Goldbach's Conjecture in non-integer contexts

by

John Stewart

Bachelor of Computer Science, University of New Brunswick 2004

A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of

Master of Computer Science

In the Graduate Academic Unit of Computer Science

Supervisor:	Rod Cooper MMath, Computer Science
Examining Board:	Joseph D. Horton, Ph.D. Computer Science, Chair
	Steven Rauch, Ph.D. Computer Science
	Gary T. Whiteford, Ph.D. Faculty of Education

This thesis is accepted by the Dean of Graduate Studies

THE UNIVERSITY OF NEW BRUNSWICK

September, 2006

Your file Votre référence
ISBN: 978-0-494-46707-7
Our file Notre référence
ISBN: 978-0-494-46707-7

Abstract

Goldbach's conjecture, an unproven mathematical claim, states that every even integer greater than 2 can be written as a sum of two prime integers. In this thesis, a more general definition of the conjecture, called *the Abstract Goldbach conjecture* is proposed, and it is used to extend the study of Goldbach's conjecture outside of the integers proper. The algebra of several non-integer contexts are studied, and Goldbach's conjecture is defined and studied in each of these. In arguing that the conjecture transcends the integers, this work argues that attempts at proving the conjecture should transcend the integers as well.

Acknowledgment

I would like to thank my family for their support, financial and otherwise. I would like to thank the University of New Brunswick for their financial support. I would like to thank Rod Cooper for his considerable time and effort towards the completion of this work.

Contents

List of Figures

List of Tables

1 Introduction

Among the open problems of mathematics, few can be stated as simply as Goldbach's Conjecture. Two hundred and fifty years after its inception, in a letter by Christian Goldbach to Leonard Euler, it remains unsolved despite a considerable amount of mathematical scrutiny. Goldbach's conjecture states that every even integer greater than 2 can be written as a sum of two prime integers in at least one way. Based on empirical evidence, it is almost certainly true.

The following pages do not contain a proof of the conjecture. However, a new perspective is offered, one which might affect the methods by which a proof is sought in the future. This idea is very simple: that *Goldbach's conjecture, as it is stated among the integers, is simply a manifestation of a more general truth about numbers.* In other words, if Goldbach's conjecture holds among the integers, it is not due to properties particular to the integers, but more general ones, properties which may be shared by many other algebraic contexts.

If Goldbach's Conjecture, or some abstraction thereof transcends the integers, then the current body of knowledge regarding the conjecture is artificially limited by the assumption otherwise. Just as escaping a maze is easier from above than within, a grander purview of the problem may be key to a solution.

The challenges posed in adapting the conjecture to non-integer contexts are numerous. The solution requires preserving the essence of the conjecture as it was originally stated, while being abstract enough to become adaptable to number systems which differ greatly from the integers. They differ in a significant way: from the number line to plane to hyper-plane, among sets with differing notions of what an even number is, to sets with no even numbers at

all, contexts where laws of commutativity do not hold, and where unique prime factorization fails. Through the study of Goldbach's conjecture in these varied contexts, it is hoped that credence will be lent to this new idea.

Although the following work does not constitute the first attempt at adapting Goldbach's conjecture outside of the integers, it is, to the knowledge of the author, the first attempt to define Goldbach's conjecture in an abstract way for the purpose of applying it to multiple algebraic contexts. This definition, called the *Abstract Goldbach conjecture*, will be used to study the conjecture among the integers, the Gaussian integers (integral complex numbers), the Hurwitz integers (integral quaternions), and subsets of the integers, the 1-monoids. To the best knowledge of the author, only one other work has discussed Goldbach's conjecture outside of the integers. Published in 1968, "The twin prime problem and Goldbach's conjecture in the Gaussian Integers" by Holben and Jordan attempts to adapt both of these problems to the Gaussian integers. This paper is discussed later.

Tools to study Goldbach's conjecture in these varied numbers contexts have been developed in the Maple programming language. All graphs and computations were done using Maple software. Routines to study Goldbach's conjecture are not built into Maple, and were built as extensions to current Maple routines, when possible. For example, since Maple contains a Gaussian integer package, it was possible to use that package when developing tools to study Goldbach's conjecture in that context. In some cases, no tools existed to study a particular algebra. For example, the integer subset monoids, described in Section 5, required the development of more sophisticated tools. These tools may be useful for further study of these monoids in the future.

Following a brief overview of the conjecture's history, a few elementary math-

ematical notions will be introduced. Afterwards, the algebra of the integers will be introduced, followed by a study of Goldbach's conjecture in that context. From there, the Abstract Goldbach conjecture will be defined, and the conjecture will then be studied in three non-integer contexts.

1.1 A Brief History of Goldbach's Conjecture

Goldbach and Euler shared a lengthy correspondence, consisting of 196 letters over 35 years[19]. In a 1742 letter, Goldbach proposed the conjecture, saying that "...it seems that every number that is greater than 2 is the sum of three primes" [15]. However, Goldbach considered 1 to be prime, a convention no longer followed.

The problem has been attacked using many advanced tools of mathematics, including analysis and sieve theory. In 1923, Hardy and Littlewood showed that nearly all even integers are composable as a sum of two prime integers, assuming the Grand Riemann Hypothesis (a problem which remains unsolved today)[18]. In 1937, I.M. Vinogradov removed the need for the assumption of the Grand Riemann Hypothesis in the result of Hardy and Littlewood[18]. From sieve theory comes one of the most important results achieved thus far: Chen's theorem. Chen's theorem states that every sufficiently large even integer can be written as either a sum of two primes or as the sum of a prime and a semiprime, a semiprime being a product of two primes[4]. The notion of a "sufficiently large" integer is that, even if there are counterexamples, there is eventually a final one.

There is a close relationship between the Riemann Hypothesis and Goldbach's conjecture, and since the Riemann Hypothesis is intimately related to the distribution of primes, so is Goldbach's conjecture. When Hilbert pre-

sented some of his 23 problems for mathematicians of the 20^{th} century in 1900, problem 8 was indeed two problems: The Riemann Hypothesis and Goldbach's Conjecture[18]. However, it has not been shown that the truth of one would directly imply the truth of the other. Twelve years after Hilbert presented these problems to 20^{th} century mathematicians, Edmund Landau stated what he felt were four unattackable problems of mathematics, the first of which was Goldbach's Conjecture[17]. Although Landau's claim predated the significant progress towards a solution discussed above, nearly 100 years after his claim, and over 250 years after the conjecture was originally made, Goldbach's conjecture remains unsolved.

2 The Integers

Following a brief study of the elementary algebra of the integers, pursued up to the fundamental theorem of arithmetic, Goldbach's conjecture among the integers is studied.

2.1 The Algebra of the Integers

The set of integers, denoted $\mathbb{Z}$, along with two binary operators $+, \cdot$ form a **ring**. A ring is a set and two binary operations satisfying the following axioms, where a, b, c are elements of the set that can, but need not be distinct from one another. [1, p84]

Axiom 2.1 (Additive Commutativity).

$$a + b = b + a \tag{1}$$

Axiom 2.2 (Additive Associativity).

$$a + (b + c) = (a + b) + c \tag{2}$$

Axiom 2.3 (Multiplicative Associativity).

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{3}$$

Axiom 2.4 (Existence of Additive Unit). *There exists an integer* 0 *such that*

$$a + 0 = 0 + a = 0 \tag{4}$$

Axiom 2.5 (Existence of Additive Inverse). *There exists a number* $-a$ *such*

that

$$a + (-a) = 0 \tag{5}$$

Axiom 2.6 (Distributivity).

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{6}$$

$$(a + b) \cdot c = a \cdot c + a \cdot b \tag{7}$$

Specifically, it is said that $\mathbb{Z}$ is a commutative ring with an identity element, since in addition to the axioms above, the integers satisfy the following two properties:

Axiom 2.7 (Multiplicative Commutativity).

$$a \cdot b = b \cdot a \tag{8}$$

Axiom 2.8 (Existence of Multiplicative Unit). *There exists an integer* $1 \in \mathbb{Z}$ *such that*

$$a \cdot 1 = 1 \cdot a = a \tag{9}$$

The positive integers, those greater than zero, are denoted $\mathbb{Z}^+$. The negative integers, those less than zero, are denoted $\mathbb{Z}^-$.

$$\mathbb{Z}^+ = \{1, 2, 3, 4, 5 \ldots\} \tag{10}$$

$$\mathbb{Z}^- = \{-1, -2, -3, -4, -5 \ldots\} \tag{11}$$

Theorem 2.1 (Mathematical Induction). *If* $P(n)$ *is some property of a positive integer* n*, and this property holds for* $P(1)$*, and* $P(n+1)$ *holds whenever* $P(n)$

holds, $P(n)$ must hold for all integers n.

Theorem 2.2 (The well-ordering principle). *If S is a non-empty subset of $\mathbb{Z}^+$, then S contains a least member. [2, p17]*

Theorem 2.3 (The Division Algorithm). *Given two integers a, $b \neq 0$, there exist unique integers m, r, $0 \leq r < |b|$ such that $a = mb + r$. [1, 28]*

Definition 2.1. *An integer a is said to **divide** the integer b if there exists an integer k such that $a \cdot k = b$. If a divides b it is denoted $a|b$, otherwise $a \nmid b$.*

Example 2.1. *(a)* $7|21$ *since* $21 = 3 \cdot 7$. *(b)* $4 \nmid 31$ *since there exists no integer k such that* $4 \cdot k = 31$.

Definition 2.2. *If an integer d divides both a and b, it is said to be a common divisor of a, b. If d is the largest integer dividing both a and b, it is called the **greatest common divisor** (gcd) of a, b and it is denoted as $(a, b) = d$.*

Example 2.2. *(a)* $(12, 9) = 3$ *since* $3|12$ *and* $3|9$ *and there exists no larger integer dividing them both. (b)* $(17, 4) = 1$ *since there are no common divisors between* 17 *and* 4 *other than* 1, *which divides all integers.*

Theorem 2.4. *If a is an integer then $(a, a-1) = 1$.*

Proof. Assume the opposite is true, and that $(a, a-1) = d, d > 1$. So d divides both $a, a-1$, which means there exist integers k_1, k_2 such that

$$d \cdot k_1 = a \tag{12}$$

$$d \cdot k_2 = a - 1 \tag{13}$$

subtracting one from the other yields

$$d \cdot k_1 - d \cdot k_2 = a - (a - 1) \tag{14}$$

$$d(k_1 - k_2) = 1 \tag{15}$$

Clearly, the left hand side of this equation cannot be equal to 1 unless $d = 1$, which contradicts the statement that $d > 1$.

□

Theorem 2.5. *if m, x, y are integers and $m|(x - y)$ it is said that that x is **congruent** to y modulo m and this is written*

$$x \equiv y \bmod m \tag{16}$$

Otherwise, it is said that x and y are non-congruent modulo m and this is written

$$a \not\equiv b \bmod m \tag{17}$$

Example 2.3. *(a)* $25 \equiv 10 \bmod 5$ *(b)* $10 \equiv 1 \bmod 3$

Definition 2.3. *If $(a, b) = 1$ it is said that a and b are **relatively prime** or **coprime**.*

Definition 2.4. *An integer p is **prime** if no integers other than 1 and p divide p. If a number is not prime it is **composite**. If an integer is a product of exactly two prime elements, it is a **semiprime**.*

From here on the letters p and q are reserved to denote prime integers.

Theorem 2.6. *If a, b, c are integers and $a|b$ and $a|c$ then $a|(bx + cy)$ for any integers x, y.*

Proof. (Adapted from [1, p20])
Since $a|b$ and $a|c$, there exist integers k_1, k_2 such that

$$ak_1 = b \tag{18}$$

$$ak_2 = c \tag{19}$$

Multiplying both sides of the first equation by x, and the second by y,

$$xak_1 = xb \tag{20}$$

$$yak_2 = yc \tag{21}$$

Summing both equations yields

$$xak_1 + yak_2 = xb + yc \tag{22}$$

$$a(xk_1 + yk_2) = xb + yc \tag{23}$$

So $a|(xb + yc)$ for any integers x, y. □

Theorem 2.7. *if one or both of a, b is non-zero and $d = (a, b)$ then d is the least element among the set of all positive integers of the form $ax + by$, where $a, x, b, y \in \mathbb{Z}$.*

Proof. (Adapted from [5, p23])
Let S be the set of all positive integers of the form $ax + by$. It must be shown that S is a non-empty set. The theorem assumes that one of a, b is non-zero. Assume $a \neq 0$. So if a is positive, it is a member of S, since $a = 1 \cdot a + 0 \cdot b$. If a is a negative number, then $-a$ is a member of S by the same argument. So S is a non-empty set.

S has some least element e

$$e = ax_0 + by_0 \tag{24}$$

From the Division Algorithm (Theorem 2.3) it is known that there exist unique integers m, r such that

$$a = em + r \quad 0 \leq r < e \tag{25}$$

and by algebraic manipulation this yields

$$\begin{aligned} r &= a - me \\ &= a - m(ax_0 + by_0) \\ &= a - amx_0 - bmy_0 \\ &= a(1 - mx_0) + b(-my_0) \end{aligned}$$

Which is of the form $ax + by$. Suppose $r \neq 0$. Then r is of the form $ax + by$ which is positive and less than e (By the inequality in Equ. 25), and hence would be the least member of S, which contradicts the prior statement that e is the least member of S. Therefore, it must be that $r = 0$. Since $r = 0$,

$$\begin{aligned} 0 &= a - me \\ em &= a \end{aligned}$$

so $e|a$.

By the same argument as for a above, there exist m, r such that

$$b = em + r \quad 0 \leq r < e \tag{26}$$

$$= \ldots \tag{27}$$

$$r = b(1 - my_0) + a(-mx_0) \tag{28}$$

by the same argument as above, $r = 0$. Therefore,

$$0 = b - me \tag{29}$$

$$me = b \tag{30}$$

so $e|b$.

Since $e|a$ and $e|b$, it must be that $e|d$, d being the common divisor of a, b. Since $e|d$, it must be that $e \leq d$.

Since $d = (a, b)$, $d|a$ and $d|b$. From Theorem 2.6 it is known that this means that $d|(ax + by)$ for all integers x, y. Therefore, from Equ. 24 it must be that $d|e$, so $d \leq e$. But earlier it was shown that $e \leq d$, so it must be that $d = e$. Therefore, the least member of S is d, which completes the proof.

□

Theorem 2.8. *if a, b, c are integers where $a|bc$ and $(a, b) = 1$ then $a|c$.*

Proof. (Adapted from [5, p26])
Since $(a, b) = 1$ by Theorem 2.7 there exist integers x, y such that

$$1 = ax + by \tag{31}$$

Multiplying both sides by c

$$c = cax + cby \tag{32}$$

Since $a|bc$, there must exist some k such that

$$ak = bc \tag{33}$$

Substituting for bc from the previous equation yields

$$c = cax + aky \tag{34}$$

$$= a(cx + ky) \tag{35}$$

So $a|c$. □

Theorem 2.9 (Euclid's Theorem). *if p is a prime integer and b, c are integers where $p|bc$ then $p|b$ or $p|c$ (or both).*

Proof. If $p|b$ then the theorem is satisfied. Otherwise, $(p, b) = 1$, so by Theorem 2.8 $p|c$. □

Corollary 2.1. *If p is prime and $a_1, a_2 \ldots a_m$ are integers where $p|a_1 a_2 \ldots a_m$, then $p|a_i$ for some i ,$1 \leq i \leq m$.*

Proof. (Adapted from [5, p26])
(By Induction) As a base case, let $m = 2$. It must be shown that if $p|a_1 a_2$, p divides one of a_1, a_2. But this has already been shown in Theorem 2.9.

If the theorem is true for n, then $p|a_1 a_2 \ldots a_n$ and $p|a_i$ for some i, $1 \leq i \leq n$. Under this assumption, it must be shown that it is also true that if $p|a_1 a_2 \ldots a_{n+1}$, then $p|a_j$ for some j , $1 \leq j \leq n+1$. But clearly this is so, since i lies within the valid range for j, and $p|a_i$. So when $j = i$, the theorem is satisfied for $m = n+1$, which proves the theorem. □

Corollary 2.2. *If $p, p_1 p_2 \ldots p_m$ are prime integers and $p|p_1 p_2 \ldots p_m$ then $p = p_i$ for some i ,$1 \leq i \leq m$.*

Proof. (Adapted from [5, p26])
From Corollary 2.1 it is known that $p|p_i$ for some i, $1 \leq i \leq m$. Therefore, there exists an integer k such that

$$pk = p_i \tag{36}$$

However, p_i is prime by definition. If k has a value other than 1, p_i is composite, which is a contradiction. Therefore, $k = 1$, and $p = p_i$. □

Theorem 2.10. *Every integer greater than one can be represented as a product of prime integers.*

Proof. (Adaptation of [5, p10])
(By Induction) As a base case, let $n = 2$. Since 2 is prime, it is the product of exactly one prime, which satisfies the theorem.

Assume that the theorem holds for all integers between 2 and k inclusively. From this assumption, it must be shown that the theorem also holds for $k + 1$.

$k+1$ is either prime or composite. If it is prime, then it is the product of exactly one prime and therefore satisfies the theorem. Otherwise, $k + 1$ is composite, which means that it is a product of at least two integers, say r and s, which must each satisfy the following inequalities:

$$2 \leq r \leq k$$

$$2 \leq s \leq k$$

However, this means that both r, s fall within the range in which the theorem is assumed to be true. Therefore, each can be written as a product of primes, and hence their product, $k + 1 = r \cdot s$ is also a product of primes.

□

Theorem 2.11. *There exist an infinity of prime integers.*

Proof. (Adapted from [7, p12])
Suppose p is the last prime integer. Let x be the product $x = 2 \cdot 3 \cdot 5 \ldots p$ of all the prime integers up to and including p. So $2|x, 3|x \ldots p|x$. Now consider $x + 1$. By Theorem 2.4, $(x + 1, x) = 1$, which means that $x + 1$ shares no common divisor with x. However, from Theorem 2.10 it is known that every integer is composable as a product of primes. Since $x+1$ is not divisible by any

of the primes numbers up to and including p, it must either be prime itself or composed of primes greater than p. Either way, p is not the last prime integer. Since no prime integer p is the last prime integer, there must exist an infinite number of prime integers.

□

Theorem 2.12 (The Fundamental Theorem of Arithmetic). *Every integer greater than one can be written as a product of prime integers in a unique way.*

Proof. (Adapted from [1, p33])
From Theorem 2.10 it is known that every integer greater than 1 can be written as a product of primes. Here, it must be shown that this representation as a product of primes is unique, in the sense that the order of the prime factors is irrelevant.

Suppose some integer x can be written as a product of prime integers in two different ways:

$$x = p_1 \cdot p_2 \dots p_m = q_1 \cdot q_2 \dots q_n \tag{37}$$

Assume that $m \leq n$, and that the primes are ordered in a way such that

$$p_1 \leq p_2 \leq \dots p_m, \quad q_1 \leq q_2 \leq \dots q_n \tag{38}$$

since $p_1 \cdot p_2 \dots p_m = p_1 \cdot k_1$, where $k_1 = p_2 \dots p_m$, it must be that $p_1 | q_1 \cdot q_2 \dots q_n$. By Corollary 2.2, p_1 must divide exactly one of $q_1 \dots q_n$, so $p_1 \geq q_1$. Similarly, since $q_1 \cdot q_2 \dots q_n = q_1 \cdot k_2$, where $k_2 = q_2 \dots q_n$, so $q_1 | p_1 \cdot p_2 \dots p_m$. By Corollary 2.2, q_1 must divide exactly one of $p_1 \dots p_n$, so $q_1 \geq p_1$. But earlier it was shown that $p_1 \geq q_1$, and now $q_1 \geq p_1$, so it must be true that $q_1 = p_1$, and these equal

factors cancel out, leaving

$$p_2 \cdots p_m = q_2 \cdots q_n \tag{39}$$

This method can be applied repeatedly, canceling p_i with q_i for all i up to $min(m, n)$. However, suppose $m < n$, then terms will be canceled until

$$1 = q_{m+1} \cdot q_{m+2} \cdots q_n \tag{40}$$

This cannot be, since $q_{m+2} \ldots q_n$ are primes, and the smallest prime number is 2. Therefore, m and n must be equal, and $p_i = q_i$ for all i, which completes the theorem. □

2.2 Goldbach's Conjecture among the Integers

Conjecture 2.1. *Goldbach's conjecture states that every positive even integer $\varepsilon \geq 4$ can be composed as a sum of two prime integers in at least one way.*

$$\forall\, \varepsilon \geq 4 \quad \exists p, q \text{ prime} \quad \varepsilon = p + q \quad p \leq q, \tag{41}$$

Example 2.4. *(a) Consider $\varepsilon = 10$, which can be written as $3 + 7$ or as $5 + 5$. (b) If $\varepsilon = 22$ then it can be written as a sum of primes in three ways: $3 + 19$, $5 + 17$ and $11 + 11$.*

The following restatement is equivalent to Conjecture 2.1:

Restatement 2.1. *For every integer $a > 1$, there exists at least one integer κ no greater than a, such that both $(a + \kappa), (a - \kappa)$ are prime integers.*

$$\forall\, a > 1 \quad \exists\, \kappa \quad (a + \kappa) = p, (a - \kappa) = q \quad 0 \leq \kappa < a \tag{42}$$

Restatement 2.1 is equivalent to Conjecture 2.1. To see this, consider any positive integer $a > 1$. Suppose there exists an integer κ, $0 \leq \kappa < a$ such that $(a+\kappa)$, $(a-\kappa)$ are both prime integers. Then the sum $(a+\kappa)+(a-\kappa) = 2a$ is an even number representable as a sum of two prime integers. If there exists such a κ for every integer a, then every integer of the form $2a$ is expressible as a sum of two prime integers. Since all even numbers greater than 4 are expressible as $2a$, where a is an integer greater than 2, Restatement 2.1 is equivalent to the original conjecture.

Example 2.5. *(a) Consider* $a = 10$. *If* $\kappa = 3$, *then* $(a+\kappa) = (10+3) = 13$ *and* $(a-\kappa) = (10-3) = 7$, *where* $7, 13$ *are prime integers. (b) Consider* $a = 1000$. *If* $\kappa = 9$, $(a+\kappa) = 1009$, $(a-\kappa) = 991$, *both of which are prime.*

When Restatement 2.1 is satisfied for an integer a, a is said to be **equidistant** to two prime integers. This is equivalent to saying that even integer $\varepsilon = 2a$ can be written as a sum of two prime integers. From here on, if an integer a is equidistant to two primes, it is said to satisfy Goldbach's conjecture. Restatement 2.1 is rarely mentioned in the literature, either because it has been overlooked or authors find it too trivial to mention. However, there are advantages to this alternative description, namely that it makes no mention of the addition operator, and that it is not a statement relegated to the even integers. A 1993 paper titled "A Reformulation of the Goldbach Conjecture" by Gerstein describes the restatement, and uses it to study the relationship between Goldbach's Conjecture and the Twin Prime conjecture. As will be discussed later, this restatement will serve an important role in defining the Abstract Goldbach's conjecture. For this reason, the remainder of this section will study Goldbach's conjecture using the notation and form of Restatement 2.1 rather than the more traditional form.

Theorem 2.13. *If an integer a is prime, it satisfies Goldbach's Conjecture.*

Proof. If a is prime, then it is trivially equidistant to two primes, since, when $\kappa = 0$, $(a+0), (a-0)$ are both equal to a, which is prime. □

Theorem 2.14. *If an integer a is equidistant to two prime integers, one of those primes is less than or equal to a and the other is greater or equal to a.*

$$3 \leq p \leq a \leq q \leq 2a - 3 \tag{43}$$

Proof. If $\kappa = 0$, $p = q = a$. Otherwise, $\kappa > 1$ so $(a - \kappa) < (a + \kappa)$. So if $p \neq q$, one must be less, the other greater than a. □

Definition 2.5. *The Goldbach number for a given integer a, denoted as $G(a)$, represents the number of integers $0 \leq \kappa < a$ such that $(a \pm \kappa)$ are both prime. [6]*

Example 2.6. *(a) $G(5) = 2$ because, as seen in Example 2.4(a), 10 can be written as a sum of primes in two distinct ways. (b) Similarly, $G(500) = 28$ because 1000 can be written as a sum of two prime numbers in 28 distinct ways.*

Goldbach's Conjecture can be restated in terms of the Goldbach number in the following way:

Restatement 2.2. *For any integer $a > 3$, it must be true that $G(a) \geq 1$.*

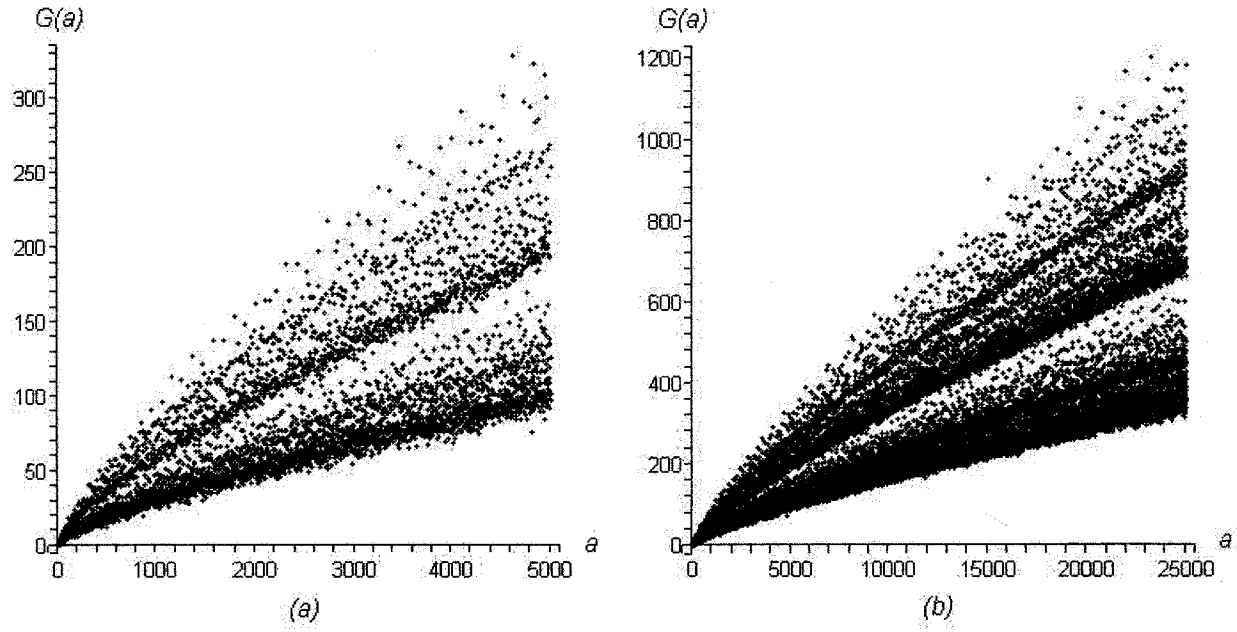

Figure 1: Goldbach's Comet

Figure 1(a) and (b) graph integer a (x-axis) with respect to $G(a)$ (y-axis) for all integers a up to 5000 and 25000 respectively. That is, it graphs every integer a relative to the number of integers κ, $0 \leq \kappa < a$ which exist such that $(a \pm \kappa)$ are both prime. Restated once more, it graphs the number of ways that $2a$ can be composed as a sum of two prime integers.

The graph of integer a relative to $G(a)$ was christened **Goldbach's Comet** by Fliegel and Robertson in a 1989 paper. In it they discuss the banded nature of the graph and study its increasing nature. In their paper, they define the Goldbach number in a slightly different way. They define $G(\varepsilon)$, ε even, to be the number of ways that ε can be written as a sum of two primes. In this work, G is defined for all integers, so that it is more easily generalizable to other number systems. In their paper, they bound the lower band of the comet of ε relative to $G(\varepsilon)$ by the equation $G(\varepsilon) \geq 0.02745 \cdot x^{0.86}$.

Examining the graph, it is evident that as the integer a increases, there tend to be more solutions to Goldbach's conjecture. Statistically, this is not surprising, since the number of potential solutions increases with respect to a. In fact,

$$G(a) \leq a \tag{44}$$

since κ can take on any of a distinct values . ($G(a)$ will be bound more strictly soon). Although the number of potential solutions increases as the integer a increases, this is partially offset by the diminishing prime density as magnitude increases.

The truth of Goldbach's Conjecture is inextricably linked to the distribution of prime numbers. In fact, Goldbach's Conjecture can be thought of as a statement of fact about that distribution. More specifically, whether or not an integer a

satisfies Goldbach's conjecture depends upon the symmetry of the prime distribution up to $2a$. This statement will benefit from an illustration.

For any integer a, let β_a represent the string of bits of length $2a-1$, where the i^{th} bit is set to 1 if i is prime, and to 0 otherwise. Let β'_a be the reverse of bitstring β_a. That is, β'_a is of the same length as β_a, and bit i in β'_a has the same value as bit $2a-i$ in β_a. So the first bit of β'_a has the same value as the last bit of β_a, the second bit of β'_a has the same value as the previous to last bit in β_a, and so forth. Table 1 depicts β_a and β'_a for $a=5$. Table 2 depicts β_a and β'_a for $a=9$.

If there is a bit position i that is set to 1 in both β_a, β'_a, then a is equidistant to two prime integers, namely i and $2a-i$. For if bit i is set to 1 in β_a, then i is prime in β_a. If bit i is set in β'_a, then $2a-i$ is set in β_a. Since i, $2a-i$ are both prime, $i+(2a-i)=2a$ is composable as a sum of primes, which is identical to the statement that a is equidistant to two primes. If there is bit i that is set for both β_a, β'_a for all $a>3$, then Goldbach's Conjecture is true in $\mathbb{Z}$.

i	1	2	3	4	5	6	7	8	9
β_{10}	0	1	*1*	0	*1*	0	*1*	0	0
β'_{10}	0	0	*1*	0	*1*	0	*1*	1	0

Table 1: Bitstrings for $a=5$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
β_9	0	0	1	0	*1*	0	*1*	0	0	0	*1*	0	*1*	0	0	0	1
β'_9	1	0	0	0	*1*	0	*1*	0	0	0	*1*	0	*1*	0	1	0	0

Table 2: Bitstrings for $a=9$

In Table 1, bit 3 is set in both β_a, β'_a, so $a=5$ is equidistant to two primes, namely $i=3$ and $2a-i=10-3=7$.

These tables and the visualization of Goldbach's conjecture as the symmetry of a bit string is useful in understanding the fundamental trade off that occurs as the integer a gets larger. For any a, there will be $a-1$ possible bit positions. As a increases then, there are more potential solutions. However, the prime distribution wanes as magnitude increases. Therefore, as a increases, there tend to be more chances but those chances are less likely to succeed.

Theorem 2.15. *If $(a \pm \kappa)$ are both prime and $\kappa > 0$, then $(a, \kappa) = 1$.*

Proof. Suppose it were otherwise, then a, κ share some factor, say m. But if that were so, then clearly both $(a+\kappa), (a-\kappa)$ would be multiples of m. So $(a+\kappa) = p = x \cdot m$ and $(a-\kappa) = q = y \cdot m$ for some integers x, y. But since p, q are distinct primes, they cannot share a common factor. □

$G(a)$ can be bound using number theoretic functions, as discussed in the two theorems that follow.

Definition 2.6. *The Euler totient function for an integer n, denoted $\phi(n)$, represents the numbers of integers no greater than n that are relatively prime to n [7, p233].*

Example 2.7. *(a) $\phi(10) = 4$, since $1, 3, 7, 9$ are relatively prime to 10. (b) $\phi(1000) = 400$.*

Theorem 2.16. *$G(\varepsilon)$ is bounded by the Euler totient function in the following way:*

$$G(a) \leq \phi(a) + 1 \tag{45}$$

Proof. From Theorem 2.15 it is known that a and κ must be relatively prime in order for both $(a \pm \kappa), \kappa > 1$ to be prime. Therefore, there can be no more solutions to Goldbach's Conjecture than there are numbers less than and relatively prime to a. □

Definition 2.7. *The prime counting function for an integer n, denoted $\pi(n)$, represents the number of prime integers no greater than n [7, p6].*

Example 2.8. *(a)* $\pi(10) = 4$ *since* $2, 3, 5, 7$ *are the primes no greater than* 10. *(b)* $\pi(1000) = 168$.

Theorem 2.17. *$G(a)$ is bounded by the prime counting function in the following way:*

$$G(a) \leq \min(\pi(a), \pi(2a) - \pi(a)) \tag{46}$$

Proof. From Theorem 2.14 it is known that if an integer a is equidistant to two primes, the smallest of those is no greater than a. Therefore, $G(a)$ can be no greater than the number of primes up to a. Similarly, since the larger prime must be no less than a but no greater than $2a$, $G(a)$ can be no greater than the number of primes in that range. □

Theorem 2.18. *If Goldbach's Conjecture is true, then every square integer can be written as the sum of a semiprime and a square.*

$$\forall a \quad \exists\, p, q, \kappa \quad a^2 = p \cdot q + \kappa^2 \tag{47}$$

Proof. As previously discussed, if Goldbach's Conjecture is true, then so is Restatement 2.1. Therefore, for every integer a there exists a κ such that both $(a \pm \kappa)$ are prime. Since $(a \pm \kappa)$ are both prime, their product is a semiprime, so $(a + k) \cdot (a - k) = a^2 - k^2 = p \cdot q$, which through simple algebraic manipulation leads to the theorem. □

2.2.1 Is Goldbach's Conjecture True in $\mathbb{Z}$?

Goldbach's Conjecture remains unproven. It is possible that among the infinite expanse of the integers, there exists some finite or infinite number of integers which do not satisfy the conjecture.

Goldbach's conjecture is closely related to the distribution of prime integers. While that distribution does exhibit structure on a grand scale, it possesses no evident structure when closely examined. For example, it is possible to estimate the number of primes within a given range, but there exists no simple formula to compute the i^{th} prime number.

Since the conjecture remains unproven, one is relegated to studying it empirically. By hand, this is a very monotonous task. Desboves confirmed the truth of the conjecture by hand for all even numbers up to 10000 in 1885[15]. With the advent of computers, which excel at monotony, it has become possible to confirm the truth of the conjecture for much higher values. As of December 2005, Oliveira e Silva, using a computer, has found the conjecture to hold up to $3 \cdot 10^{17}$[15].

2.3 Weaker Statements than Goldbach's Conjecture

Having studied Goldbach's conjecture among the integers, a study of two weaker, related statements is now offered. These weaker statements may be stepping stones towards a proof of Goldbach's conjecture in $\mathbb{Z}$.

Definition 2.8. *An integer n is said to be **squarefree** if its unique prime factorization $n = p_1^{\alpha} p_2^{\beta} \cdot p_3^{\chi} \ldots p_m^{\delta}$ has no exponent $\alpha, \beta \ldots$ etc greater than one. If a number is not squarefree, it is said to be **squarefull**[12, 32].*

Example 2.9. *(a) $20 = 2^2 \cdot 5$ is squarefull, since 2 has an exponent greater than one. (b) $30 = 2 \cdot 3 \cdot 5$ is squarefree because its unique prime factorization contains no exponents greater than one.*

Definition 2.9. *The **Mobius Function** for an integer n, denoted $\mu(n)$, evaluates to 1 if $n = 1$, 0 if n is squarefull, and to $(-1)^k$ if n is a squarefree product of k primes [12, 32].*

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n \text{ is a squarefree product of } k \text{ primes} \\ 0, & \text{otherwise} \end{cases} \tag{48}$$

Example 2.10. *(a) Consider* $n = 20$ *as in Example 2.9(a). Then* $\mu(20) = 0$, *since* 20 *is squarefull. (b) Consider* $n = 30$ *as in Example 2.9(b). Then* $\mu(30) = -1$ *since* 30 *is a squarefree product of* 3 *primes, so* $\mu(30) = (-1)^3 = -1$. *(c) Consider* $n = 17$, *which is prime. Then* $\mu(17) = (-1)^1 = -1$, *since 17 is prime and hence is a product of exactly one factor. Clearly,* $\mu(p) = -1$ *for any prime integer* p.

The author proposes the following conjecture:

Conjecture 2.2. *Every integer greater than* 1 *is equidistant to two integers that evaluate to* -1 *in the mobius function.*

$$\forall a > 1 \quad \exists\, \kappa \quad \mu(a+\kappa) = \mu(a-\kappa) = -1 \quad 0 \leq \kappa < a \tag{49}$$

Definition 2.10. *Let* $G^{\mu}(a)$ *denote the number of integers* $0 \leq \kappa < a$ *such that* $\mu(a \pm \kappa) = -1$.

Example 2.11. *(a)* $G^{\mu}(5) = 2$, *since* (5 ± 0)=*5,* $\mu(5) = -1$ *and* $(5 \pm 2) = 3, 7$, $\mu(3) = -1, \mu(5) = -1$. *(b)* $G^{\mu}(500) = 66$.

Theorem 2.19. *Every integer greater than* 1 *is equidistant to two squarefree numbers.*

$$\forall a > 1 \quad \exists\, \kappa \quad \mu(a+\kappa) \neq 0,\ \mu(a-\kappa) \neq 0 \quad 0 \leq \kappa < a \tag{50}$$

Proof. The Riemann Zeta function and Dirichlet Lambda functions are involved in this proof, but their properties, and justification of the identities relating to

them are omitted, as discussing them is beyond the bounds of this thesis.

If the integer a is itself squarefree, then the theorem is satisfied when $\kappa = 0$. The remainder of this proof assumes that a is squarefull.

Let $Q(x)$ denote the number of integers between 1 and n inclusively which are squarefree.

The first step in this proof will be to show that

$$\forall\, x \quad Q(x) > \frac{x}{2} \tag{51}$$

Any integer n where $2^2|n$ or $3^2|n \ldots$ or $p^2|n$ is squarefull. If all those integers which are divisible by squares of primes are removed, what is left are those integers which are squarefree. [14]

$$Q(x) \geq x(1 - \frac{1}{2^2} - \frac{1}{3^2} - \frac{1}{5^2} \cdots - \frac{1}{p^2}) \tag{52}$$

$$\geq x\left(1 - \sum_{n=1}^{\infty} \frac{1}{p_n^2}\right) \tag{53}$$

where p_n is meant to denote the n^{th} prime integer. The inequality present in Equ. 52 stems from the redundancy which occurs when subtracting all of those integers which are divided by a square prime. For example, consider $36 = 2^2 \cdot 3^2$. Since it contains two squares, 36 would be removed by both the $\frac{1}{2^2}$ and $\frac{1}{3^2}$ terms in Equ.52. Therefore, the right-hand side of the inequality actually overestimates the density of squarefull numbers in the equation, justifying the inequality. Restating the equation so that the summation term is limited to the

odd prime integers yields

$$Q(x) \geq x\left(1 - \frac{1}{4} - \sum_{n=2}^{\infty} \frac{1}{p_n^2}\right) \tag{54}$$

$$\geq x\left(\frac{3}{4} - \sum_{n=2}^{\infty} \frac{1}{p_n^2}\right) \tag{55}$$

It is possible to weaken the statement while retaining the inequality. This is done by changing the summation to include all odd integers, instead of all odd primes. Clearly the odd primes are contained among the odd integers, so the inequality still holds.[14]

$$Q(x) \geq x\left(\frac{3}{4} - \sum_{n=1}^{\infty} \frac{1}{(2n+1)^2}\right) \tag{56}$$

The summation term is of the same form as the Dirichlet Lambda function[16]:

$$\lambda(s) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^s} \tag{57}$$

$$= (1 - 2^{-s}) \cdot \zeta(s) \tag{58}$$

where $\zeta(s)$ is the Riemann Zeta function[7, 245] evaluated at s

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{59}$$

In this case, $\lambda(2)$ is required, so

$$\begin{aligned}\lambda(2) &= \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} \\ &= (1-2^{-2}) \cdot \zeta(2) \\ &= (1-\frac{1}{4}) \cdot \zeta(2) \\ &= \frac{3}{4}(\frac{\pi^2}{6}) \\ &= \frac{\pi^2}{8}\end{aligned}$$

The Lambda Function begins its evaluation at 0, whereas the summation term in Equ.56 begins at 1, so 1 is subtracted from $\lambda(2)$ and substituted into Equ. 56 yielding

$$Q(x) \geq x(\frac{3}{4} - (\lambda(2) - 1)) \tag{60}$$

$$\geq x(\frac{3}{4} - \frac{\pi^2}{8} + 1) \tag{61}$$

$$\geq x(0.516299450\ldots) \tag{62}$$

so $Q(x) \geq \frac{x}{2}$.

Using this fact, it must be shown that for any integer a, there exists some integer $1 \leq \kappa < a$ such that $(a \pm \kappa)$ are both squarefree. (Recall the very first assumption in this proof, that a itself is squarefull, which implies that $\kappa = 0$ is not a valid solution). Since κ can be no greater than $a-1$, $a+\kappa$ can be no greater than $2a-1$. Therefore, for any integer a, those numbers up to $2a-1$ are relevant. From Equ. 51 it is known that

$$Q(2a-1) \geq \frac{2a-1}{2} \tag{63}$$

However, since $2a-1$ is odd, $\frac{2a-1}{2}$ will not be an integer. However, $Q(x)$ must return some integer value, so

$$Q(2a-1) \geq a \tag{64}$$

For each $1 \leq \kappa < a$, there is a pair of integers $(a+\kappa), (a-\kappa)$ and the following three possibilities:

- Both are squarefree
- Neither are squarefree
- One is squarefree, the other is not

It must be shown that for at least one of the $a-1$ possible values of κ, both $(a+\kappa), (a-\kappa)$ are squarefree. Assume otherwise. In the least optimistic case, for each of the $a-1$ potential values for κ, one of $(a+\kappa), (a-\kappa)$ is squarefree and the other is not. In total, this would add up to $a-1$ squarefull numbers in the range up to $2a-1$. However, Equ. 64 states that there are at least a squarefree numbers in this range. In other words, there are more squarefree integers than there are pairs, and therefore, one pair must consist of two squarefree numbers.

Therefore, every integer is equidistant to two squarefree numbers. □

Definition 2.11. *Let $G^s(a)$ denote the number of integers $0 \leq \kappa < a$ such that $\mu(a+\kappa) \neq 0$ $\mu(a-\kappa) \neq 0$.*

Example 2.12. *(a) $G^s(10) = 2$ since $(5 \pm 0) = 5$, $\mu(5) \neq 0$ and $(5 \pm 2) = 3, 7$, where $\mu(3) \neq 0, \mu(7) \neq 0$. (b) $G^s(1000) = 253$.*

From Theorem 2.19 it is evident that $G^s(a) \geq 1$ for all $a > 1$.

Theorem 2.20.

$$\forall a > 1 \quad G(a) \leq G^{\mu}(a) \leq G^s(a) \tag{65}$$

Proof. If $G(a) = x$, then a is equidistant to x pairs of primes. Clearly, any prime p has $\mu(p) = -1$, so each of these prime pairs also satisfies the conditions of Conjecture 2.2. Therefore $G(a) \leq G^{\mu}(a)$. Similarly, if $G^{\mu}(a) = y$, then a is equidistant to y pairs of numbers who evaluate to -1 in the mobius function. However, if a number evaluates to -1 in the mobius function, then it does not evaluate to 0 in that function. Therefore, any pair satisfying Conjecture 2.2 also satisfy the conditions of Theorem 2.19. Therefore, $G^{\mu}(a) \leq G^{s}(a)$. □

Figure 3(a) and (b) graph the integer a with respect to $G(a)$ in red, a with respect to $G^{\mu}(a)$ in blue, and a with respect to $G^{s}(a)$ in green, for all a up to 1000 and 10000 respectively.

Definition 2.12. *Let $G_{min}(a)$ represent the smallest integer $0 \leq \kappa < a$ such that $(a \pm \kappa)$ are both prime integers. Let $G^{\mu}_{min}(a)$ represent the smallest integer $0 \leq \kappa < 0$ such that $\mu(a \pm \kappa) = -1$. Let $G^{s}_{min}(a)$ represent the smallest integer $0 \leq \kappa < a$ such that $\mu(a + \kappa) \neq 0$, $\mu(a - \kappa) \neq 0$.*

Example 2.13. *(a)$G_{min}(6) = 1$ since $(6 + 1) = 7$, $(6 - 1) = 5$, 5 and 7 being prime, and $\kappa = 1$ being the smallest value for which $(a \pm \kappa)$ are both prime. (b)$G_{min}(5) = 0$, since 5 is prime so $(5 + 0), (5 - 0)$ are both prime.*

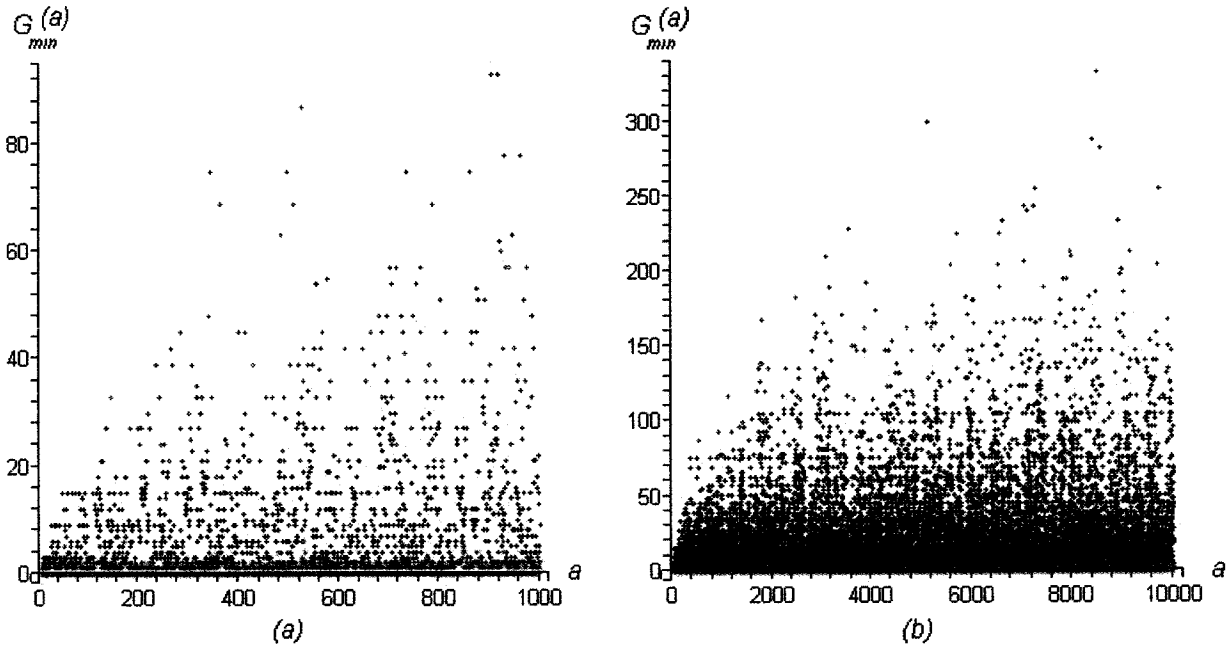

Figure 2: Minimal distance for satisfying Goldbach's Conjecture and the weaker statements

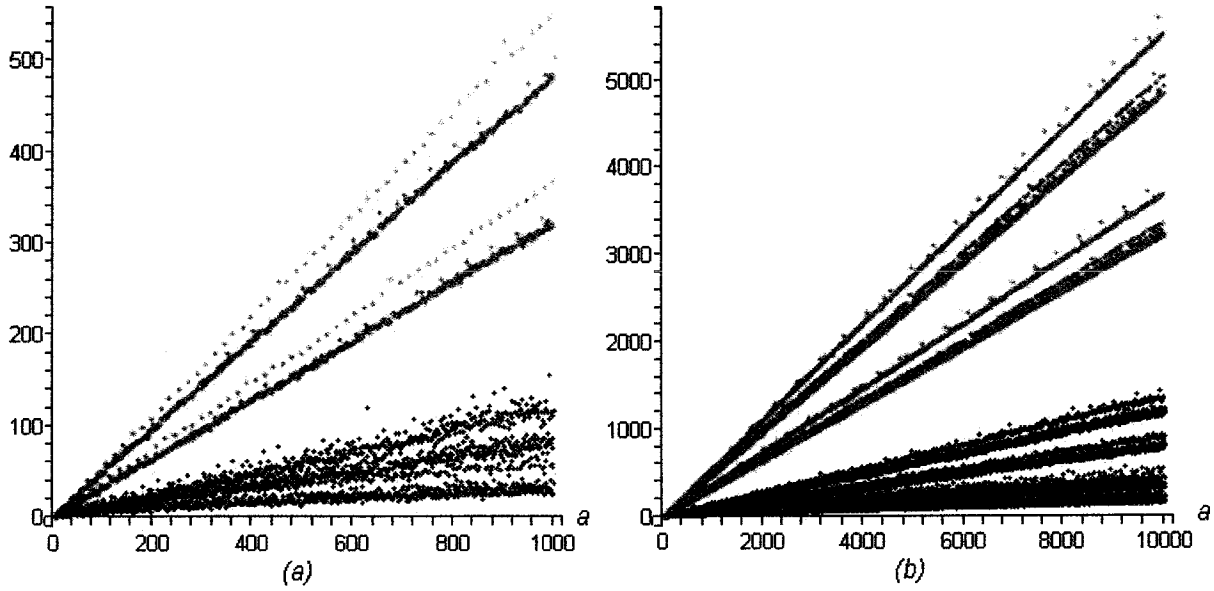

Figure 3: Goldbach's Conjecture and the two Weaker Statements

Theorem 2.21.

$$\forall\, a > 1 \quad G^{s}_{min}(a) \leq G^{\mu}_{min}(a) \leq G_{min}(a) \tag{66}$$

Proof. If $G_{min}(a) = x$, then $(a \pm x)$ are both prime. Therefore, $\mu(a \pm x) = -1$, so $G^{\mu}_{min}(a) \leq G_{min}(a)$. Similarly, if $G^{\mu}_{min}(a) = y$, then $\mu(a \pm y) = -1$, so $\mu(a \pm y) \neq 0$, so $G^{s}_{min}(a) \leq G^{\mu}_{min}(a)$. □

Figure 2(a) and (b) graph the integer a with respect to $G_{min}(a)$ in red, a with respect to $G^{\mu}_{min}(a)$ in blue, and a with respect to $G^{s}_{min}(a)$ in green, for all a up to 1000 and 10000 respectively.

2.3.1 A Discussion Regarding the Weaker Statements

Conjecture 2.2 and Theorem 2.19 are each weaker statements than Goldbach's Conjecture. If Goldbach's Conjecture is true, they must be as well. Showing either weaker statement to be false would imply that Goldbach's Conjecture is false. However, the truth of these weaker statements does not imply the truth of Goldbach's Conjecture.

Figure 3 emphasizes the relative strength of each of the three conjectures. In green, Theorem 2.19, which has been shown to have at least one solution for any integer a, in actuality tends to have many more solutions than the other two conjectures. In blue, Conjecture 2.2, which has not been shown to be true, tends to have more solutions than Goldbach's conjecture, in red, but they have a very similar shape and seem to increase at a comparable rate.

Figure 2 again emphasizes the relative strength of each conjecture. The smallest integer κ satisfying Theorem 2.19 for a given integer a, in green, tends to be smaller than the smallest κ satisfying Conjecture 2.2 for an integer a, in blue,

which in turn tends to be smaller than the smallest κ satisfying Goldbach's conjecture, in red. Table 3 lists the average G_{min} values up to 50000 and 100000 respectively.

AVG for a up to	50000	100000
$G_{min}(a)$	20.90	48.81
$G^{\mu}_{min}(a)$	3.22	6.45
$G^{s}_{min}(a)$	0.34	0.69

Table 3: Average G_{min} values in $\mathbb{Z}[i]$

Proving Conjecture 2.2 would be a significant step towards proving Goldbach's conjecture. It is not immediately clear if such a proof is within reach using current mathematics. However, any techniques used in such a proof could be useful in proving Goldbach's conjecture itself.

3 The Abstract Goldbach Conjecture

Now that Goldbach's conjecture has been studied in its original context, it is desirable to define it in non-integer contexts. For each of these, the conjecture will need to be defined. One possible method of defining the conjecture among multiple contexts would be to simply treat each definition independently, attempting to adapt the original conjecture as uniformly as possible for any given algebra. Instead, Goldbach's conjecture will be defined as abstractly as possible, and that abstraction will act as the archetype for our definition of the conjecture in all the number systems we study.

This archetype, called *The Abstract Goldbach Conjecture*, is analogous to Goldbach's Conjecture in $\mathbb{Z}$ while being as general as possible.

Conjecture 2.1, Goldbach's Conjecture as it is generally stated, is that every even integer can be written as a sum of two prime integers in at least one way. This is a very simple statement, but it is not ideal for abstraction for two reasons. First, it is a statement restricted to the even integers. Ideally, the conjecture would be applicable to all members of a set, since the notion of an even number may change in different contexts, and some sets may not contain even numbers at all. Second, the conjecture makes explicit mention of the addition operator. The integers themselves form a ring, for which both addition and multiplication are defined as binary operators. However, not all algebraic structures define addition as a binary operation. In Section 5, an algebraic structure for which addition is not a binary operator will be studied.

The Abstract Goldbach conjecture is adapted from Restatement 2.1, which is mathematically equivalent to Goldbach's Conjecture as it is originally stated (Conjecture 2.1). Restatement 2.1 states that every for every integer integer

$a > 1$ there exists an integer κ such that $(a \pm \kappa)$ are both prime integers. More generally, *every integer a is equidistant to two prime integers.*

Definition 3.1 (The Abstract Goldbach Conjecture). *If S is an infinite set for which $*$ is a binary operation, and S contains infinitely many prime elements, where any element of S has some finite number of elements of smaller magnitude than itself in S, then the Abstract Goldbach conjecture states that every element $e \in S$ greater than some initial element i is equidistant to two prime elements of S, where the smallest of those two prime elements is no greater than e, and the larger no smaller than e.*

Since is is not possible to dissasociate the notion of primality from multiplication, $*$ must be defined as a binary operator on the set S.

The magnitude function is labeled $M(x)$. Among the integers, our magnitude function for an integer a is $M(x) = |x|$, and an integer a is equidistant to two primes x, y, $x \leq y$ if there exists an integer κ, $0 \leq \kappa < a$ such that $(a - \kappa) = x$,$(a + \kappa) = y$. The integers satisfy all requirements for the Abstract Goldbach conjecture, and if the Abstract Goldbach conjecture holds for the integers, then Goldbach's conjecture is true in $\mathbb{Z}$.

It would not be apt to say that this abstraction removes all subjectivity when applying Goldbach's conjecture outside of the integers proper. After all, the notions of magnitude and equidistance need to be defined for each number system studied.

From here on, the term Goldbach's conjecture is not intended to mean the conjecture among the integers, but the statement of Goldbach's conjecture within whatever context is being discussed. For example, in the section on quaternions, the term Goldbach's conjecture is intended to mean the restate-

ment of Goldbach's conjecture among the quaternions.

The study of Goldbach's conjecture can now be extended outside of the integers, beginning with the Gaussian integers, those integral members of the Complex plane.

4 The Gaussian Integers

Having defined the Abstract Goldbach conjecture, it is now possible to study Goldbach's conjecture outside of the integers. Preceding such a discussion, an overview of the algebra of the Gaussian integers is offered.

4.1 Arithmetic of the Gaussian Integers

The set of Gaussian integers, denoted $\mathbb{Z}[i]$ consists of those numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$ and $i = \sqrt{-1}$. Like the integers, the Gaussian integers form a commutative ring with an identity element[2, 58]. Therefore the Gaussian integers satisfy Axioms 2.1-2.8 described in Section 2.1.

Definition 4.1. *If $z = a + bi$ is a Gaussian integer, a is called the real part of z, denoted $\Re(z)$. b is called the imaginary part of z, denoted $\Im(z)$.*

Example 4.1. *(a) If $z = 3 + 7i$, then $\Re(z) = 3$ and $\Im(z) = 7$. (b) If $z = -13 + i$,then $\Re(z) = -13$ and $\Im(z) = 1$.*

The Gaussian integers are a subset of the set $\mathbb{C}$ of Complex numbers, which are numbers of the form $a + bi$ where $a, b \in \mathbb{R}$. In turn, the integers are a subset of the Gaussian integers.

$$\mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{C} \tag{67}$$

Specifically, the integers are those Gaussian integers z where $\Im(z) = 0$. Sometimes when referring to an integer in $\mathbb{Z}[i]$, the imaginary part shall be omitted. For example, $3 + 0i$ abbreviated to 3.

The sum, difference and product of two Gaussian Integers are themselves Gaus-

sian integers

$$(a+bi)+(c+di) = (a+c)+(b+d)\cdot i$$
$$z_1+z_2 = (\Re(z_1)+\Re(z_2))+(\Im(z_1)+\Im(z_2))\cdot i$$
$$(a+bi)-(c+di) = (a-c)+(b-d)\cdot i$$
$$z_1-z_2 = (\Re(z_1)-\Re(z_2))+(\Im(z_1)-\Im(z_2))\cdot i$$
$$(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)\cdot i$$

Definition 4.2. *A Gaussian integer z_a **divides** $z_b \neq 0$ if there exists a Gaussian integer z_k such that $z_a \cdot z_k = z_b$. When z_a divides z_b it is denoted as $z_a | z_b$, otherwise, $z_a \nmid z_b$.*

Example 4.2. *$(1+i)|(3+7i)$ since if $z_k = (5+2i)$, $(1+i)\cdot z_k = 3+7i$.*

Definition 4.3. *The **magnitude** of a Gaussian integer $z = a+bi$, denoted $|z|$ is*

$$|z| = \sqrt{a^2+b^2} \tag{68}$$
$$= \sqrt{(\Re(z))^2+(\Im(z))^2} \tag{69}$$

Example 4.3. *(a) If $z = 3+7i$, then $|z| = \sqrt{3^2+7^2} = \sqrt{58}$. (b) If $z = -13+i$, then $|z| = \sqrt{(-13)^2+1} = \sqrt{170}$.*

Definition 4.4. *The **norm** of a Complex number $z = a+bi$, denoted $N(z)$ is*

$$N(z) = a^2+b^2 \tag{70}$$
$$= (\Re(z))^2+(\Im(z))^2 \tag{71}$$
$$= |z|^2 \tag{72}$$

Example 4.4. *(a) If $z = 3+7i$, then $N(z) = 3^2+7^2 = 58$. (b) If $z = -13+i$,*

then $N(z) = (-13)^2 + 1 = 170$.

Definition 4.5. *The* ***complex conjugate*** *of a Gaussian integer* $z = a + bi$, *denoted* $\overline{z}$, *is*

$$\overline{z} = a - bi \tag{73}$$

Example 4.5. *(a) Consider* $z = 3 + 7i$. *Then* $\overline{z} = 3 - 7i$. *(b) Consider* $z = -13 + i$. *Then* $\overline{z} = -13 - i$.

Corollary 4.1. *The product of a Gaussian integer* z *and its conjugate is its norm.*

$$z \cdot \overline{z} = (a + bi) \cdot (a - bi) = a^2 + b^2 = N(z) = |z|^2 . \tag{74}$$

Definition 4.6. *Those Gaussian Integers* z *with* $N(z) = 1$ *are the* ***units*** *of* $\mathbb{Z}[i]$. *The units of* $\mathbb{Z}[i]$ *are* $0 + i$, $0 - i$, $1 + 0i$, *and* $-1 + 0i$.*[7, 183]*

Definition 4.7. *The* ***associates*** *of a Gaussian integer* z *are those numbers of the form* $z \cdot z_u$, *where* z_u *is any of the units of* $\mathbb{Z}[i]$ *listed in Definition 4.6. Namely, the associates of any Gaussian integer* z *are* z,$-z$, zi *and* $-zi$.*[7, 183]*

Example 4.6. *Consider* $z = 3 + 7i$. *Its associates are itself,* $-3 - 7i$, $-7 + 3i$, *and* $7 - 3i$.

Theorem 4.1. *The product of the norms of two Gaussian Integers is equal to the norm of their product.*

$$N(z_1) \cdot N(z_2) = N(z_1 \cdot z_2) \tag{75}$$

Proof. Consider two Gaussian Integers $z_1 = a + bi$ and $z_2 = c + di$. Then $N(z_1) \cdot N(z_2) = (a^2 + b^2) \cdot (c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$. Now consider $N(z_1 \cdot z_2)$. The product $z_1 \cdot z_2 = (ac - bd) + (ad + bc) \cdot i$, so $N(z_1 \cdot z_2) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$ which is equal to $N(z_1) \cdot N(z_2)$. □

Theorem 4.1 can be applied indefinitely [7, 183] so that

$$N(z_1) \cdot N(z_2) \ldots N(z_k) = N(z_1 \ldots z_k) \tag{76}$$

Definition 4.8. *A Gaussian integer z is **prime** if its only divisors are itself and its associates. If z is not prime, it is **composite**. Should there be any ambiguity, those primes of $\mathbb{Z}$ will be referred to as the **rational primes** to distinguish them from the primes of $\mathbb{Z}[i]$.*

In the discussion that follows, z_p and z_q are reserved to denote Gaussian primes.

Theorem 4.2. *If the norm of a Gaussian Integer $z = a + bi$ is a rational prime p, then z is a Gaussian prime.*

Proof. (Adapted from [7, p183])
$N(z) = p$ where p is a rational prime. Assume z is a composite Gaussian integer, the product of two non-unit Gaussian integers, say z_1, z_2, so

$$z = z_1 z_2 \quad N(z_1) > 1 \quad N(z_2) > 1 \tag{77}$$

From Theorem 4.1,

$$N(z) = N(z_1)N(z_2) \tag{78}$$

$$p = N(z_1)N(z_2) \tag{79}$$

However, p is a rational prime, so it consists of a single non-unit factor. Therefore, one of $N(z_1), N(z_2)$ must be 1, and therefore, one of z_1, z_2 is a unit of $\mathbb{Z}[i]$. However, this contradicts Equ. 77. Therefore, z cannot be composite, so it is prime. □

The proof of the following theorem is omitted. This theorem will be required to

understand the relationship between the rational primes and the primes of $\mathbb{Z}[i]$.

Theorem 4.3 (Fermat's two squares theorem). *A rational prime p can be represented as a sum of two squares if and only if $p \equiv 1 \bmod 4$.[7, 219]*

$$\forall\, p \in \{4k+1, k \in \mathbb{Z}^+\} \quad \exists\, a, b \in \mathbb{Z} \quad p = a^2 + b^2 \tag{80}$$

Theorem 4.4. *If p is an odd rational prime and $p \equiv 3 \bmod 4$, it is prime in $\mathbb{Z}[i]$. Otherwise, it is composite in $\mathbb{Z}[i]$.*

Proof. All odd rational primes p are congruent to 1 or 3 mod 4. If $p \equiv 1 \mod 4$,then by Theorem 4.3 there exist integers a, b such that

$$p = a^2 + b^2 \tag{81}$$

Therefore, p can be factored as $(a - bi) \cdot (a + bi) = a^2 + b^2$, so p is composite in $\mathbb{Z}[i]$.

Suppose that $p \equiv 3 \bmod 4$ Assume that p is composite in $\mathbb{Z}[i]$. Then it is composed of two non-unit factors, say z_1, z_2, where $z_1 = a + bi$ and $z_2 = c + di$. Then the norm $N(p) = p^2 = N(z_1) \cdot N(z_2)$ by Theorem 4.1, so $N(z_1) = N(z_2) = p$ (since z_1, z_2 are not units). Therefore, p must be composable as a sum of two squares, since $N(z_1) = a^2 + b^2$ and $N(z_2) = c^2 + d^2$. However, by Theorem 4.3, p cannot be composed as a sum of squares, since $p \not\equiv 3 \bmod 4$. Therefore, p cannot be composite, so it is prime in $\mathbb{Z}[i]$. □

Theorem 4.5. *If z is a Gaussian prime, then so are the associates of z.*

Proof. If $\Re(z) > 0, \Im(z) > 0$, then z is prime if $N(z)$ is a rational prime. The associates of z are the composition $z \cdot z_u$, where z_u is any of the units of $\mathbb{Z}[i]$. Since $N(z_u) = 1$,

$$N(z) = N(z) \cdot N(z_u) \tag{82}$$

and therefore, if $N(z) = p$, p prime in $\mathbb{Z}$, the $N(z \cdot z_u) = p$ as well, and hence $z \cdot z_u$ is prime in $\mathbb{Z}[i]$.

If one of $Re(z), \Im(z) = 0$, then z is prime if the non-zero part of z is a rational prime leaving a remainder of 3 upon division by 4. If p is such a prime, then $p \cdot p_u$, any of $-p, pi, -pi$, will have a zero part and a rational prime part as well, so it remains irreducible into smaller factors, and is therefore prime. □

By the same argument, the conjugate of a Gaussian prime is prime as well, since $N(z) = N(\overline{z})$.

To recap, the primes of $\mathbb{Z}[i]$ are [7, p183-184]

- All $z = a + bi$ where $a, b > 0$ and $N(a + bi)$ is a rational prime.
- All $z = a + bi$ where one of $a, b = 0$ and the other is a rational prime congruent to 3 mod 4.
- The associates (and conjugates) of the above

Theorem 4.6. *There exist an infinity of Gaussian primes.*

Proof. From Theorem 4.3 it is known that any rational prime $p \equiv 1 \bmod 4$ can be written as a sum of two squares. From Theorem 5.4 (Dirichlet's Theorem) it is known that there exist an infinity of primes $p \equiv 1 \bmod 4$. Therefore, any of the infinity of primes $p \equiv 1 \bmod 4$, there exist integers a, b such that $p = a^2 + b^2$. Since $a^2 + b^2$ is the norm of a Gaussian integer $z = a + bi$, and since any Gaussian integer with a prime norm is a Gaussian prime, there exist an infinity of Gaussian primes. □

Definition 4.9. *A Gaussian integer z is said to be **even** if its norm $N(z)$ is an even integer. If a Gaussian integer is not even, it is odd.*

If the norm $N(z)$ is even then it can be rewritten as $N(2) \cdot N(z')$ by Theorem 4.1. Those Gaussian integers with a norm of 2 are only $1+i$ and its associates. So those numbers with an even norm will have an associate of $1+i$ in their unique prime factorizations.

Theorem 4.7. *A Gaussian integer $z = a + bi$ is even if $a + b$ is even[8, 81].*

Proof. If $a + b$ is even, then either both a and b are even, or they are both odd. Either way, the norm $N(z) = a^2 + b^2$ will have to be even, since squaring a number does not change its parity. If the norm is even, then z is even by Definition 4.9. □

Theorem 4.8. *The Gaussian prime $1 + i$ and associates are the only even Gaussian primes.*

Proof. Assume there is an even Gaussian prime $z' = a + bi$, where one or both of $a, b > 1$. If z' is even then its norm is even, so one of the prime factors of z' is $1 + i$ or one of its associates. But if $z' \neq 1 + i$ has $1 + i$ in its unique prime factorization, then clearly z' is a composite number, which is a contradiction. □

From Theorem 4.8 it is evident that any Gaussian prime $z_p \neq 1 + i$ is odd.

Theorem 4.9. *The sum of any two Gaussian primes $z_p, z_q \neq 1 + i$ is an even Gaussian integer.*

Proof. Suppose $z_p = a + bi$ and $z_q = c + di$. It must shown that their sum $z_\varepsilon = (a+c) + (b+d) \cdot i$ is an even Gaussian integer. Since z_p, z_q are both prime, by Theorem 4.8 the sum $a + b$ is odd and so is the sum $c + d$. However if $a + b$ and $c + d$ are odd, then the sum $(a + b + c + d)$ is even. Therefore, the sum of the real and imaginary parts of z_ε is even, and hence z_ε itself must be an even Gaussian integer by Theorem 4.7. □

The following proof is analogous to the division algorithm of the integers (Theorem 2.3).

Theorem 4.10. *For every pair of Gaussian integers z, z_1, with $z_1 \neq 0$ there exist Gaussian integers z_m, z_r such that*

$$z = z_m \cdot z_1 + z_r \quad N(z_r) < N(z_1) \tag{83}$$

Proof. (Adapted from [7, p85])
Since z_1 is assumed to be non-zero, there is no doubt that $\frac{z}{z_1}$ is a Complex number[1], say

$$\frac{z}{z_1} = R + Si \tag{84}$$

Where R, S are real. Clearly there exist two integers x, y such that

$$|R - x| \leq \frac{1}{2} \tag{85}$$

$$|S - y| \leq \frac{1}{2} \tag{86}$$

since in the least optimistic case, a real value would be $\frac{1}{2}$ away from the closest integer. Consider the difference

$$z' = \left| \frac{z}{z_1} - (x + yi) \right| \tag{87}$$

$$= |(R - x) + (S - y) \cdot i| \tag{88}$$

$$= ((R - x)^2 + (S - y)^2)^{\frac{1}{2}} \leq \frac{1}{\sqrt{2}} \tag{89}$$

The inequality stemming from the fact that both $(R - x), (S - y) \leq \frac{1}{2}$.

[1] Here it is assumed that the reader has elementary knowledge of the Complex numbers

Let $\kappa = x + yi$ and $z_r = z - \kappa \cdot z_1$. Therefore,

$$\left| \frac{z}{z_1} - \kappa \right| \leq \frac{1}{\sqrt{2}} \tag{90}$$

Squaring both sides yields

$$N(\frac{z}{z_1} - \kappa) \leq \frac{1}{2} \tag{91}$$

Multiplying both sides by $N(z_1)$ yields

$$N(z_1) \cdot N(\frac{z}{z_1} - \kappa) \leq \frac{1}{2} \cdot N(z_1) \tag{92}$$

Which by Theorem 4.1 yields

$$N(z - z_1 \cdot \kappa) \leq \frac{1}{2} \cdot N(z_1) \tag{93}$$

$$N(z_r) < N(z_1) \tag{94}$$

□

Definition 4.10. *If z, z_a, z_b are Gaussian integers and $z|z_a, z|z_b$, then z is said to be a common divisor of z_a, z_b. If z is the Gaussian integer of largest norm which divides both z_a, z_b, then z is said to be the greatest common divisor of z_a, z_b, denoted $(z_a, z_b) = z$. If z_a, z_b share no common factor other than units then $(z_a, z_b) = 1$ and it is said that z_a, z_b are* ***relatively prime.***

Theorem 4.11. *If $(z_1, z_2) = 1$ and $z_1|z_2 z_3$, then $z_1|z_3$.*

Proof. Since z_1, z_2 share no common divisor other than 1, multiplying them both by z_3 leads z_3 to be their greatest common divisor. [7, p186]

$$(z_1 z_3, z_2 z_3) = z_3 \tag{95}$$

The theorem assumes that $z_1|z_2z_3$, and trivially, $z_1|z_1z_3$. Since z_1 divides them both, it must divide their greatest common divisor, which is z_3. So $z_1|z_3$. □

Theorem 4.12. *If z_p is a Gaussian prime and z_1, z_2 are Gaussian integers where $z_p|z_1z_2$ then either $z_p|z_1$ or $z_p|z_2$ (or both).*

Proof. Let $(z_p, z_1) = z_d$. Then $z_d|z_p$ and $z_d|z_1$. Since $z_d|z_p$, where z_p is prime, z_d is either a unit or an associate of z_p. If it is a unit, then $(z_p, z_1) = 1$, and by Theorem 4.11 $z_p|z_2$. Otherwise, $(z_p, z_1) = z_p$, and therefore, $z_p|z_1$. □

Corollary 4.2. *If z_p is a Gaussian prime and $z_1z_2 \ldots z_m$ are Gaussian integers where $z_p|z_1z_2 \ldots z_m$, then $z_p|z_i$ for some i, $1 \leq i \leq m$.*

Proof. (By Induction)
As a base case, let $m = 2$. Then it must be shown that if $z_p|z_1z_2$, $z_p|z_1$ or $z_p|z_2$ (or both). But this is already known from Theorem 4.12. Next, from the assumption that the theorem holds up to $m = n$, it must be shown that the theorem also holds for $m = n + 1$.

If the theorem is true for n, then $z_p|z_1z_2 \ldots z_n$ and $p|z_i$ for some i, $1 \leq i \leq n$. It must be shown that under this assumption, it is also true that if $z_p|z_1z_2 \ldots z_{n+1}$, then $z_p|z_j$ for some j, $1 \leq j \leq n + 1$. However, it is already known that $z_p|z_i$, and i lies within the bounds for j, so when $j = i$, $z_p|z_j$, so the theorem is satisfied. □

Corollary 4.3. *If $z_p, \pi_1, \pi_2, \ldots \pi_m$ are Gaussian primes where $z_p|\pi_1\pi_2 \ldots \pi_m$, then $z_p = \pi_i$ for some i, $1 \leq i \leq m$.*

Proof. From Theorem 4.2 it is known that $z_p|\pi_i$ for some i, $1 \leq i \leq m$. So there must exist some Gaussian integer z_k such that

$$z_p \cdot z_k = \pi_i \tag{96}$$

However, π_i is prime, and hence its only divisors are the units of $\mathbb{Z}[i]$ and its own associates. Therefore, if z_k is not a unit of $\mathbb{Z}[i]$, π_i is composite, which is a contradiction. So z_k must be a unit, and $z_p = \pi_i$. □

Theorem 4.13. *Every Gaussian integer z with $N(z) > 1$ is divisible by some Gaussian prime.*

Proof. (Adapted from [7, p184])
If z is prime, then clearly it is divisible by a prime (namely itself), which satisfies the theorem. Otherwise, it must be the product of at least two Gaussian integers, say z_1, z_a, neither of which are units.

$$z = z_1 z_a \quad N(z_1) > 1 \quad N(z_a) > 1 \tag{97}$$

where $N(z) = N(z_1) \cdot N(z_a)$ By Theorem 4.1 so

$$1 < N(z_1) < N(z) \tag{98}$$

z_1 is not a unit so it is either prime or composite. If it is prime then z is divisible by z_1, which satisfies the theorem. Otherwise it is composite and consists of two Gaussian integers, say z_2, z_b. So

$$z_1 = z_2 z_b \quad N(z_2) > 1 \quad N(z_b) > 1 \tag{99}$$

where

$$1 < N(z_2) < N(z_1) \tag{100}$$

At any given iteration, z_i will either be prime, in which case the theorem is satisfied, or composite, in which case the same method is applied once more. In the least optimistic case, the method is applied until $N(z_i) = 2$, which will

eventually occur, since applying this method perpetually decreases the norm, but that norm will never be less than 2, since z_i is never a unit. Since those Gaussian integers with a norm of 2 are $1+i$ and its associates, which are prime, the theorem will be satisfied if $N(z_i)$ reaches 2.

□

Theorem 4.14. *Every Gaussian integer z with $N(z) > 1$ can be represented as a product of Gaussian primes.*

Proof. (Adapted from [7, p184]) From Theorem 4.13 it is known that z is divisible by some Gaussian prime, say π_1. So

$$z = \pi_1 \cdot z_1 \quad N(\pi_1) > 1 \tag{101}$$

where z_1 is some Gaussian integer where $N(z_1) < N(z)$ (since π_1 is not a unit). If z_1 is a unit or a prime, z has been written as a product of primes and the theorem is satisfied. Otherwise, z_1 is composite, and by Theorem 4.13 it must be divisible by a prime, say π_2, so

$$z_1 = \pi_2 \cdot z_2 \quad N(\pi_2) > 1 \tag{102}$$

where z_2 is a Gaussian integer where $N(z_2) < N(z_1)$ so if z_2 is neither a unit nor a Gaussian prime

$$z = \pi_1 \pi_2 z_2 \tag{103}$$

and this process is also applied to z_2. The process is applied repeatedly until z_i is a prime or a unit, at which point

$$z = \pi_1 \pi_2 \ldots \pi_{i-1} z_i \tag{104}$$

is a product of primes. □

Theorem 4.15 (The Fundamental Theorem of Arithmetic For Gaussian Integers). *Every Gaussian integer whose norm is greater than one can be written as a product of primes in a unique way.*

Proof. It has already been shown that every Gaussian integer can be written as a product of prime Gaussian integers. Next, it must be shown that this representation is unique, apart from order and units.

This proof is analogous to Theorem 2.12 of the integers. To simplify notation in this proof, p,q are used to denote Gaussian primes.

Suppose some Gaussian integer z can be written as a product of Gaussian primes in two different ways

$$z = p_1 \cdot p_2 \dots p_m = q_1 \cdot q_2 \dots q_n \tag{105}$$

Assume that $m \leq n$, and that the primes are ordered in such a way so that

$$N(p_1) \leq N(p_2) \leq \dots N(p_m), \quad N(q_1) \leq N(q_2) \leq \dots N(q_n) \tag{106}$$

since $p_1 \cdot p_2 \dots p_m = p_1 \cdot k_1$, where $k_1 = p_2 \dots p_m$, it must be that $p_1 | q_1 \cdot q_2 \dots q_n$ (See Definition 4.2). By Corollary 4.2, p_1 then must divide exactly one of $q_1 \dots q_n$, so $N(p_1) \geq N(q_1)$. Similarly, since $q_1 \cdot q_2 \dots q_n = q_1 \cdot k_2$, where $k_2 = q_2 \dots q_n$, so $q_1 | p_1 \cdot p_2 \dots p_m$. By Corollary 4.2, q_1 must divide exactly one of $p_1 \dots p_n$, so $N(q_1) \geq N(p_1)$. But earlier it was stated that $N(p_1) \geq N(q_1)$, and now that $N(q_1) \geq N(p_1)$, so it must be true that $N(q_1) = N(p_1)$. Therefore, $q_1 = p_1$, and these equal factors cancel out, leaving

$$p_2 \dots p_m = q_2 \dots q_n \tag{107}$$

This method can be applied repeatedly, canceling p_i with q_i for each i up to $\min(m, n)$. If $m = n$, all factors cancel out, so clearly $p_i = q_i$ for all i up to m. Otherwise, suppose $m < n$, the first m elements on each side are canceled out and

$$1 = q_{m+1} \cdot q_{m+2} \cdots q_n \tag{108}$$

This equation is impossible, since $q_{m+2} \ldots q_n$ are all Gaussian primes, and the smallest Gaussian prime is $1+i$. Therefore, m and n must be equal, and $p_i = q_i$ for all i up to m, and the theorem is complete. □

4.2 Goldbach's Conjecture in $\mathbb{Z}[i]$

Goldbach's Conjecture among the Gaussian Integers was studied by Holben and Jordan in a 1968 paper called *The twin prime problem and Goldbach's conjecture in the Gaussian Integers.* In it, they suggest a restatement for the conjecture in $\mathbb{Z}[i]$ and test it empirically for a small set of values. Theirs may be the sole paper among mathematical literature to study Goldbach's conjecture outside of the integers proper.

A reasonable first attempt at restating Goldbach's Conjecture among the Gaussian integers would be to directly adapt the original conjecture of the integers (Conjecture 2.1) to the Gaussian integers as follows:

Restatement 4.1. *Every even Gaussian integer z_ε can be composed as the sum of two Gaussian primes in at least one way.*

$$\forall\, z_\varepsilon \quad \exists\, z_p, z_q \quad z_\varepsilon = z_p + z_q \tag{109}$$

However, as Holben and Jordan mention, this is not an appropriate restatement

of the conjecture. For consider two Gaussian primes $z_p = a + bi$ and $z_q = -c - di$. Then $z_\varepsilon = z_p + z_q = (a - c) + (b - d)i$. This could be rewritten as $z_\varepsilon = z_p - (-z_q)$, where $-z_q$ is prime by Theorem 4.5. However, this means that Restatement 4.1 will be satisfied as long as z_ε can be written *as a sum or difference of primes.* Clearly, this is a not an appropriate restatement of Goldbach's conjecture in $\mathbb{Z}[i]$.

Holben and Jordan then set out to define the conjecture among the Gaussian integers in such a way that would not allow both sum or differences of primes as valid solutions.

Restatement 4.2. *Every even Gaussian integer z_ε can be composed as a sum of two Gaussian primes z_p, z_q, where the angles $\measuredangle z_p 0 z_\varepsilon$, $\measuredangle z_\varepsilon 0 z_q \leq 45°$, where 0 is the point of origin.*

Holben and Jordan choose Restatement 4.2 as their definition of Goldbach's conjecture in $\mathbb{Z}[i]$, and confirm its truth for a small set of values. Although the path taken by Holben and Jordan to adapt Goldbach's conjecture to the Gaussian integers is acceptable, it is not equivalent to the definition chosen in this work, which is presently proposed.

Rather than study Goldbach's conjecture for all Gaussian integers, the study can be limited to those Gaussian integers of the form $z = a+bi$, where $0 \leq a \leq b$. Every Gaussian integer is an associate or conjugate of a Gaussian integer of such a form, and from here on, when z is of this form, it is said to be of *proper form.* For example, $z = 2 + 3i$ is of proper form, but $z = 3 + 2i$ is not.

Theorem 4.16. *Any Gaussian integer z is an associate, conjugate or conjugate associate of a Gaussian integer of proper form.*

Proof. For any $z = a + bi$, the eight associates and their conjugates are as

follows:

$$(a+bi)\cdot 1 = a+bi$$

$$\overline{(a+bi)} = a-bi$$

$$(a+bi)\cdot i = -b+ai$$

$$\overline{(-b+ai)} = -b-ai$$

$$(a+bi)\cdot -1 = -a-bi$$

$$\overline{(-a-bi)} = -a+bi$$

$$(a+bi)\cdot -i = b-ai$$

$$\overline{(b-ai)} = b+ai$$

If $z = a+bi$ where a, b are both positive, then if z is not of the proper form, $\overline{z\cdot -i} = b+ai$ is. If $z = a+bi$ and a, b are both negative, then one of $z\cdot -1 = -a-bi, \overline{z\cdot i} = -b-ai$ will be of the proper form. If $z = a+bi$ is such that one of a, b is negative, and the other positive, then one of $\overline{z\cdot 1} = a-bi$, $z\cdot i = -b+ai$, $z\cdot -i = b-ai$, $\overline{z\cdot -1} = -a+bi$ will be of the proper form. □

Theorem 4.17, to follow, states that if Goldbach's conjecture is true for a Gaussian integer z, it is also true for the associates and conjugates of z. Therefore, if Goldbach's conjecture holds for all Gaussian integers $z = a+bi, 0 \leq a \leq b$, it holds for all Gaussian integers. In effect, the Gaussian plane can be cut into eight symmetrical slices, and the study here is limited to a single slice.

The magnitude function for a Gaussian integer $z = a+bi$ is $M(z) = N(z) = a^2+b^2$, and equidistance for $z = a+bi$, $0 \leq a \leq b$ is defined as follows:

Definition 4.11. *A Gaussian integer $z = a+bi$, $0 \leq a \leq b$ is said to be* ***equidistant*** *to two Gaussian integers z_1, z_2, $N(z_1) \leq N(z_2)$ if there exists a Gaussian integer $z_\kappa = c+di, 0 \leq c \leq d$, $N(z_\kappa) < N(z)$ such that $(z - z_\kappa) =$*

$z_1, (z + z_\kappa) = z_2$.

For the remainder of this section, and the section regarding the weaker statements, any Gaussian integer z or z_κ can be assumed to be of the proper form, and $0 \leq N(z_\kappa) < N(z)$.

Conjecture 4.1 (Goldbach's conjecture among the Gaussian integers)**.** *Every Gaussian integer z, $N(z) > 1$ is equidistant to two Gaussian primes, z_p, z_q.*

$$\forall\, z, N(z) > 1 \quad \exists\, z_\kappa \quad z + z_\kappa = z_p, z - z_\kappa = z_q \tag{110}$$

If Conjecture 4.1 is satisfied for a Gaussian integer z, z is said to satisfy Goldbach's conjecture.

Example 4.7. *$z = 2 + 3i$ satisfies Goldbach's conjecture, since if $h_k = 0 + 2i$, $(z + z_\kappa), (z - z_\kappa)$ are prime Gaussian integers, with norms 5 and 29 respectively.*

Theorem 4.17. *If a Gaussian integer z satisfies Goldbach's conjecture, then so do its associates.*

Proof. If z satisfies Goldbach's conjecture, it is equidistant to two primes, $z + z_\kappa = z_p$ and $z - z_\kappa = z_q$. Let z_u be any of the unities of $\mathbb{Z}[i]$. Then $z \cdot z_u + z_\kappa z_u = z_u(z + z_\kappa)$ which has norm $N(1) \cdot N(z + z_\kappa) = N(z + z_\kappa)$, which is prime. Similarly, $z_u z - z_u z_\kappa = z_u(z - z_\kappa)$ has norm $N(1) \cdot N(z - z_\kappa) = N(z - z_\kappa)$ which is prime. So any associate of $z \cdot z_u$ of z is equidistant to two primes, $z_p \cdot z_u$ and $z_q \cdot z_u$. □

One difference between this definition and that of Holben and Jordan is that it is not a statement about the even Gaussian integers, but about all Gaussian integers, regardless of parity. Suppose Conjecture 4.1 were true for all Gaussian integers. Then for any Gaussian integer z, there exists a Gaussian integer z_κ such that $(z + z_\kappa)$, $(z - z_\kappa)$ are prime. Therefore, $(z + z_\kappa) + (z - z_\kappa) = 2z$ is

composable as a sum of two prime numbers. However, those Gaussian integers of the form $2z$ do not constitute the set of all even Gaussian integers, since by Theorem 4.7, a Gaussian integer z is even if $2|(\Re(z) + \Im(z))$. For example $z_1 = 2 + 4i$ is even and can be rewritten as $z_1 = 2(1 + 2i)$, but $z_2 = 3 + 5i$ is also even, even though 2 cannot be factored out as for z_1. Therefore, the definition of Goldbach's conjecture proposed by Holben and Jordan is in effect a stronger statement than the definition extending from the Abstract Goldbach conjecture.

Definition 4.12. *The Goldbach number for a Gaussian integer z, denoted $G(z)$, represents the number of Gaussian integers z_κ that exist such that $(z \pm z_\kappa)$ are both Gaussian primes.*

Example 4.8. *(a) $G(1+5i) = 3$, since for $z_k = 1+2i, 1-2i$ and i respectively, $(z \pm z_\kappa)$ are both prime. See Figure 4 for a visual representation of this example. (b) Similarly, $G(23 + 30i) = 23$.*

Figure 4 (a) and (b) visually depict Goldbach's Conjecture in $\mathbb{Z}[i]$ on a plane, where, as by convention, the real part of a Gaussian integer is represented on the x-axis and the imaginary part on the y-axis. Figure 4 (a) depicts the various solutions to Goldbach's Conjecture for $z = 1 + 5i$, while (b) does the same for $z = 3 + 7i$.

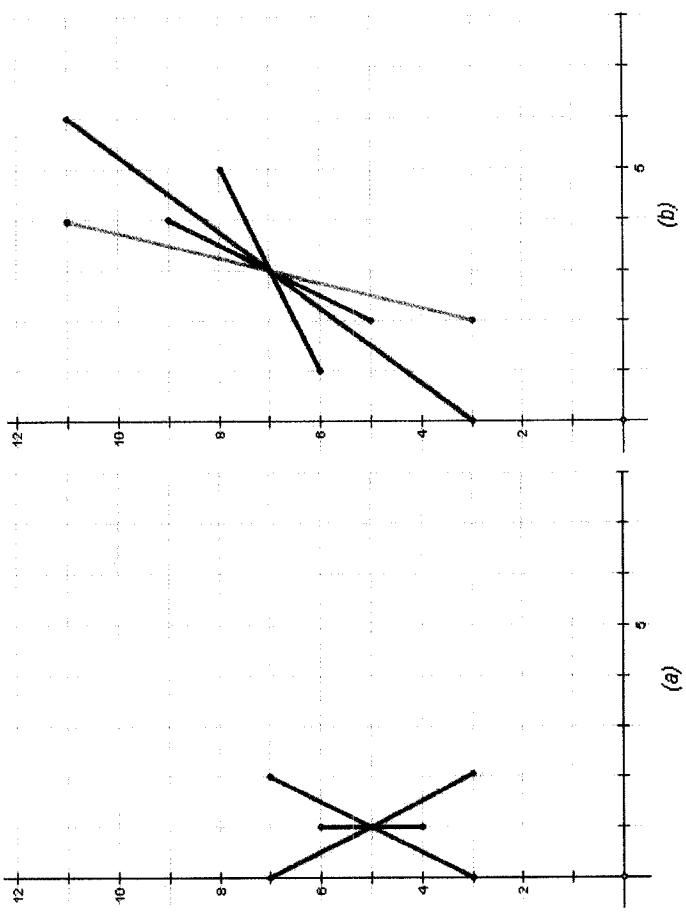

Figure 4: A Visualization of Goldbach's Conjecture in $\mathbb{Z}[i]$

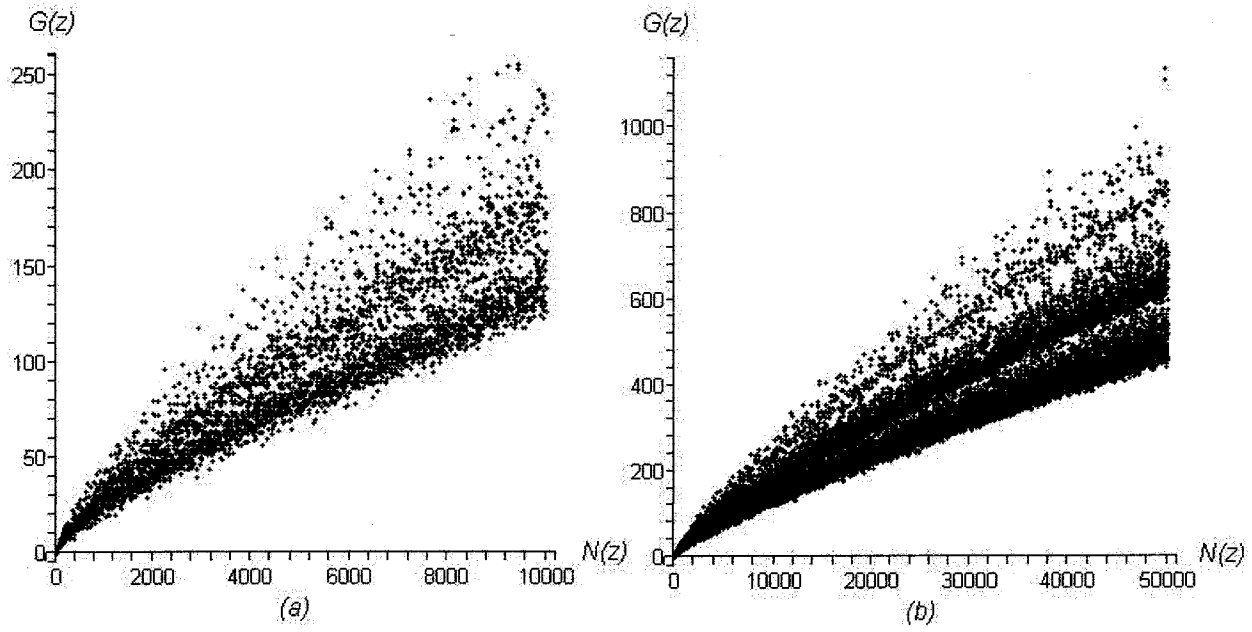

Figure 5: Goldbach's Comet in $\mathbb{Z}[i]$

Goldbach's conjecture in $\mathbb{Z}[i]$ can be restated as follows:

Restatement 4.3. *For any Gaussian integer z with $N(z) > 1$, $G(z) \geq 1$*

Figure 5 (a) and (b) graph $N(z)$ (x-axis) with respect to $G(z)$ (y-axis) for all Gaussian integers $z = a + bi, 0 \leq a \leq b$ with norms no greater than 10000 and 50000 respectively.

Theorem 4.18. *If z is a prime Gaussian integer, it satisfies Goldbach's Conjecture in $\mathbb{Z}[i]$.*

Proof. If z is prime, then it is trivially equidistant to two primes, since when $z_\kappa = 0 + 0i$, $(z \pm z_k) = z$, which is prime by the definition of the theorem. □

Theorem 4.19. *if $(z \pm z_k)$, are both prime, then $(z, z_k) = 1$.*

Proof. Suppose it were otherwise so that z, z_k share some common factor, say m. So $z + z_k = z_p = x \cdot m$ and $z - z_k = z_q = y \cdot m$. However, $(z + z_k), (z - z_k)$ are two primes, distinct from one another, so it impossible for them to share a common factor. □

Theorem 4.20. *If Goldbach's Conjecture is true in $\mathbb{Z}[i]$, then the square of any Gaussian integer can be composed as the sum of a Gaussian semiprime and a Gaussian integer square.*

$$\forall z \quad \exists\, z_p, z_q, z_\kappa \quad z^2 = z_p \cdot z_q + z_\kappa^2 \tag{111}$$

Proof. If Goldbach's Conjecture is true in $\mathbb{Z}[i]$, then there exists a Gaussian integer z_k such that $(z \pm z_k)$ are both prime. Consider the product $(z + z_k) \cdot (z - z_k) = z^2 - z_k^2$, where $(z \pm z_k)$ are both primes. By algebraic manipulation the theorem holds, assuming the truth of Goldbach's conjecture. □

4.2.1 Is Goldbach's Conjecture True in $\mathbb{Z}[i]$?

The challenges present in proving Goldbach's conjecture in $\mathbb{Z}[i]$ are similar to those of solving it in $\mathbb{Z}$. At the core, the conjecture is heavily related to the distribution of prime numbers among the Gaussian integers, a distribution that possesses an overarching structure, but is chaotic upon close examination. Again, the study of Goldbach's conjecture here is relegated to empirical observation.

Using the software tools developed for this work, Goldbach's conjecture in $\mathbb{Z}[i]$, Conjecture 4.1, was tested empirically for all Gaussian integers $z = a + bi$, $0 < a \leq b$ with $1 < N(z) \leq 1000000$. There are no counterexamples to Goldbach's conjecture within this range.

4.3 Weaker Statements of Goldbach's Conjecture in $\mathbb{Z}[i]$

As among the integers, it is possible to compute the mobius function among the Gaussian integers. Here, two weaker statements of Goldbach's conjecture similar to those proposed for the integers are studied.

Definition 4.13. *A Gaussian integer z is **squarefree** if its unique prime factorization $z = \pi_1^{\alpha}\pi_2^{\beta} \cdot \pi_3^{\chi} \ldots \pi_m^{\delta}$ has no exponent $\alpha, \beta, \ldots$ etc greater than one.*

Example 4.9. *(a) $z = 5 + 5i$ is squarefree since its unique factorization, $(1 + 2i) \cdot (1 - 2i) \cdot (1 + i)$ contains no exponent greater than one. $z = -4 + 2i$ is squarefull, since its unique prime factorization, $(1 + i)^2 \cdot (1 + 2i)$ has a square factor.*

Definition 4.14. *The **Mobius Function** for a Gaussian integer z, denoted $\mu(z)$, evaluates to 1 if z is a unit, 0 if z is squarefull, and to $(-1)^k$ if z is a squarefree product of k Gaussian primes.*

$$\mu(z) = \begin{cases} 1, & \textit{if } N(z) = 1 \\ (-1)^k, & \textit{if } z \textit{ is a squarefree product of } k \textit{ Gaussian primes} \\ 0, & \textit{otherwise} \end{cases} \tag{112}$$

Example 4.10. *Consider $z = 5 + 5i$ as in Example 4.9(a) above. $\mu(z) = -1$ since z is a squarefree product of three primes. (b) Consider $z = -4 + 2i$ as in Example 4.9(b) above. $\mu(z) = 0$, since z is squarefull.*

Conjecture 4.2. *Every Gaussian integer is equidistant to two Gaussian integers which evaluate to -1 in the mobius function.*

$$\forall\, z \quad \exists\, z_k \quad \mu(z + z_k) = -1,\ \mu(z - z_k) = -1 \tag{113}$$

Definition 4.15. *Let $G^{\mu}(z)$ denote the number of Gaussian integer pairs z_1, z_2 equidistant to z such that $\mu(z_1) = -1$, $\mu(z_2) = -1$.*

Conjecture 4.3. *Every Gaussian integer is equidistant to two squarefree Gaussian integers.*

$$\forall\, z \quad \exists\, z_k \quad \mu(z + z_k) \neq 0,\ \mu(z - z_k) \neq 0 \tag{114}$$

Definition 4.16. *Let $G^{s}(z)$ denote the number of integer pairs z_1, z_2 equidistant to z such that $\mu(z_1) \neq 0, \mu(z_2) \neq 0$.*

Theorem 4.21.

$$\forall z \quad G(z) \leq G^{\mu}(z) \leq G^{s}(z) \tag{115}$$

Proof. If $G(z) = x$, then $G^{\mu}(z) \geq x$, since any z_κ such that $(z \pm z_\kappa)$ is prime also satisfies $\mu(z \pm z_\kappa) = -1$. Similarly, if $G^{\mu}(z) = y$, $G^{s}(z) \geq y$, since any z_κ satisfying $\mu(z \pm z_\kappa) = -1$ satisfies $\mu(z \pm z_\kappa) \neq 0$. □

Figure 6(a) and (b) graph $N(z)$ with respect to $G(z)$ in red, $N(z)$ with respect to $G^{\mu}(z)$ in blue, and $N(z)$ with respect to $G^{s}(z)$ in green, for all z with norms less than 1000 and 10000 respectively.

Definition 4.17. *Let $G_{min}(z) = N(z_\kappa)$, where z_κ is the Gaussian integer with the smallest norm such that $(z \pm z_\kappa)$ are both prime. Let $G^{\mu}_{min}(z) = N(z_\kappa)$ where z_κ is the Gaussian integer with the smallest norm such that $\mu(z \pm z_\kappa) = -1$. Let $G^{s}_{min}(z) = N(z_\kappa)$ where z_κ is the Gaussian integer with the smallest norm such that $\mu(z \pm z_\kappa) \neq 0$.*

Example 4.11. *(a) If $z = 1 + 5i$ (as in Figure 4(a)), $G_{min}(z) = 1$, since when $z_k = 0 + i$, $(z \pm z_k)$ are both prime, and $N(0 + i) = 1$, and there is no integer z_k with norm less than 1 which satisfies this property. (b) If $z = 3 + 7i$ (as in Figure 4(b)), $G_{min}(z) = 5$, since when $z_k = 2 + i$, $(z \pm z_k)$ are both prime, and $N(2 + i) = 5$, and there is no integer z_k with norm less than 5 which satisfies this property.*

Figure 7(a) and (b) graph the Gaussian integr z with respect to $G_{min}(z)$ in red, z with respect to $G^{\mu}_{min}(z)$ in blue, and z with respect to $G^{s}_{min}(z)$ in green, for all z up to 1000 and 10000 respectively.

Theorem 4.22.

$$\forall z \quad G^{s}_{min}(z) \leq G^{\mu}_{min}(z) \leq G_{min}(z) \tag{116}$$

Proof. If $G_{min}(z) = x$, then there exists a Gaussian integer z_κ, $N(z_\kappa) = x$ such that $(z \pm z_\kappa)$ are both Gaussian primes. Then $\mu(z \pm z_\kappa) = -1$, since $(z \pm z_\kappa)$ are prime and for any prime z_p, $\mu(z_p) = -1$. Therefore, $G_{min}(z) \leq G^{\mu}_{min}(z)$. If $G^{\mu}_{min}(z) = y$, then there exists a Gaussian integer z_κ, $N(z_\kappa) = y$ such that $\mu(z \pm z_\kappa) = -1$. Clearly then, $\mu(z \pm z_\kappa) \neq 0$, so $G^{\mu}_{min}(z) \leq G^{s}_{min}(z)$. □

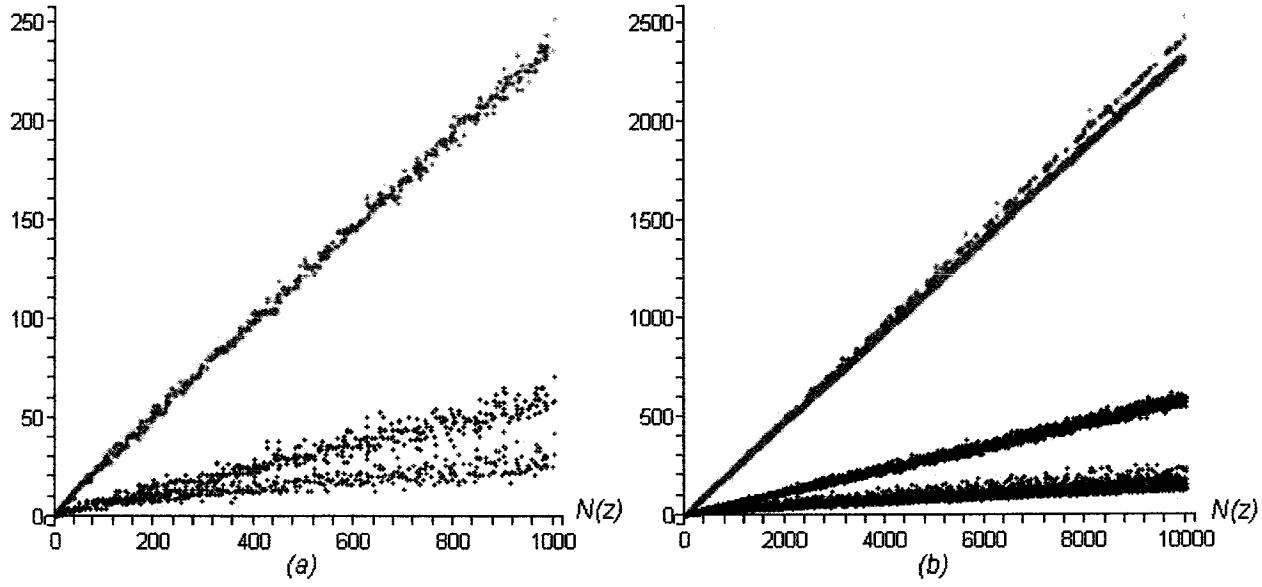

Figure 6: Goldbach's Conjecture and the Two Weaker Statements

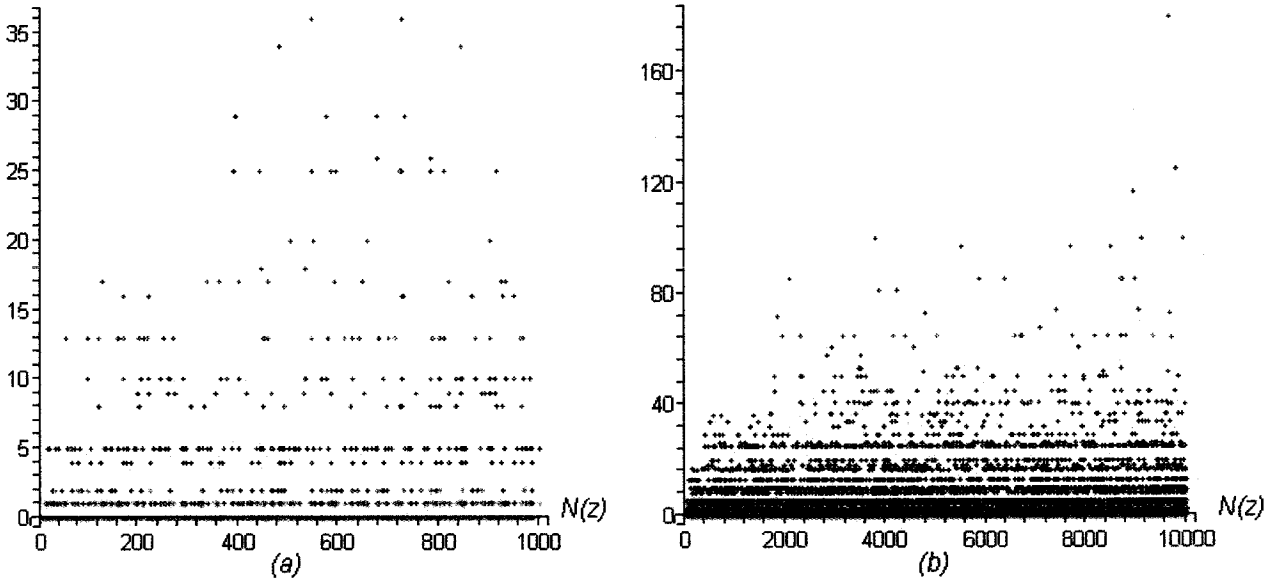

Figure 7: Minimal Distances for Goldbach's Conjecture and the Weaker Statements

4.3.1 A Discussion Regarding the Weaker Statements

Perhaps the most striking result here is the similarity between Figure 6, Goldbach's Comet and the weaker statements in $\mathbb{Z}[i]$ and its analogue among the integers, Figure 3. Their similarity lends credence to the abstract Goldbach conjecture, their coinciding structures suggesting that the essence of Goldbach's conjecture has not been lost in translation. All three conjectures appear to hold true, tending to have an increasing number of solutions as magnitude increases.

Although Conjecture 4.3 is not proven here, it is almost certainly possible to prove using the current body of mathematics. However, Conjecture 4.2 is probably not solvable at present. As in $\mathbb{Z}$, each are a step towards a proof of Goldbach's conjecture.

Figure 7 emphasizes the relative strength of each conjecture. The smallest z_κ satisfying Theorem 4.3 for a Gaussian z, in green, tends to be smaller than the smallest z_κ satisfying Conjecture 4.2 for an integer a, in blue, which in turn tends to be smaller than the smallest z_κ satisfying Goldbach's conjecture in $\mathbb{Z}[i]$, in red. Table 4 lists the average G_{min} values for all Gaussian integers with norms no greater than 1000 and 5000 respectively.

AVG for z up to	1000	5000
$G_{min}(z)$	5.76	9.28
$G^{\mu}_{min}(z)$	3.42	3.17
$G^{s}_{min}(z)$	0.40	0.39

Table 4: Average G_{min} values in $\mathbb{Z}[i]$

Since Goldbach's conjecture is satisfied for all $z = a + bi$ with $2 \leq N(z) \leq 1000000$, Conjectures 4.2 and 4.3 are also satisfied in this range (By Theorem 4.21).

5 Integer Subsets

Adapting Goldbach's conjecture to the Gaussian integers involved the transition from the number line to the number plane. Returning to the number line, particular subsets of the integers are studied here. The algebraic properties of these sets differ significantly from those studied thus far.

This section begins with a discussion about the Hilbert set, an instance of a more general algebraic structure which shall be studied here.

5.1 The Hilbert Set

Let H denote the set of all non-negative integers $n \equiv 1 \bmod 4$.

$$H = \{4k+1, k \in \mathbb{Z}^+ \cup \{0\}\}$$
$$H = \{1, 5, 9, 13, 17, 21, 25 \ldots\}$$

H is a subset of the positive integers

$$H \subseteq \mathbb{Z}^+ \tag{117}$$

and by addition and multiplication in H, it is meant the binary operations $+, *$ as defined on the integers. Since H is a subset of the ring of integers, one can ask whether or not H is closed with respect to each binary operation. (See Definition **??**). Since the product of any two elements of H is itself a member of H, *H is closed with respect to multiplication.* Since the sum of two elements of H is not a member of H, *H is not closed with respect to addition.* For any

two elements $4i+1, 4j+1 \in H$,

$$(4i+1)\cdot(4j+1) = 16ij + 4i + 4j + 1 = 4(4ij + i + j) + 1 \quad \in H$$
$$(4i+1) + (4j+1) = 4i + 4j + 2 = 4(i+j) + 2 \quad \notin H$$

Since H is not closed with respect to integer addition, it cannot be classified as a ring. However, since $*$ is closed with respect to integer multiplication in H, it can be algebraically classified as a monoid under multiplication.

Definition 5.1. *A **monoid** is a pair $< \mathcal{M}, \circ >$ consisting of a non-empty set $\mathcal{M}$ along with a binary operation $\circ$ satisfying the following properties: [2, 227]*

Associativity:

$$\forall\, a, b, c \in \mathcal{M} \quad a \circ (b \circ c) = (a \circ b) \circ c$$

Identity:

$$\forall\, a \in \mathcal{M} \quad \exists\, e \quad a \circ e = e \circ a$$

Closure:

$$\forall\, a, b \in \mathcal{M} \quad a \circ b \in \mathcal{M}$$

The closure property need not be explicitly stated, since it is implied in the definition of a binary operator. It is included here for emphasis. Since H is not closed with respect to integer addition, $< H, + >$ cannot be classified as a monoid.

The pair $< H, * >$ satisfies the properties of a monoid. More specifically, since $a \cdot b = b \cdot a \quad \forall\, a, b \in H$, $< H, * >$ is called a commutative monoid. This special monoid was studied by David Hilbert, and is sometimes referred to in the literature as the *Hilbert Monoid*[11, 26]. The Hilbert Monoid is a special

case of a more general construct which will be presently described.

5.2 The $\mathcal{M}[a]$ Monoids

Let $\mathcal{M}[a]$ represent the set of all non-negative integers $n \equiv 1 \bmod a$.

$$\mathcal{M}[a] = \{ak + 1, a > 2, k \in \mathbb{Z}^+ \cup \{0\}\}$$
$$\mathcal{M}[a] = \{1, a + 1, 2a + 1, 3a + 1 \ldots\}$$

$\mathcal{M}[a]$ is a subset of the positive integers

$$\mathcal{M}[a] \subseteq \mathbb{Z}^+ \tag{118}$$

$\mathcal{M}[1] = \{1, 2, 3, 4 \ldots\}$ corresponds to the set of positive integers

$$\mathcal{M}[1] = \mathbb{Z}^+ \tag{119}$$

$\mathcal{M}[2] = \{1, 3, 5, 7 \ldots\}$ corresponds to the set of odd positive integers.

Since Goldbach's conjecture in $\mathbb{Z}$ was studied earlier, $\mathcal{M}[1], \mathcal{M}[2]$ are ignored, since each possess the same prime distribution as the integers. From here on, when $\mathcal{M}[a]$ is written, it is meant to be a general truth for any $\mathcal{M}[a]$ monoid where $a > 2$. Therefore, $\mathcal{M}[3]$ is the first set satisfying the properties that are to follow. $\mathcal{M}[4]$ corresponds to the set H, the Hilbert Monoid introduced earlier. The collection of all $\mathcal{M}[a]$ sets,where a is an integer greater than 2 is referred

to as the **1-monoids**.

$$\mathcal{M}[3] = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40 \ldots\}$$
$$\mathcal{M}[4] = \{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53 \ldots\}$$
$$\mathcal{M}[10] = \{1, 11, 21, 31, 41, 51, 61, 71, 81, 91, 101, 111 \ldots\}$$

As with the Hilbert monoid, addition and multiplication on $\mathcal{M}[a]$ are integer addition and integer multiplication, and since $\mathcal{M}[a]$ is a subset of $\mathbb{Z}$, each binary operation of $\mathbb{Z}$ is either closed or not on $\mathcal{M}[a]$. $\mathcal{M}[a]$ is closed with respect to integer multiplication, but not with respect to integer addition. Consider any two elements of $\mathcal{M}[a]$, $ai + 1$ and $aj + 1$.

$$(ai + 1) \cdot (aj + 1) = a^2ij + ai + aj + 1 = a(aij + i + j) + 1 \quad \in \mathcal{M}[a]$$
$$(ai + 1) + (aj + 1) = ai + aj + 2 = a(i + j) + 2 \quad \notin \mathcal{M}[a]$$

Any set $\mathcal{M}[a]$ paired with integer multiplication forms a commutative Monoid $< \mathcal{M}[a], * >$. The elements of $\mathcal{M}[a]$ are associative with respect to $*$, since the elements of $\mathcal{M}[a]$ are just a subset of the integers, which themselves satisfy associativity with respect to $*$. $\mathcal{M}[a]$ satisfies the monoid requirement for an identity element, since $1 \in \mathcal{M}[a]$ for any a.

The unit $1 \in \mathcal{M}[a]$ is denoted as $\mathcal{M}[a]_0$, and $\mathcal{M}[a]_i$ denotes i^{th} non-unit element of $\mathcal{M}[a]$. Therefore, $\mathcal{M}[a]_i = ai + 1$. For example, $\mathcal{M}[3]_2 = 3 \cdot 2 + 1 = 7$, and $\mathcal{M}[4]_{10} = 4 \cdot 10 + 1 = 41$. Using this notation, the product of two elements of $\mathcal{M}[a]$, $\mathcal{M}[a]_i, \mathcal{M}[a]_j$ is

$$\mathcal{M}[a]_i \cdot \mathcal{M}[a]_j = \mathcal{M}[a]_{aij+i+j}. \tag{120}$$

Definition 5.2. *$\mathcal{M}[a]_x$ is said to* ***divide*** *$\mathcal{M}[a]_y$ and this is denoted $\mathcal{M}[a]_x \mid \mathcal{M}[a]_y$ if there exists a $\mathcal{M}[a]_k$ where $\mathcal{M}[a]_x \cdot \mathcal{M}[a]_k = \mathcal{M}[a]_y$.*

Example 5.1. *In $\mathcal{M}[3]$, $4|28$ since if $k = 7 \in \mathcal{M}[3]$, $4 \cdot 7 = 28$.*

Definition 5.3. *An integer $\mathcal{M}[a]_x$ is* ***prime*** *in $\mathcal{M}[a]$ if the only elements of the set $\mathcal{M}[a]$ which divide it are 1 and itself. Otherwise $\mathcal{M}[a]_x$ is composite. The primes of $\mathbb{Z}$ are referred to as rational primes.*

Example 5.2. *(a) The set of primes in $\mathcal{M}[3]$ are $\{1,4,7,10,13,19,22,25,31\ldots\}$. (b) In $\mathcal{M}[4]$ the primes are $\{1,5,9,13,17,21,29\ldots\}$.*

As is evident in Example 5.2, many numbers which are composite in $\mathbb{Z}$ are prime in $\mathcal{M}[a]$. For example, 25 is prime in $\mathcal{M}[4]$ but composite in $\mathbb{Z}$. Also, it is possible for a number to be prime in $\mathcal{M}[a_1]$ but composite in $\mathcal{M}[a_2]$. For example, consider 25, a member of both $\mathcal{M}[3], \mathcal{M}[4]$, which is prime in $\mathcal{M}[3]$, but composite in $\mathcal{M}[4]$.

Theorem 5.1. *If p is a rational prime, and $p \in \mathcal{M}[a]$, then p is prime in $\mathcal{M}[a]$.*

Proof. The set $\mathcal{M}[a]$ is a subset of $\mathbb{Z}$. If p cannot be decomposed into elements of $\mathbb{Z}$, then clearly it cannot be decomposed as elements of a subset of $\mathbb{Z}$. □

Theorem 5.2. *The first $a+1$ non-unit elements of $\mathcal{M}[a]$ are prime in $\mathcal{M}[a]$.*

Proof. The smallest composite element of $\mathcal{M}[a]$ will be the square of the first prime element, and the first prime element will be the first non-unit element, so the first composite element will be $(\mathcal{M}[a]_1)^2$. Clearly, any other composite element would have a larger magnitude. Since $\mathcal{M}[a]_1 = a+1$, $(\mathcal{M}[a]_1)^2 = a^2+2a+1 = a\cdot(a+2)+1$, so the smallest composite element will be $\mathcal{M}[a]_{a+2}$. □

Example 5.3. *In $\mathcal{M}[4]$, $\mathcal{M}[4]_1 = 1 \cdot 4 + 1 = 5$, and the smallest composite element is $\mathcal{M}[4]_{4+2} = 6 \cdot 4 + 1 = 25$. (b) In $\mathcal{M}[10]$, $\mathcal{M}[10]_1 = 1 \cdot 10 + 1 = 11$, and the smallest composite element is $\mathcal{M}[10]_{10+2} = 121$.*

Theorem 5.3. *For all positive integers a, b, either $\mathcal{M}[a]_b$ is prime in $\mathcal{M}[a]$, or $\mathcal{M}[b]_a$ is prime in $\mathcal{M}[b]$, or both.*

Proof. $\mathcal{M}[a]_b = \mathcal{M}[b]_a = ab + 1$. It must shown that at least one of the two is prime, either $\mathcal{M}[a]_b$ is prime in $\mathcal{M}[a]$, or $\mathcal{M}[b]_a$ is prime in $\mathcal{M}[b]$. Suppose $ab + 1$ is a rational prime, then clearly it is prime in both contexts by Theorem 5.1. Otherwise, one of a, b is greater or equal to the other. Suppose $a \geq b$. Then by Theorem 5.2, $\mathcal{M}[a]_b$ is prime. □

The proof of the following theorem regarding the integers is omitted. This theorem will be required for infinity of primes proof that is to follow.

Theorem 5.4 (Dirichlet's Theorem). *If a, b, $a > b$ are integers and $(a, b) = 1$, there exist an infinity of rational primes $p \equiv b \bmod a$ [7, p18].*

Example 5.4. *(a)* $(5, 3) = 1$ *so there are an infinity of rational primes* $p \equiv 3 \bmod 5$. *(b)* $(3, 1) = 1$ *so there exist an infinity of rational primes* $p \equiv 1 \bmod 3$.

Theorem 5.5. *There exist an infinity of primes in $\mathcal{M}[a]$.*

Proof. Since $(a, 1) = 1$ for any integer a, by Theorem 5.4 there exist an infinity of rational primes $p \equiv 1 \bmod a$. Therefore, there exist an infinity of rational primes in any set $\mathcal{M}[a]$. Since Theorem 5.1 states that every rational prime is prime in $\mathcal{M}[a]$, $\mathcal{M}[a]$ contains an infinity of primes. □

Definition 5.4. *For any integer n, the number of divisors of n is denoted $\delta(n)$.*

Example 5.5. *(a)* $\delta(20) = 6$, *since* $1, 2, 4, 5, 10, 20$ *all divide* 20. *(b)* $\delta(7) = 2$, *since only* $1, 7$ *divide* 7.

Theorem 5.6. *If n is a positive integer, there are $\delta(n-1)$ monoids containing n as a member, and if the divisors of $n - 1$ are $\delta_1, \delta_2 \ldots \delta_{\delta(n-1)}$, then those 1-monoids containing n are $\mathcal{M}[\delta_1], \mathcal{M}[\delta_2], \ldots \mathcal{M}[\delta_{\delta(n-1)}]$.*

Proof. If δ is a divisor of $n-1$, then there exists some integer k such that $\delta \cdot k = n-1$. Therefore, $\delta \cdot k + 1 = n$, so $n \in \mathcal{M}[\delta]$. If an integer d does not divide $n-1$, then there is no k such that $d \cdot k = n-1$, and hence $d \cdot k + 1 \neq n$, so $n \notin \mathcal{M}[d]$. □

Example 5.6. *$n = 21$ will belong to $\delta(20) = 6$ sets, namely $\mathcal{M}[1]$, $\mathcal{M}[2]$, $\mathcal{M}[4]$, $\mathcal{M}[5]$, $\mathcal{M}[10]$, $\mathcal{M}[20]$.*

Those integers of the form $p+1$, where p is a rational prime, will be least prominent among $\mathcal{M}[a]$ sets, since p has only $1, p$ as divisors. 1 divides all integers, but $\mathcal{M}[1]$ is trivial, so any integer $p+1$ belongs to a single $\mathcal{M}[a]$ set, namely $\mathcal{M}[p]$. Those integers where $n-1$ contains many divisors will be most prominent among $\mathcal{M}[a]$ sets.

5.2.1 On Prime Factorization in $\mathcal{M}[a]$

Theorem 5.7. *Every non-unit element of any set $\mathcal{M}[a]$ is a product of prime elements of $\mathcal{M}[a]$.*

Proof. (by Induction) $\mathcal{M}[a]_1$ is the first non-unit element of $\mathcal{M}[a]$, and it must be prime by Theorem 5.2, so it is composed of a single prime element. It must be shown that assuming the truth of the theorem for all elements up to $\mathcal{M}[a]_n$, it also holds for $\mathcal{M}[a]_{n+1}$.

If $\mathcal{M}[a]_{n+1}$ is prime, the theorem is satisfied. Otherwise, it is composite, so it is a product of two elements

$$\mathcal{M}[a]_x \cdot \mathcal{M}[a]_y = \mathcal{M}[a]_{n+1} \tag{121}$$

Neither factor is unity, so both must lie within these boundaries:

$$\mathcal{M}[a]_1 \leq \mathcal{M}[a]_x \leq \mathcal{M}[a]_n \tag{122}$$

$$\mathcal{M}[a]_1 \leq \mathcal{M}[a]_y \leq \mathcal{M}[a]_n \tag{123}$$

So $\mathcal{M}[a]_x$,$\mathcal{M}[a]_y$ both lie within the range in which the theorem is assumed to be true. Therefore, they are both composable as a product of primes. Therefore, their product, $\mathcal{M}[a]_{n+1}$, is itself a product of primes, so the theorem is proven. □

In the algebraic treatment of the integers and the Gaussian integers, algebra leading up to the fundamental theorem of arithmetic was studied. Every non-unit element of $\mathbb{Z}$ and $\mathbb{Z}[i]$ is composable as a product of prime elements of their respective sets in a unique way. This is not so in $\mathcal{M}[a]$.

As an example of a number which yields two prime factorizations, consider $\mathcal{M}[3]_{33} = 100$. $100 = (\mathcal{M}[3]_3)^2 = 10^2$, where 10 is a prime element in $\mathcal{M}[3]$. Also, $100 = \mathcal{M}[3]_1 \cdot \mathcal{M}[3]_8 = 4 \cdot 25$, where 4 and 25 are both prime in $\mathcal{M}[3]$.

Why is it possible for an element of $\mathcal{M}[3]$, a subset of the integers, to yield two distinct prime factorizations in that set when that same element has a single prime factorization among the integers? Consider the unique prime factorization of 100 among the integers.

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 \tag{124}$$

100 cannot be factored as such in $\mathcal{M}[3]$, since neither of $2, 5 \in \mathcal{M}[3]$. However, 10, 4, and 25 are prime elements of $\mathcal{M}[3]$ and their unique factorizations in $\mathbb{Z}$

are as follows:

$$10 = 2 \cdot 5$$

$$4 = 2^2$$

$$25 = 5^2$$

where both $10 \cdot 10$ and $4 \cdot 25$ yield $100 = 2^2 \cdot 5^2$. Since 100 has many representations as a product of composite integers, and some of those composite integers are prime integers in $\mathcal{M}[3]$, 100 has more than one prime factorization in $\mathcal{M}[3]$. As described in the two theorems that follow, this same notion applies to all $\mathcal{M}[a]$, and there are infinitely many elements within any $\mathcal{M}[a]$ set which have multiple prime factorizations.

Theorem 5.8. *Any set $\mathcal{M}[a]$, $a > 2$ has at least one element which has multiple prime factorizations.*

Proof. The set $\mathcal{M}[a]$, a subset of the integers, contains an infinity of, but not all of the primes of $\mathbb{Z}$. That it contains an infinite number of rational primes is clear by Dirichlet's Theorem (Theorem 5.4), since $\mathcal{M}[a]$ consists of all those integers of the form $ak + 1$, where $(a, k) = 1$. Dirichlet's Theorem can also be used to argue that $\mathcal{M}[a]$ cannot contain all the primes of $\mathbb{Z}$, for consider those integers of the form

$$\{ak + (a - 1), k \in \mathbb{Z}^+ \cup \{0\}\} \tag{125}$$

Clearly, $a - 1 \neq 1$ when $a > 2$, so elements in this progression will not be of the form $ak + 1$, and hence, will not belong to $\mathcal{M}[a]$. Clearly, $a, a - 1$ cannot share a common divisor other than 1, for any divisor d of $a - 1$ will divide $a - 1 + d$ next, which is greater than a if $d > 1$. So $(a, a - 1) = 1$, and by Dirichlet's theorem, there exist an infinity of rational primes of the form $ak + (a - 1)$. Since these

primes do not belong to $\mathcal{M}[a]$, $\mathcal{M}[a]$ does not include all of the primes in $\mathbb{Z}$.

The set of integers leaving a remainder of $(a-1)$ upon division by a (Equ.125) is of further use in this proof, so it is labeled $\mathcal{N}[a]$. Since $ak+(a-1) = a(k+1)-1$ it is restated as follows:

$$\mathcal{N}[a] = \{a(k+1)-1), k \in \mathbb{Z}^+ \cup \{0\}\} \tag{126}$$

An interesting property of $\mathcal{N}[a]$ is that the product of any two elements of the set is a member of $\mathcal{M}[a]$.

$$\begin{aligned}\mathcal{N}[a]_i \cdot \mathcal{N}[a]_j &= (a(i+1)-1)\cdot(a(j+1)-1)\\ &= a^2(i+1)(j+1) - a(i+1) - a(j+1) + 1\\ &= a(a(i+1)(j+1) - (i+1) - (j+1)) + 1 \in \mathcal{M}[a]\end{aligned}$$

Earlier it was stated that $\mathcal{N}[a]$ contains infinitely many rational primes. Consider the first two such primes, denoted $\mathcal{P}$ and $\mathcal{Q}$. Since the product of any two elements of $\mathcal{N}[a]$ belongs in $\mathcal{M}[a]$, so it must be true that

$$\mathcal{P}^2 \in \mathcal{M}[a]$$

$$\mathcal{Q}^2 \in \mathcal{M}[a]$$

$$\mathcal{P}\mathcal{Q} \in \mathcal{M}[a]$$

and since $\mathcal{P}^2$, $\mathcal{Q}^2$ are both in $\mathcal{M}[a]$, which exhibits multiplicative closure, it must be true that

$$\mathcal{P}^2\mathcal{Q}^2 \in \mathcal{M}[a] \tag{127}$$

Next, it must be shown that $\mathcal{P}^2$, $\mathcal{Q}^2$ and $\mathcal{P}\mathcal{Q}$ are prime in $\mathcal{M}[a]$. Clearly, $\mathcal{P}^2$ must be prime in $\mathcal{M}[a]$, for it is the square of a rational prime, and that rational

prime is not itself a member of $\mathcal{M}[a]$. For the same reason, $\mathcal{Q}^2$ must be prime in $\mathcal{M}[a]$. $\mathcal{PQ}$ must also be prime in $\mathcal{M}[a]$, because its only prime divisors are $\mathcal{P}, \mathcal{Q}$, and neither belong to $\mathcal{M}[a]$.

Having shown that $\mathcal{P}^2$, $\mathcal{Q}^2$ and $\mathcal{PQ}$ are prime in $\mathcal{M}[a]$, it is now time for the final result. $\mathcal{P}^2\mathcal{Q}^2$ yields two prime factorizations in $\mathcal{M}[a]$:

$$\begin{aligned}\mathcal{P}^2\mathcal{Q}^2 &= \mathcal{P}^2 \cdot \mathcal{Q}^2 \\ &= (\mathcal{PQ})^2\end{aligned}$$

□

Corollary 5.1. *Any set $\mathcal{M}[a]$, $a > 2$ contains an infinity of elements which have multiple prime factorizations.*

Proof. In proving Theorem 5.8, the first two rational primes of $\mathcal{N}[a]$ were labeled $\mathcal{P}, \mathcal{Q}$ and it was shown that $\mathcal{P}^2\mathcal{Q}^2$ has two prime factorizations in $\mathcal{M}[a]$. However, the same argument could have been made for any two rational primes belonging to $\mathcal{N}[a]$. Since $\mathcal{N}[a]$ contains an infinity of rational primes by Dirichlet's theorem, there are infinitely many elements of $\mathcal{M}[a]$ with multiple prime factorizations. □

Although the preceding theorem and corollary are sufficient to show that the 1-monoids each contains an infinity of elements which have multiple prime factorizations, one should not infer that all those numbers yielding multiple prime factorizations are of the form $\mathcal{P}^2\mathcal{Q}^2$, $\mathcal{P}, \mathcal{Q} \in \mathcal{N}[a]$. In theory, any composite integer, other than a semiprime (see the following theorem), can potentially yield multiple prime factorizations. Although the theorem above specifically described elements with two prime factorizations, some elements have many more.

Theorem 5.9. *If n is an integer semiprime and $n \in \mathcal{M}[a]$, n has a unique prime factorization in $\mathcal{M}[a]$.*

Proof. Recall that a semiprime is an integer that is the product of exactly two primes integers. n is either prime or composite in $\mathcal{M}[a]$. If it is prime then it has a single representation. Otherwise, n is composite in $\mathcal{M}[a]$, and hence is a product of two elements $\in \mathcal{M}[a]$. Since n is a semiprime, it is a product of two prime integers, say p, q. So if n is composite in $\mathcal{M}[a]$, both $p, q \in \mathcal{M}[a]$, and n yields the factorization $p \cdot q \in \mathcal{M}[a]$. In order for it to yield another prime factorization, there would need to be other prime elements of $\mathcal{M}[a]$ whose composition yielded n. But n is a semiprime, so only $1, p, q, n$ are divisors of n. And hence no other composition of elements of $\mathcal{M}[a]$ yields n, and hence n has a single representation as a product of prime elements of $\mathcal{M}[a]$. □

5.3 Goldbach's Conjecture in $\mathcal{M}[a]$

Now that the algebraic properties of the $\mathcal{M}[a]$ set have been introduced, Goldbach's conjecture can be studied in this context. The first order of business then, will be to define Goldbach's conjecture for $\mathcal{M}[a]$. Again, Goldbach's Conjecture is defined in terms of the abstract Goldbach conjecture. Before doing so, the issues which arise when attempting to adapt the original statement of Goldbach's Conjecture to $\mathcal{M}[a]$ will be discussed. This will emphasize the need for the abstract Goldbach conjecture in the first place.

Once again consider Conjecture 2.1, Goldbach's conjecture as it is generally stated among the literature. It states that every even integer can be composed as a sum of two prime integers in at least one way. There are two factors which limit adapting this statement to $\mathcal{M}[a]$. First, the requirement that those numbers composable as a sum of two primes be even. Consider $\mathcal{M}[4]$={1,5,9,13 ...}, a set which consists entirely of odd numbers. Since there are no even elements

in $\mathcal{M}[4]$, it would not be possible to adapt the conjecture to this monoid, or more generally, any monoid where $2|a$, without redefining the notion of an even number. The second issue lies in the explicit mention of the addition operator. As described earlier, any $\mathcal{M}[a]$ set lacks additive closure. Since the sum of two elements of $\mathcal{M}[a]$ is not itself a member of $\mathcal{M}[a]$, it is impossible for an element of $\mathcal{M}[a]$ to be composed as a sum of two prime elements of that set.

Upon initial inspection then, it might seem strange to study Goldbach's conjecture within any $\mathcal{M}[a]$ set. However, the abstract Goldbach conjecture makes no mention of even numbers, nor of the addition operator. The Abstract Goldbach conjecture is used as an archetype for defining Goldbach's Conjecture in $\mathcal{M}[a]$. In essence, the following question is asked: is every element of $\mathcal{M}[a]$ equidistant to two prime elements in that set? Formally,

Definition 5.5 (Goldbach's conjecture among the 1-monoids). *For every element $\mathcal{M}[a]_i$ of $\mathcal{M}[a]$, $i \geq 1$, there exists an integer $0 \leq \kappa < i$ such that both $\mathcal{M}[a]_{i-\kappa}$,$\mathcal{M}[a]_{i+\kappa}$ are prime in $\mathcal{M}[a]$.*

Here, the magnitude function $M(\mathcal{M}[a]_i) = ai + 1$, and $\mathcal{M}[a]_i$ is said to be equidistant to $\mathcal{M}[a]_x, \mathcal{M}[a]_y$, $\mathcal{M}[a]_x < \mathcal{M}[a]_y$, if there exists an integer κ, $0 \leq \kappa < i$ such that $\mathcal{M}[a]_{i-\kappa} = \mathcal{M}[a]_x, \mathcal{M}[a]_{i+\kappa} = \mathcal{M}[a]_y$.

Example 5.7. *(a) Consider $\mathcal{M}[3]_5 = 16$. It is equidistant to two primes, since if $\kappa = 1$, $\mathcal{M}[3]_{5-\kappa} = 13$, which is prime in $\mathcal{M}[3]$ and $\mathcal{M}[3]_{5+\kappa} = 19$, which is prime in $\mathcal{M}[3]$. (b) Consider $\mathcal{M}[4]_{21} = 85$. It is equidistant to two primes, since if $\kappa = 2$, $\mathcal{M}[4]_{21-\kappa} = 77$, $\mathcal{M}[4]_{21+\kappa} = 93$, both of which are prime in $\mathcal{M}[4]$.*

Definition 5.6. *The Goldbach number for $\mathcal{M}[a]_i$, denoted $G(\mathcal{M}[a]_i)$, represents the number of integers κ, $0 \leq \kappa < i$ such that $\mathcal{M}[a]_{i-\kappa}$, $\mathcal{M}[a]_{i+\kappa}$ are both prime in $\mathcal{M}[a]$.*

Example 5.8. *(a)* $G(\mathcal{M}[3]_5) = 3$, *since when* $\kappa = 1, 2$ *or* 3, $\mathcal{M}[3]_{5\pm\kappa}$ *are both prime in* $\mathcal{M}[3]$. *(b)* $G(\mathcal{M}[4]_{500}) = 138$.

Goldbach's Conjecture in $\mathcal{M}[a]$ can therefore be restated as follows:

Restatement 5.1.

$$\forall\, i \geq 1 \quad G(\mathcal{M}[a]_i) \geq 1 \tag{128}$$

Figure 8 (a) and (b) graph $\mathcal{M}[4]_i$ (x-axis) with respect to $G(\mathcal{M}[4]_i)$ (y-axis) for the first 10000 and 25000 elements of $\mathcal{M}[4]$ respectively. Figure 9 examines $\mathcal{M}[4]$ a little more closely, graphing $\mathcal{M}[4]_i$ with respect to $G(\mathcal{M}[4]_i)$ for $20000 \leq i \leq 25000$. Figure 10 Graphs the first 5000 elements of $\mathcal{M}[a]$ for $a = 3, 4, 5, 6$ respectively.

If $\mathcal{M}[a]_i$ is equidistant to two primes, then one is no greater, the other no smaller than $\mathcal{M}[a]_i$. Therefore, there can be no more solutions for a given element than there are elements of lesser magnitude in the set, so

$$G(\mathcal{M}[a]_i) \leq i \tag{129}$$

More specifically, there can be no more solutions than there are prime elements no greater than $\mathcal{M}[a]_i$, or between $\mathcal{M}[a]_i$ and $\mathcal{M}[a]_{2i-1}$, so if $\pi(\mathcal{M}[a]_i)$ represents the number of prime elements no greater than $\mathcal{M}[a]_i$ in $\mathcal{M}[a]$,

$$G(\mathcal{M}[a]_i) \leq \min(\pi(\mathcal{M}[a]_i), \pi(\mathcal{M}[a]_{2i-1}) - \pi(\mathcal{M}[a]_i)) \tag{130}$$

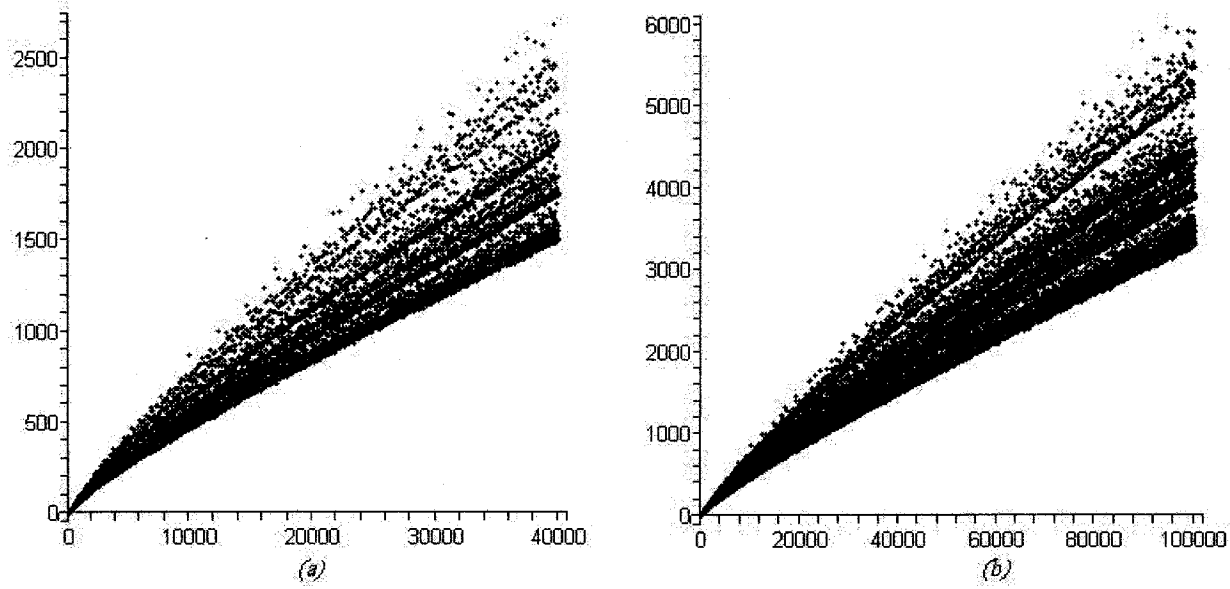

Figure 8: The Hilbert Monoid: $G(\mathcal{M}[4]_i)$ for i up to (a) 10000 and (b) 25000

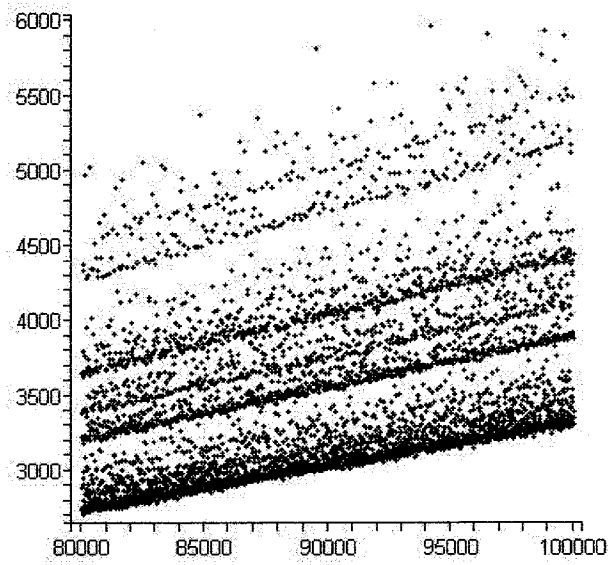

Figure 9: The Hilbert Monoid Up Close: $G(\mathcal{M}[4]_i)$ for i from 20000 to 25000

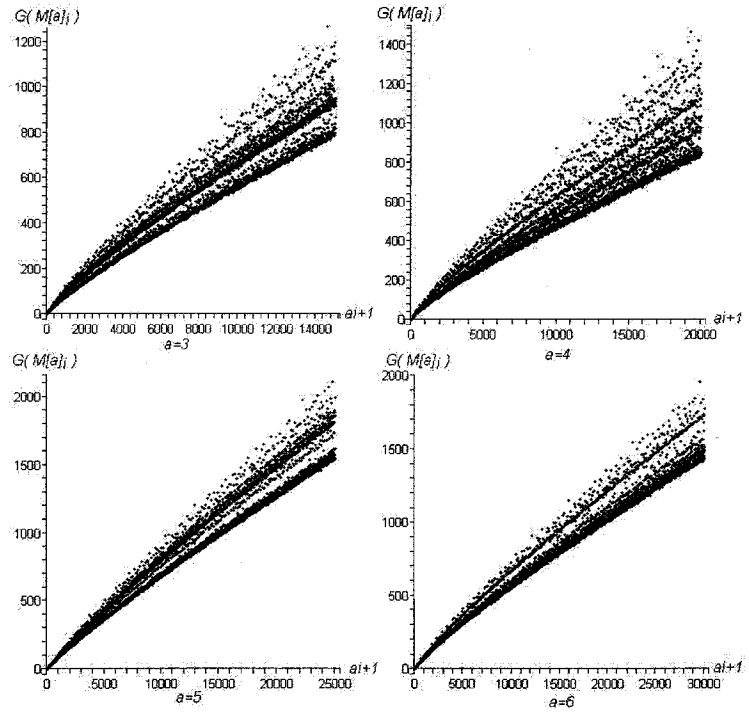

Figure 10: $G(\mathcal{M}[a])$ for first 5000 elements of $\mathcal{M}[3], \mathcal{M}[4], \mathcal{M}[5]\mathcal{M}[6]$

During the earlier discussion regarding the integers, Tables 1 and 2 provided insight into the relationship between Goldbach's conjecture and the symmetry of the distribution of prime integers relative to itself. Here a similar table is provided for $\mathcal{M}[a]$.

For the element $\mathcal{M}[a]_i$, let $\beta[a]_i$ be the bit string of length $2i-1$ where the j^{th} bit is set to 1 if $\mathcal{M}[a]_j$ is prime in $\mathcal{M}[a]$, and has a value of 0 otherwise. The bit string $\beta[a]'_i$ is the reverse bit string of $\beta[a]_i$. If these bit strings have a position where they are both set, then $\mathcal{M}[a]_i$ is equidistant to two prime elements of $\mathcal{M}[a]$. Table 5 displays $\beta[3]_5$ and $\beta'[3]_5$. In this example, bits $1, 3, 5$ are set in both (bits 7 and 9 too, but they are mirror images of $1, 3$).

i	$\mathcal{M}[3]_1$	$\mathcal{M}[3]_2$	$\mathcal{M}[3]_3$	$\mathcal{M}[3]_4$	$\mathcal{M}[3]_5$	$\mathcal{M}[3]_6$	$\mathcal{M}[3]_7$	$\mathcal{M}[3]_8$	$\mathcal{M}[3]_9$
$\beta[3]_5$	1	1	1	0	1	1	1	0	1
$\beta[3]'_5$	1	0	1	1	1	0	1	1	1

Table 5: Monoid bitstrings for $\mathcal{M}[3]_5$

Definition 5.7. *Let $G_{min}(\mathcal{M}[a]_i)$ represent the smallest integer κ, $0 \leq \kappa < i$ such that $\mathcal{M}[a]_{i-\kappa}$, $\mathcal{M}[a]_{i+\kappa}$ are both prime in $\mathcal{M}[a]$.*

Example 5.9. *(a) $G_{min}(\mathcal{M}[3]_5) = 1$, since when $\kappa = 1$, $\mathcal{M}[3]_{5\pm\kappa}$ are prime in $\mathcal{M}[3]$, and no smaller κ satisfies this property. (b) $G_{min}(\mathcal{M}[4]_{500}) = 5$, so $\mathcal{M}[4]_{500\pm\kappa}$ are both prime when $\kappa = 5$, and no smaller κ satisfies this property.*

5.3.1 On Weaker Statements in $\mathcal{M}[a]$

The sections studying the integers and Gaussian integers each included a discussion on weaker statements related to the mobius function. However, in any set $\mathcal{M}[a]$, $a > 2$, unique prime factorization does not hold for all elements (Theorem 5.8). Therefore, it is not possible to evaluate a distinct value for the mobius function. Consider $\mathcal{M}[3]_{33} + 1 = 100$, which yields two prime factorizations: $10 \cdot 10$ and $25 \cdot 4$. The former factorization can be considered squarefull,

while the latter would be considered squarefree. Therefore, there is no distinct value for the mobius function in this case, or for any other element which yields more than one prime factorization. For this reason, the study of the weaker statements is omitted for $\mathcal{M}[a]$.

5.3.2 Is Goldbach's Conjecture True in $\mathcal{M}[a]$?

It is possible that Goldbach's Conjecture holds for all $\mathcal{M}[a]$ sets, $a > 2$. Alternatively, it is possible that the conjecture fails in all of them, or is satisfied in some sets and fails in others. For example, it might hold in $\mathcal{M}[3]$ and fail in $\mathcal{M}[4]$.

There is reason to believe that the conjecture is more likely to be satisfied as the integer a increases is size. After all, by Theorem 5.2, the first $a+1$ elements in $\mathcal{M}[a]$ are prime. Consider $\mathcal{M}[100]$, which will have 101 consecutive prime elements. In order for an element $\mathcal{M}[100]_i$ to fail satisfying the conjecture, there would need to be 101 consecutive composite numbers, namely $\mathcal{M}[100]_{2i-1}$, $\mathcal{M}[100]_{2i-2}, \ldots \mathcal{M}[100]_{2i-1-101}$. In general, in order for $\mathcal{M}[a]_i$ to fail in satisfying Goldbach's Conjecture, $\mathcal{M}[a]_{2i-1}$, $\mathcal{M}[a]_{2i-2}$ $\ldots \mathcal{M}[a]_{2i-a-2}$ must all be composite in $\mathcal{M}[a]$. And even still, this a necessary condition for failure, not a sufficient one.

However, there is an offsetting effect to consider. As the integer a increases, $\mathcal{M}[a]$ will tend to have less rational primes. This is so because the distribution of primes in $\mathbb{Z}$ tapers off as magnitude increases. Given two sets $\mathcal{M}[a_1]$, $\mathcal{M}[a_2]$, where $a_1 < a_2$, $\mathcal{M}[a_1]$ will tend to have more rational primes, since it will have more small numbers than $\mathcal{M}[a_2]$, and small numbers are more likely to be prime than large ones. Table 6 lists the number of rational primes among the first 1000 elements for many $\mathcal{M}[a]$ sets.

Although all rational primes are prime in $\mathcal{M}[a]$, it is the distribution of primes, not rational primes that is crucial to the truth of Goldbach's conjecture in $\mathcal{M}[a]$. Table 7 lists the number of primes among the first 1000 and 5000 elements of various $\mathcal{M}[a]$ monoids.

	# of rational primes among first 1000 elements
$\mathcal{M}[3]$	208
$\mathcal{M}[5]$	163
$\mathcal{M}[7]$	147
$\mathcal{M}[9]$	185
$\mathcal{M}[11]$	134
$\mathcal{M}[13]$	125

Table 6: The number of rational primes among the first 1000 elements of $\mathcal{M}[a]$

	# of primes among first 1000	# of primes among first 5000
$\mathcal{M}[3]$	465	2002
$\mathcal{M}[5]$	631	2864
$\mathcal{M}[7]$	720	3324
$\mathcal{M}[9]$	772	3609
$\mathcal{M}[11]$	816	3866
$\mathcal{M}[13]$	844	4011

Table 7: The number of primes among the first 1000 elements of $\mathcal{M}[a]$

Since there are infinitely many $\mathcal{M}[a]$ sets, they cannot all be tested empirically. The first 25000 elements of $\mathcal{M}[3]$ through $\mathcal{M}[7]$ were tested and were all found to be equidistant to two primes. The average G_{min} values for these are listed in Table 8. Based on the G_{min} values, the conjecture seems easily satisfied in all $\mathcal{M}[a]$ monoids, and seems to become more quickly satisfiable as integer a increases.

	$AVG(G_{min}(\mathcal{M}[a]_i), 1 \leq i < 25000$
$\mathcal{M}[3]$	1.6532
$\mathcal{M}[4]$	1.4704
$\mathcal{M}[5]$	0.61826
$\mathcal{M}[6]$	0.77326
$\mathcal{M}[7]$	0.36732

Table 8: Average G_{min} values for various 1-monoids

6 The Quaternion Integers

The Quaternion integers, specifically the set of Hurwitz integers, constitutes the final number context for which Goldbach's conjecture is studied in this work. The algebra of the Hurwitz integers is most comparable to that of the Gaussian integers, with some differences. Most significantly, quaternions do not satisfy the property of multiplicative commutativity.

The algebra of the quaternions is relatively challenging, and few sources discuss the material in detail. Most of the algebra in this section follows very closely from Hardy and Wright's treatment of the subject. Even still, some of those proofs are omitted, and the subject is not treated up to the fundamental theorem, even though unique prime factorization does hold here. For the purposes of this work, The most noteworthy result among the algebra is Theorem 6.6, which emphasizes the close relationship between primality in $\mathbb{Z}$ and the quaternion integers.

6.1 Algebra of the Quaternion Integers

Definition 6.1. *The set $\mathbb{H}$ of Quaternions consists of those numbers of the form $a+bi+cj+dk$, where $a, b, c, d \in \mathbb{R}$ and i, j, k are imaginary units satisfying the following properties:*

$$i^2 = j^2 = k^2 = -1 \tag{131}$$

The Quaternions form a non-commutative ring with identity element [2, 35], and hence satisfy Axioms 2.1-2.6 and 2.8 described in Section 2.1.

The imaginary units i, j, k do not exhibit multiplicative commutativity. Specifically, they are said to be anticommutative, since the product of two such units differs in parity depending on the order in which the units are multiplied.

$$\begin{aligned} j \cdot k = i \quad k \cdot j = -i \\ i \cdot j = k \quad j \cdot i = -k \\ k \cdot i = j \quad i \cdot k = -j \end{aligned} \tag{132}$$

Definition 6.2. *The set of* ***Lipschitz integers*** *consists of those Quaternions* $a + bi + cj + dk$ *where all of* $a, b, c, d \in \mathbb{Z}$.

The set of Lipschitz integers are the most obvious adaptation of quaternions into an integral form. However, there is another set which extends the Lipshitz integers which has more desirable properties. These are the Hurwitz integers.

Definition 6.3. *The set* $\mathbb{Z}[i, j, k]$ *of* ***Hurwitz integers*** *consists of those Quaternions* $a + bi + cj + dk$ *where either all* $a, b, c, d \in \mathbb{Z}$ *or all of* $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$ *[3, p55].*

Example 6.1. $h = 1 + 2i + 3j + 4k$ *is a Lipschitz integer and a Hurwitz integer,* $h = 1\frac{1}{2} + 1\frac{1}{2}i + 3\frac{1}{2}j + 10\frac{1}{2}k$ *is a Hurwitz integer, and* $h = 1 + 2\frac{1}{2}i + 3j + 4k$ *is neither.*

The Hurwitz integers, like the quaternions, form a non-commutative ring with identity element. It turns out that the Hurwitz integers are somewhat simpler to study, while posessing properties that the Lipschitz integers do not [7, 316].

The algebra that follows regards the Hurwitz integers. The terms quaternion, quaternion integer and Hurwitz integer are used interchangeably. if $h = a + bi +$

$cj + dk$, a, b, c, d are called the *coordinates* of h. The sum or difference of two quaternions is also a quaternion

$$(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k) = \tag{133}$$
$$(a_0 + b_0) + (a_1 + b_1) \cdot i + (a_2 + b_2) \cdot j + (a_3 + b_3) \cdot k$$
$$(a_0 + a_1 i + a_2 j + a_3 k) - (b_0 + b_1 i + b_2 j + b_3 k) = \tag{134}$$
$$(a_0 - b_0) + (a_1 - b_1) \cdot i + (a_2 - b_2) \cdot j + (a_3 - b_3) \cdot k$$

The product of two quaternions is also itself a quaternion,

$$(a_0 + a_1 i + a_2 j + a_3 k) \cdot (b_0 + b_1 i + b_2 j + b_3 k) = \tag{135}$$
$$(a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) \quad +$$
$$(a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2) \cdot i +$$
$$(a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1) \cdot j +$$
$$(a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0) \cdot k +$$

If a quaternion contains no imaginary components, it is called a *rational quaternion.* If $h_1 = a_0 + a_1 i + a_2 j + a_3 k$ and $h_2 = b_0$ (a rational quaternion), then

$$h_1 h_2 = a_0 b_0 + a_1 b_0 + a_2 b_0 + a_3 b_0 \tag{136}$$

and $h_1 h_2 = h_2 h_1$. In general, if h_1, h_2 are quaternions, $h_1 \neq h_2$. However, if h_r is a rational quaternion among other quaternions, it can be moved about at will. For example, suppose h_r is a rational quaternion among quaternion integers $h_1 \ldots h_k$:

$$\begin{aligned} h_r h_1 h_2 h_3 \ldots h_k &= \\ &= h_1 h_r h_2 h_3 \ldots h_k \\ &= h_1 h_2 h_r h_3 \ldots h_k \\ &\vdots \\ &= h_1 h_2 \ldots h_k h_r \end{aligned} \tag{137}$$

Definition 6.4. *The **conjugate** of a quaternion $h = a + bi + cj + dk$, denoted $\overline{h}$, is*

$$\overline{h} = a - bi - cj - dk \tag{138}$$

Definition 6.5. *The **norm** of a quaternion $h = a + bi + cj + dk$, denoted $N(h)$ is*

$$N(h) = a^2 + b^2 + c^2 + d^2 \tag{139}$$

Corollary 6.1. *The product of a quaternion integer h and its conjugate is its norm.*

$$h \cdot \overline{h} = (a + bi + cj + dk) \cdot (a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 = N(h) \tag{140}$$

Definition 6.6. *Those quaternion integers with norm 1 are said to be the **units** of $\mathbb{Z}[i, j, k]$. In order for a Lipschitz integer to have a norm of 1, exactly one of a, b, c, d would have to be 1. Therefore, there are eight Lipshitz units, namely $\pm 1, \pm i, \pm j, \pm k$. Now let's consider the Hurwitz integers. Clearly, the units among the Lipshitz integers are also units among the Hurwitz integers. In addition, those units consisting of half-integers must be considered. Suppose $q =$*

$a+bi+cj+dk$ *and* a, b, c, d *are all* $\pm\frac{1}{2}$. *Then the norm* $N(q) = \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$. *Any quaternion with* a, b, c, d *all* $\frac{1}{2}$, *independent of parity, will be a unit among the Hurwitz integers. So along with the Lipshitz units, every combination of the form* $\frac{1}{2} \cdot (\pm 1 \pm i + \pm j + \pm k)$ *is a Hurwitz unit. These* 16 *possibilities, along with the* 8 *from the Lipschitz integers, means that there are in total* 24 *units among the Hurwitz integers [3, p56].*

Definition 6.7. *The* ***associates*** *of a quaternion integer* h *are those numbers* $h \cdot h_u$, $h_u \cdot h$, *where* h_u *is any of the units of* $\mathbb{Z}[i, j, k]$ *listed in Definition 6.6.*

Theorem 6.1. *For any two quaternions* h_1, h_2,

$$\overline{h_1 h_2} = \overline{h_2} \cdot \overline{h_1} \tag{141}$$

Proof. Let $h_1 = a_0 + a_1 i + a_2 j + a_3 k$, $h_2 = b_0 + b_1 i + b_2 j + b_3 k$. Then $\overline{h_1 h_2} = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (-a_0 b_1 - a_1 b_0 - a_2 b_3 + a_3 b_2) \cdot i + (-a_0 b_2 + a_1 b_3 - a_2 b_0 - a_3 b_1) \cdot j + (-a_0 b_3 - a_1 b_2 + a_2 b_1 - a_3 b_0) \cdot k$. $\overline{h_2} \cdot \overline{h_1} = (b_0 - b_1 i - b_2 j - b_3 k) \cdot (a_0 - a_1 i - a_2 j - a_3 k) = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (-a_0 b_1 - a_1 b_0 - a_2 b_3 + a_3 b_2) \cdot i + (-a_0 b_2 + a_1 b_3 - a_2 b_0 - a_3 b_1) \cdot j + (-a_0 b_3 - a_1 b_2 + a_2 b_1 - a_3 b_0) \cdot k = \overline{h_1 h_2}$. □

Theorem 6.2. *The product of the norms of two quaternion integers is equal to the norm of their product.*

$$N(h_1) \cdot N(h_2) = N(h_1 h_2) \tag{142}$$

Proof. Consider $h = h_1 h_2$. $N(h_1 h_2) = h_1 h_2 \cdot \overline{h_1 h_2}$ by Corollary 6.1. By Theorem 6.1, it can be rewritten as $N(h_1 h_2) = h_1 h_2 \cdot \overline{h_2} \cdot \overline{h_1}$. By Corollary 6.1, $h_2 \cdot \overline{h_2} = N(h_2)$, so $N(h_1 h_2) = h_1 N(h_2) \overline{h_1}$. Since $N(h_2) \in \mathbb{Z}$ (a rational quaternion), it can be shifted among the divisors regardless of non-commutativity. So $N(h_1 h_2) = h_1 \overline{h_1} N(h_2)$. Again by Corollary 6.1, $h_1 \overline{h_1} = N(h_1)$, so $N(h_1 h_2) =$

$N(h_1)N(h_2)$. □

Theorem 6.2 can be applied indefinitely so that

$$N(h_1) \cdot N(h_2) \ldots N(h_k) = N(h_1 \ldots h_k) \tag{143}$$

Definition 6.8. *If $h = h_1 h_2$, h_1 is said to be a **left-hand divisor** of h and h_2 is said to be a **right-hand divisor** of h.*

The distinction between left and right divisors is necessary because of the non-commutative nature of quaternions. For example, Consider $h_1 = 1 + i + j + 4k$, $h_2 = 2j + 3k$.

$$h_1 h_2 \neq h_2 h_1 \tag{144}$$

$$(1 + i + j + 4k)(3j + 2k) \neq (3j + 2k)(1 + i + j + 4k) \tag{145}$$

$$(-11 - 10i + j + 5k) \neq (-11 + 10i + 5j - k) \tag{146}$$

Definition 6.9. *The greatest common right-hand divisor of h_1, h_2 is denoted $(h_1, h_2)_r$. Similarly, the greatest left-hand divisor is denoted $(h_1, h_2)_l$.*

Definition 6.10. *A non-unit quaternion h is **prime** if its only divisors are itself and its associates. If h is not prime, it is **composite**. Should there be any ambiguity, the primes of $\mathbb{Z}$ are referred to as **rational primes** to distinguish them from the primes of $\mathbb{Z}[i, j, k]$*

From here on h_p and h_q are reserved to denote prime quaternion integers.
The following two theorems are left unproven, but are required to prove Theorem 6.5.

Theorem 6.3. *If h_1 is a quaternion and k some integer where $h_2 = k$ is a rational quaternion, in order for $(h_1, h_2)_r = 1$, it must be that $(N(h_1), k) = 1$.*

Theorem 6.4. *If p is an odd rational prime, there exist two integers x, y such that*

$$1 + x^2 + y^2 = mp \quad 0 < m < p \tag{147}$$

Theorem 6.5. *If p is a rational prime, then the rational quaternion $h = p + 0i + 0j + 0k$ (or an associate thereof) cannot be a quaternion prime.*

Proof. (Adapted from [7, p309])
Since 2 can be factored as $(1 + i)(1 - i)$, and 2 is the only even prime, the following assumes that p is odd.

From Theorem 6.4 it is known that for any odd prime p, there exist integers r, s such that

$$1 + r^2 + s^2 = mp \quad 0 < r < p \quad 0 < s < p \quad 0 < m < p \tag{148}$$

so

$$1 + r^2 + s^2 \equiv 0 \bmod p \quad 0 < r < p \quad 0 < s < p \tag{149}$$

Consider the quaternion integer $h = 1 + sj - rk$, which has norm $N(h) = 1 + s^2 + r^2 \equiv 0 \bmod p$, and so $(N(h), p) \neq 1$.

From Theorem 6.3, h and p share some non-unit right hand divisor, say δ.

$$h = \delta_1 \delta \tag{150}$$

$$p = \delta_2 \delta \tag{151}$$

but δ_2 cannot be a unit either. For suppose it were. Then δ would be an

associate of p, and hence

$$p = \delta_2 \delta \quad N(\delta_2) = 1 \tag{152}$$

$$p\delta_2^{-1} = \delta \tag{153}$$

$$h = \delta_1 \delta_2^{-1} p \tag{154}$$

Since p is a rational integer, each of the coordinates of h will need to divide p. (see Equ.136). But h was defined to be $1 + sj - rk$, and clearly $p \nmid 1$, so this is not possible. Therefore, δ_2 is not a unit, and so the rational quaternion $p + 0i + 0j + 0k$, or any associate thereof, is the product of two non-unit quaternions, and hence is composite in $\mathbb{Z}[i, j, k]$. □

Theorem 6.6. *A Hurwitz integer h is prime if and only if its norm is a rational prime.*

Proof. (Adapted from [7, p309])
Suppose h is a prime quaternion. It's norm $N(h)$ is an integer, and hence a product of primes. Let p be one of the primes that divide $N(h)$. Since $(N(h), p) \neq 1$, h, p share a common non-unit right-hand divisor (Theorem 6.3), say δ, so

$$h = \delta_1 \delta \tag{155}$$

$$p = \delta_2 \delta \tag{156}$$

since h is a prime quaternion, it has at most one non-unit factor, and δ is not a unit, so δ_1 is a unit, and $N(h) = N(\delta)$.

From Theorem 6.5, p cannot be a prime quaternion. Therefore, since δ is a prime quaternion, δ_2 cannot be a unit. $N(p) = p^2$, so $N(\delta_2) \cdot N(\delta) = p^2$, and neither are unities, so $N(\delta_2) = p, N(\delta) = p$.

So $N(h) = N(\delta) = p$. Therefore, the rational prime p is the only divisor of $N(h)$, the norm of a prime quaternion integer.

□

Theorem 6.7. *Any rational prime integer p can be written as the sum of four squares.*

Proof. By Theorem 6.5, p cannot be a quaternion prime. Therefore, the quaternion factorization of p consists of two non-unit elements, so

$$p = \delta_1 \delta_2 \tag{157}$$

where $N(p) = p^2$, so $N(\delta_1) = N(\delta_2) = p$. δ_1 is a quaternion integer, say $\delta_1 = a+bi+cj+dk$, whose norm is p. Therefore, it must be that $a^2+b^2+c^2+d^2 = p$, which means that p is composable as a sum of four squares.

□

Theorem 6.8 (Lagrange's Theorem)**.** *Every positive integer can be written as a sum of four squares in at least one way.*

Proof. If two integers x, y are both composable as a sum of four squares, then their product xy is also composable as a product of four squares.

(Euler's Identity) [12, 142]:

$$x = (x_1^2 + x_2^2 + x_3^2 + x_4^2) \tag{158}$$

$$y = (y_1^2 + y_2^2 + y_3^2 + y_3^2) \tag{159}$$

$$xy = (x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (y_1^2 + y_2^2 + y_3^2 + y_3^2) = \tag{160}$$

$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \tag{161}$$

$$+(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$

$$+(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2$$

$$+(x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.$$

Since every integer can be written as a product of primes (Theorem 2.12), and every prime integer can be written as a sum of four squares (Theorem 6.7), where the product of any sum of four squares is itself a sum of four squares, it must be that every integer can be written as a sum of four squares.

□

Theorem 6.9. *There exist an infinity of Quaternion primes.*

Proof. By Theorem 6.8, every rational prime integer can be written as a sum of four squares. If $p = a^2 + b^2 + c^2 + d^2$, then p is the norm of the prime quaternion $h = a + bi + cj + dk$. By Theorem 6.6, h is a prime quaternion. Since there are infinitely many prime integers (Theorem 2.11), there are infinitely many prime quaternions. □

6.2 Goldbach's Conjecture among Quaternion Integers

To the knowledge of the author, there exists no previous attempt at defining Goldbach's conjecture among the quaternion integers. The following, again based on the abstract Goldbach conjecture, is similar to its counterpart among

the Gaussian integers. A discussion of weaker statements is omitted for the quaternions.

As with the Gaussian integers, only a portion of the integral quaternions are studied, specifically those of the form $h = a+bi+dj+dk$ where $0 \leq a \leq b \leq c \leq d$. When a Gaussian integer is of this form, it is said to be of the *proper form.* For example, $h = 1+2i+3j+4k$ is of the proper form, but $h = 4+3i+2j+k$ is not, and nor is $h = -4-3i-2j-k$. It will be argued that if all quaternion integers of the proper form satisfy Goldbach's conjecture in $\mathbb{Z}[i,j,k]$, so do all quaternion integers.

Here, the magnitude function is $M(h) = N(h) = a^2+b^2+c^2+d^2$, and equidistance is defined as follows.

Definition 6.11. *A quaternion integer $z = a+bi+cj+dk$, $0 \leq a \leq b \leq c \leq d$ is said to be* ***equidistant*** *to two quaternion integers h_1, h_2, $N(h_1) \leq N(h_2)$ if there exists a quaternion integer $z_\kappa = w+xi+yj+zk$, $0 \leq w \leq x \leq y \leq z$ such that $(h+h_\kappa) = h_1, (h-h_\kappa) = h_2$.*

For the remainder of this section, both quaternion integers $h = a+bi+cj+dk$ and $h_k = w+xi+yj+zk$ are assumed to be of the proper form, and it is assumed that $0 \geq N(h_\kappa) \geq N(h)$.

Conjecture 6.1 (Goldbach's Conjecture among the quaternion integers)**.** *Every quaternion integer h, $N(h) > 1$ is equidistant to two quaternion primes, h_p, h_q.*

If Conjecture 6.1 is satisfied for a quaternion integer h, h is said to satisfy Goldbach's conjecture.

Example 6.2. *$h = 0+1i+2j+2k$ satisfies Goldbach's conjecture, since if $h_k = 1+i+j+k$, $(h+h_\kappa), (h-h_\kappa)$ are prime quaternions, with norms 3 and*

23 *respectively.*

Theorem 6.10. *If h is a prime quaternion integer, it satisfies Goldbach's Conjecture in $\mathbb{H}[i,j,k]$.*

Proof. If h is prime, then it is trivially equidistant to two primes, since when $h_\kappa = 0+0i+0j+0k$, $(h \pm h_\kappa) = h$, which is prime by definition. □

It was stated earlier that if Goldbach's conjecture holds for all quaternion integers of proper form, it holds for all quaternion integers. To see this, suppose $h = a+bi+cj+dk$ is of the proper form and let $N(h) = m$, and suppose h' has the same coordinates a, b, c, d, but in any order and of any parity. For example, $h' = c - ai - dj + bk$ has coordinates a, b, c, d, but in differing order and parity than h. However, $N(h') = N(h) = m$, since changing order and parity of the coordinates in any way will not affect the norm. Suppose h satisfies Goldbach's conjecture. If h is itself a quaternion prime, then it trivially satisfies Goldbach's conjecture (Theorem 6.10), and so does h', since h is prime if and only if $N(h)$ is prime, and $N(h') = N(h)$. Otherwise, h is not prime, and there must exist some $h_\kappa = w+xi+yj+zk$, of the proper form, where $(h \pm h_\kappa)$ are both prime. Now let h'_κ be a modified version of h_κ, differing in order and parity in the same way that h' is a modification of h. So in this case, $h'_\kappa = y - wi - zj + xk$. Then $h + h_\kappa = (a+w) + (b+x)i + (c+y)j + (d+z)k$ and $h - h_\kappa = (a-w)+(b-x)i+(c-y)j+(d-z)k$, and $N(h+h_\kappa) = p_1, N(h-h_\kappa) = p_2$, where p_1, p_2 are rational prime integers. $h'+h'_\kappa = (c+y)-(a+w)i-(d+z)j+(b+x)k$ and $h' - h'_\kappa = (c-y) - (a-w)i - (d-z)j + (b-x)k$, and it is evident that $N(h' + h'_\kappa) = N(h + h_\kappa) = p_1$ and $N(h' - h'_\kappa) = N(h - h_\kappa) = p_2$. Clearly, if there exists an h_κ such that $(h \pm h_\kappa)$ are rational primes, then for any h' with the same coordinates as h, varying in order and parity , there will exist an h'_κ, which differs in order and parity from h_κ in the same way h' differs from h, such

that $(h' \pm h'_\kappa)$ are rational primes with the same norms as $(h \pm h_\kappa)$.
And this also applies to the conjugates of h.

Definition 6.12. *The Goldbach number for a quaternion integer h, denoted $G(h)$, represents the number of quaternion prime pairs which are equidistant to h.*

Example 6.3. *(a) If $h = 1 + i + j + 2k$, then $G(h) = 3$. The three solutions are as follows: (1) $h_\kappa = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$, $N(h + h_\kappa) = 13$ and $N(h - h_\kappa) = 3$. (2) $h_\kappa = 0 + 0i + 0j + 0k$, where $N(h + \kappa) = N(h - \kappa) = N(h) = 7$, which is prime. (3) $h_k = 0 + 0i + 0j + 2k$, so that $N(h + h_\kappa) = 19$, $N(h - h_\kappa) = 3$. (b) Similarly, if $h = 2 + 5i + 8j + 10k$, $G(h) = 134$.*

Goldbach's conjecture in $\mathbb{Z}[i, j, k]$ can therefore be restated as follows:

Restatement 6.1. *For any quaternion integer h with $N(h) > 1$, $G(h) \geq 1$*

Figure 11 (a) and (b) graph $N(h)$ (x-axis) with respect to $G(h)$ (y-axis) for all $h = a + bi + cj + dk, 0 \leq a \leq b \leq c \leq d$ with norms no greater than 100 and 500 respectively. Due to the added computational complexity in working with quaternions, and given that there are many integers in a small norm range, it is not currently possible to graph them for very high values.

Since quaternions have four coordinates, they are very difficult to visualize. One approach is to use two planes. Figure 12 graphs the quaternion $h = 1+i+j+2k$ and its two equidistant primes (As in Example 6.3(a)) in this way. The real and i portions lie in the left plane and the j and k portions on the right plane.

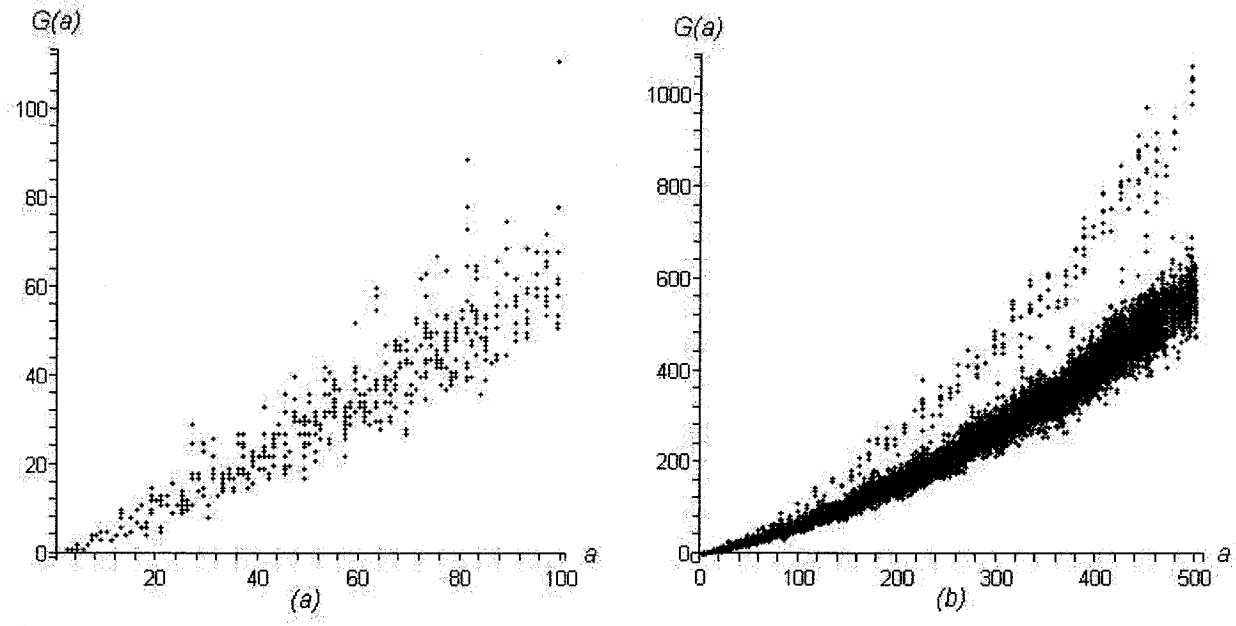

Figure 11: Goldbach's Comet in $\mathbb{Z}[i, j, k]$

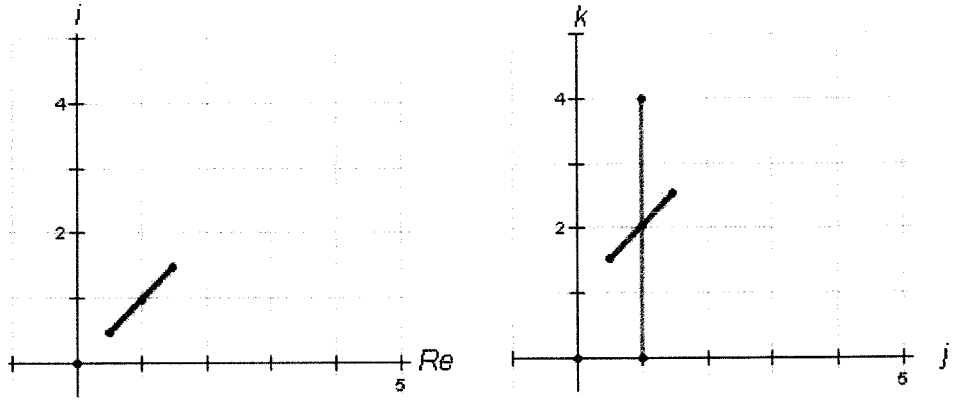

Figure 12: A Visualization of Goldbach's Conjecture in $\mathbb{Z}[i, j, k]$

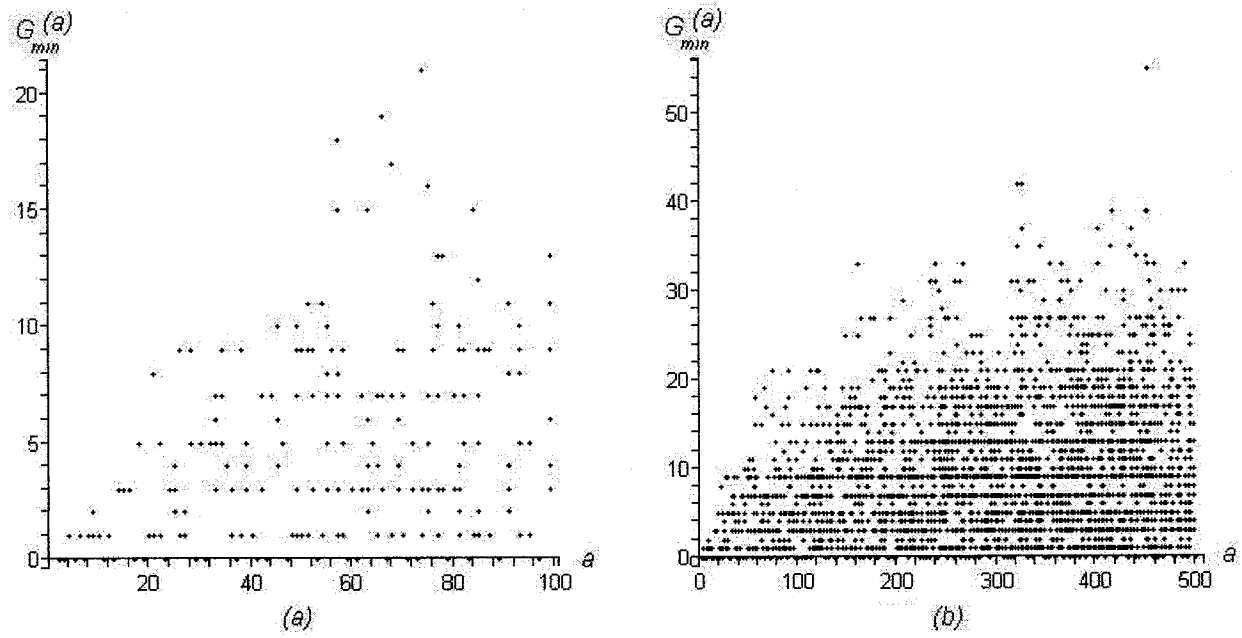

Figure 13: Minimal Distances for Goldbach's Conjecture

Theorem 6.11. *if* $(h \pm h_\kappa)$ *are both prime quaternions, then* $(h, h_\kappa) = 1$.

Proof. Suppose it were otherwise so that h, h_κ share some common factor, say h_m. So $h + h_\kappa = h_p = h_x \cdot h_m$ and $h - h_\kappa = h_q = h_y \cdot h_m$. However, $(h + h_\kappa), (h - h_\kappa)$ are distinct prime quaternions, so it impossible for them to share a common factor. □

Definition 6.13. *Let* $G_{min}(h) = N(h_\kappa)$ *where* h_κ *is the quaternion integer with the smallest norm such that* $(h \pm h_\kappa)$ *are both prime quaternions.*

Example 6.4. *(a) if* $h = 1+2i+3j+4k$, $G_{min}(h) = 5$, *since the quaternion* h_κ *of smallest magnitude such that* $(h \pm h_\kappa)$ *are both prime is* $h_\kappa = \frac{1}{2}+\frac{1}{2}i+1\frac{1}{2}j+1\frac{1}{2}k$ *and* $N(h_\kappa) = 5$.

6.2.1 Is Goldbach's Conjecture True in $\mathbb{Z}[i, j, k]$?

Conjecture 6.1, Goldbach's conjecture among the quaternion integers, was tested empirically for all quaternions $q = a + bi + cj + dk$ where $0 \leq a \leq b \leq c \leq d$, $2 \leq N(h) \leq 10000$. This constitutes well over two million quaternions, each of which satisfies the conjecture.

Based on Figure 11, it seems that $G(h) > N(h)$ for some quaternions, a property which does not appear to manifest itself in any of the other algebras studied in this work. It is certainly impossible among the integers, but not strictly so among the Gaussian integers.

7 Final Remarks

7.1 Implementation Details

For each of the four algebraic contexts studied in this work, tools to study Goldbach's conjecture were developed in the Maple programming language. All of the empirical results and graphs presented in this work stem from these tools.

These include functions to compute G, G_{min} for all contexts, and G^{μ}, G^{s}, G^{μ}_{min}, G^{s}_{min} where relevant. Since Maple does not include tools to study the quaternions, an elementary library of tools to study these was also developed. The tools to study the integer subset monoids were developed in a general way, applicable to $\mathcal{M}[a]$ for any integer $a > 2$. Maple does not include tools to study such integer subsets, and so tools to study primality in such a context, analogous to those of the integers were developed, including a function analogous to $\pi(n)$ in the integers, to compute the number of primes no greater than some element of $\mathcal{M}[a]$, a function to determine whether an element $\mathcal{M}[a]_i$ is prime, and a function to compute the i^{th} prime element of $\mathcal{M}[a]$.

In total, the implementation consists of approximately two thousand lines of Maple code.

7.2 Conclusion

After defining and studying Goldbach's conjecture among the integers, the Abstract Goldbach conjecture was defined. This abstraction, based on a redefinition of the conjecture in $\mathbb{Z}$, allowed the study of Goldbach's conjecture to extend outside of the integers. The Abstract Goldbach conjecture was applied to the Gaussian integers, the 1-monoids and the Hurwitz integers.

In each context, Goldbach's conjecture was empirically tested, and no coun-

terexample was found. Two benchmarks were used in each context: $G(x)$ and $G_{min}(x)$, the former representing the number of solution for a given element, the latter representing the solution of minimal magnitude for that element. The graph of $G(x)$, Goldbach's Comet, is surprisingly similar among $\mathbb{Z}, \mathbb{Z}[i]$, and the variety of $\mathcal{M}[a]$ monoids. The comet does differ visually among the Hurwitz integers, having a shape more representative of the number of solutions increasing exponentially relative to magnitude. (See Figure 11). Figure 14 graphs the comet for various values in $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathcal{M}[4]$ to emphasize their similarity, and Table 9 lists average G_{min} values in these three contexts for all those elements of magnitude no greater than 2000 and 5000 respectively.

$AVG(G_{min}) \in$	$\mathbb{Z}$	$\mathbb{Z}[i]$	$\mathcal{M}[4]$
2000	17.22	6.07	0.97
5000	22.64	8.28	1.38

Table 9: Average G_{min} values

Countless number systems remain to be studied using the Abstract Goldbach conjecture. Among these, the variety of sets $\mathbb{Z}[\sqrt{d}]$ containing algebraic integers of the form $a + b\sqrt{d}$, the integral octonions, and the integral sedenions. The abstraction may also apply to less obvious contexts, such as polynomials (eg $\mathbb{Z}[x]$), or even to ideals. Any contexts possessing notions of composability and primality (or irreducibility) are potential candidates.

Locating an algebra in which the conjecture fails would be of tremendous value, since, upon comparing it with those algebras that do appear to satisfy the conjecture, it might become more evident which algebraic properties lead to the conjecture's truth. For example, suppose failure occurs among the integral

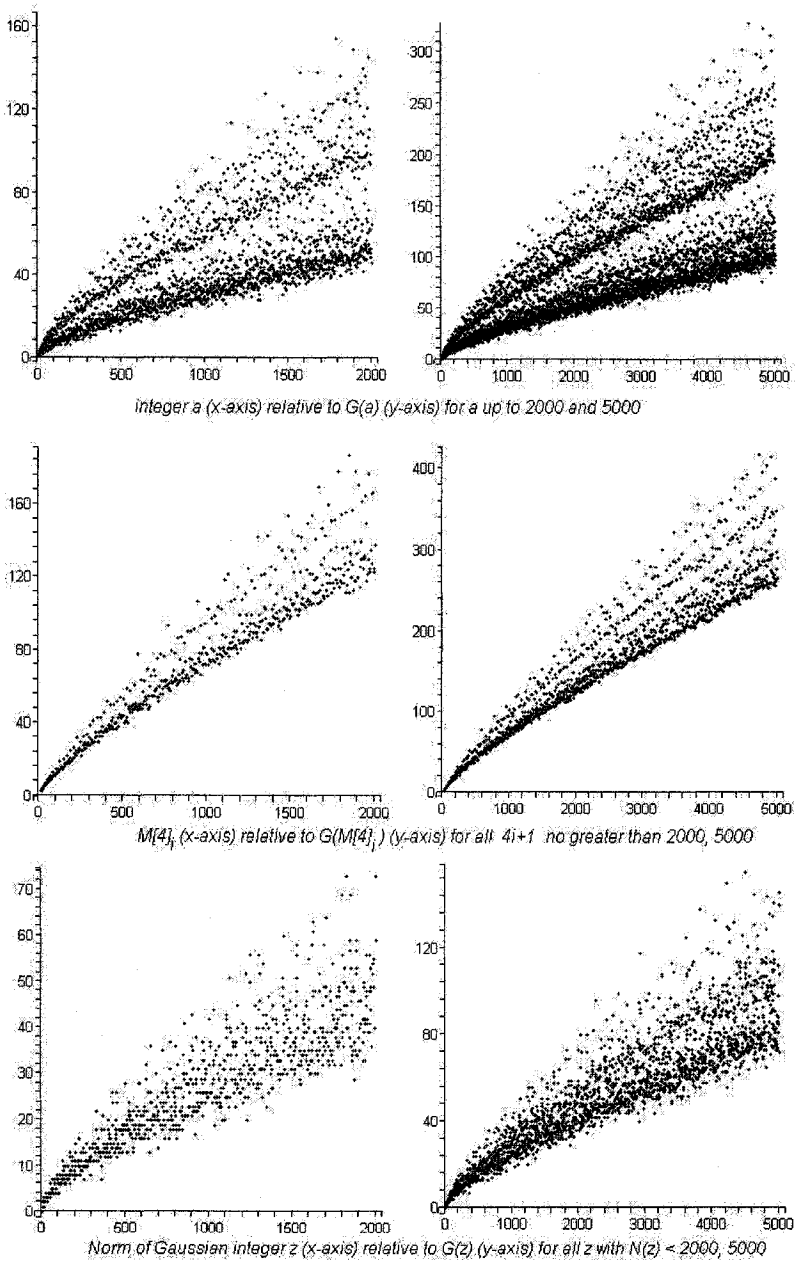

Figure 14: Goldbach's Comet

octonions, an algebraic context which lacks multiplicative associativity. This would imply that associativity is crucial to the truth of Goldbach's conjecture.

From the body of evidence presented in this work, certain properties can be dismissed as being likely algebraic properties crucial to the truth of the conjecture. For example, unique prime factorization is not likely to be crucial, given that the 1-monoids appear to satisfy Goldbach's conjecture. Similarly, multiplicative commutativity is not likely crucial, given that the integral quaternions appear to satisfy Goldbach's conjecture. As a greater variety of number contexts with differing algebraic properties are studied, various suspects can be exonerated, as in a murder mystery. In the end, it may be Associativity, in the conservatory, with a candlestick.

If there is a very simple algebraic property which draws the line between those algebras which satisfy Goldbach's conjecture and those that do not, then a proof of Goldbach's conjecture would almost certainly involve that property. If that property holds in many algebras, then such a proof would be very general in nature, since the scope of the mathematics shared by all algebras satisfying such a property would likely be very small. For example, consider the mathematical properties shared by $\mathbb{Z}, \mathbb{Z}[i], \mathcal{M}[a]$ and $\mathbb{Z}[i,j,k]$. They do not all satisfy unique prime factorization, nor multiplicative commutativity, and addition is not a binary operator on them all. However, they do share some properties related to multiplication, such as associativity. And they share other very high-level algebraic properties, such as the property that every element can be factored into a product of primes. As more algebras are shown to satisfy Goldbach's conjecture, the mathematical properties shared collectively by all those which satisfy it diminishes in scope and complexity,implying that a proof of the conjecture may be very simple, rather than grandly complex, as is currently assumed.

There is another, less seductive possibility: that Goldbach's conjecture is simply true, and no argument can be formulated to prove it. That Goldbach's conjecture is just some stochastic phenomenon is not entirely out of the question. Although it seems very likely that all integers, and the other algebras studied in this work satisfy Goldbach's conjecture, there is no guarantee that this can be argued conclusively through some entailment of logic.

In any of the algebras studied in this work, the truth of Goldbach's conjecture is intimately related to the distribution of prime elements there. In turn, the distribution of prime elements in the non-integer contexts discussed in this work are very closely related to the distribution of the prime integers themselves. Therefore, there is a relationship between the truth of Goldbach's conjecture in the integers and the non-integer contexts. The author has been unable to construct a chain of logic whereby the assumption of Goldbach's conjecture in one algebra implies its truth in another. However, such arguments do not seem entirely implausible.

This work began with a very simple idea, that Goldbach's conjecture among the integers is just a manifestation of a more general truth, one that the integers share with other number systems. Given that empirical observations found no counterexample in any of the non-integer contexts, it seems likely that the notion of equidistance to a pair of primes is a property common to these, and other number systems. It seems likely then, that the original statement of Goldbach's conjecture, the claim that every even integer can be written as a sum of two prime integers, is itself a manifestation of this more general phenomon, and that a better understanding of this equidistance principle could yield new methods of proof towards what is perhaps the most deceptively simple and longstanding problem remaining in number theory today.

References

[1] Allenby, R. *Rings, Fields and Groups. An Introduction to Abstract Algebra.* Edward Arnold. Scotland. 1983.

[2] Cameron, P. J. *Introduction to Algbera*, Oxford Science Publications.1998

[3] Conway, J.H. and Smith, D.A. *On Quaternions and Octonions. Their Geometry, Arithmetic and Symmetry*, Natick, Ma.: A K Peters. 2003.

[4] Chen, J. R. "On the representation of a large even integer as the sum of a prime and the product of at most two primes. *I. Sci. Sinica* 16, 157-176, 1973.

[5] Long. C. *Elementary Introduction to Number Theory*, D.C. Heath and Company. Lexington, Massachusetts. 1965.

[6] Fliegel, H. F. Robertson, D. S. "Goldbach's Comet: The Numbers Related to Goldbach's Conjecture.", *J. Recreational Mathematics*, 21(1), 1-7, 1989.

[7] Hardy G.H.,Wright E.M. *An Introduction to the Theory of Numbers*, Oxford University Press. London. 1960.

[8] Holben, C. A. and Jordan, J.H. "The twin prime problem and Goldbach's conjecture in the Gaussian Integers." *Fibonacci Quarterly* , 6(5), 1968.

[9] Gehring, F. W. *Elementary Methods in Number Theory*, Springer-Verlag New York. 1999.

[10] Gerstein L. J. "A Reformulation of the Goldbach Conjecture." *Mathematics Magazine*, 66(1), 44-45. 1993.

[11] Grosswald, E. *Topics from the Theory of Numbers*, Birkhauser. 1984.

[12] Landau, E. *Elementary Number Theory*, Chelsea Publishing Company. New York. 1966.

[13] Lang, S. *Algebraic Structures*, Addison-Wesley Publishing Company. 1967.

[14] Thomas, Hugh. Private Communication. 31 October 2005.

[15] Weissten E.W., Goldbach Conjecture. *MathWorld - A Wolfram Resource*, http://mathworld.wolfram.com/GoldbachConjecture.html.

[16] Weissten E.W., Dirichlet Lambda Function, *MathWorld - A Wolfram Resource*, http://mathworld.wolfram.com/DirichletLambdaFunction.html.

[17] Weissten E.W., Landau's Problems,*MathWorld - A Wolfram Resource.* http://mathworld.wolfram.com/LandausProblems.html.

[18] Wang,Yuan *The Goldbach Conjecture*, World Scientific, 2003.

[19] Euler's major correspondents, *The works of Leonhard Euler online*, http://www.eulerarchive.org/.

Vita

Candidate's full name: John-Keith Stewart

Universities attended:

University of New Brunswick, Bachelor of Computer Science, 2004