# AN ALGEBRAIC APPROACH TO THE GOLDBACH AND POLIGNAC CONJECTURES

JASON R. SOUTH
MAY 16, 2024

Abstract. This paper will give both the necessary and sufficient conditions required to find a counter-example to the Goldbach Conjecture by using an algebraic approach where no knowledge of the gaps between prime numbers is needed. To eliminate ambiguity the set of natural numbers, $\mathbb{N}$, will include zero throughout this paper. It will be shown there exists a counter-example to the Goldbach Conjecture, given by $2a$ where $a \in \mathbb{N}_{>3}$, if and only if for each prime $p_i < a$ there exists some unique $q_i, \alpha_i \in \mathbb{N}$ where $a < q_i < 2a$ and $2a = q_i + p_i$ along with the condition that $\prod_{i=1}^{\pi(a)} q_i = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}$. A substitution of $q_i = 2a - p_i$ for each $q_i$ from each sum gives the product relationship $\prod_{i=1}^{\pi(a)}(2a-p_i) = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}$. Therefore, if a counter-example exists to the Goldbach Conjecture, then there exists a mapping $\mathcal{G}_- : \mathbb{C} \to \mathbb{C}$ where

$$\mathcal{G}_-(z) = \prod_{i=1}^{\pi(a)}(z-p_i) - \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}$$

and $\mathcal{G}_-(2a) = 0$. A proof of the Goldbach Conjecture will be given utilizing Hensel's Lemma to show $2a$ must be of the form $2a = p_i^{\alpha_i} + p_i$ for all primes up to $a$ when $a > 3$. However, this leads to contradiction since $2a < a\#$ for all $a > 4$.

A similar method will be employed to give the necessary and sufficient conditions when an even number is not the difference of two primes with one prime being less than that even number. To begin, let $a \in \mathbb{N}_{>3}$ with the condition that the function $\gamma(a+1)$ is equal to one if $a+1$ is prime and zero otherwise. $2a$ is a counter-example if and only if for each prime $p_i < a$ there exists some unique $u_i, \beta_i \in \mathbb{N}$ where $2a < u_i \leq 3a$ and $2a = u_i - p_i$ along with product relationship $\prod_{i=1}^{\pi(a)} u_i = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta_i}$. A substitution of $u_i = 2a + p_i$ for each $u_i$ from each sum gives $\prod_{i=1}^{\pi(a)}(2a+p_i) = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta_i}$. Therefore, if a counter-example exists, it is possible to define the mapping $\mathcal{G}_+ : \mathbb{C} \to \mathbb{C}$ where

$$\mathcal{G}_+(z) = \prod_{i=1}^{\pi(a)}(z+p_i) - (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta_i}$$

and $\mathcal{G}_+(2a) = 0$. A proof will then be given that every even number is the difference of two primes by showing $2a$ must be of the form $2a = p_i^{\beta_i} - p_i$ for all odd primes up to $a$ when $a > 3$ to the equation above, leading to the same contradiction as the Goldbach Conjecture since $2a < a\#$ for $a > 4$. These proofs will have implications for proving the Polignac Conjecture.

## Contents

## 1. Introduction

The Goldbach Conjecture, page 117 in [8], appeared in a correspondence between Leonard Euler and Christian Goldbach in 1742 where it was suspected that every number greater than two could be written as the sum of three primes. Since the number one was considered a prime, however, no longer is, this conjecture has been split up into a strong and a weak version. The strong version in some texts may be referred to as the "binary" Goldbach Conjecture. The weak version is sometimes named the "ternary" conjecture as it involves three prime numbers.

The strong version of the Goldbach Conjecture states that for every even integer greater than two there will exist two primes whose sum is that even number. Although this conjecture is simple to state all attempts to prove it, or find a counter-example, have failed. With that said, this conjecture has been verified to an astonishing degree. In July of 2000 Jörg Richstein published a paper [9] using computational techniques showing that the Goldbach Conjecture was valid up to $4 \times 10^{14}$. In November of 2013 a paper [4] was published by Thomás Oliveira e Silva, Siegfried Herzog, and Silvo Pardi which also used advances in computational computing proving that the binary form of the Goldbach Conjecture is true up to $4 \times 10^{18}$.

The weaker version of the Goldbach Conjecture, or Ternary Conjecture, states that every odd number greater than 7 can be written as the sum of three prime numbers. Much like the strong version, this conjecture has also been verified up to large orders of magnitude. As an example, in 1998 [11] Yannick Saouter proved this conjecture up to $10^{20}$. In fact, it was shown that if the generalization of the Reimann Hypothesis were true, that the Ternary Conjecture would follow. This was proven by Hardy and Littlewood [5] in 1923. Since the Generalized Reimann Hypothesis is still an open question, this did not give a definitive answer as to the truth of the Ternary Conjecture, however, it did provide a possible path to follow.

Another breakthrough in the Ternary Conjecture came in 2013 when Herald Helfgott verified in a paper [7] that the Ternary Conjecture was valid up to $10^{30}$. Later that year a preprint [6] by Harold Helfgott was placed on the ARXIV claiming that the Ternary Conjecture is true. Although this paper has not been published as of yet, it has been accepted by many in the mathematics community as being true.

## 2. Methodology and Summary of Results

All attempts to prove the Goldbach Conjecture have failed. Many of these attempts rely on an analytic number theory approach such as analyzing the gaps between primes [14]. Another method is to assume a certain hypothesis is true, such as the Generalized Reimann Hypothesis, to show that hypothesis implies one of these conjectures [5]. If that hypothesis can then be proven, the conjecture would follow. There are also experimental [3] along with computational results from [9], [4], and [11], however, these methods will most likely require major breakthroughs in order to proceed. For this reason, a new approach is needed.

The method which will be explored in this paper is a novel technique that will be used to determine algebraically both the necessary and sufficient conditions for a counter-example to the Goldbach Conjecture to be discovered. The advantage of this method lies in the fact that it circumvents two main reasons why a proof of the Goldbach Conjecture has not been discovered. The first of these difficulties in finding a proof is simply that there is no known formula that allows one to determine precisely how many prime numbers there are in a given range. The Prime Number Theorem[1] [12] does give an approximation to the number of primes up to a given value; however, this alone is not sufficient to give strong enough evidence that

[1] A good approximation for $\pi(n)$, where $n > 1$, is given by $\frac{n}{\ln(n)}$

the conjectures hold for any value chosen. For this reason most probabilistic arguments about how many primes pairs there could be which sum up to a desired even number will fail.

The second issue is that there is no known parameterization of the prime numbers, or even a computationally efficient way to determine when a number is prime. Wilson's Theorem[2] [13] does provide both the necessary and sufficient conditions for determining if a number is prime; however, since it is a function of the factorial it is computationally inefficient to use in any practical manner. Because of these two facts, any question about additive properties of the primes has been destined to run into near insurmountable difficulties using current techniques.

To begin laying the foundation for this new method a thought experiment will be given. Suppose one wished to show that the number 20 satisfied the Goldbach Conjecture. A simple way to proceed is to take each prime up to 10, labeled by the sequence $p_1 < p_2 < p_3 < p_4$, and assign to it a unique $q_i$ labeled by the sequence $q_1 > q_2 > q_3 > q_4$ where $20 = q_i + p_i$. This allows for the following set of arithmetic relationships.

$$20 = 18 + 2 = 17 + 3 = 15 + 5 = 13 + 7 \tag{2.1}$$

Assuming that 20 is not the sum of two prime numbers, it then follows from The Fundamental Theorem of Arithmetic [1] that there must exist a unique sequence of $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{N}$ where

$$q_1 q_2 q_3 q_4 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} p_4^{\alpha_4}. \tag{2.2}$$

However,

$$18 \times 17 \times 15 \times 13 \neq 2^{\alpha_1} \times 3^{\alpha_2} \times 5^{\alpha_3} \times 7^{\alpha_4} \tag{2.3}$$

for any sequence of exponents restricted to the natural numbers. Since each $q_i$ on the L.H.S. ranges between 10 and 20 it can be seen that equation 2.3 is true if and only if at least one number on the L.H.S. is not divisible by any prime on the R.H.S., thus proving at least one $q_i$ is a new prime. Therefore, it may be concluded that 20 can be written as the sum of two primes without having any particular knowledge about the distribution of the prime numbers or which prime numbers sum up to 20. All that is needed is the closure property of the integers, page 1 in [8], along with the Fundamental Theorem of Arithmetic. This method can be extended to a general case given by Definition 4.1 in the following section. An analysis of this polynomial, along with the condition where $2a$ is a root will be explored.

This same method will be used to determine if every even number, again given by $2a$, is the difference of two primes where one prime is less than $a$. Slight modifications need to be made which will be made evident with a similar thought experiment used for the Goldbach Conjecture. To begin, assume that the number 20 was not the difference of two primes where one prime was less than 10. Taking the same approach as in the Goldbach Conjecture shows each prime up to 10, labeled by the sequence $p_1 < p_2 < p_3 < p_4$, may be assigned a unique $q_i$ labeled by the sequence $q_1 < q_2 < q_3 < q_4$ where $20 = q_i - p_i$. This allows for the following

$$20 = 22 - 2 = 23 - 3 = 25 - 5 = 27 - 7. \tag{2.4}$$

At this point careful attention needs to be given to the fact that the $q_1 = 22$ term is divisible by a prime greater than 10, but composite. Defining $p_5 = 11$ will be useful since 11 is a prime greater than 10. However, it is important to note that this is the only time this can occur since $q_1$ is the only even term and any odd $20 < q_i \leq 30$ can not be divisible by any primes greater than 10 unless it is itself prime. Assuming that 20 is not the difference of two prime numbers, then The Fundamental Theorem of Arithmetic states that there exists a unique sequence of $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{N}$ where

$$q_1 q_2 q_3 q_4 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} p_4^{\alpha_4} p_5. \tag{2.5}$$

However,

$$27 \times 25 \times 23 \times 22 \neq 2^{\alpha_1} \times 3^{\alpha_2} \times 5^{\alpha_3} \times 7^{\alpha_4} \times 11 \tag{2.6}$$

[2] A number $p$ is a prime only if there is some integer $n$ where $(p-1)! + 1 = pn$.

for any sequence of exponents restricted to the natural numbers. Since each $q_i$ on the L.H.S. ranges between 20 and 30 it can be seen that equation 2.6 is true if and only if at least one number on the L.H.S. is not divisible by any prime on the R.H.S., thus proving at least one $q_i$ is a new prime. Therefore, 20 can be written as the difference of two prime numbers. As with the Goldbach Conjecture, formalizing to a general case will be done in Definition 5.1.

## 3. The Goldbach Conjecture and Goldbach Difference Conjecture

In order to begin this paper each conjecture will be stated along with the necessary and sufficient conditions required to find a count-example. Once this is done, it will be shown that a counter-example cannot exist, hence proving the conjectures true. The method for finding counter-examples to each conjecture is very similar.

*Conjecture* 3.1. Let $a \in \mathbb{N}_{>3}$ and the primes up to $a$ are given by $p_1 < p_2 < \cdots < p_{\pi(a)}$. The *Goldbach Conjecture* (G.C.) states there exists two primes $q_i, p_i$ where $2a = q_i + p_i$.

**Theorem 3.2.** *Let $a \in \mathbb{N}_{>3}$. Then $2a$ is a counter-example to the G.C. iff for each prime $p_i \leq a$ there exists a unique $\alpha_i \in \mathbb{N} \cup \{0\}$ where $\prod_{i=1}^{\pi(a)}(2a - p_i) = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}$.*

*Proof.* If there exists a counter-example to the G. C. given by $2a$, then for each prime $p_i < a$ there exists some unique $q_i$ where $a < q_i < 2a$ and

$$2a = q_i + p_i \tag{3.1}$$

with $q_i$ being a composition of primes up to $a$. Therefore, under the Fundamental Theorem of Arithmetic it follows that for each prime $p_i < a$ there must exist a unique $\alpha_i \in \mathbb{N}$ where

$$\prod_{i=1}^{\pi(a)} q_i = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}. \tag{3.2}$$

A substitution of $q_i = 2a - p_i$ for each $q_i$ from 3.1 in equation 3.2 gives

$$\prod_{i=1}^{\pi(a)} (2a - p_i) = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}. \tag{3.3}$$

Conversely, if there exists some $2a > 6$ where equation 3.3 holds for some $\alpha_1, \alpha_2, \ldots, \alpha_{\pi(a)} \in \mathbb{N}$, then equations 3.1 and 3.2 are true with the Fundamental Theorem of Arithmetic showing no $q_i$ can be prime in equation 3.1. Therefore, the G.C. would be shown false. □

**Lemma 3.3.** *For any $\alpha_i$ it follows that $\alpha_i > 0$ if and only if $p_i | q_i$ or $p_i | q_j$ for some $j \neq i$.*

*Proof.* From equation 3.2 it can be seen upon inspection that if any $\alpha_i > 0$, then that $p_i$ must be a divisor of the R.H.S. of the equation and $p_i | p_i^{\alpha_i}$. Therefore, that $p_i$ divides the L.H.S. of the equation and must divide its corresponding $q_i$ or some other $q_j$.

Conversely, from equation 3.2 if any prime $p_i$ is a divisor of its corresponding $q_i$ or some other $q_j$, then that $p_i$ divides the R.H.S. of equation 3.2 showing $p_i | p_i^{\alpha_i}$ where $\alpha_i > 0$. □

**Lemma 3.4.** *For any prime $p_i < a$ it follows $p_i | 2a$ if and only if $p_i | q_i$.*

*Proof.* Under equation 3.1 it is seen upon inspection if $p_i | q_i$, then $p_i | 2a$. Conversely, from equation 3.1 it follows that if any $p_i | 2a$, then $p_i | q_i$. □

**Lemma 3.5.** *For any prime $p_i \leq a$, if $p_i | q_i$, then $p_i \nmid q_j$ for any $j \neq i$.*

*Proof.* Under equation 3.1 of Theorem 3.2 it follows for any primes $p_i, p_j \leq a$

$$q_i + p_i = q_j + p_j. \tag{3.4}$$

If some $p_i$ existed where $p_i | q_i$ and $p_i | q_j$ for some $j \neq i$ in equation 3.4, then $p_i | p_j$. Since both $p_i, p_j$ are primes, then $p_i \nmid p_j$ when $j \neq i$. Thus, if any $p_i | q_i$, then $p_i \nmid q_j$ for any $j \neq i$. □

**Proposition 3.6.** *If $p_i | 2a$, there exists $n_i, \alpha_i \in \mathbb{N} \backslash \{0\}$ s.t. $2a = n_i p_i^{\alpha_i} + p_i$ and $GCD(p_i, n_i) = 1$.*

*Proof.* Suppose some $p_i|2a$. From Lemmas 3.3 through 3.5 it can be seen that $p_i$ only divides its corresponding $q_i$ in equations 3.1 and 3.2 showing that there exists some $n_i \in \mathbb{N}$ where $q_i = n_i p_i^{\alpha_i}$. A substitution into equation 3.1 shows $2a = n_i p_i^{\alpha_i} + p_i$ where $GCD(p_i, n_i) = 1$. □

A similar conjecture to the G.C. can be defined by asking whether or not every even number may be written as the difference of two prime numbers.

*Conjecture* 3.7. Let $a \in \mathbb{N}_{>3}$ and the primes up to $a$ are given by the sequence $p_1 < p_2 < \cdots < p_{\pi(a)}$. The *Goldbach Difference Conjecture* (G.D.C.) states that for every value of $a > 3$ there exists two primes $u_i, p_i$ such that $2a = u_i - p_i$ and $p_i \leq a$.

**Remark 3.8.** At this point it is necessary to define a function that will account for the case where $a+1$ is prime. This lies in the fact that in Conjecture 3.7 it is possible for $a+1$ to be prime, but $2a+2$ to be composite. Since all other $2a < u_i \leq 3a$ every other $u_i$ is either a new prime greater than $a+1$ or a composition of primes up to $a$.

**Definition 3.9.** Let the function $\gamma(a+1)$ be defined by characteristics

$$\gamma(a+1) = \begin{cases} 1, & \text{if } a+1 \text{ is prime} \\ 0, & \text{if } a+1 \text{ is not prime.} \end{cases} \tag{3.5}$$

**Theorem 3.10.** *Let $a \in \mathbb{N}_{>3}$. Then $2a$ is a counter-example to the G.D.C. iff for each prime $p_i \leq a$ there exists a unique $\beta_i \in \mathbb{N} \cup \{0\}$ where $\prod_{i=1}^{\pi(a)}(2a+p_i) = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta}$.*

*Proof.* If there exists a counter-example to the G.D.C. given by $2a$, then for each prime $p_i < a$ there exists some unique $u_i$ where $2a < u_i \leq 3a$ and

$$2a = u_i - p_i \tag{3.6}$$

with $u_i$ being a composition of primes up to $a$. Therefore, under the Fundamental Theorem of Arithmetic it follows that for each prime $p_i < a$ there must exist a unique $\beta_i \in \mathbb{N}$

$$\prod_{i=1}^{\pi(a)} u_i = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta}. \tag{3.7}$$

Substituting $u_i = 2a + p_i$ from equation 3.6 into 3.7 gives

$$\prod_{i=1}^{\pi(a)} (2a+p_i) = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta}. \tag{3.8}$$

Conversely, if there exists some $2a > 6$ where equation 3.8 holds, then under the Fundamental Theorem of Arithmetic equations 3.6 and 3.7 are true with no $u_i$ being prime in equation 3.6. A substitution of each $u_i$ from 3.6 into equation 3.7 shows $2a$ is a solution to equation 5.1 and it must be a counter-example to the G.D.C. □

**Lemma 3.11.** *For any $\beta_i$ it follows that $\beta_i > 0$ if and only if $p_i|u_i$ or $p_i|u_j$ for some $j \neq i$.*

*Proof.* From equation 3.7 it can be seen upon inspection that if any $\beta_i > 0$, then that $p_i$ must be a divisor of the R.H.S. of the equation. Therefore, that $p_i$ divides the L.H.S. of the equation and must divide its corresponding $u_i$ or some other $u_j$.

Conversely, from equation 3.7 if any prime $p_i$ is a divisor of its corresponding $u_i$ or some other $u_j$, then that $p_i$ divides the R.H.S. of equation 3.7 showing $p_i | p_i^{\beta_i}$ where $\beta_i > 0$. □

**Lemma 3.12.** *For any prime $p_i < a$ it follows $p_i|2a$ if and only if $p_i|u_i$.*

*Proof.* Under equation 3.6 it is seen upon inspection if $p_i|u_i$, then $p_i|2a$. Conversely, from equation 3.6 it follows that if any $p_i|2a$, then $p_i|u_i$. □

**Lemma 3.13.** *For any prime $p_i \leq a$, if $p_i|u_i$, then $p_i \nmid u_j$ for any $j \neq i$.*

*Proof.* Under equation 3.6 of Theorem 3.10 it follows for any primes $p_i, p_j \leq a$

$$u_i - p_i = u_j - p_j. \tag{3.9}$$

If some $p_i$ existed where $p_i | u_i$ and $p_i | u_j$ for some $j \neq i$ in equation 3.9, then $p_i | p_j$. Since both $p_i, p_j$ are primes, then $p_i \nmid p_j$ when $j \neq i$. Thus, if any $p_i | u_i$, then $p_i \nmid u_j$ for any $j \neq i$. □

**Proposition 3.14.** *If $p_i | 2a$, there exists $m_i, \beta_i \in \mathbb{N} \backslash \{0\}$ s.t. $2a = m_i p_i^{\beta_i} - p_i$, $GCD(p_i, m_i) = 1$.*

*Proof.* Suppose some $p_i | 2a$. From Lemmas 3.11 through 3.13 it can be seen that $p_i$ only divides its corresponding $u_i$ in equations 3.6 and 3.7 showing there exists some non-zero $m_i \in \mathbb{N}$ where $u_i = m_i p_i^{\beta_i}$. A substitution into equation 3.6 shows $2a = m_i p_i^{\alpha_i} - p_i$ where $GCD(p_i, m_i) = 1$. □

**Proposition 3.15.** *Let $a \in \mathbb{N}_{>3}$. Then $2a$ is neither the sum nor difference of two primes where one prime $p_i \leq a$ if and only if it is a solution to equations 3.3 and 3.8*

*Proof.* This follows directly from Theorems 3.2 and 3.10. □

*Conjecture* 3.16. No even number greater than six is a counter-example to the G.C. and G.D.C.

## 4. Construction of the Goldbach Polynomial Type I

The above conjecture will be proven by assuming there exists a counter-example, given by $2a$ where $a \in \mathbb{N}_{>3}$ along with the condition that $2a$ is a solution to both equations 3.3 and 3.8 in Theorems 3.2 and 3.10. Using Theorems 3.2 and 3.10 it is possible to define polynomials based on the behavior of equations 3.3 and 3.8. It will then be shown no counter-examples exist as they would lead to contradiction. To begin, it is possible to turn equations 3.3 and 3.8 into polynomials below where a more in-depth analysis is possible.

**Definition 4.1.** It was shown under Theorem 3.2 that a counter-example to the G.C. 3.1 is given by $2a$ where $a \in \mathbb{N}_{>3}$ if and only if it is possible to assign to each prime $p_i \leq a$ some unique $\alpha_i \in \mathbb{N}$ where equation 3.3 holds. Assume $2a$ is a counter-example. To construct the *Goldbach Polynomial Type I* (G.P.I.), it is possible to define the mapping $\mathcal{G}_- : \mathbb{C} \to \mathbb{C}$ where

$$\mathcal{G}_-(z) = \prod_{i=1}^{\pi(a)} (z - p_i) - \prod_{i=1}^{\pi(a)} p_i^{\alpha_i} \tag{4.1}$$

and $2a$ is a root. This shows $\mathcal{G}_-(2a) = 0$ produces equation 3.3 in Theorem 3.2.

**Definition 4.2.** The Fundamental Theorem of Algebra ensures that there exists, with reciprocity allowed, *Goldbach Polynomial Roots* where the set $G = \{r_k \in \mathbb{C} : \mathcal{G}_-(r_k) = 0\}$. It then follows that equation 4.1 may be written as

$$\mathcal{G}_-(z) = \prod_{k=1}^{\pi(a)} (z - r_k). \tag{4.2}$$

where Definition 4.1 in conjunction with the above factorization shows

$$\prod_{k=1}^{\pi(a)} (z - r_k) = \prod_{k=1}^{\pi(a)} (z - p_k) - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k}. \tag{4.3}$$

**Lemma 4.3.** *There exists some root unique $r_i \in G$ where $r_i \equiv 0 \pmod{p_i}$ iff $\alpha_i > 0$.*

*Proof.* Assume $\alpha_i > 0$. From equation 4.3 in Definition 4.2 it follows for any integer $1 \leq \mu \leq \alpha_i$

$$\prod_{k=1}^{\pi(a)} (z - r_k) \pmod{p_i^{\alpha_i - \mu + 1}} \equiv \prod_{k=1}^{\pi(a)} (z - p_k) \pmod{p_i^{\alpha_i - \mu + 1}} \tag{4.4}$$

where it can be seen that there is a singular root at $z \equiv 0 \pmod{p_i}$ proving if $\alpha_i > 0$, there must exist a unique root $r_i \in G$ where $r_i \equiv 0 \pmod{p_i}$.

Alternatively, assume some $\alpha_i = 0$. From equation 4.3 in Definition 4.2

$$\prod_{k=1}^{\pi(a)}(z - r_k) \pmod{p_i} \equiv \prod_{k=1}^{\pi(a)}(z - p_k) - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i}. \tag{4.5}$$

Evaluating the equation above at $z = p_i$ gives $\prod_{k=1}^{\pi(a)}(p_i - p_k) = 0$ showing

$$\prod_{k=1}^{\pi(a)}(p_i - r_k) \pmod{p_i} \equiv -\prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i}. \tag{4.6}$$

Since the R.H.S. of the equation cannot be 0 because $p_i^{\alpha_i} = p_i^0 = 1$, it must follow that the L.H.S. is also not zero. Thus, if $\alpha_i = 0$, there exists no $r_i \equiv 0 \pmod{p_i}$. □

**Example 4.4.** Let $a = 3$. There exists a G.P.I., $\mathcal{G}_-(z) = (z-2)(z-3) - 2^2 \times 3$ and $\mathcal{G}_-(6) = 0$. Note $6 = 2^2 + 2 = 3 + 3$ in accordance with equations 3.1 and 3.2. There exists another root $r_2 = -1$ in accordance with Definition 4.2. Thus, the roots are given by the set $G = \{-1, 6\}$.

**Definition 4.5.** The *Goldbach Polynomial Type I Derivative* is given by

$$\mathcal{G}'_-(z) = \prod_{i=1}^{\pi(a)}(z - p_i)\left[\frac{1}{z - p_1} + \frac{1}{z - p_2} + \cdots + \frac{1}{z - p_{\pi(a)}}\right] \tag{4.7}$$

and follows directly from equation 4.1.

**Definition 4.6.** The *Goldbach Polynomial Type I Coefficients* are produced by Vietas Formulas [13] for equation 4.1 of Definition 4.1. It is possible to write out each constant term $c_{\pi(a)}, c_{\pi(a)-1}, \ldots, c_0$ for the G.P.I. in equations 4.1 and 4.7 in Definitions 4.1 and 4.5 in terms of the primes $p_i < a$. For this paper the only constants of importance are given by $c_1 = \mathcal{G}'_-(0)$ and $c_0 = \mathcal{G}_-(0)$ below.

$$\mathcal{G}'_-(0) = (-1)^{\pi(a)-1} a\#\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_{\pi(a)}}\right). \tag{4.8}$$

and

$$\mathcal{G}_-(0) = (-1)^{\pi(a)} a\# - \prod_{i=1}^{\pi(a)} p_i^{\alpha_i} \tag{4.9}$$

**Corollary 4.7.** *For any prime $p_i \leq a$ the $GCD(p_i, c_1) = 1$.*

*Proof.* The $c_1$ term in equation 4.8 of Definition 4.6 is the sum of $\pi(a)$ products consisting of $\pi(a) - 1$ primes. Since any prime $p_i \leq a$ is only absent from one product in the sum, $p_i \nmid c_1$ □

**Proposition 4.8.** *$\alpha_i > 0$ if and only if $\mathcal{G}_-(0) \equiv 0 \pmod{p_i}$.*

*Proof.* This follows directly From equation 4.9 where $\mathcal{G}_-(0) = (-1)^{\pi(a)} a\# - \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}$. □

**Proposition 4.9.** *For all prime $p_i \leq a$ the $\mathcal{G}'_-(0) \not\equiv 0 \pmod{p_i}$.*

*Proof.* This is a direct consequence of equation 4.8 of Definition 4.6. □

**Corollary 4.10.** *For any prime $p_i \leq a$ the $\mathcal{G}'_-(0) \equiv (-1)^{\pi(a)-1} \frac{a\#}{p_i} \pmod{p_i}$.*

*Proof.* Using equation 4.8 proves the corollary since only one term is not divisible by $p_i$. □

## 5. Construction of the Goldbach Polynomial Type II

Using a nearly identical procedure as was used in the previous section it is also important to expand this idea to Theorem 3.10 below.

**Definition 5.1.** It was shown under Theorem 3.10 that a counter-example to the G.D.C. is given by $2a$ where $a \in \mathbb{N}_{>3}$ if and only if it is possible to assign to each prime $p_i \leq a$ some unique $\beta_i \in \mathbb{N}$ where equation 3.8 holds. Assume $2a$ is a counter-example. To construct the *Goldbach Polynomial Type II* (G.P.II), it is possible to define the mapping $\mathcal{G}_+ : \mathbb{C} \to \mathbb{C}$

$$\mathcal{G}_+(z) = \prod_{i=1}^{\pi(a)}(z + p_i) - (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta}. \tag{5.1}$$

and $2a$ is a root. This shows $\mathcal{G}_+(2a) = 0$ produces equation 3.8 in Theorem 3.10.

**Definition 5.2.** The Fundamental Theorem of Algebra ensures that there exists, with reciprocity allowed, *Goldbach Difference Polynomial Roots* where $G' = \{r'_k \in \mathbb{C} : \mathcal{G}_+(r'_k) = 0\}$. It then follows that equation 5.1 may be written as

$$\mathcal{G}_+(z) = \prod_{k=1}^{\pi(a)}(z - r'_k). \tag{5.2}$$

where Definition 5.1 in conjunction with the above factorization shows

$$\prod_{k=1}^{\pi(a)}(z - r'_k) = \prod_{k=1}^{\pi(a)}(z + p_k) - (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k}. \tag{5.3}$$

**Lemma 5.3.** *There exists some root unique $r'_i \in G'$ where $r'_i \equiv 0 \pmod{p_i}$ iff $\beta_i > 0$.*

*Proof.* Assume $\beta_i > 0$. From equation 5.3 in Definition 5.2, for any integer $1 \leq \mu \leq \beta_i$

$$\prod_{k=1}^{\pi(a)}(z - r'_k) \pmod{p_i^{\beta_i-\mu+1}} \equiv \prod_{k=1}^{\pi(a)}(z + p_k) \pmod{p_i^{\beta_i-\mu+1}} \tag{5.4}$$

where it can be seen that there is a singular root at $z \equiv 0 \pmod{p_i}$ proving if $\beta_i > 0$, there must exist a unique root $r'_i \in G'$ where $r'_i \equiv 0 \pmod{p_i}$.

Alternatively, assume some $\beta_i = 0$. From equation 5.3 in Definition 5.2

$$\prod_{k=1}^{\pi(a)}(z - r_k) \pmod{p_i} \equiv \prod_{k=1}^{\pi(a)}(z + p_k) - (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i}. \tag{5.5}$$

Evaluating the equation above at $z = p_i$ gives $\prod_{k=1}^{\pi(a)}(p_i + p_k) \equiv 0 \pmod{p_i}$ showing

$$\prod_{k=1}^{\pi(a)}(p_i - r_k) \pmod{p_i} \equiv -(a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i}. \tag{5.6}$$

Since the R.H.S. of the equation cannot be 0 because $p_i^{\beta_i} = p_i^0 = 1$ and Definition 3.9 ensures $p_i \nmid (a+1)$, the L.H.S. is not zero. Thus, if $\beta_i = 0$, there exists no $r'_i \equiv 0 \pmod{p_i}$. ☐

**Example 5.4.** Let $a = 3$. There exists a G.P.II, $\mathcal{G}_+(z) = (z+2)(z+3) - 2^3 \times 3^2$ since $\mathcal{G}_+(6) = 0$. Note $6 = 2^3 - 2 = 3^2 - 3$ in accordance with equations 3.6 and 3.7. There exists another root $r'_2 = -11$ in accordance with Definition 5.2 the roots are given by $G' = \{-11, 6\}$.

**Definition 5.5.** The *Goldbach Polynomial Type II Derivative* is given by

$$\mathcal{G}'_+(z) = \prod_{i=1}^{\pi(a)}(z + p_i)\left[\frac{1}{z+p_1} + \frac{1}{z+p_2} + \dots \frac{1}{z+p_{\pi(a)}}\right] \tag{5.7}$$

and follows directly from equation 5.1.

**Definition 5.6.** The *Goldbach Polynomial Type II Difference Coefficients* are produced by Vietas Formulas [13] in the same manner as equations 4.1 and 4.5 of Definitions 4.1 and 4.5. It is possible to write out each constant term $d_{\pi(a)}, d_{\pi(a)-1}, \ldots, d_0$ for the G.P.II in equations 5.1 and 5.7 in Definitions 5.1 and 5.5 in terms of the primes $p_i < a$. For this paper the only constants of importance are given by $d_1 = \mathcal{G}'_+(0)$ and $d_0 = \mathcal{G}_+(0)$ below. The only difference in these equations from previous sections are the minus signs and $a+1$ term below.

$$\mathcal{G}'_+(0) = a\#\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_{\pi(a)}}\right) \tag{5.8}$$

and

$$\mathcal{G}_+(0) = a\# - (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta}. \tag{5.9}$$

**Corollary 5.7.** *For any prime $p_i \leq a$ the $GCD(p_i, d_1) = 1$.*

*Proof.* The $d_1$ term in equation 5.8 of Definition 5.6 is the sum of $\pi(a)$ products consisting of $\pi(a)-1$ primes. Since any prime $p_i \leq a$ is only absent from one product in the sum, $p_i \nmid d_1$ □

**Proposition 5.8.** *$\beta_i > 0$ if and only if $\mathcal{G}_+(0) \equiv 0 \pmod{p_i}$.*

*Proof.* This follows From Definition 5.1 where $\mathcal{G}_+(0) = a\# - (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta_i}$. □

**Proposition 5.9.** *For all prime $p_i \leq a$ the $\mathcal{G}'_+(0) \not\equiv 0 \pmod{p_i}$.*

*Proof.* This is a direct consequence of equation 5.8 of Definition 5.6. □

It is actually possible to calculate an explicit value for $\mathcal{G}'_+(0)$ using Definition 5.6

**Corollary 5.10.** *For any prime $p_i \leq a$ the $\mathcal{G}'_+(0) \equiv \frac{a\#}{p_i} \pmod{p_i}$.*

*Proof.* Using equation 5.8 proves the corollary since only one term is not divisible by $p_i$. □

## 6. Preliminary Analysis of $\mathcal{G}_-(z)$ when $\mathcal{G}_-(2a) = 0$

**Proposition 6.1.** *Under equation 4.1 of Definition 4.1 it follows that $2a|\mathcal{G}_-(0)$.*

*Proof.* With it assumed $\mathcal{G}_-(2a) = 0$ in 4.1, it then follows that $2a|\mathcal{G}_-(0)$ since $2a$ is a root. □

**Proposition 6.2.** *The $GCD(2a, \frac{\mathcal{G}_-(0)}{2a}) = 1$.*

*Proof.* From Definition 4.6 and Corllary 4.7, it follows that the $GCD(2a, c_1) = 1$. With $\mathcal{G}_-(2a) = 0$ the equation 4.1 becomes

$$2a\left[(2a)^{\pi(a)-1} + c_{\pi(a)-1}(2a)^{\pi(a)-2} + c_{\pi(a)-2}(2a)^{\pi(a)-3} + \cdots + c_1\right] = -c_0 \tag{6.1}$$

where the only term in the brackets not multiplied by $2a$ is the $c_1$ term. Therefore, the $GCD(2a, \frac{c_0}{2a}) = 1$ is a consequence of $\mathcal{G}_-(2a) = 0$ in equation 4.1 and Corollary 4.7. □

**Corollary 6.3.** *$2a$ is not a repeated root when $\mathcal{G}_-(2a) = 0$.*

*Proof.* This follows directly from Proposition 6.2 and the Rational Root Theorem. □

**Corollary 6.4.** *Any rational root other than $2a$ is odd when $\mathcal{G}_-(2a) = 0$.*

*Proof.* Under Proposition 6.2 it was shown that $GCD(2a, \frac{c_0}{2a}) = 1$. Taking all roots with multiplicity to be $r_1, r_2, \ldots r_{\pi(a)} \in \mathbb{C}$ with $r_1 = 2a$, it then follows that $GCD(2a, \frac{r_2 \cdots r_{\pi(a)}}{2a}) = 1$. Thus, W.L.O.G. assume there exist a rational root $r_2$. With the G.P. being monic, it follows that all rational roots are integers. Therefore, $r_2 \in \mathbb{Z}$. Since $r_2|c_0$ and $c_0 \in \mathbb{Z}$, there exists some integer $x$ where $\frac{c_0}{2a} = r_2 x$ and the $GCD(2a, r_2 x) = 1$, proving that $GCD(2a, r_2) = 1$. □

**Corollary 6.5.** *If $\mathcal{G}_-(2a) = 0$, then there are no other rational roots to the G.P. for $\pi(a) > 2$.*

*Proof.* W.L.O.G. let the G.R. $r_1 = 2a$ and assume for the sake of contradiction there exists some other rational root $r_2$. Since the G.P. is monic, the Rational Root Theorem shows that $r_2 \in \mathbb{Z}$. Proposition 6.2 ensures $2a$ can not be a repeated root, and Corollary 6.4 ensures $2 \nmid r_2$. Therefore, it must follow from equation 4.1 with $\mathcal{G}_-(r_2) = 0$ that

$$\prod_{i=1}^{\pi(a)} (r_2 - p_i) = \prod_{i=1}^{\pi(a)} p_i^{\alpha_i}. \tag{6.2}$$

With $2 \nmid r_2$, only one term of the L.H.S. above is not divisible by 2. Hence, $\alpha_1 \geq \pi(a) - 1$ where

$$2^{\alpha_1} \geq 2^{\pi(a)-1}. \tag{6.3}$$

Knowing the minimum value for $\alpha_1$, equation 3.1 allows for again to write

$$2a = q_1 + 2. \tag{6.4}$$

It follows from Corllary 3.5 that $q_1$ is the only even $q_i$ corresponding to the root $2a$, as all other $q_{i>1}$ must be odd since all other prime $p_{i>1}$ are odd. Hence, from equation 6.3 in conjunction with equation 6.4 it may be seen that $q_1 \geq 2^{\pi(a)-1}$. Therefore, it follows

$$2a \geq 2^{\pi(a)-1} + 2$$
$$a - 1 \geq 2^{\pi(a)-2}.$$

However, when $a = 19$ and $\pi(19) = 8$ a substitution of $a = 19$ in the equations above gives

$$18 \ngeq 2^6$$

producing a contradiction. Furthermore, Chebyshev's Theorem says that there for any $a \in \mathbb{N}$ where $a > 1$ there is always some prime $p$ such that $a \leq p < 2a$. Therefore, whenever $a \geq 19$ then $a \ngeq 2^{\pi(a)-2}$. This result can even be made stronger given there are no solutions to the G.P. where $2a$ is a G.R. and $2 < \pi(a) \leq 19$. Therefore, the corollary is true. $\square$

It is possible to use this same line of reasoning to analyze the structure of $2a$ when $\mathcal{G}_+(2a) = 0$.

## 7. Preliminary Analysis of $\mathcal{G}_+(z)$ when $\mathcal{G}_+(2a) = 0$

**Proposition 7.1.** *Under equation 5.1 of Definition 5.1 it follows that* $2a|\mathcal{G}_+(0)$.

*Proof.* With it assumed $\mathcal{G}_+(2a) = 0$ in 5.1, it then follows that $2a|\mathcal{G}_+(0)$ since $2a$ is a root. $\square$

**Proposition 7.2.** *The* $GCD(2a, \frac{\mathcal{G}_+(0)}{2a}) = 1$.

*Proof.* From Definition 5.6 Corollary 5.7 any prime $p_i \leq a$ has $GCD(p_i, d_1) = 1$. Hence, it follows that the $GCD(2a, d_1) = 1$. With $\mathcal{G}_+(2a) = 0$ the equation 5.1 becomes

$$2a\left[(2a)^{\pi(a)-1} + d_{\pi(a)-1}(2a)^{\pi(a)-2} + d_{\pi(a)-2}(2a)^{\pi(a)-3} + \cdots + d_1\right] = -d_0 \tag{7.1}$$

where the only term in the brackets not multiplied by $2a$ is the $d_1$ term. Therefore, the $GCD(2a, \frac{\mathcal{G}_+(0)}{2a})$ is a consequence of $\mathcal{G}_+(2a) = 0$ in equation 5.1 and Corollary 5.7. $\square$

**Corollary 7.3.** $2a$ *is not a repeated root when* $\mathcal{G}_+(2a) = 0$.

*Proof.* This follows directly from Proposition 7.2 and the Rational Root Theorem. $\square$

**Corollary 7.4.** *Any rational root other than* $2a$ *is odd when* $\mathcal{G}_+(2a) = 0$.

*Proof.* Under Proposition 7.2 it was shown that $GCD(2a, \frac{d_0}{2a}) = 1$. Taking all roots with multiplicity to be $r_1, r_2, \ldots r_{\pi(a)} \in \mathbb{C}$ with $r_1 = 2a$, it then follows that $GCD(2a, \frac{r_2 \cdots r_{\pi(a)}}{2a}) = 1$. Thus, W.L.O.G. assume there exist a rational root $r_2$. With the G.P. being monic, it follows that all rational roots are integers. Therefore, $r_2 \in \mathbb{Z}$. Since $r_2|d_0$ and $d_0 \in \mathbb{Z}$, there exists some integer $x$ where $\frac{d_0}{2a} = r_2 x$ and the $GCD(2a, r_2 x) = 1$, proving that $GCD(2a, r_2) = 1$. $\square$

**Corollary 7.5.** *If* $\mathcal{G}_+(2a) = 0$, *then there are no other rational roots to the G.P. for* $\pi(a) > 2$.

*Proof.* W.L.O.G. let the G.R. $r_1 = 2a$ and assume for the sake of contradiction there exists some other rational root $r_2$. Since the G.P. is monic, the Rational Root Theorem shows $r_2 \in \mathbb{Z}$. Proposition 7.2 ensures $2a$ can not be a repeated root, and Corollary 7.4 ensures $2 \nmid r_2$. Therefore, it must follow from equation 5.1 with $\mathcal{G}_+(r_2) = 0$ that

$$\prod_{i=1}^{\pi(a)}(r_2 + p_i) = (a+1)^{\gamma(a+1)} \prod_{i=1}^{\pi(a)} p_i^{\beta_i}. \tag{7.2}$$

With $2 \nmid r_2$, only one term of the L.H.S. above is not divisible by 2. Hence,

$$2^{\beta_1} \geq 2^{\pi(a)-1}. \tag{7.3}$$

Knowing the minimum value for $\beta_1$, equation 3.6 allows for again to write

$$2a = u_1 - 2. \tag{7.4}$$

It follows from Corollary 3.13 $u_1$ is the only even $u_i$ corresponding to the root $2a$, as all other $u_{i>1}$ must be odd since all other prime $p_{i>1}$ are odd. Hence, from equation 7.3 in conjunction with equation 7.4 it may be seen that $u_1 \geq 2^{\pi(a)-1}$. Therefore, it follows

$$2a \geq 2^{\pi(a)-1} - 2$$
$$a + 1 \geq 2^{\pi(a)-2}.$$

However, when $a = 19$ and $\pi(19) = 8$ a substitution of $a = 19$ in the equations above gives

$$20 \ngeq 2^6$$

producing a contradiction. Furthermore, Chebyshev's Theorem says that there for any $a \in \mathbb{N}$ where $a > 1$ there is always some prime $p$ such that $a \leq p < 2a$. Therefore, whenever $a \geq 19$ then $a \ngeq 2^{\pi(a)-2}$. This result can even be made stronger given there are no solutions to the G.D.P. where $2a$ is a G.D.R. and $2 < \pi(a) \leq 19$. Therefore, the corollary is true. ☐

Given everything so far it is actually possible to construct solutions for a counter-example to Conjecture 3.16. The strategy is to Use Hensel's Lemma to construct solutions for $2a$ based on the Lemmas 3.3, through 3.5 and Lemmas 3.11 through 3.13.

## 8. Hensel's Lemma and $p$-adic Analysis

A proof of Hensel's Lemma [2] is given below.

**Theorem 8.1.** *Hensel's Lemma.*

*Proof.* Let $f : \mathbb{C} \to \mathbb{C}$ where $f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots a_1 z + a_0$ and $f(z) \in \mathbb{Z}[z]$. It is possible to use a Taylor Series $f(z_0 + t_\mu p_i^\mu) \pmod{p_i^{\mu+1}} \equiv f(z_0) + t_\mu p^\mu f'(z_0) \pmod{p_i^{\mu+1}}$. If $f(z_0 + t_\mu p_i^\mu) \equiv 0 \pmod{p_i^{\mu+1}}$ and $f'(z_0) \not\equiv 0 \pmod{p_i}$, then $t_\mu p_i^\mu f'(z_0) \equiv -f(z_0) \pmod{p_i^{\mu+1}}$ where lifting allows $z_0 = t_0 + t_1 p_i + \cdots + t_{\mu-1} p_i^{\mu-1} + t_\mu p_i^\mu$ for a unique set $t_0, \ldots, t_{\mu-1}, t_\mu \in \mathbb{Z}_{p_i}$ ☐

**Example 8.2.** Let $f(z) = z^2 + 4$ whose derivative is given by $f'(z) = 2z$. To find the 5-adic expansion of the roots for $f(z)$ notice that $f(1) \equiv 0 \pmod 5$ and $f'(1) \equiv 2 \not\equiv 0 \pmod 5$. It is now possible to approximate the root, $r_k$ with $r_k \equiv 1 \pmod 5$ allowing the 5-adic expansion

$$r_k = 1 + t_1 \times 5 + t_2 \times 5^2 + \times 5^3 + \cdots \tag{8.1}$$

where Hensel's Lemma may be used to solve for the coefficients above. To solve for $t_1$ the equation use the fact that $f'(1) = 2$ and $f(1) = 5$ to obtain

$$-t_1 \times 5 \times f'(1) \equiv f(1) \pmod{5^2}$$
$$t_1 \equiv 2 \pmod 5$$

Now that $t_1$ is known the 5-adic expansion of the root is given by

$$r_k = 1 + 2 \times 5 + t_2 \times 5^2 + t_3 \times 5^3 + \cdots \tag{8.2}$$

Using the approximation $r_k = 11$ where $f(11) = 125$ and $f'(11) = 22$ allows for

$$-t_2 \times 5^2 \times f'(11) \equiv f(11) \pmod{5^3}$$
$$t_2 \equiv 0 \pmod{5}.$$

With $t_2$ known, the process can be repeated indefinitely to find next iteration of the 5-adic root

$$r_k = 1 + 2 \times 5 + 0 \times 5^2 + \cdots. \tag{8.3}$$

**Theorem 8.3.** *Suppose the integer polynomial, given by $f(z) = z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ has a root $r_1$ where $f(r_1) = 0$ and for some prime $p_i$ that $f'(r_1) \not\equiv 0 \pmod{p_i}$ along with the condition $c_0 \neq 0$. The p-adic series for $r_1$ terminates if and only if $r_1 \in \mathbb{Z}$.*

*Proof.* Assume $r_1 \in \mathbb{Z}$ where $f(r_1) = 0$ and $f'(r_1) \not\equiv 0 \pmod{p_i}$. Since any integer root can be written as a $p$-adic series, then there exists finitely many integers $a_0, a_1, \ldots, a_m \in \mathbb{Z}_{p_i}$ where

$$r_1 = a_0 + a_1 p_i + a_{m-1}p_i^{m-1} + a_m p_i^m. \tag{8.4}$$

Alternatively, if $r_1$ does terminate, the function $f(z)$ being monic shows $r_1$ is an integer. ☐

**Example 8.4.** Let $f(z) = z^3 - 16z^2 + 83z - 140$ where $f'(z) = 3z^2 - 32z + 83$. If there is an even integer root, it can be written as a finite 2-adic series given by

$$r_k = a_0 + a_1 2 + a_2 2^2 + \cdots + a_m 2^m \tag{8.5}$$

It can be seen $f(0) \equiv 0 \pmod{2}$ and $f'(0) \equiv 1 \pmod{2}$ where $a_0 = 0$. The next iteration is

$$-a_1 \times 2 \times f'(0) \equiv f(0) \pmod{2^2}$$
$$-a_1 \times 2 \times 83 \equiv -140 \pmod{2^2}$$
$$a_1 \equiv 0 \pmod{2}$$

Moving on to solve for $a_2$ gives the root still approximated by 0 where

$$-a_2 \times 2^2 \times f'(0) \equiv f(0) \pmod{2^3}$$
$$-a_2 \times 2^2 \times 83 \equiv -140 \pmod{2^3}$$
$$a_2 \equiv 1 \pmod{2}$$

where the root is now given by

$$r_k = 0 + 0 \times 2 + 1 \times 2^2 + \cdots + a_m 2^m. \tag{8.6}$$

Note that $f(4) = 0$ identically, therefore trying to apply Hensel's Lemma will always give

$$-\, a_m \times 2^m \times f'(4) \equiv 0 \pmod{2^{m+1}}. \tag{8.7}$$

Since $f'(4)$ is always odd, the only solutions for any $m > 2$ are given by $a_m = 0$.

**Corollary 8.5.** *From Propositions 4.8 and 4.9 Hensel's Lemma may be used for any $p_i^{\alpha_i} > 1$.*

*Proof.* Hensel's Lemma 8.1 states that for any $s \in \mathbb{Z}_p$ where $\mathcal{G}_-(s) \equiv 0 \pmod{p}$ along with condition $\mathcal{G}'_-(s) \not\equiv 0 \pmod{p}$, then there exists a unique $t \in \mathbb{Z}_p$ where $\mathcal{G}_-(t) \equiv 0 \pmod{p}$ and $s \equiv t \pmod{p}$. From Proposition 4.8 and 4.9, Hensel's Lemma is satisfied for any $p_i^{\alpha_i} > 1$. ☐

**Corollary 8.6.** *From Propositions 5.8 and 5.10 Hensel's Lemma may be used for any $p_i^{\beta_i} > 1$.*

*Proof.* Hensel's Lemma 8.1 states that for any $s \in \mathbb{Z}_p$ where $\mathcal{G}_+(s) \equiv 0 \pmod{p}$ along with condition $\mathcal{G}'_+(s) \not\equiv 0 \pmod{p}$, then there exists a unique $t \in \mathbb{Z}_p$ where $\mathcal{G}_+(t) \equiv 0 \pmod{p}$ and $s \equiv t \pmod{p}$. From Proposition 5.8 and 5.10, Hensel's Lemma is satisfied for any $p_i^{\beta_i} > 1$. ☐

In the next section it will be shown Hensel's lemma may be used to construct the root $2a$ when it is a solution to either the G.P.I. 4.1 or the G.P.II. 5.1.

## 9. A Derivation of the Hensel-Goldbach Equations

Given everything so far it is actually possible to construct solutions for the Goldbach Polynomial. The strategy is to Use Hensel's Lemma 8.1 to construct solutions for $2a$ based on the Lemmas 3.3, 3.4, and 3.5. A definition of Hensel's Lemma is given below.

**Lemma 9.1.** *Any $\alpha_i > 0$ if and only if $2a \equiv 0 \pmod{p_i}$ or $2a \equiv p_j \pmod{p_i}$ for some $j \neq i$.*

*Proof.* This follows directly from equations 3.1 and 3.2 in Theorem 3.2 and Lemma 3.3. ☐

The strategy now is to use Hensel's Lemma 8.1 in conjunction with Lemma 9.1 to construct the form of $2a$ in terms of its prime divisors. The Hensel-Goldbach Equations are defined below.

**Definition 9.2.** From Proposition 4.8 it was shown any $\alpha_i > 0$ if and only if 0 is a root of $\mathcal{G}_{-}(z) \pmod{p_i}$. It was also shown from Proposition 4.9 that for any prime $p_i \leq a$ that $\mathcal{G}'_{-}(0) \not\equiv 0 \pmod{p_i}$ where Corollary 4.10 shows $\mathcal{G}'_{-}(0) \equiv (-1)^{\pi(a)-1}\frac{a\#}{p_i} \pmod{p_i}$. Therefore, for any $\alpha_i > 0$ Theorem 8.1 and Corollary 8.5 show there exists some unique root $r_i \in G$ from Definition 4.2 where $r_i \equiv 0 \pmod{p_i}$ and $\mathcal{G}'_{-}(0) \not\equiv 0 \pmod{p_i}$. This allows for the production of the *Hensel-Goldbach Equations* for any integer $0 \leq \mu \leq \alpha_i$ below

$$-t_{\alpha_i-\mu}p_i^{\alpha_i-\mu}\mathcal{G}'_{-}(r_i) \equiv \mathcal{G}_{-}(r_i) \mod p_i^{\alpha_i-\mu+1}. \tag{9.1}$$

Therefore, for any $\alpha_i > 0$, Definition 4.2 allows the following relation for all integers $1 \leq \mu \leq \alpha_i$

$$\prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i-\mu+1}} \equiv 0 \pmod{p_i^{\alpha_i-\mu+1}}, \tag{9.2}$$

showing equation 4.1 may be simplified greatly to

$$\begin{cases} -t_{\alpha_i-\mu}p_i^{\alpha_i-\mu}\mathcal{G}'_{-}(r_i) \equiv \prod_{k=1}^{\pi(a)}(r_i - p_k) \pmod{p_i^{\alpha_i-\mu+1}} \text{ for all integers } 1 \leq \mu \leq \alpha_i \\ -t_{\alpha_i}p_i^{\alpha_i}\mathcal{G}'_{-}(r_i) \equiv \prod_{k=1}^{\pi(a)}(r_i - p_k) - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+1}} \end{cases} \tag{9.3}$$

where

$$r_i = t_0 + t_1p_i + \cdots + t_{\alpha_i-1}p_i^{\alpha_i-1} + t_{\alpha_i}p_i^{\alpha_i} + \cdots \tag{9.4}$$

for unique $t_0, \ldots, t_{\alpha_i-1}, t_{\alpha_i}, \ldots, \in \mathbb{Z}_{p_i}$ and $r_i \equiv t_0 \pmod{p_i}$.

**Example 9.3.** Let $\mathcal{G}_{-}(z) = (z-2)(z-3) - 2^2 \times 3$ where $\mathcal{G}'_{-}(z) = 2z - 5$. It can be seen that $\mathcal{G}_{-}(0) \equiv 0 \pmod 2$ and $\mathcal{G}'_{-}(0) \equiv -5 \pmod 2 \equiv 1 \pmod 2$. Using the Hensel-Goldbach Equations gives the 2-adic root approximation $r_k = 0 + t_1 2 + t_2 2^2 + \cdots$ with the next iteration

$$\begin{gathered} -t_1 \times 2 \times \mathcal{G}'_{-}(0) \equiv \mathcal{G}_{-}(0) \pmod{2^2} \\ -t_1 \times 2 \times (2 \times 0 - 5) \equiv (0-2) \times (0-3) - 2^2 \times 3 \pmod{2^2} \\ t_1 \equiv 1 \pmod 2 \end{gathered}$$

where the root is $r_k = 0 + 2 + t_2 2^2 + \cdots$ where the next iteration gives

$$\begin{gathered} -t_2 \times 2^2 \times \mathcal{G}'_{-}(2) \equiv \mathcal{G}_{-}(2) \pmod{2^3} \\ -t_2 \times 2^2 \times (2 \times 2 - 5) \equiv (2-2) \times (2-3) - 2^2 \times 3 \pmod{2^3} \\ t_2 \equiv 1 \pmod 2 \end{gathered}$$

where $r_k = 0 + 2 + 2^2 + \cdots$. However, note that $\mathcal{G}_{-}(6) = (6-2)(6-3) - 2^2 \times 3 = 0$ identically. Therefore any lifts of 2 in the 2-adic root will vanish, as was demonstrated by Theorem 8.3. It can also be seen that $6 = 2 \times 3$ is 3-adic and is also a root derived working in $\pmod 3$.

**Theorem 9.4.** *There exists a unique root $r_i \in G$ to equations 9.3 of Definition 9.2 where $r_i \equiv t_{\alpha_i}p_i^{\alpha_i} + p_i \pmod{p_i^{\alpha_i+1}}$ and $t_{\alpha_i} \in \mathbb{Z}_{p_i}$ is non-zero if and only if $\alpha_i > 0$.*

*Proof.* Assume $\alpha_i > 0$. Using the Hensel-Goldbach Equation in 9.3 gives the set of equations

$$-t_0\mathcal{G}'_-(\bar{r}_i) \equiv \prod_{k=1}^{\pi(a)}(\bar{r}_i - p_k) \pmod{p_i} \tag{9.5}$$

$$\vdots \tag{9.6}$$

$$-t_{\alpha_i-1}p_i^{\alpha_i-1}\mathcal{G}'_-(r_i) \equiv \prod_{k=1}^{\pi(a)}(r_i - p_k) \pmod{p_i^{\alpha_i}} \tag{9.7}$$

$$-t_{\alpha_i}p_i^{\alpha_i}\mathcal{G}'_-(r_i) \equiv \prod_{k=1}^{\pi(a)}(r_i - p_k) - \prod_{i=k}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+1}}. \tag{9.8}$$

From Proposition 4.8 Corollary 4.10 it follows that $0 \pmod{p_i}$ is a root to the Hensel-Goldbach Equations above where plugging in the root zero to equation 9.5 shows $t_0 \equiv 0 \pmod{p_i}$. To solve for the next term it is possible to use the fact that $r_i$ may be written as the $p_i$-adic series

$$r_i = 0 + t_1p_i + t_2p_i^2 + \cdots + t_{\alpha_i-1}p_i^{\alpha_i-1} + t_{\alpha_i}p_i^{\alpha_i} + \cdots \tag{9.9}$$

where all $t \in \mathbb{Z}_{p_i}$. Moving to the second iteration and plugging in $r_i = 0 \pmod{p_i}$ gives

$$-\, t_1p_i\mathcal{G}'_-(0) \equiv (-1)^{\pi(a)}a\# \pmod{p_i^2} \tag{9.10}$$

where a substitution from Corollary 4.10 for $\mathcal{G}'_-(0)$ on the L.H.S. shows

$$\begin{aligned}
-t_1p_i\mathcal{G}'_-(0) &\equiv (-1)^{\pi(a)}a\# \pmod{p_i^2}\\
-t_1\mathcal{G}'_-(0) &\equiv (-1)^{\pi(a)}\frac{a\#}{p_i} \pmod{p_i}\\
-t_1(-1)^{\pi(a)-1}\frac{a\#}{p_i} &\equiv (-1)^{\pi(a)}\frac{a\#}{p_i} \pmod{p_i}\\
t_1 &\equiv 1 \pmod{p_i}
\end{aligned}$$

where the root becomes

$$r_i = 0 + p_i + t_2p_i^2 + \cdots + t_{\alpha_i-1}p_i^{\alpha_i-1} + t_{\alpha_i}p_i^{\alpha_i} + \cdots \tag{9.11}$$

This allows equation above to be used in the next iteration to give

$$\begin{aligned}
-t'_2p_i^2\mathcal{G}'_+(p_i) &\equiv \prod_{k=1}^{\pi(a)}(p_i - p_k) \pmod{p_i^3}\\
-t'_2p_i^2\mathcal{G}'_+(p_i) &\equiv (p_i - p_1)(p_i - p_2)\cdots(p_i - p_i)\cdots(p_i - p_{\pi(a)}) \pmod{p_i^3}\\
-t'_2p_i^2\mathcal{G}'_+(p_i) &\equiv 0 \pmod{p_i^3}\\
t_2 &\equiv 0 \pmod{p_i}
\end{aligned}$$

where

$$r_i = 0 + p_i + 0 \times p_i^2 + \cdots + t_{\alpha_i-1}p_i^{\alpha_i-1} + t_{\alpha_i}p_i^{\alpha_i} + \cdots \tag{9.12}$$

Note the root above shows the R.H.S. of equations 9.5 to 9.7 must be 0 and gives the value for all $t_{1<i\leq\alpha_i} = 0$ where the roots becomes

$$r_i = p_i + t_{\alpha_i}p_i^{\alpha_i} + \cdots . \tag{9.13}$$

Moving to the final iteration and plugging in the appropriate value for $r_i$ into 9.8 shows

$$-t_{\alpha_i} p_i^{\alpha_i} \mathcal{G}'_-(p_i) \equiv \prod_{k=1}^{\pi(a)} (p_i - p_k) - \prod_{i=k}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+1}}$$

$$-t_{\alpha_i} p_i^{\alpha_i} \mathcal{G}'_-(p_i) \equiv (p_i - p_1)(p_i - p_2) \cdots (p_i - p_i) \cdots (p_i - p_{\pi(a)}) - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+1}}$$

$$-t_{\alpha_i} p_i^{\alpha_i} \mathcal{G}'_-(p_i) \equiv - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+1}}$$

$$-t_{\alpha_i} \mathcal{G}'_-(p_i) \equiv - \prod_{k \neq i}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i}$$

$$-t_{\alpha_i} \mathcal{G}'_-(0) \equiv - \prod_{k \neq i}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i}$$

Since $p_i^{\alpha_i}$ was cancelled from both sides above, the R.H.S. of the equation above is never 0. Hence, $t_{\alpha_i} \neq 0$ where equation 9.9 shows $r_i \equiv t_{\alpha_i} p_i^{\alpha_i} + p_i \pmod{p_i^{\alpha_i+1}}$ for some $t_{\alpha_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$.

Alternatively, assume that $\alpha_i = 0$. From Proposition 4.8 there is no root $\bar{r}_i \equiv 0 \pmod{p_i}$. □

**Proposition 9.5.** $2a = t_{\alpha_i} p_i^{\alpha_i} + p_i$ *if and only if* $2a \equiv 0 \pmod{p_i}$.

*Proof.* Suppose $2a \equiv 0 \pmod{p_i}$. Hence, from Lemma 9.1 it follows that $\alpha_i > 0$. Since $2a$ is a root to the G.P.I. in Definition 4.1, it is also a root to Hensel-Goldbach Equations 9.3 and must have a unique representation under Proposition 3.6. The solutions in Theorem 9.4 are given by $2a = t_{\alpha_i} p_i^{\alpha_i} + p_i$ since Theorem 8.3 states no higher lifts can exist.

Alternatively, suppose $2a \not\equiv 0 \pmod{p_i}$ and $\alpha_i > 0$. From Theorem 9.4 $\bar{r}_i = t_i p_i^{\alpha_i} + p_i$ exists if and only if $\alpha_i > 0$. From Lemma 9.1 it must then follow that if $r_i$ exists for $p_i$, then $r_i \equiv 0 \pmod{p_i}$. Since $r_i \not\equiv 2a \pmod{p_i}$ it follows that $2a \neq \bar{r}_i$. □

**Theorem 9.6.** *If* $\mathcal{G}_-(2a) = 0$, *then* $2a = 2^{\alpha_1} + 2$ *and* $2a > 6$.

*Proof.* This is a direct consequence of Proposition 3.6, Theorem 9.4, and Proposition 9.5. □

Following a similar approach to the one in this section it is possible to derive a set of equations that will allow for the construction of roots to the G.P.II in Definition 5.1.

## 10. A Derivation of The Hensel-Goldbach Difference Equations

**Lemma 10.1.** *Any* $\beta_i > 0$ *if and only if* $2a \equiv 0 \pmod{p_i}$ *or* $2a \equiv p_j \pmod{p_i}$ *for some* $j \neq i$.

*Proof.* This follows directly from equations 3.6 and 3.7 in Theorem 3.2 and Lemma 3.3. □

**Definition 10.2.** From Proposition 5.8 it was shown that any $\beta_i > 0$ if and only if $p_i$ is a root of $\mathcal{G}_+(z) \pmod{p_i}$. It was also shown from Proposition 5.9 that for for any prime $p_i \leq a$ that $\mathcal{G}'_+(0) \not\equiv 0 \pmod{p_i}$ where Corollary 5.10 shows $\mathcal{G}'_+(0) \equiv \frac{a\#}{p_i} \pmod{p_i}$. Therefore, for any $\beta_i > 0$ Theorem 8.1 and Corollary 8.6 show there exists some unique root $r'_i \in G'$ from Definition 5.2 where $r'_i \equiv 0 \pmod{p_i}$ and $\mathcal{G}'_+(0) \not\equiv 0 \pmod{p_i}$. This root allows for the *Hensel-Goldbach Difference Equations* given below

$$-t_{\beta_i-\mu} p_i^{\beta_i-\mu} \mathcal{G}'_+ r'_i) \equiv \mathcal{G}_+(r'_i) \mod p_i^{\beta_i-\mu+1} \tag{10.1}$$

for any $0 \leq \mu \leq \beta_i$. Therefore, for any $\beta_i > 0$, Definition 5.1 allows the following relation for all integers $1 \leq \mu \leq \beta_i$

$$(a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i-\mu+1}} \equiv 0 \pmod{p_i^{\beta_i-\mu+1}} \tag{10.2}$$

where using equation 5.1 and equation 10.1 may be simplified greatly to

$$\begin{cases} -t'_{\beta_i-\mu}p_i^{\beta_i-\mu}\mathcal{G}'_+(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i+p_k) \pmod{p_i^{\beta_i-\mu+1}} : \text{for all } 1 \leq \mu \leq \beta_i \\ -t'_{\beta_i}p_i^{\beta_i}\mathcal{G}'_+(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i+p_k) - (a+1)^{\gamma(a+1)}\prod_{i=k}^{\pi(a)}p_k^{\beta_k} \pmod{p_i^{\beta_i+1}} \end{cases} \tag{10.3}$$

where it is now possible to use these equations to find roots for the G.P.II given by

$$r'_i = t'_0 + t'_1 p_i + t'_{\beta_i-1}p_i^{\beta_i-1} + t'_{\beta_i}p_i^{\beta_i} + \cdots \tag{10.4}$$

for unique $t'_0, \ldots, t'_{\beta_i-1}, t'_{\beta_i} \in \mathbb{Z}_{p_i}$ and $r'_i \equiv t'_0 \pmod{p_i}$.

**Example 10.3.** Let $\mathcal{G}_+(z) = (z+2)(z+3) - 2^3 \times 3^2$ where $\mathcal{G}'_+(z) = 2z+5$. It can be seen that $\mathcal{G}_+(0) \equiv 0 \pmod 3$ and $\mathcal{G}'_+(0) \equiv 5 \pmod 3 \equiv 2 \pmod 3$. Using the Hensel-Goldbach Difference Equations allows for the 3-adic root $r'_k = 0 + t'_1 3 + t'_2 3^2 + \cdots$ where the next iteration gives

$$\begin{aligned} -t'_1 \times 3 \times \mathcal{G}'_+(0) &\equiv \mathcal{G}_+(0) \pmod{3^2} \\ -t'_1 \times 3 \times (2 \times 0 + 5) &\equiv (0+2) \times (0+3) - 2^3 \times 3^2 \pmod{3^2} \\ -t'_1 \times 3 \times (2 \times 0 + 5) &\equiv (0+2) \times (0+3) \pmod{3^2} \\ -t'_1 \times 5 &\equiv 2 \pmod 3 \\ t'_1 &\equiv 2 \pmod 3 \end{aligned}$$

At this point it is best to write $2 = (3-1)$ where the root is $r_k = 0 + (3-1) \times 3 + t_2 2^2 + \cdots$. However, note that $\mathcal{G}_+(6) = (6+2)(6+3) - 2^3 \times 3^2 = 0$ identically. Therefore any higher lifts in the 3-adic root will vanish demonstrated by Theorem 8.3. Notice also that $6 = (3-1) \times 3 = 3^2 - 3$ in accordance with Proposition 3.14 and will have relevance in the following theorem.

**Theorem 10.4.** *There exists a root $r'_i$ to the Hensel-Goldbach Difference Equations in equations 10.3 of Definition 10.2 where $r'_i \equiv t'_{\beta_i}p_i^{\beta_i} - p_i \pmod{p_i^{\beta_i+1}}$ and $t'_{\beta_i} \in \mathbb{Z}_{p_i}$ is non-zero iff $\beta_i > 0$.*

*Proof.* Assume $\beta_i > 0$. Using the Hensel-Goldbach Difference Equations in 10.3 gives

$$-t'_0\mathcal{G}'_-(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i+p_k) \mod p_i \tag{10.5}$$

$$\vdots \tag{10.6}$$

$$-t_{\beta_i-1}p_i^{\beta_i-1}\mathcal{G}'_-(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i+p_k) \mod p_i^{\beta_i} \tag{10.7}$$

$$-t'_{\beta_i}p_i^{\beta_i}\mathcal{G}'_+(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i+p_k) - (a+1)^{\gamma(a+1)}\prod_{i=k}^{\pi(a)}p_k^{\beta_k} \pmod{p_i^{\beta_i+1}}. \tag{10.8}$$

From Proposition 5.8 Corollary 5.10 it follows that $0 \pmod{p_i}$ is a root to the Hensel-Goldbach Difference Equations above where plugging in the root zero to equation 10.5 shows $t'_0 \equiv 0 \pmod{p_i}$. To solve for the next term it is possible to use the fact that $r'_i$ may be written as a series of the prime powers $p_i$ below

$$r'_i = 0 + t'_1 p_i + t'_2 p_i^2 + \cdots + t'_{\beta_i-1}p_i^{\beta_i-1} + t'_{\beta_i}p_i^{\beta_i} + \cdots \tag{10.9}$$

where all $t' \in \mathbb{Z}_{p_i}$. Moving to the next iteration and plugging in the root $\bar{r}_i = 0$ gives

$$-t'_1 p_i \mathcal{G}'_-(0) \equiv a\# \mod p_i^2 \tag{10.10}$$

where a simplification of the R.H.S. and a substitution from Corollary 5.10 for $\mathcal{G}'_+(0)$ on the L.H.S. shows $t_1 \equiv -1 \pmod{p_i}$ showing $t_1 = p_i - 1$. This allows equation **??** to be written as

$$r'_i = 0 + (p_i - 1)p_i + t'_2 p_i^2 + \cdots + t'_{\beta_i-1}p_i^{\beta_i-1} + t'_{\beta_i}p_i^{\beta_i} + \cdots \tag{10.11}$$

where $r_i' = p_i^2 - p_i \pmod{p_i^3}$. Moving to the next iteration to solve for $t_2$ gives

$$
\begin{aligned}
-t_2' p_i^2 \mathcal{G}_+'(p_i^2 - p_i) &\equiv \prod_{k=1}^{\pi(a)} (p_i^2 - p_i + p_k) \mod p_i^3 \\
-t_2' p_i^2 \mathcal{G}_+'(p_i^2 - p_i) &\equiv (p_i^2 - p_i + p_1)(p_i^2 - p_i + p_2) \cdots (p_i^2 - p_i + p_i) \cdots (p_i^2 - p_i + p_{\pi(a)}) \mod p_i^3 \\
-t_2' p_i^2 \mathcal{G}_+'(p_i^2 - p_i) &\equiv p_i^2 \prod_{k \neq i}^{\pi(a)} (p_i^2 - p_i + p_k) \mod p_i^3 \\
-t_2' \mathcal{G}_+'(p_i^2 - p_i) &\equiv \prod_{k \neq i}^{\pi(a)} (p_i^2 - p_i + p_k) \mod p_i \\
-t_2' \mathcal{G}_+'(0) &\equiv \frac{a\#}{p_i} \mod p_i
\end{aligned}
$$

where Corllary 5.10 gives $t_2 \equiv -1 \pmod{p_i}$ showing $t_2' = p_i - 1$. Plugging into 10.11 gives

$$
\begin{aligned}
r_i' &= 0 + (p_i - 1)' p_i + (p_i - 1)' p_i^2 + \cdots + t_{\beta_i - 1}' p_i^{\beta_i - 1} + t_{\beta_i}' p_i^{\beta_i} + \cdots \\
r_i' &= p_i^3 - p_i + t_3 p_i^3 + \cdots + t_{\beta_i - 1}' p_i^{\beta_i - 1} + t_{\beta_i}' p_i^{\beta_i} + \cdots
\end{aligned}
$$

Note, that this pattern continues in the R.H.S. of all equations 10.5 to 10.7 where it must follow that all $t_{1<i<\alpha_i}' = p_i - 1$. This allows for

$$
\begin{aligned}
r_i' &= 0 + (p_i - 1)' p_i + (p_i - 1)' p_i^2 + \cdots + (p_i - 1) p_i^{\beta_i - 1} + (p_i - 1) p_i^{\beta_i - 1} + t_{\beta_i}' p_i^{\beta_i} + \cdots \\
r_i' &= p_i^{\beta_i} - p_i + t_{\beta_i}' p_i^{\beta_i} + \cdots
\end{aligned}
$$

where it is possible to substitute in $r_i = p_i^{\beta_i} - p_i$ into equation 10.8 to find $t_{\beta_i}$ below.

$$
\begin{aligned}
-t_{\beta_i}' p_i^{\beta_i} \mathcal{G}_+'(p_i^{\beta_i} - p_i) &\equiv \prod_{k=1}^{\pi(a)} (p_i^{\beta_i} - p_i + p_k) - (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i + 1}} \\
-t_{\beta_i}' p_i^{\beta_i} \mathcal{G}_+'(p_i^{\beta_i} - p_i) &\equiv (p_i^{\beta_i} - p_i + p_1) \cdots (p_i^{\beta_i} - p_i + p_{\pi(a)}) - (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i + 1}} \\
-t_{\beta_i}' p_i^{\beta_i} \mathcal{G}_+'(p_i^{\beta_i} - p_i) &\equiv p_i^{\beta_i} \prod_{k \neq i}^{\pi(a)} (p_i^{\beta_i} - p_i + p_k) - (a+1)^{\gamma(a+1)} p_i^{\beta_i} \prod_{k \neq i}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i + 1}} \\
-t_{\beta_i}' \mathcal{G}_+'(p_i^{\beta_i} - p_i) &\equiv \prod_{k \neq i}^{\pi(a)} (p_i^{\beta_i} - p_i + p_k) - (a+1)^{\gamma(a+1)} \prod_{k \neq i}^{\pi(a)} p_k^{\beta_k} \pmod{p_i} \\
-t_{\beta_i}' \mathcal{G}_+'(0) &\equiv \frac{a\#}{p_i} - (a+1)^{\gamma(a+1)} \prod_{k \neq i}^{\pi(a)} p_k^{\beta_k} \pmod{p_i}
\end{aligned}
$$

From Corollary 5.10 the equation above becomes

$$
-t_{\beta_i}' \frac{a\#}{p_i} \equiv \frac{a\#}{p_i} - (a+1)^{\gamma(a+1)} \prod_{k \neq i}^{\pi(a)} p_k^{\beta_k} \pmod{p_i} \tag{10.12}
$$

where a simplification gives

$$
-(t_{\beta_i}' + 1) \frac{a\#}{p_i} \equiv -(a+1)^{\gamma(a+1)} \prod_{k \neq i}^{\pi(a)} p_k^{\beta_k} \pmod{p_i} \tag{10.13}
$$

From Definition 3.9 there are no solutions to 10.13 where $t'_{\beta_i} \equiv -1 \pmod{p_i}$ since the R.H.S. is never divisible by $p_i$. Therefore, it must follow that $0 \leq t'_{\beta_i} < p_i - 1$ showing $t'_{\beta_i} + 1 \in \mathbb{Z}_{p_i}$. A rescaling of $t'_{\beta_i} \mapsto t'_{\beta_i} + 1$ shows $r'_i \equiv t'_{\beta_i} p_i^{\beta_i} - p_i \pmod{p_i^{\beta_i+1}}$ where $t'_{\beta_i} \in \mathbb{Z}_{p_i}$.

Alternatively, assume that $\beta_i = 0$. Then, from Proposition 5.8 it can be seen that there is no root where $r'_i \equiv 0 \pmod{p_i}$. □

**Proposition 10.5.** *$2a = t'_{\beta_i} p_i^{\beta_i} - p_i$ if and only if $2a \equiv 0 \pmod{p_i}$.*

*Proof.* Suppose $2a \equiv 0 \pmod{p_i}$. It then follows from Lemma 10.1 that $\beta_i > 0$. Since $2a$ is assumed to be a rational root to the G.P.II, it is also a root to Hensel-Goldbach Difference Equations and must have a unique representation which terminates under Theorem 8.3. Proposition 3.14 and Theorem 10.4 demonstrate that $2a = t'_{\beta_i} p_i^{\beta_i} - p_i$.

Alternatively, suppose $2a \not\equiv 0 \pmod{p_i}$ and $\beta > 0$. From Theorem 10.4 there exists a root $r'_i = t'_i p_i^{\beta_i} - p_i \pmod{p_i^{\beta_i+1}}$ if and only if $\beta_i > 0$. From Lemma 9.1 $r'_i \equiv 0 \pmod{p_i}$. Since $r'_i \not\equiv 2a \pmod{p_i}$ it follows that $2a \neq r'_i$. □

**Corollary 10.6.** *If $\mathcal{G}_+(2a) = 0$, then $2a = 2^{\beta_1} - 2$.*

*Proof.* Since $2a \equiv 0 \pmod 2$, it can be seen that if $\mathcal{G}_+(2a) = 0$, then $2a = 2^{\beta_1} - 2$ follows directly from Theorem 10.4, Corollary 10.1, and Proposition 10.5. □

**Theorem 10.7.** *Every even number greater than six is the sum or difference of two primes.*

*Proof.* Suppose, for the sake of contradiction, that there was a number, $2a > 6$, that was a counter-example to the G.C. and the G.D.C. then under Theorems 3.2 and 3.10 it must follow that $\mathcal{G}_+(2a) = 0$ and $\mathcal{G}_-(2a) = 0$. However, under Corollaries 9.6 and 10.6 then $2^{\beta_1} - 2 = 2^{\alpha_1} + 2$ where a simplification shows $2^{\beta_1} - 2^{\alpha_1} = 2^2$ where $\alpha_1$ is at most equal to 2, thus $2a = 6$, contradicting the assumption that $a > 3$. Therefore, it may be concluded that no counter-examples exist and Conjecture 3.16 is true. □

## 11. Constructing the Root $2a$ when $\mathcal{G}_-(2a) = 0$

It was shown in Proposition 6.5 that $2a$ is the only rational root to the G.P. in Definition 4.1. Under Theorem 9.4 it was shown that there exists a root of the form $r_i \equiv t_{\alpha_i} p_i^{\alpha_i} + p_i \pmod{p_i^{\alpha_i+1}}$. It was also shown that when $2a \equiv 0 \pmod{p_i}$ that $2a = t_{\alpha_i} p_i^{\alpha_i} + p_i$ since Theorem 8.3 and Proposition 3.6 shows no higher lifts are possible for rational roots of the G.P. The final step is to show that all $r_i \equiv t_{\alpha_i} p_i^{\alpha_i} + p_i \pmod{p_i^{\alpha_i+1}}$ must be rational roots and terminate.

**Lemma 11.1.** *For any $r_i \in G$ from Definition 4.2 it follows that the product relationship in 4.1 produces $\prod_{k=1}^{\pi(a)}(r_i - p_k) \equiv \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+2+s}}$ or all $s \in \mathbb{N}$.*

*Proof.* For any $x, y, z \in \mathbb{Z}$ where $z > 0$ it follows that if $x = y$, then $x \equiv y \pmod z$. Thus, for any $r_i \in G$ Definition 4.1 shows $\prod_{k=1}^{\pi(a)}(r_i - p_k) = \prod_{k=1}^{\pi(a)} p_k^{\alpha_k}$. Since the R.H.S. is an integer, the L.H.S. must also be an integer giving $\prod_{k=1}^{\pi(a)}(r_i - p_k) \equiv \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+2+s}}$ for all $s \in \mathbb{N}$. □

**Lemma 11.2.** *If $\alpha_i > 0$, there exists some $r_i \in G$ where $r_i = t_{\alpha_i} p_i^{\alpha_i} + p_i$ and $r_i \in \mathbb{Z}$.*

*Proof.* From Theorem 9.4 iff $\alpha_i > 0$ there exists some unique $r_i = t_{\alpha_i} p_i^{\alpha_i} + p_i \pmod{p_i^{\alpha_i+1}}$. Recall, The Hensel-Goldbach Equations 9.3 allow for as many lifts as possible where

$$-t_{\alpha_i+1+s} p_i^{\alpha_i+1+s} \mathcal{G}'_-(r_i) \equiv \prod_{k=1}^{\pi(a)}(r_i - p_k) - \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+2+s}}. \tag{11.1}$$

However, by Definition 4.2 and Lemma 11.1 for all $s \in \mathbb{N}$

$$\prod_{k=1}^{\pi(a)}(r_i - p_k) \equiv \prod_{k=1}^{\pi(a)} p_k^{\alpha_k} \pmod{p_i^{\alpha_i+2+s}} \tag{11.2}$$

where it clearly follows from equations 11.1 and 12.2

$$-t_{\alpha_i+1+s}p_i^{\alpha_i+1+s}\mathcal{G}'_-(r_i) \equiv 0 \pmod{p_i^{\alpha_i+2+s}} \tag{11.3}$$

for all $s \in \mathbb{N}$. This shows the R.H.S. above is always zero where all $t_{k>\alpha_i} = 0$ terminating all lifts above $\alpha_i$. Therefore, it may be concluded from Theorem 8.3 that for any $\alpha_i > 0$ there is a unique root $r_i \in G$ where $r_i = t_{\alpha_i}p_i^{\alpha_i} + p_i$ for some $t_{\alpha_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. □

**Proposition 11.3.** *$\alpha_i > 0$ if and only if $2a \equiv 0 \pmod{p_i}$.*

*Proof.* Under Corollary 11.2 it was shown that if $\alpha_i > 0$, then there exists a rational root $r_i \equiv 0 \pmod{p_i}$ and $r_i = t_{\alpha_i}p_i^{\alpha_i} + p_i$ for some $t_{\alpha_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. From Proposition 6.5 it was shown that $2a$ is the only rational root to the G.P. in Definition 4.1. Therefore, $2a = t_{\alpha_i}p_i^{\alpha_i} + p_i$ showing if $\alpha_i > 0$, then $2a \equiv 0 \pmod{p_i}$.

If $2a \equiv 0 \pmod{p_i}$, then Proposition 9.5 ensures $2a = t_{\alpha_i}p_i^{\alpha_i} + p_i$ for some $t_{\alpha_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. □

**Corollary 11.4.** *There is no prime $p_i < a$ where $p_i|q_j$ for some $j \neq i$.*

*Proof.* Assume, for the sake of contradiction, that there exists some prime $p_i < a$ where $p_i|q_j$ for some $j \neq i$ in Theorem 3.2. From Lemma 3.3 $\alpha_i > 0$. Under Proposition 12.3 it then follows that $2a \equiv 0 \pmod{p_i}$. However, since $p_i|2a$ Lemma 3.4 states $p_i|q_i$ where Lemma 3.5 states that $p_i \nmid q_j$ for any $j \neq i$, contradicting the assumption that there exists some prime $p_i < a$ where $p_i|q_j$ for some $j \neq i$. Therefore, no prime $p_i < a$ where $p_i|q_j$ for some $j \neq i$ □

**Theorem 11.5.** *There are no solutions to equation 4.1 where $\mathcal{G}_-(2a) = 0$ and $a > 3$.*

*Proof.* From Corollary 11.4 it was shown that there is no scenario where any $p_i|q_j$ when $j \neq i$. From Lemmas 3.3, 3.4, and 3.5, the only solutions when $\mathcal{G}_-(2a) = 0$ and $a > 3$ are given when each $q_i$ is of the form $q_i = p_i^{\alpha_i}$. It can then be seen via a substitution into equation 3.1

$$2a = p_i^{\alpha_i} + p_i \text{ for all prime } p_i < a. \tag{11.4}$$

This forces all prime $p_i > a$ to be divisors of $2a$. However, since Bertrand's Postulate ensures there always exists some prime between in the interval $[a, 2a]$, then $2a < a\#$ for $a > 4$. Thus, no counter-examples exist when $a > 3$ and Theorem 3.2, the Goldbach Conjecture is true. □

**Theorem 11.6.** *The Ternary Conjecture*[3] *is true.*

*Proof.* For any odd $n \in \mathbb{N}$ such that $n \geq 7$ there exists some even $m \in \mathbb{N}$ where $n = 3 + m$. Under Theorem 11.5 for any even $m > 2$ there exists $p_2, p_3 \in \mathbb{P}$ where $m = p_1 + p_2$. Thus, for any odd $n \geq 7$ there exists $p_1, p_2, p_3 \in \mathbb{P}$ where $n = p_1 + p_2 + p_3$. □

**Corollary 11.7.** *Every prime larger than 7 is the sum of three odd primes.*

*Proof.* This follows trivially from Theorem 11.6 since all primes greater than seven are odd. □

**Definition 11.8.** Let $a \in \mathbb{N}$ such that $a > 1$. Since

$$2a = (a + b) + (a - b) \tag{11.5}$$

for any $b \in \mathbb{N}$, a *Prime Reflective Point (P.R.P.)* is any $b_R \in \mathbb{N}$ where both $a \pm b_R \in \mathbb{P}$.

Theorem 11.5 along with Definition 11.8 allow for a slightly stronger conjecture than the G.C. if it can be shown that there are no solutions to the G.P. when $a > 3$ and $2a$ is a G.R.

**Theorem 11.9.** *Every $a \in \mathbb{N}$ where $a > 3$ has some non-zero P.R.P.*

*Proof.* Since no solutions exist to Theorem 3.2 when $2a > 6$, this must also hold when $a$ is prime. This would allow for a cancellation of $a$ from both sides of equation 3.2. Since solutions would still not exist, another $q_i$ must be prime in equation 3.1. Thus, since every prime has a non-zero P.R.P. and any composite $a$ must also have a non-zero P.R.P., the theorem is true. □

The next section will follow a nearly identical approach to this section in order to prove that there are no counter-examples to the G.D.C. 3.7

[3]Harald Helfgott's 2013 work is generally accepted as sufficient for proving this conjecture.

## 12. Constructing the Root $2a$ when $\mathcal{G}_+(2a) = 0$

This section will mirror the last as It was shown in Proposition 7.5 that $2a$ is the only rational root to the G.D.P. in Definition 5.1. Under Theorem 10.4 it was shown that there exists a root of the form $r_i \equiv t'_{\beta_i} p_i^{\beta_i} + p_i \pmod{p_i^{\beta_i+1}}$. It was also shown that when $2a \equiv 0 \pmod{p_i}$ that $2a = t'_{\beta_i} p_i^{\beta_i} + p_i$ since Theorem 8.3 and Proposition 3.14 shows no higher lifts are possible for rational roots of the G.D.P. The final step is to show that all $r'_i \equiv t'_{\beta_i} p_i^{\beta_i} + p_i \pmod{p_i^{\beta_i+1}}$ must be rational roots and terminate. This is the equivalent of saying $\beta_i > 0$ iff $2a \equiv 0 \pmod{p_i}$.

**Lemma 12.1.** *For any $r'_i \in G'$ from Definition 5.2 it follows that the product relationship in 5.1 produces $\prod_{k=1}^{\pi(a)}(r'_i + p_k) \equiv (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i+2+s}}$ or all $s \in \mathbb{N}$.*

*Proof.* For any $x, y, z \in \mathbb{Z}$ where $z > 0$ it follows that if $x = y$, then $x \equiv y \pmod z$. Thus, for any $r'_i \in G'$ Definition 5.1 shows $\prod_{k=1}^{\pi(a)}(r'_i + p_k) = (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k}$. Since the R.H.S. is an integer, the L.H.S. must also be an integer giving rise to the product relationship where $\prod_{k=1}^{\pi(a)}(r'_i + p_k) \equiv (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i+2+s}}$ for all $s \in \mathbb{N}$. □

**Lemma 12.2.** *If $\beta_i > 0$, there exists some $r'_i \in G'$ where $r'_i = t'_{\beta_i} p_i^{\beta_i} + p_i$ where $r'_i \in \mathbb{Z}$.*

*Proof.* From Theorem 10.4 iff $\beta_i > 0$ there exists some unique $r'_i = t'_{\beta_i} p_i^{\beta_i} + p_i \pmod{p_i^{\beta_i+1}}$. The Hensel-Goldbach Difference Equations 10.3 allow for as many lifts as possible where

$$-t'_{\beta_i+1+s} p_i^{\beta_i+1+s} \mathcal{G}'_+(r'_i) \equiv \prod_{k=1}^{\pi(a)}(r'_i + p_k) - (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i+2+s}} \tag{12.1}$$

for all $s \in \mathbb{N}$. However, by Definition 5.2 and Lemma 12.1

$$\prod_{k=1}^{\pi(a)}(r'_i + p_k) \equiv (a+1)^{\gamma(a+1)} \prod_{k=1}^{\pi(a)} p_k^{\beta_k} \pmod{p_i^{\beta_i+2+s}} \tag{12.2}$$

where it clearly follows from equations 11.1 and 12.2

$$-t'_{\alpha_i+1+s} p_i^{\alpha_i+1+s} \mathcal{G}'_-(r_i) \equiv 0 \pmod{p_i^{\alpha_i+2+s}} \tag{12.3}$$

for all $s \in \mathbb{N}$. This shows the R.H.S. above is always zero where all $t'_{k>\beta_i} = 0$ terminating all lifts above $\beta_i$. Therefore, it may be concluded from Theorem 8.3 that for any $\beta_i > 0$ there is a unique root $r'_i \in G'$ where $r'_i = t'_{\beta_i} p_i^{\beta_i} + p_i$ for some $t'_{\beta_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. □

**Proposition 12.3.** *$\beta_i > 0$ if and only if $2a \equiv 0 \pmod{p_i}$.*

*Proof.* Under Lemma 12.2 it was shown that if $\beta_i > 0$, there is a rational root $r'_i \equiv 0 \pmod{p_i}$ and $r'_i = t'_{\beta_i} p_i^{\beta_i} + p_i$ for some $t'_{\beta_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. From Corollary 7.5 it was shown that $2a$ is the only rational root to the G.P. in Definition 5.1. Therefore, $2a = t'_{\beta_i} p_i^{\beta_i} + p_i$ showing if $\beta_i > 0$, then $2a \equiv 0 \pmod{p_i}$.

If $2a \equiv 0 \pmod{p_i}$, Propositions 10.5 and 3.14 ensure $2a = t'_{\beta_i} p_i^{\beta_i} + p_i$ for a $t'_{\beta_i} \in \mathbb{Z}_{p_i} \setminus \{0\}$. □

**Corollary 12.4.** *There is no prime $p_i < a$ where $p_i | u_j$ for some $j \neq i$.*

*Proof.* Assume, for the sake of contradiction, that there exists some prime $p_i < a$ where $p_i | u_j$ for some $j \neq i$. From Lemma 3.11 it then follows that $\beta_i > 0$. Under Proposition 12.3 it then follows that $2a \equiv 0 \pmod{p_i}$. However, since $p_i | 2a$, Lemma 3.12 states $p_i | u_i$ where Lemma 3.13 states that $p_i \nmid u_j$ for any $j \neq i$, contradicting the assumption that there exists some prime $p_i < a$ where $p_i | u_j$ for some $j \neq i$. Thus, no prime $p_i < a$ exists where $p_i | u_j$ for some $j \neq i$ □

**Theorem 12.5.** *There are no solutions to equation 5.1 where $\mathcal{G}_+(2a) = 0$ and $a > 3$.*

*Proof.* From Lemma 12.4 it was shown that there is no scenario where any $p_i|u_j$ when $j \neq i$. From Lemmas 3.11, 3.12, and 3.13, the only solutions when $\mathcal{G}_+(2a) = 0$ and $a > 3$ are given when each $u_i$ is of the form $u_i = p_i^{\beta_i}$. It can then be seen via a substitution into equation 3.6

$$2a = p_i^{\beta_i} - p_i \text{ for all prime } p_i < a. \tag{12.4}$$

This forces all prime $p_i > a$ to be divisors of $2a$. However, since Bertrand's Postulate ensures there always exists some prime between in the interval $[a, 2a]$, then $2a < a\#$ for $a > 4$. Thus, no counter-examples exist when $a > 3$ and theorem 3.10 states the G.D.C. 3.7 is true. □

*Conjecture* 12.6. The Polignac Conjecture states that for any even number there exist an infinite number of prime pairs whose difference is that even number.

It will be shown that the proof of the G.C. 3.1, G.D.C. 3.7, along with Theorem 11.6 will be all that is needed to prove this conjecture is true.

**Theorem 12.7.** *The Polginac Conjecture is true.*

*Proof.* Under Theorems 11.5 and 12.5 it follows for all even $m, n \in \mathbb{N}$, with $m \geq 6$, there exists odd $p_4, p_3, p_2, p_1 \in \mathbb{P}$, where $p_4 - p_3 = m + n$, and $p_2 + p_1 = m$. Allowing $n$ to be fixed for some even number, and $m$ to cycle through all of the positive even numbers greater than 4 gives an infinite set of equations for $n$ of the form $p_4 - (p_3 + p_2 + p_1) = n$. If the Polignac Conjecture were false for some $n$, there would be only finitely many primes that were the sum of three odd, prime numbers. Theorem 11.6, and Euclid's proof for the infinitude of the primes, shows this cannot be the case, proving the Polignac Conjecture is true. □

## 13. Acknowledgements

I wish to thank Jeff Roush and Dr. Robert Daly for their conversations with me on these topics and support. I would also like to thank Adreana Julander, Farley Ferrante, and Bhat Rhagavendra for their input and help with structuring this paper.

## References

[1] Apostol, Tom M. "The Fundamental Theorem of Arithmetic." Introduction to Analytic Number Theory. Springer, New York, NY, 1976. 13-23.

[2] Conrad, Keith. "Hensel's lemma." Unpublished notes. Available at https://kconrad. math. uconn. edu/blurbs/gradnumthy/hensel. pdf (2015).

[3] Deshouillers, J-M., Herman JJ te Riele, and Yannick Saouter. "New Ezperimental Results Concerning the Goldbach Conjecture." International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 1998.

[4] e Silva, Tomás Oliveira, Siegfried Herzog, and Silvio Pardi. "Empirical Verification of the Even Goldbach Conjecture and Computation of Prime Gaps up to $4 \cdot 10^{18}$." Mathematics of Computation (2014): 2033-2060.

[5] Hardy, Godfrey H., and John E. Littlewood. "Some Problems of 'Partitio Numerorum'; III: On the Ezpression of a Number as a Sum of Primes." Acta Mathematica 44.1 (1923): 1-70.

[6] Helfgott, Harald A. "The Ternary Goldbach Conjecture is True." arziv preprint arziv:1312.7748 (2013).

[7] Helfgott, Harald A., and David J. Platt. "Numerical Verification of the Ternary Goldbach Conjecture up to $8.875 \cdot 10^{30}$." Ezperimental Mathematics 22.4 (2013): 406-409.

[8] J. J. Tattersall Elementary Number Theory in Nine Chapters. Cambridge University Press, ISBN 978-0-521-58503-3, 1999.

[9] Jörg Richstein, "Verifying the Goldbach Conjecture up to $4 \cdot 10^{14}$." Mathematics of Computation 70.236 (2001): 1745-1749.

[10] Ruiz, Sebastián Martín. "80.52 An Algebraic Identity Leading to Wilson's Theorem." The Mathematical Gazette 80.489 (1996): 579-582.

[11] Saouter, Yannick. "Checking the Odd Goldbach Conjecture up to $10^{20}$." Mathematics of Computation 67.222 (1998): 863-866.

[12] Selberg, Atle. "An Elementary Proof of the Prime-Number Theorem." Annals of Mathematics (1949): 305-313.

[13] Viéte, Francios. "Opera Mathematica." 1579. Reprinted Leiden, Netherlands, 1646.

[14] Zhang, Yitang. "Bounded Gaps Between Primes." Annals of Mathematics (2014): 1121-1174.

email: jrsouth@smu.edu