A PROOF OF THE GOLDBACH AND POLIGNAC CONJECTURES

JASON R. SOUTH
email: jrsouth@smu.edu
MAY 21, 2025

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. Also, for any sufficiently large $a \in \mathbb{N}$ the set $\mathcal{P}$ is the set of all primes $p_i \leq a$. 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 $p_i \in \mathcal{P}$ there exists some unique $\alpha_i \in \mathbb{N}$ and a mapping $\mathcal{G}_- : \mathbb{C} \to \mathbb{C}$ where

$$\mathcal{G}_-(z) = \prod_{p_i \in \mathcal{P}} (z - p_i) - \prod_{p_i \in \mathcal{P}} p_i^{\alpha_i} : \mathcal{G}_-(2a) = 0.$$

A proof of the Goldbach Conjecture will be given utilizing Hensel's Lemma and Catalan's Conjecture showing that $a = 3$ is the largest solution and no counter-examples exist.

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

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

$2a$ is a counter-example if and only if for each prime $p_i \in \mathcal{P}$ there exists some unique $\beta_i \in \mathbb{N}$ with the mapping $\mathcal{G}_+ : \mathbb{C} \to \mathbb{C}$ where

$$\mathcal{G}_+(z) = \prod_{p_i \in \mathcal{P}} (z + p_i) - (a+1)^{\gamma(a+1)} \prod_{p_i \in \mathcal{P}} p_i^{\beta_i} : \mathcal{G}_+(2a) = 0.$$

A proof will then be given that every even number is the difference of two primes by utilizing Hensel's Lemma and Catalan's Conjecture that $a = 3$ is the largest solution and no counter-examples exist. A proof of the Polignac Conjecture will then follow.

Contents

1. Introduction

1.1. **Historical Underpinnings.** 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 [10] using computational techniques showing that the Goldbach Conjecture was valid up to 4×10^{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 4×10^{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 [13] 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.

1.2. **Motivation for a New Thought Experiment.** The three conjectures this paper will be focused on are given below and it will be shown that once the first two conjectures are proven that the Polignac Conjecture follows as a direct consequence.

Conjecture 1.1. 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 $2a = q_i + p_i$.

An analogue to the Goldbach Conjecture concerning differences of primes is given below.

Conjecture 1.2. 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 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 $p_i \leq a$.

Finally, the Polignac Conjecture is given below.

Conjecture 1.3. Let $a \in \mathbb{N}$. The *Polignac Conjecture* states that there exists an infinite number of prime pairs whose difference is $2a$.

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 [16]. Another method is to assume a certain hypothesis is true, such as the Generalized Reimann Hypothesis, and 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 [10], [4], and [13], 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] [14] 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 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] [15] 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 the method explored in this paper 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.

$$20 = 18 + 2 = 17 + 3 = 15 + 5 = 13 + 7 \tag{1.1}$$

Assuming that 20 is not the sum of two prime numbers, it then follows from The Fundamental Theorem of Arithmetic [1] that there exists a unique sequence of $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{N} \cup \{0\}$ where

$$q_1 q_2 q_3 q_4 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} p_4^{\alpha_4}. \tag{1.2}$$

However, a substitution of each $q_i = 20 - p_i$ into the product above shows

$$(20 - 2) \times (20 - 3) \times (20 - 5) \times (20 - 7) \neq 2^{\alpha_1} \times 3^{\alpha_2} \times 5^{\alpha_3} \times 7^{\alpha_4} \tag{1.3}$$

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 1.3 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 same method will be used to determine if every even number 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 u_i labeled by the sequence $u_1 < u_2 < u_3 < u_4$ where $20 = u_i - p_i$. This allows for the following

$$20 = 22 - 2 = 23 - 3 = 25 - 5 = 27 - 7. \tag{1.4}$$

At this point careful attention needs to be given to the fact that the $u_1 = 22$ term is divisible by a prime greater than 10, but composite. Defining $(10 + 1) = 11$ 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 $20 < u_i \leq 30$ 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 $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathbb{N} \cup \{0\}$ where

$$u_1 u_2 u_3 u_4 = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} p_4^{\beta_4} (a + 1). \tag{1.5}$$

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

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

However, a substitution of each $u_i = 20 + p_i$ into the product above shows

$$(20+2) \times (20+3) \times (20+5) \times (20+7) \neq 2^{\beta_1} \times 3^{\beta_2} \times 5^{\beta_3} \times 7^{\beta_4} \times (10+1) \tag{1.6}$$

for any sequence of exponents restricted to the natural numbers. Since each u_i on the L.H.S. ranges between 20 and 30 it can be seen that equation 1.6 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 u_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 1.8 below.

1.3. **Preliminary Definitions and Theorems.** Since the thought experiments are so similar, the definitions will give the generalizations for both in order to be succinct.

Definition 1.4. Let the set of primes be denoted by $\mathbb{P}$. For sufficiently large $a \in \mathbb{N}$ the *Prime Divisor Set* of $2a$ is given by the set $\mathcal{D} = \{p_i \in \mathbb{P} : p_i | 2a\}$.

Definition 1.5. Let $a \in \mathbb{N}_{\geq 2}$ where the *Prime Set* of a is $\mathcal{P} = \{p_i \in \mathbb{P} : p_i \leq a\}$.

Remark 1.6. At this point it is necessary to define the function in Definition 1.7 that will account for the case where $a+1$ is prime. This lies in the fact that in Conjecture 1.2 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 1.7. Let the function $\gamma(a+1)$ be defined by the conditions

$$\gamma(a+1) = \begin{cases} 1, & \text{if } a+1 \text{ is prime} \\ 0, & \text{if } a+1 \text{ is not prime.} \end{cases} \tag{1.7}$$

Definition 1.8. For brevity both the *Goldbach Polynomial Type I and II* will be defined here. To begin, Take some sufficiently large value of $a \in \mathbb{N}$. If it is possible to define the mappings $\mathcal{G}_- : \mathbb{C} \to \mathbb{C}$ where for each prime $p_i \in \mathcal{P}$ there exists some unique $\alpha_i \in \mathbb{N} \cup \{0\}$ where

$$\mathcal{G}_-(z) \coloneqq \prod_{p_i \in \mathcal{P}} (z - p_i) - \prod_{p_i \in \mathcal{P}} p_i^{\alpha_i} \tag{1.8}$$

along with the condition that $\mathcal{G}_-(2a) = 0$, then $\mathcal{G}_-(z)$ is a *Goldbach Polynomial Type I* (G.P.I). Similarly, take some sufficiently large value of $a \in \mathbb{N}$. If it is possible to define the mapping $\mathcal{G}_+ : \mathbb{C} \to \mathbb{C}$ where for each prime $p_i \in \mathcal{P}$ there exists some unique $\beta_i \in \mathbb{N} \cup \{0\}$ where

$$\mathcal{G}_+(z) \coloneqq \prod_{p_i \in \mathcal{P}} (z + p_i) - (a+1)^{\gamma(a+1)} \prod_{p_i \in \mathcal{P}} p_i^{\beta_i}. \tag{1.9}$$

along with the condition that $\mathcal{G}_+(2a) = 0$, then $\mathcal{G}_+(z)$ is a *Goldbach Polynomial Type II* (G.P.II).

Exploration of how to construct the Goldbach Roots will be the focus of subsequent sections. However, the derivative of the Goldbach Polynomials will also be important and is given below.

Definition 1.9. The *Goldbach Polynomial Type I Derivative* is given by

$$\mathcal{G}'_-(z) \coloneqq \prod_{p_i \in \mathcal{P}} (z - p_i) \left[\frac{1}{z - p_1} + \frac{1}{z - p_2} + \cdots + \frac{1}{z - p_{\pi(a)}} \right] \tag{1.10}$$

and follows directly from equation 1.8. The *Goldbach Polynomial Type II Derivative* is

$$\mathcal{G}'_+(z) \coloneqq \prod_{p_i \in \mathcal{P}} (z + p_i) \left[\frac{1}{z + p_1} + \frac{1}{z + p_2} + \cdots + \frac{1}{z + p_{\pi(a)}} \right] \tag{1.11}$$

and follows directly from equation 1.9.

It is shown by Theorem 1.10, stated below with proof, that the Goldbach Polynomial Type I is both necessary and sufficient to produce a counter-example to the G.C.

Theorem 1.10. *Let $a \in \mathbb{N}_{>3}$. $2a$ is a counter-example to the G.C. iff $\mathcal{G}_-(2a) = 0$.*

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

$$2a = q_i + p_i \tag{1.12}$$

with q_i being a composition of primes up to a. Therefore, under the Fundamental Theorem of Arithmetic it follows that for each prime $p_i \in \mathcal{P}$ there must exist a unique $\alpha_i \in \mathbb{N} \cup \{0\}$ where

$$\prod_{i=1}^{\pi(a)} q_i = \prod_{p_i \in \mathcal{P}} p_i^{\alpha_i}. \tag{1.13}$$

A substitution of $q_i = 2a - p_i$ for each q_i from 1.12 in equation 1.13 gives

$$\prod_{p_i \in \mathcal{P}} (2a - p_i) = \prod_{p_i \in \mathcal{P}} p_i^{\alpha_i} \tag{1.14}$$

where it must follow that $\mathcal{G}_{-}(2a) = 0$ from Definition 1.8.

Conversely, if there exists some $2a > 6$ where $\mathcal{G}_{-}(2a) = 0$, the Fundamental Theorem of Arithmetic shows no $2a - p_i$ can be prime for any $p_i \leq a$. Thus, the G.C. would be false. □

It is then shown by Theorem 1.11, stated below with proof, that the Goldbach Polynomial Type II is both necessary and sufficient to produce a counter-example to the G.D.C.

Theorem 1.11. *Let $a \in \mathbb{N}_{>3}$. Then $2a$ is a counter-example to the G.D.C. iff $\mathcal{G}_{+}(2a) = 0$.*

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

$$2a = u_i - p_i \tag{1.15}$$

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

$$\prod_{p_i \in \mathcal{P}} u_i = (a+1)^{\gamma(a+1)} \prod_{p_i \in \mathcal{P}} p_i^{\beta}. \tag{1.16}$$

Substituting $u_i = 2a + p_i$ from equation 1.15 into 1.16 gives

$$\prod_{p_i \in \mathcal{P}} (2a + p_i) = (a+1)^{\gamma(a+1)} \prod_{p_i \in \mathcal{P}} p_i^{\beta} \tag{1.17}$$

where it may be seen that $\mathcal{G}_{+}(2a) = 0$ from Definition 1.8.

Conversely, if there exists some $2a > 6$ where $2a$ is a solution to equation 1.9 and it must be a counter-example to the G.D.C. □

An example of a Goldbach Polynomial Type I and II is given below.

Example 1.12. Let $a = 3$. There exists a G.P.II, $\mathcal{G}_{-}(z) = (z-2)(z-3) - 2^2 \times 3$ since $\mathcal{G}_{-}(6) = 0$. Note $6 = 2^2 + 2 = 3 + 3$ in accordance with equations 1.12 and 1.13. There exists another root $r_2 = -1$ where both roots are given by $G = \{6, -1\}$. Again, 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 1.15 and 1.16. There exists another root $r_2' = -11$ where both roots are given by $G' = \{6, -11\}$.

2. Strategy and Synopsis for the G.C. and G.D.C Proofs

2.1. **Main Results.** The main result of this paper is given by Theorem 2.20 which relies on the proofs for the Goldbach Conjecture and Goldbach Difference Conjecture in Theorems 2.9 and 2.17, along with Theorem 2.10. To begin, note if the G.C. and the G.D.C. in 1.1 and 1.2 are both true, the Polignac Conjecture would follow. This is demonstrated below with proof.

Theorem 2.1. *If the G.C. and G.D.C. are true, then the Polginac Conjecture is true.*

Proof. Assume the G.C. and G.D.C. are true. It then follows that the Ternary Conjecture must also be true. Hence, 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. The Ternary Conjecture and Euclid's proof for the infinitude of the primes shows this cannot be the case, proving the Polignac Conjecture is true if both the G.C. and G.D.C. are true. □

The key is to now prove the G.C. and G.D.C. are true by analyzing the Polynomials in Definition 1.8. and showing there are no solutions for degree greater than 2. The strategy of the proof of both the G.C. and G.D.C. is given below. All steps will be stated explicitly for the G.C.; however, these steps given will apply to the G.D.C. as well, and will be proven.

2.2. **Necessary Axioms and Notation.**

Notation 2.2. The convention $p^\tau || f(a)$ where $\tau \in \mathbb{N} \cup \{0\}$ denotes $p^\tau | f(a)$ and $p^{\tau+1} \nmid f(a)$. Standard conventions and notations will apply throughout where $\mathbb{F}_{p_i}$ denotes the field of integers for the prime p_i given by $\{0, 1, \ldots, p_i - 1\}$. The symbol : will be defined in its usual context as "such that" for brevity in theorems. Finally, the prime counting function is $\pi(a)$ and the symbol $a\#$ has its standard definition of the primorial where $a\# = 2 \times 3 \times \cdots \times p_{\pi(a)}$

Theorems 2.9 and 2.17 will rely heavily on the use Hensel's Lemma [2] as a method for discovering properties about the root $2a$ that is assumed to be a counter-example to the G.C. It turns out a more general version of this lemma is needed which can be found in Section 2.6 of [9] whose full proof is stated below and will follow closely from the source.

Theorem 2.3 (**Generalized Hensel Lemma**). *Let $f(x) \in \mathbb{Z}[x]$. Suppose $f(a) \equiv 0 \pmod{p^j}$, $p^\tau || f'(a)$ from Notation 2.2, and $j \geq 2\tau + 1$. If $b \equiv a \pmod{p^{j-\tau}}$, then $f(b) \equiv f(a) \pmod{p^j}$ and $p^\tau || f'(b)$. Moreover, there is a unique $t \in \mathbb{F}_p$ such that $f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{j+1}}$.*

Proof. Using the Taylor expansion

$$f(b) \equiv f(a + tp^{j-\tau}) = f(a) + tp^{j-\tau} f'(a) \pmod{p^{2j-2\tau}}. \tag{2.1}$$

The modulus is divisible by p^{j+1} since $2j - 2\tau = j + (j - 2\tau) \geq j + 1$. This allows for

$$f(a + tp^{j-\tau}) = f(a) + tp^{j-\tau} f'(a) \pmod{p^{j+1}}. \tag{2.2}$$

Since both terms on the R.H.S. above are divisible by p^j, so to is the L.H.S. showing

$$\frac{f(a + tp^{j-\tau})}{p^j} = \frac{f(a)}{p^j} + t\frac{f'(a)}{p^\tau} \pmod{p} \tag{2.3}$$

where the condition that $p^\tau || f'(a)$ shows that t must be relatively prime to p and must therefore be unique in modulo p. To complete the proof note that $f'(x) \in \mathbb{Z}[x]$ where

$$f'(a + tp^{j-\tau}) = f'(a) \pmod{p^{j-\tau}} \tag{2.4}$$

for any integer t. However, since $j - \tau \geq \tau + 1$ this congruence holds $\pmod{p^{\tau+1}}$ it follows that $p^\tau || f'(a)$ and therefore $p^\tau || f'(a + tp^{j-\tau})$ proving the theorem. □

Remark 2.4. Note that if $\tau = 0$ in the theorem above, then Hensel's Lemma is produced by $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$. Given $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$ it can be seen $tp^j f'(a) \equiv -f(a) \pmod{p^{j+1}} : \exists! t \in \mathbb{F}_{p_i}$.

The final piece that will be needed to prove the Goldbach Conjecture and Goldbach Difference Conjecture is Catalan's Conjecture proven in [11] and stated below.

Theorem 2.5 (**Mihailescu's Theorem**). *Catalan's Conjecture states that the largest non-trivial solutions to the Diophantine Equation $x^\mu - y^\nu = 1$ is given by $3^2 - 2^3 = 1$.*

Proof. The proof of this conjecture is given in [11]. □

2.3. **Overview and Strategy of the Goldbach Conjecture Proof.** All Theorems, propositions, lemmas, and corollaries will be proven in the following section. To begin the overview of the G.C. proof, it is assumed for the sake of contradiction, that there exists a Goldbach Polynomial with degree greater than 2 where it may then be concluded from Theorem 1.10 that $2a$ is a counter-example to the Goldbach Conjecture. It follows from p-adic analysis that for any prime $p_i \in \mathcal{P}$ from Definition 1.5 there is a finite, unique sequence where

$$2a = t_0 + t_1 p_i + t_2 p_i^2 + \cdots + t_n p_i^n : \text{each } t \in \mathbb{F}_{p_i}. \tag{2.5}$$

Using the fact that the transitive property lets equation 1.12 to be written explicitly as

$$2a = q_1 + 2 = \cdots = q_i + p_i = \cdots = q_j + p_j = \cdots = q_{\pi(a)} + p_{\pi(a)} \tag{2.6}$$

allowing for a unique solution of q_i in terms of a p_i-adic series. The question to be answered is how to build up each q_i in equation 1.12. This is not trivial to answer since equations 2.5 and 2.6 allows for $\pi(a)$ q's and $\pi(a)$ p-adic series to keep track of. It turns out that finding these series is achievable and actually quite simple using Hensel's Lemma in Theorem 2.3. We begin by defining the relationship which is established between the exponents of the Goldbach Polynomial in 1.8 and specific congruences that $2a$ must abide by whenever those exponents are greater than zero. These relationships are reflected in Lemma 2.6 which is stated below.

Lemma 2.6. *Any $\alpha_i > 0$ if and only if $2a \equiv 0 \pmod{p_i}$ or $2a \equiv p_j \pmod{p_i}$ for some $p_j \in \mathcal{P}$.*

Once this has been established it is simply an analysis of each case in Lemma 2.6. However, the simplest and most efficient way to analyze these cases is to note that for any $\alpha_i > 0$ each $p_m \in \mathcal{P}$ is a root to the Goldbach Polynomial in 1.8 for modulus $p_i^{\alpha_i}$ but not $p_i^{\alpha_i+1}$ since

$$\mathcal{G}_-(p_1) = \cdots = \mathcal{G}_-(p_j) \equiv \cdots = \mathcal{G}_-(p_i) = \cdots = \mathcal{G}_-(p_{\pi(a)}) = -\prod_{p_k \in \mathcal{P}} p_k^{\alpha_k} \equiv 0 \pmod{p_i^{\alpha_i}}. \tag{2.7}$$

Using Hensel's Generalized Lemma in 2.3 it is a possible to prove the following proposition.

Proposition 2.7. *If $\alpha_i > 0$, it then follows that for each $p_m \in \mathcal{P}$ there is a unique modular root $\mathcal{G}_-(r_m) \equiv 0 \pmod{p_i^{\alpha_i+1}} : r_m \equiv t_{\alpha_i} p_i^{\alpha_i} + p_m \pmod{p_i^{\alpha_i+1}}$ with the condition that $t_{\alpha_i} \in \mathbb{F}_{p_i} \setminus \{0\}$.*

The reason for doing this lays the framework for finding the necessary divisibility properties for the q's in equation 2.6. Since $2a$ must either be congruent to 0 or some other $p_j \in \mathcal{P}$ for modulus p_i whenever $\alpha_i > 0$, it can be seen from the Proposition above that either $2a = n_i p_i^{\alpha_i} + p_i$ or $2a = n_j p_i^{\alpha_i} + p_j$ for some $p_j \in \mathcal{P}$ since $2a$ is a root. However, since α_i is the largest value the exponent can take in equation 1.13 from the proof of Theorem 1.10, it then must be the case that p_i only divides one q in equation 2.6. This is proven in detail in Corollary 2.8.

Corollary 2.8. *If $\mathcal{G}_-(2a) = 0$, then for any q_i, q_j in 2.6 the $GCD(q_i, q_j) = 1$.*

Since there are $\pi(a)$ q's and $\pi(a)$ primes $p_i \in \mathcal{P}$ where all q's must be composites of only primes in $\mathcal{P}$ along with the condition from Corollary 2.8 that the $GCD(q_i, q_j) = 1$, it must follow that each q must be a distinct prime power. Since Catalan's Conjecture 2.5 was proven in [11] and equation 2.6 shows that there must be some perfect power where $2^{\alpha_1} + 2 = p_j^{\alpha_j} + 3$, it follows that the largest solution is given by $\alpha_i = 2$ showing $2a = 2^2 + 2 = 6$, contradicting the assumption $2a > 6$. This is stated below in Theorem 2.9.

Theorem 2.9. *There are no solutions to equation 1.8 where $\mathcal{G}_-(2a) = 0$ and $a > 3$.*

All of the same proof structures hold in relation to the Goldbach Difference Conjecture for Goldbach Polynomials of the second type and will be proven in detail throughout section 2.5. Once the Goldbach Conjecture is proven, along with the Goldbach Difference Conjecture, the weak version of the Goldbach Conjecture in 2.10 follows trivially. Finally, to complete the proof for the Polignac Conjecture in 1.3 all that is needed is Theorem 2.20.

2.4. **A Proof of the Goldbach Conjecture.**

Lemma 2.6. *Any $\alpha_i > 0$ if and only if $2a \equiv 0 \pmod{p_i}$ or $2a \equiv p_j \pmod{p_i}$ for some $p_j \in \mathcal{P}$.*

Proof. From equation 1.13 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 where $p_i | p_i^{\alpha_i}$. Therefore, that p_i divides the L.H.S. of the equation and must divide its corresponding q_i or some other q_j where equation 2.6 shows $2a \equiv 0 \pmod{p_i}$ or $2a \equiv p_j \pmod{p_i}$ for some $p_j \in \mathcal{P}$.

Conversely, equations 1.12 and 2.6 show if $2a \equiv 0 \pmod{p_i}$ or $2a \equiv p_j \pmod{p_i}$ for some $p_j \in \mathcal{P}$, then it may be seen from equation 1.13 that p_i is a divisor of its corresponding q_i or q_j. Therefore it may be concluded that p_i divides the R.H.S. of equation 1.13 showing $\alpha_i > 0$. $\square$

The next step is to use Hensel's Lemma and its generalization to construct $2a$ in order to discover properties about how the q's behave in equation 2.6. Before doing this it is important to note that whenever $\alpha_i > 0$ each $p_m \in \mathcal{P}$ is a root of the Goldbach Polynomial in Definition 1.8. Since Lemma 2.6 restricts the values that $2a$ can take in modulo p_i whenever $\alpha_i > 0$ it will be shown in the following proposition that it is in fact possible discover the precise form of each modular root for any prime $p_m \in \mathcal{P}$ whenever that $\alpha_i > 0$.

Proposition 2.7. *If $\alpha_i > 0$, it then follows that for each $p_m \in \mathcal{P}$ there is a unique modular root $\mathcal{G}_-(r_m) \equiv 0 \pmod{p_i^{\alpha_i+1}} : r_m \equiv t_{\alpha_i} p_i^{\alpha_i} + p_m \pmod{p_i^{\alpha_i+1}}$ with the condition that $t_{\alpha_i} \in \mathbb{F}_{p_i} \setminus \{0\}$.*

Proof. Assume $\alpha_i > 1$. From Definition 1.8 it can be seen below that every $p_m \in \mathcal{P}$

$$\mathcal{G}_-(p_1) = \cdots = \mathcal{G}_-(p_j) \equiv \cdots = \mathcal{G}_-(p_i) = \cdots = \mathcal{G}_-(p_{\pi(a)}) = -\prod_{p_k \in \mathcal{P}} p_k^{\alpha_k} \equiv 0 \pmod{p_i^{\alpha_i}}. \tag{2.8}$$

Hence, for every $p_m \in \mathcal{P}$ it follows from Notation 2.2 that $p_i^{\alpha_i} || \mathcal{G}_-(p_m)$ since no $p_m \in \mathcal{P}$ is a root modulus $p_i^{\alpha_i+1}$. Allowing for the possibility of repeated roots $p_j \equiv p_r \cdots \equiv p_l \pmod{p_i}$ it must follow that there exists some τ where $p_i^{\tau} || \mathcal{G}'_-(p_j)$ where $\tau < \alpha_i$ since $p_i^{\alpha_i} || \mathcal{G}_-(p_j)$. W.L.O.G. let $r_j \equiv p_j \pmod{p_i} : p_j \in \mathcal{P}$ where following Theorem 2.3 shows the Taylor Series gives

$$\mathcal{G}_-(r_j) \equiv \mathcal{G}_-(tp_i^{\alpha_i-\tau} + p_j) = \mathcal{G}_-(p_j) + tp_i^{\alpha_i} \frac{\mathcal{G}'_-(p_j)}{p_i^{\tau}} \pmod{p_i^{2\alpha_i-2\tau}}. \tag{2.9}$$

The modulus is divisible by p^{α_i+1} since $\alpha_i + 1 \leq 2\alpha_i - 2\tau$ when $\alpha_i \geq 2\tau + 1$ showing

$$\mathcal{G}_-(tp_i^{\alpha_i-\tau} + p_j) = \mathcal{G}_-(p_j) + tp_i^{\alpha_i} \frac{\mathcal{G}'_-(p_j)}{p_i^{\tau}} \equiv 0 \pmod{p_i^{\alpha_i+1}} \tag{2.10}$$

where t is really the t_{α_i} component in the p_i-adic series for r_j. Since $\mathcal{G}_-(p_j) \not\equiv 0 \pmod{p_i^{\alpha_i+1}}$ from equation 2.8, it may be seen that equation 2.10 shows

$$-t_{\alpha_i} p_i^{\alpha_i} \frac{\mathcal{G}'_-(p_j)}{p_i^{\tau}} \equiv \mathcal{G}_-(p_j) \not\equiv 0 \pmod{p_i^{\alpha_i+1}}. \tag{2.11}$$

Hence, $r_j \equiv t_{\alpha_i} p_i^{\alpha_i} + p_j \pmod{p_i^{\alpha_i+1}} : t_{\alpha_i} \in \mathbb{F}_{p_i} \setminus \{0\}$ proving the proposition is true. $\square$

Corollary 2.8. *If $\mathcal{G}_-(2a) = 0$, then for any q_i, q_j in 2.6 the $GCD(q_i, q_j) = 1$.*

Proof. Equation 2.6 shows if $p_i | q_i$, then $2a \equiv 0 \pmod{p_i}$ where it may be seen from Theorem 2.7 there exists some non-zero integer n_i where $2a = n_i p_i^{\alpha_i} + p_i$ and the $GCD(n_i, p_i) = 1$. Under equation 2.6 this is equivalent to stating $q_i = n_i p_i^{\alpha_i}$ showing if $p_i | 2a$, then it can only divide its corresponding q_i since α_i is the largest prime power for p_i in Definition 1.8 and equation 1.13.

Alternatively, if $\alpha_i > 0$ where $2a \not\equiv 0 \pmod{p_i}$, then Lemma 2.6 states that there must exist at least one $p_j \in \mathcal{P}$ where $2a \equiv p_j \pmod{p_i}$. From Theorem 2.7 it is shown there must exist some non-zero integer m_j where $2a = m_j p_i^{\alpha_i} + p_j$ and $GCD(m_j, p_i) = 1$. Since α_i is the largest value the exponent for p_i may take on the R.H.S. of Definition 1.8 and equation 1.13 it must follow that p_i only divides q_j. Therefore, it follows that if $\alpha_i > 0$, then no $p_i \in \mathcal{P}$ divides any two q's in equation 2.6. Since all q's are assumed to be composites of only primes in $\mathcal{P}$, and there are $\pi(a)$ q's, then $GCD(q_i, q_j) = 1$ for all q's in equation 2.6. $\square$

The final step is to use Catalan's Conjecture [11] which showed that the largest solutions to the Diophantine Equation of the form $x^\mu - y^\nu = 1$ is given by $3^2 - 2^3 = 1$.

Theorem 2.9. *There are no solutions to equation 1.8 where* $\mathcal{G}_-(2a) = 0$ *and* $a > 3$.

Proof. From Corollary 2.8 it was shown that no prime p_i divides any two q's. Since, there are $\pi(a)$ q's that share no primes and they are all only comprised of the $\pi(a)$ primes in $\mathcal{P}$, then all $\alpha_i > 0$ and all q's are perfect prime powers. Therefore, for any $p_i \in \mathcal{D}$ from 1.4 it follows that

$$2a = p_i^{\alpha_i} + p_i \text{ for all prime } p_i \in \mathcal{D}. \tag{2.12}$$

Using the transitive property from equation 2.6, and the fact that $2|2a$, it follows that there exists some prime power where $2^{\alpha_1} + 2 = p_j^{\alpha_j} + 3$. However, the proof of Catalan's Conjecture 2.5 ensures that the largest values this equation has is $2^2+2 = 3+3$. Therefore, that the largest value for $2a$ satisfying $\mathcal{G}_-(2a) = 0$ is when $a = 3$. Under Theorem 1.10 no counter-examples to the Goldbach Conjecture and it is proven to be true. □

Theorem 2.10. *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 2.9 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 2.11. *Every prime larger than 7 is the sum of three odd primes.*

Proof. This follows trivially from Theorem 2.10 since all primes greater than seven are odd. □

Definition 2.12. Let $a \in \mathbb{N}_{>3}$. A *Prime Reflective Point (P.R.P.)* is any $b_R \in \mathbb{N} : a \pm b_R \in \mathbb{P}$.

Theorem 2.9 along with Definition 2.12 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 2.13 (Prime Midpoint Theorem). *Every* $a \in \mathbb{N}_{>3}$ *has some non-zero P.R.P.*

Proof. Since no solutions exist to Theorem 1.10 when $2a > 6$, this must also hold when a is prime. This would allow for a cancellation of a from both sides of equation 1.13. Since solutions would still not exist, another q_i must be prime in equation 1.12. 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. □

2.5. **A Proof of the Goldbach Difference and Polignac Conjectures.** This section is nearly identical to the section proving the Goldbach Conjecture. However, all steps will be followed and explicitly stated. The Polignac Conjecture will then follow.

Lemma 2.14. $\beta_i > 0$ *if and only if* $2a \equiv 0 \pmod{p_i}$ *or* $2a \equiv -p_j \pmod{p_i}$ *for some* $p_j \in \mathcal{P}$.

Proof. From equation 1.16 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 1.16 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 1.16 showing $p_i | p_i^{\beta_i}$ where $\beta_i > 0$. □

Proposition 2.15. *If* $\beta_i > 0$, *it then follows that for each* $p_m \in \mathcal{P}$ *there is a unique modular root* $\mathcal{G}_+(r_m) \equiv 0 \pmod{p_i^{\beta_i+1}} : r_m \equiv t_{\beta_i} p_i^{\beta_i} - p_m \pmod{p_i^{\beta_i+1}}$ *with the condition that* $t_{\beta_i} \in \mathbb{F}_{p_i} \setminus \{0\}$.

Proof. Assume $\beta_i > 1$. From Definition 1.8 it can be seen below that every $p_m \in \mathcal{P}$

$$\mathcal{G}_+(-p_1) \equiv \cdots \equiv \mathcal{G}_+(-p_r) \equiv \cdots = \mathcal{G}_+(-p_{\pi(a)}) \equiv -(a+1)^{\gamma(a+1)} \prod_{p_k \in \mathcal{P}} p_k^{\beta_k} \equiv 0 \pmod{p_i^{\beta_i}}. \tag{2.13}$$

Hence, for every $p_m \in \mathcal{P}$ it follows from Notation 2.2 that $p_i^{\beta_i} || \mathcal{G}_+(-p_m)$ since no $-p_m \in \mathcal{P}$ is a root modulus $p_i^{\beta_i+1}$. Allowing for the possibility of repeated roots $p_j \equiv p_r \cdots \equiv p_l \pmod{p_i}$

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

it must follow that there exists some τ where $p_i^\tau || \mathcal{G}'_+(-p_j)$ where $\tau < \beta_i$ since $p_i^{\beta_i} || \mathcal{G}_-(-p_j)$. W.L.O.G. let $r_j \equiv -p_j \pmod{p_i} : p_j \in \mathcal{P}$ where following Theorem 2.3 shows the Taylor Series

$$\mathcal{G}_+(r_j) \equiv \mathcal{G}_+(tp_i^{\beta_i - \tau} - p_j) = \mathcal{G}_+(-p_j) + tp_i^{\beta_i} \frac{\mathcal{G}'_+(-p_j)}{p_i^\tau} \pmod{p_i^{2\beta_i - 2\tau}}. \tag{2.14}$$

The modulus is divisible by p^{β_i+1} since $\beta_i + 1 \leq 2\beta_i - 2\tau$ when $\beta_i \geq 2\tau + 1$.

$$\mathcal{G}_+(tp_i^{\alpha_i - \tau} - p_j) = \mathcal{G}_+(-p_j) + tp_i^{\beta_i} \frac{\mathcal{G}'_+(-p_j)}{p_i^\tau} \equiv 0 \pmod{p_i^{\beta_i+1}}. \tag{2.15}$$

where t is really the t_{β_i} component in the p_i-adic series for r_j. Since $\mathcal{G}_+(-p_j) \not\equiv 0 \pmod{p_i^{\beta_i+1}}$ from equation 2.13, it may be seen that equation 2.15 shows

$$- t_{\beta_i} p_i^{\beta_i} \frac{\mathcal{G}'_+(-p_j)}{p_i^\tau} \equiv \mathcal{G}_+(-p_j) \not\equiv 0 \pmod{p_i^{\beta_i+1}}. \tag{2.16}$$

Hence, $r_j \equiv t_{\beta_i} p_i^{\beta_i} - p_j \pmod{p_i^{\beta_i+1}} : t_{\beta_i} \in \mathbb{F}_{p_i} \setminus \{0\}$ proving the proposition is true. □

Corollary 2.16. *For any u_i, u_j in 1.15 and 1.16 of Theorem 1.11, the $GCD(u_i, u_j) = 1$.*

Proof. Lemma 2.14 shows if $p_i | u_i$, then $2a \equiv 0 \pmod{p_i}$ where it may be seen from Theorem 2.15 there exists some non-zero integer n_i where $2a = m_i p_i^{\beta_i} - p_i$ and $GCD(m_i, p_i) = 1$. Under equation 1.15 this is equivalent to stating $u_i = m_i p_i^{\beta_i}$ showing that if $p_i | 2a$ it can only divide its corresponding u_i since β_i is the largest prime power for p_i in Definition 1.8 and equation 1.16.

Alternatively, if $\beta_i > 0$ where $2a \not\equiv 0 \pmod{p_i}$, then Lemma 2.14 states that there must exist at least one $p_j \in \mathcal{P}$ where $2a \equiv -p_j \pmod{p_i}$. Under Theorem 2.15 it then follows there must exist some non-zero integer m_j where $2a = m_j p_i^{\beta_i} - p_j$ and $GCD(m_j, p_i) = 1$. Since β_i is the largest value the exponent for p_i may take on from the R.H.S. of equation 1.16, it must follow that p_i only divides u_j. Since all u's are assumed to be composites of only primes in $\mathcal{P}$, then $GCD(u_i, u_j) = 1$ for all u's in equation 1.16. □

Theorem 2.17. *There are no solutions to equation 1.9 where $\mathcal{G}_+(2a) = 0$ and $a > 3$.*

Proof. From Corollary 2.16 it was shown that no prime p_i divides any two u's. Since, there are $\pi(a)$ u's that share no primes and they are all only comprised of the $\pi(a)$ primes in $\mathcal{P}$, then all $\beta_i > 0$ and all u's are perfect prime powers. Therefore, for any $p_i \in \mathcal{D}$ from 1.4 it follows that

$$2a = p_i^{\beta_i} - p_i \text{ for all prime } p_i \in \mathcal{D}. \tag{2.17}$$

Using the transitive property from equation 1.15, and the fact that $2|2a$, it follows that there exists some prime power where $2^{\beta_1} - 2 = p_j^{\beta_j} - 3$. However, the proof of Catalan's Conjecture 2.5 ensures that the largest values this equation has is $2^3 - 2 = 3^2 - 3$. Therefore, the largest value for $2a$ satisfying $\mathcal{G}_+(2a) = 0$ is $a = 3$. From Theorem 1.11 the G.D.C. is true. □

Definition 2.18. Let $a \in \mathbb{N}$. A *Prime Difference Point (P.D.P.)* is any $b_D > a : ||a \pm b_D|| \in \mathbb{P}$.

Theorem 2.19. *Every $a \in \mathbb{N}$ where $a > 3$ has some non-zero P.D.P.*

Proof. Since no solutions exist to Theorem 1.11 when $2a > 6$, this must also hold when a is prime. This would allow for a cancellation of a from both sides of equation 1.17. Since solutions would still not exist, another u_i must be prime in equation 1.15. Thus, since every prime has a non-zero P.D.P. and any composite a must also have a non-zero P.D.P., the theorem is true. □

Theorem 2.20. *The Polignac Conjecture is true.*

Proof. Under Theorems 2.1, 2.9, 2.17, and Corollary 2.10 the Polignac Conjecture is true. □

3. 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] I. Niven, H. S. Zuckerman and H. L. Montgomery, " An Introduction to the Theory of Numbers," 5th Edition, Oxford University Press, Oxford, 1991.

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

[11] Metsankyla, Tauno. "Catalan's Conjecture: Another Old Diophantine Problem Solved." Bulletin of the American Mathematical Society 41.1 (2004): 43-57.

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

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

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

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

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