



UPPSALA  
UNIVERSITET

U.U.D.M. Project Report 2020:37

# Goldbach's Conjecture

Johan Hårdig

Examensarbete i matematik, 15 hp  
Handledare: Veronica Crispin Quinonez  
Examinator: Martin Herschend  
Augusti 2020



Department of Mathematics  
Uppsala University



# Goldbach's Conjecture

Johan Härdig

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Definition of the Conjectures . . . . .	3
<b>2</b>	<b>Prime Numbers and their Distribution</b>	<b>4</b>
2.1	Early Results . . . . .	4
2.2	Prime Number Theorem . . . . .	6
<b>3</b>	<b>Heuristic and Probabilistic Justification</b>	<b>8</b>
3.1	Method Presented by Gaze & Gaze . . . . .	8
3.1.1	Sieve Method by Gaze & Gaze . . . . .	9
3.1.2	Example . . . . .	10
3.2	Prime Number Theorem for Arithmetic Progressions . . . . .	11
3.3	Distribution of Primes Across Prime Residue Classes . . . . .	14
3.4	Heuristic Justification by Gaze & Gaze . . . . .	15
3.4.1	Conclusion . . . . .	16
3.5	Goldbach's Comet . . . . .	17
<b>4</b>	<b>The Ternary Goldbach's Conjecture</b>	<b>18</b>
4.1	Historical Overview . . . . .	18
4.2	Approach . . . . .	19
4.3	Theorems and Methods in the Proof . . . . .	20
4.3.1	Hardy-Littlewood Circle Method . . . . .	20
4.3.2	Vinogradov's Theorem . . . . .	22
4.3.3	The Large Sieve . . . . .	24
4.3.4	$L$ -functions . . . . .	24
4.3.5	Computational Methods . . . . .	26
4.4	The Proof . . . . .	29

### Abstract

The following text will provide a historical perspective as well as investigate different approaches to the unsolved mathematical problem *Goldbach's conjecture* stated by Christian Goldbach in the year 1742.

First off, there will be an overview of the early history of prime numbers, and then a brief description of the Prime Number Theorem.

Subsequently, an example of a heuristic and probabilistic method of justifying the binary *Goldbach's conjecture*, proposed by Gaze and Gaze, will be discussed.

Lastly, the proposed solution of the ternary *Goldbach's conjecture* by H. Helfgott will be discussed, including the main ideas and the method behind the proof.

# 1 Introduction

Goldbach's conjecture is an unsolved mathematical problem within number theory that was formulated by the German mathematician Christian Goldbach in letter correspondence with the famous Swiss mathematician Leonhard Euler in the year 1742. The problem sounds fairly simple in its statement but yet no one has achieved a solution for the original problem and it still draws the attention of mathematicians even to this date, more than 250 years after it was proposed. Worth mentioning is that the weak form of the conjecture, the ternary Goldbach's conjecture, was claimed to have been solved in 2014 by the Peruvian mathematician Harald Helfgott.

In the letter where the problem first makes an appearance, C. Goldbach wrote that “*Every integer greater than 2 can be written as the sum of three primes*” and that “*Every even number is the sum of two primes*”. [Vau]

These two simple statements has since aroused mathematicians, and countless hours have been spent in trying to draw up a solution.

## 1.1 Definition of the Conjectures

When the original statements were made, C. Goldbach considered the integer 1 to be a prime number, which calls for the modern expression of the conjecture:

**Definition 1.1.** (*Binary or strong Goldbach's conjecture*) *Every even integer greater than 2 can be written as the sum of two primes.*

**Definition 1.2.** (*Ternary or weak Goldbach's conjecture*) *Every odd integer greater than 5 can be written as the sum of three primes.*

There are generally more than one way to express an integer in sums of two or three prime numbers. For the binary case there is a definition, namely:

**Definition 1.3.** (*Goldbach partition [Sil]*) *The pair of two prime numbers,  $p$  and  $q$ , where  $p + q = n$  and  $n$  being an even integer, is called a Goldbach partition of  $n$ .*

In the table below follow a few examples of partitions of the binary conjecture.

Even integer:	10	22	48	150
Partitions:	3+7 5+5	3+19 5+17 11+11	5+43 7+41 11+37 17+31 19+29	11+139 13+137 19+131 23+127 37+113 41+109 ... 71+79
Number of partitions:	2	3	5	15

There are several different ways mathematicians have tried to solve the conjecture, ranging from statistical and probabilistic approaches to analytic number theory. In the following sections of the thesis, the many different approaches to both the binary and ternary versions of the conjecture will be investigated.

## 2 Prime Numbers and their Distribution

As the *Goldbach's conjecture* lies in the field of number theory and its very core is prime numbers, the distribution of such numbers may be an integral part of any attempted solution to the conjecture. The following section provides a brief overview regarding primes, their infinity, and their distribution.

### 2.1 Early Results

As early as 300 B.C, the Greek mathematician Euclid constructed a proof that there is an infinite number of prime numbers. The following version is a paraphrasing of Euclid original version, with some comments from [Sie] being left out:

**Theorem 2.1.** (*Euclid's theorem, [Sie]*) Given any finite set  $S$  of primes, one considers their product  $P$  and adds the unit 1. If  $P + 1$  is a prime, one has found an additional prime, which means a prime that is not in the original set  $S$ . If  $P + 1$  is not a prime, it is divided by a prime. This latter prime cannot, however, be one of the primes in original finite set either, because in this case it could not divide  $P + 1$ . Therefore we have also in this case found an additional prime that does not lie in the original set  $S$  of prime numbers assumed.

As the infinity of the primes have been known for 2300 years, a function that expresses their distribution in a reasonable fashion was formulated and proved much later. The oldest known method of finding the primes up to a integer  $n$  is the *Sieve of Eratosthenes*, yet again originating from the ancient Greece. There is no strict mathematical definition of the sieve as it is more of a practical, rigorous and, as said in 1772 by [Hor], "*excellent invention*", method, or algorithm.

When using the sieve to find the primes up to an integer  $n$ , all the multiples of every prime less than  $\sqrt{n}$  are removed. Therefore, what we need to know are all the primes less than  $\sqrt{n}$ . The integers that are not sieved in the range between  $\sqrt{n}$  and  $n$  must therefore be prime numbers. The sieve can be used for a, not so perfect, approximation of the primes up to an integer  $n$ . When the multiples of the prime 2 are sieved out, half of the remaining integers can not be prime, and when the multiples of the prime 3 are sieved out, another 1/3 of the remaining integers cannot be prime. After sieving out both 2 and 3, the remaining integers are:

$$\left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{2}\right) n = \frac{1}{3}n. \quad (1)$$

This follows from the computations by Granville [Gra], and leads to the formula to approximate the primes between  $\sqrt{n}$  and  $n$ , where  $p$  is prime, using the *Sieve of Eratosthenes*:

$$\prod_{p \leq \sqrt{n}} \left(1 - \frac{1}{p}\right) n. \quad (2)$$

Although he addresses the issue that the approximation is rather weak, and there are far better and more modern ways of computing the approximation.

## 2.2 Prime Number Theorem

The function counting the number of primes up to an integer  $n$ , denoted  $\pi(n)$ , was first proposed in the very late 18th century and the first proof emerged almost a century later in the year 1896 by the French mathematicians Jacques Hadamard and the Belgian mathematician Charles Jean de la Vallée Poussin, where both of them proved the theorem independently. As their proof involved complex analysis, credit also is due to the Norwegian mathematician Atle Selberg and the Hungarian mathematician Paul Erdős that proposed an elementary proof of the *Prime Number Theorem* in the year 1948, which eventually lead to Selberg receiving the Fields Medal. [Gol]

**Theorem 2.2.** (*Prime Number Theorem, [Gor]*) For a real  $x > 0$ , denote by  $\pi(x)$  the number of primes less than  $x$ . The asymptotic law for the distribution of prime numbers asserts that  $\pi(x) \sim x / \ln x$ .

The notation  $\sim$  is referred to as the *asymptotic notation* and has the meaning that if  $f(x) \sim g(x)$ , then  $f(x)/g(x) \rightarrow 1$  as  $x$  increases to infinity. The theorem will henceforth be referred to as the PNT.

There have been plenty of different proofs for the PNT, and here we have chosen to give a brief review of a short proof formulated by the American mathematician Donald. J. Newman, using a breakdown of the proof provided by [Zag].

D. J. Newman's proof of the PNT focuses on three main functions and their properties, mainly the *Riemann Zeta Function*,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad (3)$$

secondly,

$$\Phi(s) = \sum_p \frac{\ln p}{p^s}, \quad (4)$$



and lastly,

$$\vartheta(x) = \sum_{p \leq x} \ln p, \quad (5)$$

where for all three functions,  $s \in \mathbb{C}$  and  $x \in \mathbb{R}$ .

**Equation (3)** and **equation (4)** are used in order to, in several steps, prove different properties of **equation (5)**, concluding with proving that

$$\vartheta(x) \sim x. \quad (6)$$

We also need the formal definition of  $\pi(x)$ .

**Definition 2.3.** *The number of primes,  $p$ , less than or equal to  $x$ , can be expressed as*

$$\pi(x) = \sum_{p \leq x} 1. \quad (7)$$

**Equation (6)**, together with **definition 2.3**, leads us to

$$\vartheta(x) = \sum_{p \leq x} \ln p \leq \sum_{p \leq x} \ln x = \sum_{p \leq x} 1 \cdot \ln(x) = \pi(x) \cdot \ln(x) \quad (8)$$

where, for  $x \rightarrow \infty$ ,  $\vartheta(x) \sim x$ , which leads to the conclusion that, asymptotically,

$$x \leq \pi(x) \cdot \ln(x) \implies \pi(x) \geq \frac{x}{\ln(x)}. \quad (9)$$

It is also shown in [Zag] that, asymptotically,  $\pi(x) \leq \frac{x}{\ln(x)}$ , and therefore  $\pi(x) \sim \frac{x}{\ln(x)}$ , and the PNT is proven.

For the interested reader, the elementary proof by A. Selberg, [Sel1], for which he received the Field's medal, is recommended for further study.

These theories and ideas regarding prime numbers will play an pivotal role in this thesis' further study of the *Goldbach's Conjecture*.

### 3 Heuristic and Probabilistic Justification

“Every heuristic argument can be said to have some sort of *leap of faith*, with some more sound than others. [...] Such step, usually, is backed by some probabilistic reasoning or density-type argument which leads to an apparently sensible conclusion.” [Taf]

Using probabilistic arguments, heuristic assumptions can be made whether the binary conjecture holds for large integers  $n$ , and how large (or small for that matter) the probability is that it fails.

One key concept to tackle the problem is to investigate how the prime numbers are distributed over remainder classes, or modular arithmetic.

**Definition 3.1.** (*Congruence*) Given two integers  $a$  and  $b$ , we say that  $a$  is congruent to  $b$  modulo  $m$ , denoted by  $a \equiv b \pmod{m}$ , if  $m \mid (a - b)$ . The integer  $m$  is the modulus of the congruence. Moreover, we have that if  $a \equiv b \pmod{m}$ , then  $\gcd(a, m) = \gcd(b, m)$ .

#### 3.1 Method Presented by Gaze & Gaze

Henceforth we account for ideas presented in Gaze & Gaze [Gaz], that use a combination of sieve techniques and the concept of prime numbers being evenly distributed over remainder classes, something that will be addressed later, to propose a heuristic justification of the strong *Goldbach’s conjecture*, fully aware of this not being a valid proof in any way. The fundamental statement of this idea is the following definition.

**Definition 3.2.** Consider an even integer  $n \equiv m \pmod{p}$ , where  $p$  is a prime less than  $n$  and  $m$  being an integer. Then all primes  $q$ , less than  $n$ , that are in the same remainder class  $m$  modulo  $p$  as the even integer  $n$ , will have an integer partner  $r$ ,  $q + r = n$ , where  $r$  is not prime, except for the special case where  $r = p$ .

This holds because if we consider an even integer  $n$ , where  $n \equiv m \pmod{p}$ ,  $m$  being an integer and  $p$  being prime, a prime  $q$ , where  $q \neq p$ ,  $q < n$ , and  $q \equiv m \pmod{p}$  will be one of the primes of the Goldbach partition  $(q, (n-q))$ . But the additive property of congruence classes implies that  $n-q$  is a multiple of  $p$ , and hence not prime, due to  $n - q \equiv m - m \equiv 0 \pmod{p}$ , unless in the special case where  $n - q = p$ .

### 3.1.1 Sieve Method by Gaze & Gaze

The concept with remainder classes and primes propose a method of finding Goldbach partitions of even integers, using a sieve inspired by the *Sieve of Eratosthenes*. Instead of sieving out integers that are not prime, the method is sieving out primes that are unable to be part of a Goldbach partition of an even integer  $n$ . By formalizing this method and partnering it with the PNT, and the *PNT for Arithmetic Progressions*, stated below, a heuristic justification that the strong Goldbach Conjecture holds for large even integers  $n$  can be proposed.

There are now some concepts that need to be explained more thoroughly. First off, an example of the sieve technique used to remove primes unfit for Goldbach partitions is needed.

This technique functions in such a way that when searching for all the Goldbach partitions of an even integer  $n$ , one needs to sieve out the primes less than  $n$  that are in the same residue class as any of the primes,  $p < \sqrt{n}$ . This follows from **definition 3.2** which states that these primes can not be part of a Goldbach partition of  $n$ . Notice that the prime 2 is being left out here because the only Goldbach partition that 2 can be part of is  $2 + 2 = 4$  due to for any even integer  $n$ , except  $n = 4$ ,  $n - 2$  must be another even integer which can not be prime.

One might ask why there is a need only to sieve out residue classes of primes less than  $\sqrt{n}$ . The reason for this was provided by the supervisor of this thesis, [Cri].

**Lemma 3.3.** *When applying the sieve method proposed by Gaze & Gaze, it is sufficient to sieve out primes less than  $n$  with the same residue class as any of the primes  $p$ , for which it holds that  $p < \sqrt{n}$ .*

*Proof.* Let us say that  $a$  is an even integer,  $p$  and  $q$  are primes, and that  $q < p$ . Let us also assume that  $p > \sqrt{a}$ . The statement that

$$a \equiv q \pmod{p} \quad (10)$$

is equivalent of saying that

$$a - q = k \cdot p \quad (11)$$

for some integer  $k$ .

As we know that  $p > \sqrt{a}$  and that  $a - q < a$ , it must be true that  $k < \sqrt{a}$ , by **equation 11**. Now we have  $k < \sqrt{a}$ . Combining **equation 10** and **equation 11** provides us with the realization that the congruence can be instead expressed as

$$a \equiv q \pmod{k}. \quad (12)$$

We know that  $k < p$  due to  $p > \sqrt{a} > k$ . If  $k$  is prime, the prime  $q$  would already have been sieved when we used the method modulo  $k$ , and our calculations with modulo  $p$  would have been unnecessary.

If  $k$  is not prime, it will have a prime factorization of  $k = p_1 \cdot p_2 \cdot p_3 \cdots p_n$ , which gives us that  $a - q = (p_1 \cdot p_2 \cdot p_3 \cdots p_n) \cdot p$ , which let us make the statement that

$$a \equiv q \pmod{p_1} \quad (13)$$

or for an other  $p$  of  $k$ 's prime factorization, and therefore  $q$  would already have been sieved without the need of sieving with modulo  $p$ .

Therefore it is enough to sieve all primes with the same residue class as another prime,  $p$ , for  $p < \sqrt{n}$ . [Cri]  $\square$

### 3.1.2 Example

Here we will provide an easy to follow example in finding the Goldbach partitions of the even integer 26, formulated by the author. As  $26 \neq 4$  the prime 2 is being left out. Therefore the primes leading up to 26 are the following:

$$\begin{array}{cccccccc}
3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 \\
5 & 7 & 11 & 13 & 17 & 19 & 23 & \\
2 & 1 & 2 & 1 & 2 & 1 & 2 & \pmod{3}
\end{array}$$

The only primes that are less than  $\sqrt{26}$  are 3 and 5.  $26 \equiv 2 \pmod{3}$  and for the primes above:

Notice that 3 is not being included when the sieve is using modulo 3 (this is not unique for the integer 3, but for all primes,  $p$ , used in the sieve).

As 5, 11, 17, and 23 all are congruent 2 modulo 3, these primes are being sieved out. The primes left are:

$$3 \quad 7 \quad 13 \quad 19$$

$26 \equiv 1 \pmod{5}$  and the remaining primes modulo 5 are the following:

$$\begin{array}{cccc}
3 & 7 & 13 & 19 \\
3 & 2 & 3 & 4 \pmod{5}
\end{array}$$

As none of the primes left are in the same congruence class as 26 modulo 5 all of them are part of a Goldbach partition of 26. Clearly,  $(13 + 13) = 26$  and  $(7 + 19) = 26$ , but what happened to 3 that has not been sieved out? This is a consequence of the special case mentioned in **definition 3.2** and its explanation, with  $n = 26$ ,  $q = 23$  and  $p = 3$ . The fact that  $n - q = p$  implies that this is indeed the special case. Therefore the prime 23 is reintroduced and the Goldbach partitions of the even integer 26 are the following pairs:

$$(7+19) \quad (13+13) \quad (3+23)$$

### 3.2 Prime Number Theorem for Arithmetic Progressions

The next part of explaining the idea in [Gaz] is the concept of primes being distributed evenly across modulo  $p$ ,  $p$  being prime, and therefore the PNT for *Arithmetic Progressions*.

First we need to describe the Euler phi-function ( $\phi(n)$ ) and its multiplicative property.

**Definition 3.4.** (*Euler phi-function  $\phi(n)$* ) Let  $n$  be a positive integer. The Euler phi-function  $\phi(n)$  is defined to be the number of positive integers not exceeding  $n$  that are relatively prime to  $n$ , or the number of integers  $x \leq n$  such that  $\gcd(x, n) = 1$ .

In order to prove the proposition regarding the multiplicativity of  $\phi(n)$ , we also need the following definitions.

**Definition 3.5.** (*Complete system of residues modulo  $m$ , [Ros]*) A complete system of residues modulo  $m$  is a set of integers such that every integer is congruent modulo  $m$  to exactly one integer of the set.

**Proposition 3.1.** If  $r_1, r_2, \dots, r_m$  is a complete system of residues modulo  $m$ , and if  $a$  is a positive integer with  $\gcd(a, m) = 1$ , then

$$ar_1 + b, ar_2 + b, \dots, ar_m + b \quad (14)$$

is a complete system of residues modulo  $m$ . [Ros]

We state this definition without a proof, and refer the reader to the proof in [Ros].

The implications of a *complete system of residues modulo  $m$* , is that the number of integers in the set that are relatively prime to  $m$  is equal to  $\phi(m)$ . Say that we have  $m = 8$ . Then a *complete system of residues modulo  $m$*  will contain, for example, the integers 0, 1, 2, 3, 4, 5, 6, 7 (as long as the integers in the set are congruent to the latter, modulo  $m$ .) Clearly the integers that are relatively prime to 8 are 1, 3, 5, 7, and  $\phi(8) = 4$ . This definition is crucial in the proof of the following proposition.

**Proposition 3.2.** (*Multiplicativity of the Euler phi-function  $\phi(n)$* ) For relatively prime positive integers  $m$  and  $n$ , where  $\gcd(m, n) = 1$ , the Euler phi-function  $\phi(n)$  is multiplicative, meaning that  $\phi(m) \cdot \phi(n) = \phi(mn)$ .

*Proof.* We start by listing all positive integers not exceeding  $mn$  in the following way.

$$\begin{array}{ccccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\cdot & \cdot & \cdot & & \cdot \\
\cdot & \cdot & \cdot & & \cdot \\
\cdot & \cdot & \cdot & & \cdot \\
m & 2m & 3m & & mn
\end{array}$$

The integers are listed in columns with length  $m$ , and in  $n$  number of rows, starting with 1 in the top-right corner and ending with  $mn$  in the bottom-left corner.

Now say that we have a positive integer  $r$ , with  $r \leq m$ , meaning that we will find  $r$  in the first column. For now it holds for  $r$  that  $\gcd(m, r) = d > 1$ . This implies that no integer in the  $r$ th row will be relatively prime to  $mn$ , because every integer on the  $r$ th row can be written as  $km + r$ , for which  $k$  is an integer with  $1 \leq k \leq n-1$ , and  $d$  must be divisor of  $km + r$  because  $d$  divides both  $r$  and  $m$ . We have therefore shown that for every integer in the first column that is a divisor of  $m$ , there can be no integers in the divisor's row that are relatively prime to  $mn$ .

This implies that in order to find integers in the list that *are* relatively prime to  $mn$ , we must seek in the rows of integers of the first column where it holds that  $\gcd(m, r) = 1$ . So if we find an integer  $r$  in the first column, with  $1 \leq r \leq m$ , all elements in that row must be relatively prime to  $mn$  due to all of them being of the form  $km + r$  with  $1 \leq k \leq n-1$  and  $\gcd(m, r) = 1$ .

By using **proposition 3.1**, we know that if  $\gcd(m, r) = 1$ , the integers in the  $r$ th row must form a *complete system of residues modulo  $n$* , which lead us to the realization that  $\phi(n)$  of these integers are relatively prime to  $n$ , as well as they are, from  $\gcd(m, r) = 1$ , also relatively prime to  $m$ .

This lead us to the conclusion, that since we have  $\phi(m)$  rows, where each of them contain  $\phi(n)$  integers that are relatively prime to  $mn$ , it must hold that  $\phi(m) \cdot \phi(n) = \phi(mn)$ . [Ros]

□

We are now ready to introduce the *PNT for Arithmetic Progressions*.

**Theorem 3.6.** (*Prime Number Theorem for Arithmetic Progressions, [Sop]*)  
 Let  $\pi(x, q)$  denote the number of all primes  $p$  no greater than  $x$ , congruent to  $a$  modulo  $q$ , for  $a, q \in \mathbb{N}$  such that  $\gcd(a, q) = 1$ . Then,

$$\pi(x, q) \sim \frac{1}{\phi(q)} \frac{x}{\ln x},$$

where  $\phi(q)$  is the Euler phi-function.

Henceforth this will be referred to as the PNTAP.

As it lies beyond the scope of this thesis to prove the PNTAP, we refer the reader to the elementary proof of [Sel2].

It is important to be aware of that both the PNT and the PNTAP yield asymptotic results, and therefore are not perfect nor accurate with low valued integers, instead they become more accurate as  $x, q \rightarrow \infty$ . There is also a somewhat large error term associated with **theorem 2.2** and **theorem 3.6**, that will be discussed later.

### 3.3 Distribution of Primes Across Prime Residue Classes

The idea from [Gaz], that the primes are distributed evenly across residue classes of primes, is a consequence of the PNTAP. The integer  $q$  will be chosen to be prime, and the integer  $a$  will be less than  $q$ . The theorem states that  $\gcd(a, q) = 1$ , and as  $q$  is being prime,  $\gcd(a, q) = 1$  must hold for all  $a$ . This implies that for a given prime  $q$ , any  $a$  chosen, due to the right-hand side of the PNTAP not containing the variable  $a$ , asymptotically  $\pi(x, q)$  will yield the same result for all  $a$ , resulting in an even distribution of the primes across a prime residue class.

This is also expressed in more accuracy in [Gaz], with the following reasoning: It follows from **definition 3.4** that  $\phi(p) = p - 1$  where  $p$  is prime, and therefore each of the remainder classes of a prime  $p$ , as  $x \rightarrow \infty$ , will contain  $1/(p - 1)$  of the primes up to  $x$ . Since the Euler phi-function is multiplicative, so if we are applying the PNTAP over a sequence of prime numbers it will yield the function

$$\pi(x, p_1 \cdot p_2 \cdots p_j) \sim \frac{1}{\prod_{p \leq p_j} (p - 1)} \frac{x}{\ln x}, \quad (15)$$



which implies that the primes are evenly distributed across remainder classes.

### 3.4 Heuristic Justification by Gaze & Gaze

All of this eventually lead to the conclusion, using the proposed sieve, that for each prime  $p$  used as modulus in the sieve,  $1/\phi(p)$  or  $1/(p-1)$  of the remaining primes will be unable to be part of a *Goldbach partition*.

The following section is [Gaz] summarized by our own words.

Using the sieve, the remaining primes fit for *Goldbach partitions* can be expressed as:

$$\pi_{gold}(x) \approx \prod_{3 \leq p \leq \sqrt{x}} (1 - 1/(p-1)) \cdot \pi(x), \quad (16)$$

because one remainder class of each prime, less than or equal to  $\sqrt{x}$ , is being sieved out, resulting in  $1/(p-1)$  per prime, and then multiplied with  $\pi(x)$ .

Now we want to express  $\pi_{gold}(x)$  in a way so that we can find a limit as  $x \rightarrow \infty$ , and this can be done using some clever algebra. The Polish mathematician Franz Mertens showed the following asymptotic equality in his efforts to find  $\pi(x)$  (which eventually was dismissed as a good approximation of  $\pi(x)$ ):

$$\prod_{p \leq \sqrt{x}} (1 - 1/p) \cdot x \sim \frac{2e^{-\gamma}}{\ln x} \cdot x, \quad (17)$$

where  $\gamma$  is the Euler-Mascheroni constant and  $2e^{-\gamma} \approx 1.12292...$

**Definition 3.7.** (*Euler-Mascheroni constant, [Top]*) The Euler-Mascheroni constant  $\gamma$  is defined by

$$\gamma = \left[ \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{k} - \ln n \right] = 0.57721566....$$

Multiplying both sides of **equation 17** with  $1/\ln x$  yields

$$\prod_{p \leq \sqrt{x}} (1 - 1/p) \cdot \pi(x) \sim \frac{2e^{-\gamma}}{\ln^2 x} \cdot x, \quad (18)$$

by PNT. We can then use the property that

$$\prod_{p \leq \sqrt{x}} (1 - 1/p) < \prod_{3 \leq p \leq \sqrt{x}} (1 - 1/(p-1)) \quad (19)$$

in order to interchange the right-hand side of the  $\pi_{gold}(x)$ -function. Because the new expression is smaller than the old, and we are striving for large values on the right-hand side, it will not change the value in a biased way. The new function can then be expressed as

$$\pi_{gold}(x) \approx \prod_{p \leq \sqrt{x}} (1 - 1/p) \cdot \pi(x), \quad (20)$$

and therefore

$$\pi_{gold}(x) \approx \frac{2e^{-\gamma} \cdot x}{\ln^2 x} \approx \frac{1.12292 \cdot x}{\ln^2 x}. \quad (21)$$

### 3.4.1 Conclusion

For large integers  $x$  we have,  $x > \ln^2 x$ , and  $\pi_{gold}(x)$  tends to infinity as  $x$  become larger and larger, implying that for large  $x$  there are plenty of primes suitable for *Goldbach partitions*. But we must take the aforementioned error terms into consideration. The PNT and **equation (17)** are involved in the making of the expression, and they come with large error terms. Just by looking at the over-counts of the expressions for  $x = 1.00 \cdot 10^{11}$ , the actual result is  $\pi(x) \approx 4.1 \cdot 10^9$ , but  $x/\ln x$  over-counts by 170 million primes and the equation by F. Mertens, **equation 17**, by 315 million primes.

These error terms associated with the expressions were not taken into account in [Gaz], and it is beyond the scope of this thesis to do so. It clearly shows what problems we can run into when dealing with asymptotic results and the difference between such results and, for example, results from

direct proofs. The method presented although presents a good example of a heuristic justification of the *Goldbach's conjecture*.

### 3.5 Goldbach's Comet

One interesting phenomenon generated by the conjecture is the so called *Goldbach's comet* which is a visual representation of the number of possible *Goldbach partitions* of an even integer  $n$ . The comet-like structure can probably be explained as a consequence of how the number of partitions varies between different congruence classes. Now this figure just expresses the number of partitions up to  $n = 5 \cdot 10^4$ , but we can clearly see that the number is steadily increasing. This would make us assume that the conjecture holds, but this has nothing to do with a proof as we can not know that there is no exception for a large  $n$  where the number of partitions will be zero.

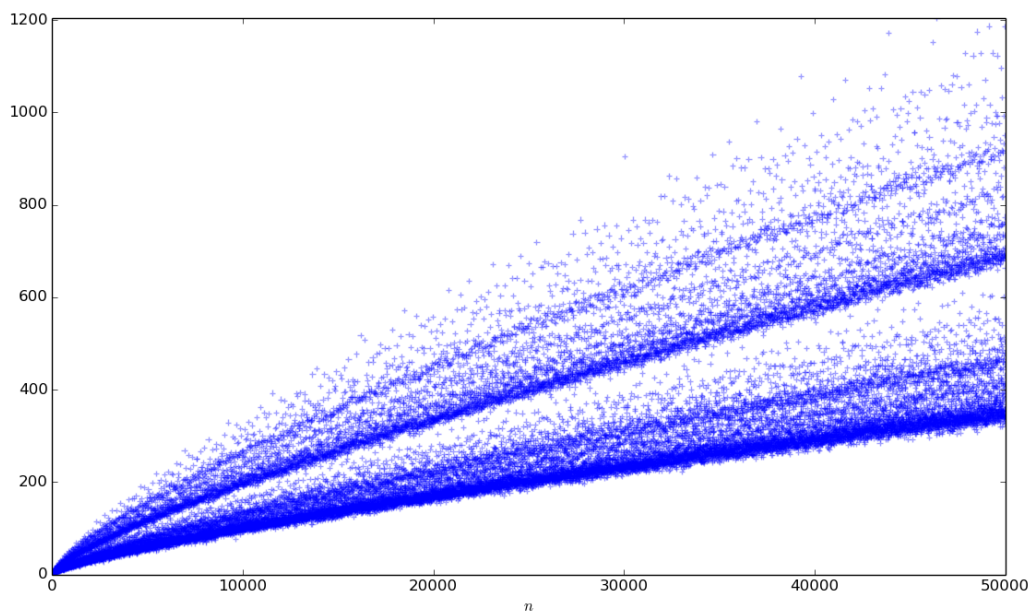


Figure 1: *Goldbach's Comet*, Goldbach partitions up to the integer  $n = 50000$  on the  $x$ -axis, and number of partitions on the  $y$ -axis. Generated by a Python script using a modified version of the code from [Sci].

## 4 The Ternary Goldbach's Conjecture

This thesis will now focus its attention to the ternary, or weak *Goldbach's conjecture*, and its proposed solution by H. Helfgott in 2014, where from we will introduce and explain some of the main concept and ideas. An important note to make is that the proof has yet to be published in a peer-reviewed publication but H. Helfgott has since then been awarded an *Alexander von Humboldt Professorship* at the University of Göttingen and no one seem to have been able to confute his proof yet.

### 4.1 Historical Overview

The ternary *Goldbach's conjecture* have been the interest of many mathematicians, and especially for those in the field of number theory. The German mathematician Edmund Landau thought that the problem was *unangreifbar* but was later proven wrong when the British mathematicians Godfrey Harold Hardy and John Edensor Littlewood, assuming the *generalized Riemann hypothesis* to hold, were able to show that the ternary conjecture was true for every odd integer larger than a unspecified constant  $C$ . The Soviet mathematician, Ivan Vinogradov, was able to remove the condition that the *generalized Riemann hypothesis* must hold in the year of 1937, and the first value of the constant  $C$  was calculated to  $C = 3^{3^{15}}$  by K. G. Borodzkin, another Soviet mathematician. The best result for  $C$  that was proven before H. Helfgott announced his proof was  $C = 2 \cdot 10^{1346}$  by Liu and Wang. [Hel2]

Other approaches have been tried as well, and another Soviet mathematician, Lev Schnirelmann, was able to prove that every integer larger than one, "can be written as the sum of at most  $K$  primes for some unspecified constant  $K$ ", and the most recent progression on this approach is to specify the constant  $K$  to  $K = 5$ , which was done by the Australian-American mathematician Terence Tao, who is a recipient of the Fields medal in 2006.

Another interesting approach, this time regarding a variant of the *Goldbach's conjecture*, is that of the Chinese mathematician Jing-Run Chen that proved that every even integer larger than an unknown constant is the sum of a prime and the product of at most two primes, which can be expressed as  $n = p_1 + p_2 p_3$  with  $p_3$  being the integer 1 or a prime. [Hel2]

Assuming the *generalized Riemann hypothesis*, Dmitrii Zinoviev was able to improve on the work of G. H. Hardy and J. E. Littlewood and specified their constant to  $C = 10^{20}$ , which, after a check was done for all the integers less than  $10^{20}$ , gives a proof of the ternary *Goldbach's conjecture*, although conditional of the *generalized Riemann hypothesis*. As the hypothesis has yet to be proven, the proof of D. Zinoviev is not complete. [Hel2]

The approach that H. Helfgott follows in his proof of the ternary *Goldbach's conjecture* is the progression of bringing down the constant  $C$  from Vinogradov's Theorem, and therefore unconditional of the *generalized Riemann hypothesis*, such that all odd integers below  $C$  can be assessed by computational power. [Hel1]

## 4.2 Approach

The main idea behind an analytic proof of this kind is to find a function, referred to as the *main term*, in how many ways the conjecture, in our case the ternary *Goldbach's conjecture* and the *Goldbach partitions*, can be expressed for an integer  $n$ . Such a function will though have another associated function that can be seen as the error in the first functions result. This is referred to as the *error term*.

When combining these functions, the maximum number of partitions will therefore be

$$\text{main term} + \text{error term} \tag{22}$$

and the minimum number of partitions will be

$$\text{main term} - \text{error term}. \tag{23}$$

As long as the *main term* is larger than the *error term*, the number of partitions is larger than zero, and the conjecture holds.

Therefore the approach consists of finding functions for the *main term* and the *error term* so that **equation (23)** holds for such small integer  $n$  that it can be shown by computational methods that the conjecture holds for all integers less than  $n$ . [Hel2]

In finding the *main term* and the *error term*, the so called Hardy-Littlewood circle method, described below, will be used. The *main term* will be found in the *major arcs*, the part of the circle in the method mentioned, that have the largest contribution to the integral, and the *error term* will be found in the *minor arcs*, which are the parts of the circle with a much smaller contribution than the *major arcs*. [Hel2]

In defining the *major arcs* and thereby the large-scale distribution of the primes, a concept known as *L-functions* will play a pivotal role. The main idea behind the *minor arcs* seem to be more scattered, but one of the crucial components is the *Large Sieve* which will, alongside the *L-functions*, be concisely discussed in the next section. [Hel2]

### 4.3 Theorems and Methods in the Proof

As the proof of the ternary *Goldbach's conjecture* is incredible immense, we will only discuss some of the important method and theorems that are used as the main ideas behind the proof.

#### 4.3.1 Hardy-Littlewood Circle Method

The Circle Method was developed by G. H. Hardy and J. E. Littlewood, with input from the Indian prodigy S. A. Ramanujan, in the beginning of the 1920's in order to solve additive problems in number theory.

First off, a clarification of the meaning of an additive problem must be stated. We are given two or more subsets of the natural numbers,  $\mathbb{N}$ , which we can call  $A_1, \dots, A_s$ . We are seeking the potential number of solutions for

$$n = a_1 + a_2 + \dots + a_s \quad (24)$$

for some given  $n \in \mathbb{N}$ , with the restriction that  $a_j \in A_j$  for  $j = 1, \dots, s$ . [Zac]

In our specific case with the ternary *Goldbach's conjecture* there would be three subsets, with  $A_1 = A_2 = A_3 = A$ , where  $A$  is the set of prime numbers, and  $n$  being all odd integers greater than 5.

The ternary *Goldbach's conjecture* is then determined by

$$O = \{p_1 + p_2 + p_3 \mid p_1, p_2, p_3 \in \mathbb{P}\} \cap \mathbb{N}, \quad (25)$$

where  $\mathbb{P}$  is the set of prime numbers and  $O$  is the set of integers for which it holds for. [Ras]

Henceforth, we will follow an overview of the circle method provided by [Ras]. The problem that we are trying to address is: *"In other words, determine which natural numbers can be represented as the sum of  $k$  elements of the set  $S$  and in how many ways."* [Ras].

This can be expressed with the notation  $R(n, k, S)$ , which, in [Ras]'s words is *"[...] equal to the number of ways that  $n$  can be represented as the sum of  $k$  elements of the set  $S$ ."*

In our case with the ternary *Goldbach's conjecture*,  $k = 3$ , and  $S$  is the set of all prime numbers,  $\mathbb{P}$ . So for example,  $R(9, 3, \mathbb{P}) = 2$ , as the odd integer 9 can be expressed as a sum of three primes by  $3 + 3 + 3$  and  $5 + 2 + 2$ . We now need to define *Cauchy's Integral Formula*.

**Theorem 4.1.** (*Cauchy's Integral Formula, [Saf]*) *Let  $\Gamma$  be a simple closed positively oriented contour. If  $f$  is analytic in some simply connected domain  $D$  containing  $\Gamma$  and  $z_0$  is any point inside  $\Gamma$ , then*

$$f(z_0) = \frac{1}{2\pi i} \int_{\Gamma} \frac{f(z)}{z - z_0} dz. \quad (26)$$

As we state this theorem without a proof, the reader is referred to the proof provided in [Saf].

Using complex analysis and Cauchy's formula, the number of ways that the natural numbers we seek can be represented, is expressed as **equation 27**,

$$R(n, k, S) = \int_0^1 f_S(x)^k e^{-2\pi i n x} dx, \quad (27)$$

where

$$f_S(x)^k = \sum_{n=1}^{+\infty} R(n, k, S) x^n. \quad (28)$$

For a detailed account for the complex analysis, that is involved here, we refer the reader to *chapter 4* in [Saf], and for the circle method more specific, we refer the reader to [Ras].

The main idea hereafter is that, for most problems, the integral can not be evaluated in an easy way. Therefore the integral is split into two different parts, dependent on their contribution to the integral as a whole. These are then referred to as the *major arcs*, as they have the most contribution to the integral, and the *minor arcs*, as they have the least contribution.

This can be expressed as

$$R(n, k, S) = \int_{\mathfrak{M}} f_s(x)^k e^{-2\pi i n x} dx + \int_{\mathfrak{m}} f_s(x)^k e^{-2\pi i n x} dx, \quad (29)$$

where  $\mathfrak{M}$  are the *major arcs* and  $\mathfrak{m}$  are the *minor arcs*.

When evaluating the integral, the idea is to evaluate the *major arcs*,  $\mathfrak{M}$ , asymptotically and that the *minor arcs*,  $\mathfrak{m}$ , will turn out to be of lower order than  $\mathfrak{M}$ . If that is the case,  $\mathfrak{M}$  will have a much larger contribution than  $\mathfrak{m}$ , and as it will yield an asymptotic result, the contribution from  $\mathfrak{m}$  can be disregarded. It is referred to as the circle method as we are evaluating a circle, and therefore it is split into different arcs.

H. Helfgott makes an interesting statement regarding the circle method and the binary *Goldbach's conjecture*. As it becomes clear that the *major arcs* in the ternary *Goldbach's conjecture* contributes more than the *minor arcs*, the same can not be said for the binary *Goldbach's conjecture*. This is, as we interpret it, a consequence of the fact that in the ternary problem, the *major arcs* are cubed due to the three primes used, and thus much more enhanced in their contribution, in contrast to the binary problem when the *major arcs* are only squared. This impedes the use of the Hardy-Littlewood circle method on the binary *Goldbach's conjecture*.

### 4.3.2 Vinogradov's Theorem

I. Vinogradov's proof, unconditional of the *generalized Riemann hypothesis*, of that there exists a constant  $C$  for which above the ternary *Goldbach's conjecture* holds, is a vital stepping stone for the proof proposed by H. Helfgott.



**Theorem 4.2.** (*Vinogradov's Theorem, [Ras]*) *There exists a natural number  $N$ , such that every odd positive integer  $n$ , with  $n \geq N$ , can be represented as the sum of three prime numbers.*

There are several different proofs to *Vinogradov's Theorem*, and here a brief overview of Bob Vaughan's proof will be provided, although taken from [Ras]. The proof actually use the Hardy-Littlewood circle method that we have just described.

First off, the sum of the integers that can be expressed as a sum of three primes is,

$$R(n, 3, \mathbb{P}) = \sum_{n=p_1+p_2+p_3} 1. \quad (30)$$

with  $R(n, 3, \mathbb{P})$  being the same notation as used in the previous section regarding the Hardy-Littlewood circle method. As this sum is rather bland and hard to further expand on, we will use the following inequality,

$$\sum_{n=p_1+p_2+p_3} 1 > \sum_{n=p_1+p_2+p_3} \frac{\ln p_1 \cdot \ln p_2 \cdot \ln p_3}{\ln^3(p_1 + p_2 + p_3)} = \sum_{n=p_1+p_2+p_3} \frac{\ln p_1 \cdot \ln p_2 \cdot \ln p_3}{\ln^3 n}, \quad (31)$$

which therefore states that

$$R(n, 3, \mathbb{P}) > \frac{1}{\ln^3 n} \sum_{n=p_1+p_2+p_3} \ln p_1 \cdot \ln p_2 \cdot \ln p_3. \quad (32)$$

This allows us to use the sum  $\sum_{n=p_1+p_2+p_3} \ln p_1 \cdot \ln p_2 \cdot \ln p_3$  instead of  $\sum_{n=p_1+p_2+p_3} 1$  in the method.

B. Vaughan then continues the proof by determining the *major arcs* and the *minor arcs*, and for the interested reader, we strongly recommend the detailed step-by-step walk through of the proof, provided in [Ras].

What was eventually proven by A. Vinogradov is that

$$\sum_{n=p_1+p_2+p_3} \ln p_1 \cdot \ln p_2 \cdot \ln p_3 \gg n^2 \quad (33)$$

where the meaning of  $\gg$  is "*much greater*" [Car].

Combining **equation (32)** and **equation (33)** leads to the realization that

$$R(n, 3, \mathbb{P}) \gg \frac{n^2}{\ln^3 n}, \quad (34)$$

which amounts to, that for some unspecified integer  $n$ , all integers above can be written as the sum of three primes, thus proving *Vinogradov's Theorem*. [Ras]

### 4.3.3 The Large Sieve

*"[...], one of the main general lessons of the proof is that there is a very close relationship between the circle method and the large sieve, we will use the large sieve not just as a tool - which we shall, incidentally, sharpen in certain contexts - but as a source for ideas on how to apply the circle method more effectively."* [Hel2]

The large sieve is not the name of a single method, but rather a family of different methods with the same basic concept. The main idea, in its simplest form, is to have a certain interval of integers and then remove different residue classes of modulo  $p$ , where  $p$  is prime [Gal]. The sieve was first proposed by the Soviet mathematician Yuri Linnik, and since then it has been developed over the decades.

A large sieve for primes is, for example, used in the proof by H. Helfgott in order to deal with functions,  $f(x)$ , that have prime support, meaning that they follow the rule that,

$$f(x) \neq 0, \quad \text{if and only if } x \in \mathbb{P}. \quad (35)$$

The large sieve is also used as a tool when evaluating the integral given by the circle method, where the large sieve can provide information of the regularities, or perhaps irregularities, in the distribution of prime numbers.

### 4.3.4 $L$ -functions

*"On some of the crucial questions on  $L$ -functions, the limits of our knowledge have barely budged in the last century. There is something relatively new now, namely, rigorous numerical data of non-negligible scope; still, such data is, by definition, finite, and, as a consequence, its range of applicability is very*

*narrow. Thus, the real question in the major-arc regime is how to use well the limited information we do have on the large-scale distribution of the primes.*" [Hel2]

$L$ -series and  $L$ -functions were first introduced by the German mathematician Peter Dirichlet in the beginning of the 19th century in his effort to prove a theorem regarding the existence of infinite number of primes in certain arithmetic progressions. [Bom]

**Definition 4.3.** (Dirichlet  $L$ -series, [Bom]) Let  $q$  be a positive integer, a Dirichlet  $L$ -series is given by

$$L(s, \mathcal{X}) := \sum_{n=1}^{\infty} \frac{\mathcal{X}(n)}{n^s} \quad (36)$$

where  $\mathcal{X}$  is a Dirichlet character (mod  $q$ ) with the following properties:

- $\mathcal{X}(1) = 1$  and  $\mathcal{X}(n) = 0$  if  $n, q$  have a common factor.
- Multiplicativity:  $\mathcal{X}(mn) = \mathcal{X}(m)\mathcal{X}(n)$ .
- Periodicity:  $\mathcal{X}(n + q) = \mathcal{X}(n)$ .

For a fixed Dirichlet character  $\mathcal{X}$ , the series  $L(s, \mathcal{X})$  gives a complex function in the variable  $s$  defined for all  $s$  with  $\Re(s) > 1$ . By analytic continuation it can be extended to a meromorphic function on the entire complex plane.

The *generalized Riemann hypothesis* is the famous, or infamous, conjecture, that for every  $\mathcal{X}$ , the complex numbers  $s$  such that  $L(s, \mathcal{X}) = 0$  are either real negative numbers, or satisfy  $\Re(s) = 1/2$ . As this has vast significance for the distribution of primes, it is a very useful concept in proving the ternary *Goldbach's conjecture*. [Hel2]

Although, problems arise as the *generalized Riemann hypothesis* is yet to be proven, and to then propose an unconditional proof of the ternary conjecture, a method that by-passes this complication is needed.

As mentioned in the quotation at the beginning of this section, H. Helfgott make use of computations to remove the need of a proven *generalized Riemann hypothesis*. Some very finite intervals of the line  $\Re(s) = 1/2$  can

then be verified to contain no zeroes of  $L$  that would contradict the *generalized Riemann hypothesis*, and then the results concerning the distribution of the primes in connection to the verified parts can be used. For the finite verification of intervals of the *generalized Riemann hypothesis*, H. Helfgott uses the work from [Pla].

### 4.3.5 Computational Methods

As stated before, the best  $C$  for Vinogradov's Theorem found before H. Helfgott's proof, was  $C = 2 \cdot 10^{1346}$ . H. Helfgott acknowledges in [Hel2] that it would be practically impossible to ever validate the ternary *Goldbach's conjecture* for all integers less than the given  $C$ . As it would take at least  $\sqrt{C}$  calculations, and that there are approximately, by today's knowledge,  $10^{80}$  protons in the observable universe, the task would take an practically impossible amount of time to complete, even if the whole universe was in some way turned into a computer trying to verify the conjecture. In order to prove the ternary *Goldbach's conjecture*, there was consequently a need to improve the mathematics regarding the problem, and therefore reducing the constant  $C$ , not improving the computational methods. [Hel2]

As H. Helfgott was eventually able to bring down the constant  $C$  in Vinogradov's Theorem to a more tangible number, a verification for all integers  $n \leq C$  is still necessary. H. Helfgott recounts several different methods of validating the ternary *Goldbach's conjecture* up to, and above, the proven  $C$ , one method relying on checking the intervals between primes, mainly by numerical verification of the *Riemann hypothesis*, and the other method using more direct computations. Here we will use [Hel3], that uses the more direct method to verify the conjecture up to  $8.875 \cdot 10^{30}$ .

First of all, the binary *Goldbach's conjecture* implies the ternary *Goldbach's conjecture* because, say we know that the binary conjecture is true for all even integers  $n$ , then it must also be true for the odd integer  $n - 1$ , because,  $n - 1 = (n - 4) + 3$ , where  $n - 4$  is another even integer and 3 is prime. Thus, the ternary *Goldbach's conjecture* is true because  $n - 4$  is the sum of two primes and  $(n - 4) + 3$  is the sum of three primes. As there is an earlier work from [Sil] that verifies the binary *Goldbach's conjecture* up to  $4 \cdot 10^{18}$ , the process of verifying the ternary *Goldbach's conjecture* could begin with a head start.

In computer science, the amount of computational power required to calculate something is referred to as *time complexity*. In order to verify if a given large odd integer is prime or not, an algorithm associated with a large *time complexity* is needed. As we are to check all odd integers up to, and above,  $10^{30}$ , there is a need to minimize the time complexity in order for the computation to be easily achieved. [Hel3] uses a concept with integers known as *Proth numbers* or, as in our case, *Proth primes*.

Before we can give the definition of *Proth numbers* and *Proth primes*, there is a need to state the so called *Pocklington's criterion*, which is a corollary of the *Pocklington's Theorem*, which we state without a proof, but refer the reader to [Fin].

**Definition 4.4.** (Pocklington's criterion, [Fin]) Suppose  $N - 1 = FR$  with  $\gcd(F, R) = 1$  and suppose that a complete factorization of  $F$  is known. Suppose that there exists an  $a$  such that

$$a^{N-1} \equiv 1 \pmod{N} \quad \text{and} \quad (a^{\frac{N-1}{q}}, N) = 1 \quad (37)$$

for every prime factor  $q$  of  $F$ . Then if  $F \geq \sqrt{N}$ , it follows that  $N$  is prime.

With these definitions stated, we are now ready to prove *Proth's Theorem*.

**Theorem 4.5.** (*Proth's Theorem*, [Rie]) A *Proth number* is an integer of the form  $N = k \cdot 2^n + 1$ , where  $k$  and  $n$  are positive integers, with  $k < 2^n$  and odd. Then the *Proth number*  $N$  is prime, referred to as a *Proth prime*, if there exists an integer  $a$  with

$$a^{\frac{N-1}{2}} \equiv -1 \pmod{N}. \quad (38)$$

*Proof.* Set  $F = 2^n$  and  $R = k$ , then we have

$$N = RF + 1 \implies N - 1 = RF \quad (39)$$

and therefore  $\gcd(F, R) = 1$  because  $F$  is even and  $R$  is odd, also, a complete factorization of  $F$  is known. That is the first criteria of Pocklington.

We are given  $a^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ , and by squaring both sides we get  $a^{n-1} \equiv 1 \pmod{N}$ , which is the second criteria of Pocklington.

As the prime factorization of  $F$  contains only the prime 2, we can write

$$a^{\frac{N-1}{q}} = a^{\frac{N-1}{2}}, \quad (40)$$

and for  $a^{\frac{N-1}{2}}$  we have

$$a^{\frac{N-1}{2}} \equiv -1 \pmod{N}, \quad (41)$$

and by using **definition 3.1**,

$$(a^{\frac{N-1}{2}}, N) = (-1, N) = -1 \implies (a^{\frac{N-1}{2}}, N) = 1, \quad (42)$$

which is the third criteria of Pocklington.

We have  $k < 2^n$  and therefore,  $R < F$ . We have  $N = FR + 1$ , which leads us to

$$N = \sqrt{N} \cdot \sqrt{N} = FR + 1 \quad (43)$$

and because of  $R < F$  we reach  $F \geq \sqrt{N}$ , with  $\geq$  and not  $>$  due to  $+1$  on the right-hand side of **equation (43)**. This was the last criteria of Pocklington and therefore it is proven that  $N$  is prime.

This proof was constructed with inspiration from [Lan]. □

The main reason for using these *Proth numbers* is that the *time complexity* of the algorithm used for verifying them as prime numbers is much smaller than that for a random integer. For those integers that could not be verified with a *Proth prime*, an existing function known as *Pari's precprime* was used to give probable primes, and then these were verified using another function known as *Pari's isprime*. [Hel3]

Using this method, H. Helfgott and David Platt were able to verify the ternary *Goldbach's conjecture* up to

$$T = 8,875,694,145,621,773,516,800,000,000,000 \quad (44)$$

or  $T > 8.875 \cdot 10^{30}$ . No further verification is needed as H. Helfgott is able to show that the conjecture is true for all odd integers larger than  $T$ .

## 4.4 The Proof

The proof takes its leap from the Hardy-Littlewood circle method. The *main term* is given by the *major arcs* and the *error term* is given by the *minor arcs*. For the *major arcs*, H. Helfgott takes advantage of the *L*-functions and the finite verification of the *generalized Riemann hypothesis*, and notes that the *major arcs* are the easiest part of the proof.

The *minor arcs*, on the other hand, "*are more delicate*" [Hel2]. Due to consequences by the use of the circle method, for example, a single  $\ln x$  in the wrong expression for the *minor arcs* would ruin the proof. Here the large sieve becomes convenient, as it is used to remove the factors of  $\ln$  in certain expressions.

With the use of the techniques mentioned, H. Helfgott is able to verify the conjecture for all odd integers larger than  $10^{27}$ , and together with the numerical verification of the ternary *Goldbach's conjecture*, as well as a multitude of other methods, H. Helfgott is eventually able to write the final conclusion.

*"Since the ternary Goldbach conjecture has already been checked for all  $N \leq 8.875 \cdot 10^{30}$ , we conclude that every odd number  $N > 7$  can be written as the sum of three odd primes, and every odd number  $N > 5$  can be written as the sum of three primes. The main results is hereby proven: the ternary Goldbach conjecture is true."* [Hel2]

The binary *Goldbach's conjecture* remains unproven, and a proof seems to be far away into the future. This leaves the curiosity for the centuries old conjecture still extant. With these final word we choose to finish the thesis with the desire that the reader has found it intelligible and, as we have, captivating.

## References

- [Bom] Bombieri, Enrico. *The Classical Theory of Zeta and L-functions*. Milan journal of mathematics 78.1 (2010): 11-59, doi: 10.1007/s00032-010-0121-8
- [Car] Carr, Richard and Weisstein, Eric W. *Much Greater*. From MathWorld—A Wolfram Web Resource. <https://mathworld.wolfram.com/MuchGreater.html> Retrieved June 22, 2020.
- [Cri] Crispin Quinonez, Veronica. Private communication via veronica.crispin@math.uu.se
- [Fin] Fine, Benjamin., Rosenberger, Gerhard. *Number Theory: An Introduction via the Distribution of Primes*. Birkhäuser Boston, 2007.
- [Gal] Gallagher, Patrick. Ximenes. *A Larger Sieve*. Acta Arithmetica, 18.1 (1971), 77-81.
- [Gaz] Gaze, Eric., Gaze, Joseph. *On the Even Distribution of Primes Mod  $P$  (And Why This is Not a Proof of the Goldbach Conjecture)*. Math Intelligencer, 38.1, (2016): 14–21, doi: 10.1007/s00283-015-9585-2
- [Gol] Goldfeld, Dorian. *The Elementary Proof of the Prime Number Theorem: An Historical Perspective*. Number Theory. Springer, New York, NY, 2004. 179-192.
- [Gor] Gorin, Evgenii. Alekseevich. *Asymptotic Law for the Distribution of Prime Numbers in the Context of Free Abelian Semigroups*. Russian Journal of Mathematical Physics 13.1 (2006): 31-54, doi: 10.1134/S1061920806010043
- [Gra] Granville, Andrew. *Harald Cramér and the Distribution of Prime Numbers*. Scandinavian Actuarial Journal 1995.1 (1995): 12-28, doi: 10.1080/03461238.1995.10413946.
- [Hel1] Helfgott, Harald. Andrés. (2013). *The Ternary Goldbach Conjecture is True*. Available on ArXiv, <https://arxiv.org/abs/1312.7748>
- [Hel2] Helfgott, Harald. Andrés. (2015). *The Ternary Goldbach Problem*. Available on ArXiv, <https://arxiv.org/pdf/1501.05438.pdf>



- [Hel3] Helfgott, Harald. Andrés., and David. John. Platt. *Numerical Verification of the Ternary Goldbach Conjecture up to  $8.875 \cdot 10^{30}$* . Experimental Mathematics 14.1 (2013): 391-405, doi: 10.1080/10586458.2013.831742
- [Hor] Horsley, Samuel. *ΚΟΣ ΚΙΝΟΝ ΕΠΑΤΟΣ Θ ΕΝΟΥ Σ. or, The Sieve of Eratosthenes. Being an Account of His Method of Finding all the Prime Numbers, by the Rev. Samuel Horsley, FR S.* Philosophical Transactions of the Royal Society of London vol. 62 (1772): 327-347.
- [Lan] Lance, Stefan. *A Survey Of Primality Tests*. Retrieved on May 25, 2020, <http://math.uchicago.edu/~may/REU2014/REUPapers/Lance.pdf>
- [Lia] Liang, Wang, Huang Yan, and Dai Zhi-cheng. (2016). *Fractal in the Statistics of Goldbach Partition*. Available on ArXiv, <https://arxiv.org/pdf/nlin/0601024.pdf>
- [Pla] Platt, David. *Numerical Computations Concerning the GRH*. Mathematics of Computation 85.302 (2016): 3009-3027, doi: 10.1090/mcom/3077
- [Ras] Rassias, Michael T., and SpringerLink (Online service). *Goldbach's Problem: Selected Topics*. Springer International Publishing, Cham, 2017.
- [Rie] Riesel, Hans. *Prime Numbers and Computer Methods for Factorization*. Vol. 126. Springer Science & Business Media, 2012.
- [Ros] Rosen, Kenneth H. *Elementary Number Theory & Its Applications*, 6th. E. (2011).
- [Saf] Saff, Edward B., and Arthur D. Snider. *Fundamentals of Complex Analysis: With Applications to Engineering and Science*. Prentice Hall, Upper Saddle River, N.J, 2003.
- [Sci] *The Goldbach Comet*, (2017). <https://scipython.com/blog/the-goldbach-comet/> Retrieved May 18, 2020.
- [Sel1] Selberg, Atle. *An Elementary Proof of the Prime-Number Theorem*. Annals of Mathematics (1949): 305-313, doi: 10.2307/1969455
- [Sel2] Selberg, Atle. *An Elementary Proof of the Prime-Number Theorem for Arithmetic Progressions*. Canadian Journal of Mathematics 2 (1950): 66-78, doi: 10.4153/CJM-1950-007-5

- [Sie] Siegmund-Schultze, Reinhard. *Euclid's Proof of the Infinitude of Primes: Distorted, Clarified, made Obsolete, and Confirmed in Modern Mathematics*. The Mathematical Intelligencer 36.4 (2014): 87-97, doi: 10.1007/s00283-014-9506-9
- [Sil] Oliveira e Silva, Tomás, Siegfried Herzog, and Silvio Pardi. *Empirical Verification of the Even Goldbach Conjecture and Computation of Prime Gaps up to  $4 \cdot 10^{18}$* . Mathematics of Computation 83.288 (2014): 2033-2060, doi:10.1090/S0025-5718-2013-02787-1
- [Sop] Soprounov, Ivan. (2010). *A Short Proof of the Prime Number Theorem for Arithmetic Progressions*. Available on CiteSeerX, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.179.460&rep1&type=pdf>. Retrieved June 17, 2020.
- [Taf] Táfula, Christian. *An Elementary Heuristic for Hardy–Littlewood Extended Goldbach's Conjecture*. São Paulo Journal of Mathematical Sciences, 14.1 (2020): 391-405, doi: 10.1007/s40863-019-00146-3
- [Top] Topçu, Hatice, and Necdet Batir. *Bounds for the Generalized Euler-Constant Function*. International Journal of Mathematical Education in Science and Technology 46.2 (2015): 292-297, doi: 10.1080/0020739X.2014.950704
- [Vau] Vaughan, Robert. Charles. *Goldbach's Conjectures: A Historical Perspective*. Open problems in mathematics. Springer, Cham, 2016. 479-520, doi: 10.1007/978-3-319-32162-2\_16
- [Zac] Zaccagnini, Alessandro. (2005). *Introduction to the Circle Method of Hardy, Ramanujan and Littlewood*. Available on Semantic Scholar, <https://www.semanticscholar.org/paper/Introduction-to-the-circle-method-of-Hardy-%2C-and-Zaccagnini/3d3ab414e5bf271e1f4ec4e8eec20bbcaaa5b5b5>. Retrieved June 17, 2020.
- [Zag] Zagier, Don. *Newman's Short Proof of the Prime Number Theorem*. The American Mathematical Monthly, 104.8 (1997), 705-708.