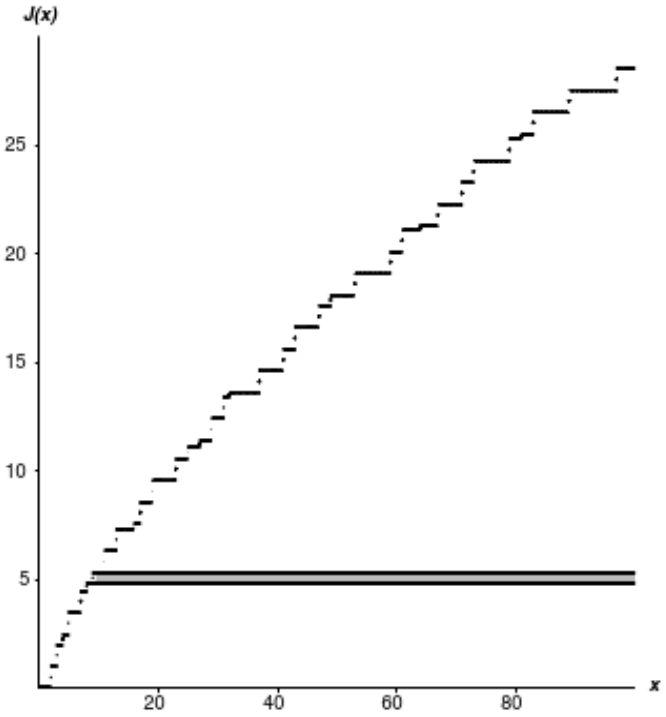

Figure 5: The function of $J(x)$ with an exemplary stripe starting from $x = 3^2$.

By analyzing the graph of $J(x)$, as shown in Fig. 5, more closely, one can see that there are infinitely many stripes going to infinity. The ones starting from each prime have the height 1, from each square of a prime have the height $\frac{1}{2}$, from each cube of a prime have the height $\frac{1}{3}$, and so forth. In the end, one obtains

[106] Derbyshire 2003, pp. 304-305

$$\int_0^\infty J(x)dx = \sum_{p\in P}\sum_{n=1}^{\infty}\int_{p^n}^{\infty}\frac{1}{n}dx$$

$$= \int_2^\infty 1dx + \int_{2^2}^\infty \frac{1}{2}dx + \int_{2^3}^\infty \frac{1}{3}dx + \int_{2^4}^\infty \frac{1}{4}dx + \dots$$

$$+ \int_3^\infty 1dx + \int_{3^2}^\infty \frac{1}{2}dx + \int_{3^3}^\infty \frac{1}{3}dx + \int_{3^4}^\infty \frac{1}{4}dx + \dots$$

$$+ \int_5^\infty 1dx + \int_{5^2}^\infty \frac{1}{2}dx + \int_{5^3}^\infty \frac{1}{3}dx + \int_{5^4}^\infty \frac{1}{4}dx + \dots$$

$$+ \cdots$$

Therefore, the integral of $J(x)$ is infinite. To connect the infinite integral of $J(x)$ with the zeta function, one has to squish down the J function at the right side by multiplying it with x^{-s-1}. This leads to the following integral.

$$\int_0^\infty J(x)x^{-s-1}dx = \sum_{p\in P}\sum_{n=1}^{\infty}\int_{p^n}^{\infty}\frac{1}{n}x^{-s-1}dx$$

$$= \int_2^\infty 1x^{-s-1}dx + \int_{2^2}^\infty \frac{1}{2}x^{-s-1}dx + \int_{2^3}^\infty \frac{1}{3}x^{-s-1}dx + \int_{2^4}^\infty \frac{1}{4}x^{-s-1}dx + \dots$$

$$+ \int_3^\infty 1x^{-s-1}dx + \int_{3^2}^\infty \frac{1}{2}x^{-s-1}dx + \int_{3^3}^\infty \frac{1}{3}x^{-s-1}dx + \int_{3^4}^\infty \frac{1}{4}x^{-s-1}dx + \dots$$

$$+ \int_5^\infty 1x^{-s-1}dx + \int_{5^2}^\infty \frac{1}{2}x^{-s-1}dx + \int_{5^3}^\infty \frac{1}{3}x^{-s-1}dx + \int_{5^4}^\infty \frac{1}{4}x^{-s-1}dx + \dots$$

$$+ \cdots$$ [107]

[107] Derbyshire 2003, pp. 306-309

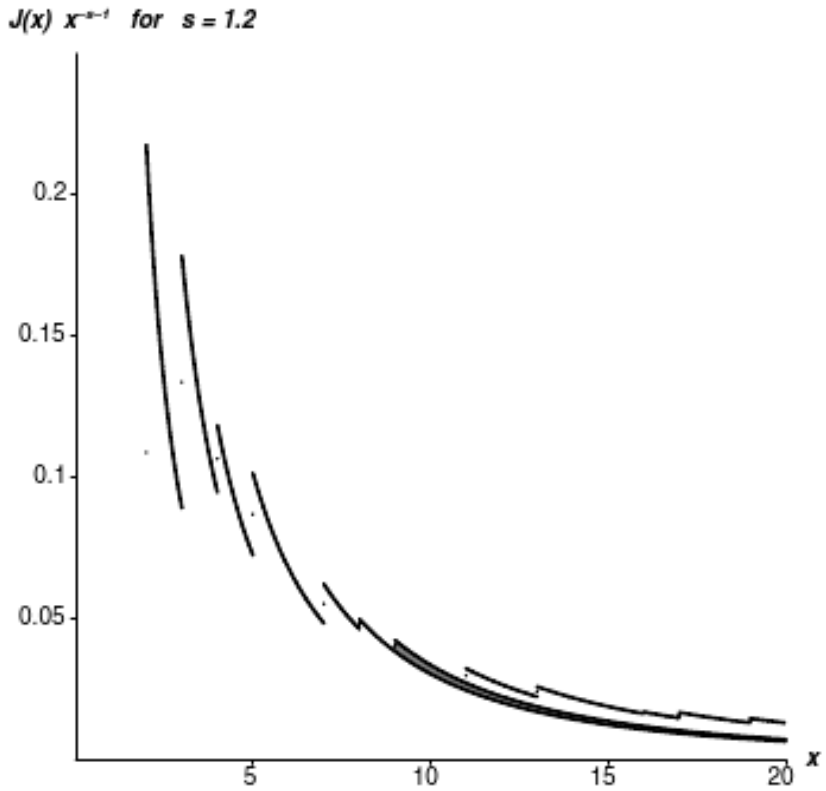

Figure 6: The function of $J(x)x^{-s-1}$ for $s = 1{,}2$ with an exemplary stripe starting from $x = 3^2$.

The last step to finally get to Riemann's achievement and see the connection between the J and the zeta function is only shown exemplarily. If one picks the integral $\int_{3^2}^{\infty} \frac{1}{2} x^{-s-1} dx$ out of the infinite sum of infinite sums of integrals, one can show that

$$\frac{1}{2} \int_{3^2}^{\infty} x^{-s-1}\, dx = \frac{1}{2 * 3^{2s} s}$$

Proof: Since

$$\int x^{-s-1} dx = -\frac{1}{s x^s},$$

one obtains

$$\tfrac{1}{2} \int_{3^2}^{\infty} x^{-s-1}\, dx = \tfrac{1}{2} \left(0 + \tfrac{1}{3^{2s} s}\right) = \tfrac{1}{2 * 3^{2s} s}$$ [108].

□

[108] Derbyshire 2003, p. 305

Therefore, it can be seen that $\frac{1}{2}\int_{3^2}^{\infty} x^{-s-1}\,dx$ is exactly the same as the term found in $\log\zeta(s)$ divided by s.

$$\log\zeta(s) = \sum_{p\in P}\sum_{n=1}^{\infty}\frac{1}{np^{ns}} \qquad \int_0^{\infty} J(x)x^{-s-1}dx = \sum_{p\in P}\sum_{n=1}^{\infty}\int_{p^n}^{\infty}\frac{1}{n}x^{-s-1}dx$$

$$= \frac{1}{2^s} + \frac{1}{2*2^{2s}} + \frac{1}{3*2^{3s}} + \frac{1}{4*2^{4s}} + \cdots \qquad = \int_2^{\infty} 1x^{-s-1}dx + \int_{2^2}^{\infty}\frac{1}{2}x^{-s-1}dx + \ldots$$

$$+\frac{1}{3^s} + \frac{1}{2*3^{2s}} + \frac{1}{3*3^{3s}} + \frac{1}{4*3^{4s}} + \cdots \qquad + \int_3^{\infty} 1x^{-s-1}dx + \int_{3^2}^{\infty}\frac{1}{2}x^{-s-1}dx + \ldots$$

$$+\frac{1}{5^s} + \frac{1}{2*5^{2s}} + \frac{1}{3*5^{3s}} + \frac{1}{4*5^{4s}} + \cdots \qquad + \int_5^{\infty} 1x^{-s-1}dx + \int_{5^2}^{\infty}\frac{1}{2}x^{-s-1}dx + \ldots$$

$$+\cdots \qquad +\cdots$$

Consequently,

$$\frac{\log\zeta(s)}{s} = \int_0^{\infty} J(x)x^{-s-1}dx.$$

This was Riemann's great achievement. If one now inverted this expression, one would then be able to express the prime counting function $\pi(x)$ in terms of $\zeta(s)$, since it has already been shown how to express $\pi(x)$ in terms of $J(x)$. Riemann managed to connect the prime counting function belonging to number theory with the zeta function belonging to analysis und calculus. This bridge between mere counting and actual measuring was Riemann's greatest achievement[109].

Some of the most important results of this finding are:

- The fact that $\zeta(s) \to \infty$ as $s \to 1$ implies that there are infinitely many prime numbers.

[109] Derbyshire 2003, pp. 309-310

- The fact that $\zeta(s)$ has no zeros on the line $Re(s) = 1$ immediately leads to the Prime Number Theorem.
- The properties of the zeta function in the critical strip $(0 < Re(s) < 1)$ lead to deep aspects of the prime counting function, such as the essential error term in the Prime Number Theorem[110].

5.3. Riemann Hypothesis, the Greatest Unsolved Problem in Mathematics

The Riemann Hypothesis says that all non trivial zeros of the zeta function have real part $\frac{1}{2}$ [111].

This Hypothesis became very famous when David Hilbert presented a list of 23 open problems at the 1990 International Congress of Mathematicians[112]. He began his speech with the following words:

> "Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries?"[113]

He finished his address with a list of 23 mathematical problems on which he wanted mathematicians to concentrate, because he thought that a discussion of these might result in an advancement of science[114]. Only three of these problems have not been solved yet, one of it being the Riemann Hypothesis[115].

The importance of this hypothesis gets clear if one looks at the hundreds of theorems beginning with "Assuming the truth of the Riemann Hypothesis…"[116]. It beggars the imagination what will happen if the Riemann Hypothesis can be proved wrong, if someone finally finds a zero not being on the critical line.

---

[110] Crandall & Pomerance 2005, pp. 34-35
[111] Derbyshire 2003, p. 77
[112] Encyclopedia of Mathematics 2012
[113] Hilbert 1990
[114] Hilbert 1990
[115] Yandell 2001, p. 385
[116] Derbyshire 2003, p. 357

Andrew Odlyzko once said that:

> It was said that whoever proved the Prime Number Theorem would attain immortality. Sure enough, both Hadamard and de la Vallée Poussin lived into their late nineties. It may be that there is a corollary here. It may be that the RH is false; but, should anyone manage to actually *prove* its falsehood – to find a zero off the critical line – he will be struck dead on the spot, and his result will never become known[117].

[117] Derbyshire 2003, p. 356

6. Conclusion

Prime numbers are an incredibly vital and fascinating part of mathematics. As shown in this paper, there is much which has been discovered about prime numbers. The mathematicians of Pythagoras' school already knew that every number is either a prime number or can be decomposed into prime numbers. The fundamental theorem of arithmetic, which was proved much later, adds that this factorization is in fact unique. Thus, prime numbers can be seen as the DNA of every number. About 300 BC, Euclid proved that there exist infinitely many prime numbers, although one nowadays also knows that there exist arbitrarily big gaps in this infinite prime number sequence.

However, prime numbers still contain one of the greatest unsolved problems in today's mathematics, their distribution. Both Gauss and Legendre noticed that the prime counting function $\pi(x)$ is asymptotically equal to $\frac{x}{\log x}$ known as the Prime Number Theorem. About 100 years later, Hadamard and de la Vallée Poussin managed to prove this theorem. Moreover, Riemann made great progress in the field of prime numbers and the growth of $\pi(x)$ by examining the zeta function for complex numbers. His hypothesis about the location of the non trivial zeros of the zeta function has had an immense influence not only on the field of prime numbers but also on other areas of mathematics and even physics.

Regardless of the numerous great mathematicians who have spent many years of their lives studying prime numbers and the zeta function, no one has managed to completely understand the distribution of prime numbers or find any pattern in their sequence.

Euler once said:

> Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery, into which human mind will never penetrate[118].

[118] Verkhovsky & Mutovic 2005, p. 2

7. Bibliography

Andreescu, T.; Andrica, D. (2009). *Number theory: structures, examples, and problems,* Boston: Birkhäuser.

Bressoud, D. M. (1989). *Factorization and primality testing,* New York: Springer Verlag.

Crandall, R.; Pomerance, C. (2005). *Prime numbers: A computational perspective.* (2nd ed.). New York: Springer.

Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics*. Washington, DC: Joseph Henry Press. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10039746

Du Sautoy, M. (2004). *Die Musik der Primzahlen: auf den Spuren des größten Rätsels der Mathematik*. (3rd ed.). Translated from English by T. Filk. Munich: C.H. Beck

Encyclopedia of Mathematics. (2012, March 31). *Hilbert problems*. Retrieved from http://www.encyclopediaofmath.org/index.php?title=Hilbert_problems&oldid=24081

Euclid (2003). *Die Elemente – Bücher I-XIII*. Translated from Greek by C. Thaer. Introduction by P. Schreiber. Frankfurt am Main: Harri Deutsch.

Hardy, G. H., & Wright, E. M. (1979). *An introduction to the theory of numbers*. (5 ed.). Oxford: Oxford University Press.

Harman, G. (2007). *Prime-Detecting Sieves*. New Jersey: Princeton University Press.

Hilbert, D. (1990). *Mathematical problems: Lecture delivered before the international congress of mathematicians at paris in 1990*. Translated from German by M. Winton Newson. Retrieved from http://aleph0.clarku.edu/~djoyce/hilbert/problems.html

Hlawka, E.; Schoißengeier, J.; Taschner, R. (1986). *Geometrische und analytische Zahlentheorie*, Wien: Manz.

Kerkhoff, A., Krycki, K., & Stuckenholz, J. (1998). *Die geschichte der primzahlen*. Retrieved from http://www.gm.nw.schule.de/~gymwiehl/prim/geschi.htm

Kraft, J.; Bürger, H.; Unfried, H.; Götz, S. (2006). *Mathematische Formelsammlung*, 9. Auflage, Wien: öbvhpt.

Nathanson, M. B. (2000). *Elementary methods in number theory*. New York: Springer-Verlag.

Niven, I.; Zuckerman, H. S. (1976). *Einführung in die Zahlentheorie I*. (3rd ed.). Translated from English by R. Taschner. Mannheim: Bibliographisches Insitut.

Niven, I.; Zuckerman, H. S. (1976). *Einführung in die Zahlentheorie II*. (3rd ed.). Translated from English by R. Taschner. Mannheim: Bibliographisches Insitut.

O'Connor, J. J., & Robertson, E. F. (1998, September). *Georg Friedrich Bernhard Riemann*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Riemann.html

O'Connor, J. J., & Robertson, E. F. (2009, May). *Prime numbers*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/HistTopics/Prime_numbers.html

Ribenboim, P. (1996). *The New Book of Prime Number Records*. (3rd ed.). New York: Springer.

Riemann, B. (1859, November). *On the number of prime numbers less than a given quantity*. Translated from German by D. R. Wilkins in 1998. Retrieved from http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf

Sato, N. (n.d.). *Number theory*. Retrieved from http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf

Verkhovsky, B. S., & Mutovic, A. (2005). *Primality testing algorithm using phytagorean integers*. Unpublished manuscript, Computer Science Department, New Jersey Institute of Technology, Newark, New Jersey. Retrieved from http://web.njit.edu/~verb/PrimalityTestingAlgorithm.pdf

Weisstein, E. W. (n.d.). *Geometric series*. Retrieved from *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/GeometricSeries.html

Yandell, B. H. (2001). *The honors class: Hilbert's problems and their solvers*. Natick, Massachusetts: A K Peters, Limited. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10159702

Zagier, D. (1975). *The first 50 million prime numbers*. Translated from German by R. Perlis. Retrieved from http://sage.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf.

8. List of Images and Figures

Image 1: O'Connor, J. J., & Robertson, E. F. (1999, January). *Pythagoras of Samos*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Pythagoras.html

Image 2: O'Connor, J. J., & Robertson, E. F. (1999, January). *Euclid of Alexandria*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Euclid.html

Image 3: O'Connor, J. J., & Robertson, E. F. (1999, January). *Eratosthenes of Cyrene*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Eratosthenes.html

Image 4: O'Connor, J. J., & Robertson, E. F. (1996, December). *Pierre de Fermat*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Fermat.html

Image 5: O'Connor, J. J., & Robertson, E. F. (2005, August). *Marin Mersenne*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Mersenne.html

Image 6: O'Connor, J. J., & Robertson, E. F. (1998, September). *Leonhard Euler*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Euler.html

Image 7: O'Connor, J. J., & Robertson, E. F. (1996, December). *Johann Carl Friedrich Gauss*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Gauss.html

Image 8: O'Connor, J. J., & Robertson, E. F. (1998, September). *Georg Friedrich Bernhard Riemann*. Retrieved from http://www-history.mcs.st-andrews.ac.uk/Biographies/Riemann.html

Figure 1: Zagier, D. (1975). *The first 50 million prime numbers* (p. 10). Translated from German by R. Perlis. Retrieved from http://sage.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf

Figure 2: Zagier, D. (1975). *The first 50 million prime numbers* (p. 12). Translated from German by R. Perlis. Retrieved from http://sage.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf.

Figure 3: Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics* (p. 298). Washington, DC: Joseph Henry Press. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10039746

Figure 4: Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics* (p. 301). Washington, DC: Joseph Henry Press. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10039746

Figure 5: Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics* (p.306). Washington, DC: Joseph Henry Press. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10039746

Figure 6: Derbyshire, J. (2003). *Prime obsession: Bernhard Riemann and the greatest unsolved problem in mathematics* (p.308). Washington, DC: Joseph Henry Press. Retrieved from http://site.ebrary.com/lib/portsmouth/docDetail.action?docID=10039746

9. Appendix

9.1. Primes up to 1,000 in Decimal Notation

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	742	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		

Twin primes

9.2. Primes up to 100 in Binary Notation

10	11	101	111	1011
1101	10001	10011	10111	11101
11111	100101	101001	101011	101111
110101	111011	111101	1000011	1000111
1001001	1001111	1010011	1011001	1100001

Twin primes

9.3. Song: “Where are the zeros of zeta of s?”

Where are the zeros of zeta of s?[119]

by Tom M. Apostol

(To the tune of *Sweet Betsy from Pike)*

Where are the zeros of zeta of s?
G.F.B. Riemann has made a good guess:
“They're all on the critical line,” stated he,
“And their density's one over two pi log *T*.”

This statement of Riemann's has been like trigger,
And many good men, with vim and with vigor,
Have attempted to find, with mathematical rigor,
What happens to zeta as mod *t* gets bigger.

The efforts of Landau and Bohr and Cramér,
Hardy and Littlewood and Titchmarsh are there.
In spite of their effort and skill and finesse,
In locating the zeros there's been no success.

In 1914 G.H. Hardy did find,
An infinite number that lie on the line.
His theorem, however, won't rule out the case,
That there might be a zero at some other place.

Let *P* be the function pi minus *Li*;
The order of *P* is not known for *x* high.
If square root of *x* times log *x* we could show,
Then Riemann's conjecture would surely be so.

Related to this is another enigma,
Concerning the Lindelöf function mu sigma,

[119] Derbyshire 2003, pp. 394-395

Which measures the growth in the critical strip;
On the number of zeros it gives us a grip.

But nobody knows how this function behaves.
Convexity tells us it can have no waves.
Lindelöf said that the shape of its graph
Is constant when sigma is more than one-half.

Oh, where are the zeros of zeta of s?
We must know exactly. It won't do to guess,
In order to strengthen the prime number theorem,
The integral's contour must never go near 'em.

André Weil has improved on old Riemann's fine guess
By using a fancier zeta of s.
He Proves that the zeros are where they should be,
Provided the characteristic is *p*.

There's a moral to draw from this long tale of woe
That every young genius among you must know:
If you tackle a problem and seem to get stuck,
Just take I mod *p* and you'll have better luck.

Non-Plagiarism Declaration

I hereby declare that the information on which my work is based has been collected by me personally and has not been plagiarized from any unacknowledged sources. I have properly credited the source of any and all quoted or paraphrased material.

April 2012, _____ (Daniela Schwendinger)