8-2018

On Some Conjectures in Additive Number Theory

Huixi Li
Clemson University, huixil@g.clemson.edu

On Some Conjectures in Additive Number Theory

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematics

---

by
Huixi Li
August 2018

Accepted by:
Dr. Jim Brown, Committee Chair
Dr. Michael Burr
Dr. Kevin James
Dr. Hui Xue

Abstract

In the first part of the thesis we prove that every sufficiently large odd integer can be written as a sum of a prime and 2 times a product of at most two distinct odd primes. Together with Chen's theorem and Ross's observation, we know every sufficiently large integer can be written as a sum of a prime and a square-free number with at most three prime divisors, which improves a theorem by Estermann that every sufficiently large integer can be written as a sum of a prime and a square-free number.

In the second part of the thesis we prove some results that specialize to confirm some conjectures of Sun, which are related to Fermat's theorem on sums of two squares and other representations of primes in arithmetic progressions that can be represented by quadratic forms. The proof uses the equidistribution of primes in imaginary quadratic fields.

Dedication

I would like to thank my parents, Yangchun Li and Zhenyun Shen, for their support.

I would like to thank the course coordinators, Meredith Burr, Judy Cottingham, Randy Davidson, Donna Simms, and many others for their help in my teaching.

I would like to thank all of my math lecturers for giving me a solid background in math.

I would like to thank Michael Burr and Mishko Mitkovski for encouraging me to study number theory.

I would like to thank my friends Soumendra Ganguly, Hugh Geller, Luke Giberson, Andrew Green, Rodney Keaton, Dania Zantout, and Daozhou Zhu for discussing number theory questions with me.

I would like to thank my advisor, Jim Brown, and all other committee members, Michael Burr, Kevin James, and Hui Xue for turning me from a student into a researcher.

I would like to thank everyone at Clemson. The Clemson spirit always cheers me on.

Go Tigers!

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In additive number theory, we study subsets of integers and their behavior under addition. As the building blocks of integers, prime numbers are particularly interesting. There are many questions related to integers and prime numbers that are easy to state but hard to answer.

Goldbach's conjecture and the twin prime conjecture are two classical examples of such questions. In 1742 Goldbach wrote a letter to Euler to discuss his two discoveries. Goldbach conjectured that every even integer greater than 2 can be written as the sum of two primes, and every odd integer greater than 5 can be written as the sum of three primes. Even though his conjectures look easy, they are very hard to prove. The odd integer case conjecture is a known as the weak Goldbach conjecture, and it was completely solved in 2013 [12]. The even integer case conjecture, i.e., the strong Goldbach conjecture, remains unsolved. Lemoine's conjecture is similar to the strong Goldbach conjecture. It states that every odd integer greater greater than 5 can be written as the sum of a prime and 2 times another prime.

In 1846 Polignac stated the twin prime conjecture. In fact, his original conjecture was more general. If we look at the sequence of prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, \cdots$, we see there are many consecutive primes with distance 2, for example, $5 - 3 = 2$, $7 - 5 = 2$, $13 - 11 = 2$, and $19 - 17 = 2$. We call such pairs of primes "twin primes". The twin prime conjecture states that there are infinitely many pairs of twin primes. In the past few years, Green, Maynard, the Polymath Project 8 group, Tao, and Zhang made some great achievements on the bounded gaps between primes in [18, 21, 29]. It is natural to ask whether $p - 2q$ has a bounded gap or not for prime numbers p and q.

In Chapter 2, I will give a short survey on sieve theory and some known results on Goldbach's conjecture, Lemoine's conjecture, and the twin prime conjecture. Then I will prove some related results that improve a theorem by Estermann, which states that every sufficiently large odd integer is a sum of a prime and a square-free number. The work in this chapter has been published in [15].

There are a lot of new conjectures about prime numbers too, for example, in [25] Sun posed 100 new conjectures on representations involving primes. There is also a series of videos [24] by Sun on Goldbach's conjecture, in which he mentioned a couple of interesting conjectures. In joint work with Brown and James, I successfully proved two of these conjectures.

Fermat's theorem on sums of two squares states that an odd prime p can be written as a sum of two integers squares $a_p^2 + b_p^2$ if and only if $p \equiv 1 \pmod 4$. There is a similar result that a prime $p > 3$ can be written as a sum of $a_p^2 + a_p b_p + b_p^2$ for integers a_p and b_p if and only if $p \equiv 1 \pmod 3$. When we restrict that $0 < b_p < a_p$ in both cases, such representations are unique. Sun conjectured that

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} b_p} = 1+\sqrt{2}$$

and

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 3 \text{ prime}\\ p\le x\\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1 \pmod 3 \text{ prime}\\ p\le x\\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} b_p} = 1+\sqrt{3}.$$

In Chapter 3, I will prove of some more generalized results, which confirm these two conjectures by Sun. Part of the work in this chapter has been submitted in [1].

Chapter 2

On Lemoine's Conjecture

2.1 Notation

Let f and g be arithmetic functions, where g is positive. We write

$$f = O(g),$$

or

$$f \ll g,$$

or

$$g \gg f,$$

if there exists a constant $c > 0$, such that

$$|f(x)| \leq cg(x)$$

for all x in the domain of f.

Given a constant U, we write

$$f = O_U(g)$$

if there exists a constant $c > 0$ that depends on U, such that

$$|f(x)| \leq cg(x)$$

for all x in the domain of f.

We write

$$f = o(g)$$

if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

We write

$$f \sim g,$$

if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

The Möbius function is defined by

$$\mu(n) = \begin{cases} (-1)^{\nu(n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\nu(n)$ is the number of distinct prime divisors of n.

2.2 Sieve Methods and Applications

Before stating the main results of this chapter, let me briefly introduce the sieve methods and give a short survey on the applications related to Goldbach's Conjecture and the twin prime conjecture.

A classical reference for sieve methods is the book by Halberstam and Richert [11]. In the book, the authors introduce the sieve of Eratosthenes, the combinatorial sieve, and Selberg's sieve. I will briefly write down some important theorems from the book, and mention their applications. For more details please see [11].

The oldest sieve method is attributed to Eratosthenes. The idea is quite simple, for example,

if we want to find all primes from 2 to 100, since any non-prime number up to 100 must have a prime divisor less than 11, we only need to cross off multiples of 2, 3, 5, and 7 from 11 to 100. Then the left over numbers, together with 2, 3, 5, and 7, are all of the primes up to 100. See Tables 2.1, 2.2, 2.3, and 2.4 for the process. Thus, we know all primes up to 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Table 2.1: Cross off Multiples of 2

11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

Table 2.2: Cross off Multiples of 3

11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Table 2.3: Cross off Multiples of 5

In order to introduce the main result on the Eratosthenes sieve, let me introduce some

11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Table 2.4: Cross off Multiples of 7

notation. Let

$$P_M(z) = \prod_{\substack{p<z \\ p\nmid M}} p,$$

and denote $P(z) = P_1(z)$. Let $\mathcal{A}$ be a finite set of integers, let $X \sim |\mathcal{A}|$, and let q be a positive integer that satisfies $(q, MP_M(x)) = 1$. Let

$$S_M(\mathcal{A}, q, z) = \{n : n \in \mathcal{A}, q \mid n, (n, P_M(z)) = 1\}$$

be the set of integers from $\mathcal{A}$ that are divisible by q and relatively prime to $P_M(z)$. When $q = 1$, we use $S_M(\mathcal{A}, z)$ to denote $S_M(\mathcal{A}, 1, z)$; when $M = 1$, we use $S(\mathcal{A}, q, z)$ to denote $S_1(\mathcal{A}, q, z)$; finally, $S(\mathcal{A}, z)$ means $S_1(\mathcal{A}, z)$. Sometimes we refer to $S_M(\mathcal{A}, q, z)$ as the cardinality of the set $S_M(\mathcal{A}, q, z)$ defined above; it should be clear from the context in which way we are using $S_M(\mathcal{A}, q, z)$. This notation will show up throughout the rest of this chapter, so let us look at an easy example:

Example 2.2.1. *When $\mathcal{A}$ is the set of integers from 1 to n, $M = 1$, $q = 1$, and $z = \sqrt{N}$, we see $S_M(\mathcal{A}, q, z) = S_1(\{1, \cdots, n\}, 1, \sqrt{n}) = S(\{1, \cdots, n\}, \sqrt{n})$ is the set of integers from 1 to n that are divisible by 1 and relatively primes to the product of all primes that are bigger or equal to 2 and less than $\sqrt{n}$. Therefore, it is the set of primes from $\sqrt{n}$ to n.*

For each prime p we choose $\omega(p)$ so that $(\omega(p)/p)X$ approximates to $|\mathcal{A}_p|$, where $\mathcal{A}_p = S_1(\mathcal{A}, p, 1)$, and we write the remainder as

$$R_p = |\mathcal{A}_p| - \frac{\omega(p)}{p}X.$$

For each square-free d, we define

$$\omega(1) = 1,\ \omega(d) = \prod_{p|d} \omega(p)$$

so that $\omega(d)$ is a multiplicative function. For each square-free d, let $\mathcal{A}_d = S_1(\mathcal{A}, d, 1)$, and we define

$$R_d = |\mathcal{A}_d| - \frac{\omega(d)}{d} X.$$

With the function ω we define

$$W(z) = \prod_{p<z} \left(1 - \frac{\omega(p)}{p}\right).$$

Then, we have the following theorem of the Eratosthenes-Legendre sieve:

Theorem 2.2.2 ([11, Eratosthenes-Legendre sieve, Theorem 1.1])**.** *We have*

$$S(\mathcal{A}, q, z) = \frac{\omega(q)}{q} XW(z) + \theta \sum_{d|P(x)} |R_{qd}|,$$

and, under some conditions, we have also that

$$S(\mathcal{A}, q, z) = XW(z) + \theta(1 + A_0)^z,$$

where $|\theta| \leq 1$ *and* A_0 *are constants.*

Since this is a short survey, I will not list the conditions here. One can read page 32 of [11] to see that Theorem 2.2.2 implies

$$\pi(x) \ll \frac{x}{\log \log x},$$

where $\pi(x)$ is the number of primes up to x.

Combinatorial sieves are largely attributed to Brun. In Chapter 2 of [11], the authors discuss Brun's pure sieve and Brun's sieve.

Theorem 2.2.3 ([11, Brun's pure sieve, Equation (2.16)])**.** *Under some conditions, we have*

$$S(\mathcal{A}, z) = XW(z)\left(1 + \theta e^{-\sqrt{\log X}}\right) + \theta' X^{\frac{1}{2}},$$

where $\log z \leq \sqrt{\log X}$, $|\theta| \leq 1$, $|\theta'| \leq 1$.

One can read page 51 of [11] to see that Theorem 2.2.3 implies the series

$$\sum_{\substack{p \text{ prime} \\ p+2=p' \text{ prime}}} \frac{1}{p}$$

is convergent.

Theorem 2.2.4 ([11, Brun's sieve, Theorem 2.1])**.** *Let b be a positive integer, and let λ be a real number satisfying*

$$0 < \lambda e^{1+\lambda} < 1.$$

Then, under some conditions, we have

$$S(\mathcal{A}, z) \leq XW(z)\left\{1 + 2\frac{\lambda^{2b+1}e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} e^{\frac{(2b+3)c_1}{\lambda \log z}}\right\} + O\left(z^{2b+\frac{2.01}{e^{2\lambda/\kappa}-1}}\right)$$

and

$$S(\mathcal{A}, z) \geq XW(z)\left\{1 - 2\frac{\lambda^{2b}e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}} e^{\frac{(2b+2)c_1}{\lambda \log z}}\right\} + O\left(z^{2b-1+\frac{2.01}{e^{2\lambda/\kappa}-1}}\right),$$

where

$$c_1 = \frac{A_2}{2}\left\{1 + A_1\left(\kappa + \frac{A_2}{\log 2}\right)\right\},$$

and κ, A_1, and A_2 are constants.

One can read pages 62 and 63 of [11] to see that Theorem 2.2.4 implies every sufficiently large even integer can be written as a sum of two numbers which both have at most 7 prime factors, and there are infinitely many numbers n such that both n and $n+2$ have at most 7 prime divisors. If we count the largest number of prime divisors of each summand in the decomposition, then Theorem 2.2.4 implies "$7+7$" for sufficiently large even integers and "$7-7$" for every even integer.

A modified version of Theorem 2.2.4 is the following theorem:

Theorem 2.2.5 ([11, Mordified Brun's sieve, Theorem 2.1′])**.** *Let b be a positive integer, and let λ and c_1 be constants satisfying the conditions in the previous theorem. Let*

$$u = \frac{\log X}{\log z}.$$

Then under some conditions we have

$$S(\mathcal{A},z) \leq XW(z)\Bigg\{1+2\frac{\lambda^{2b+1}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{\frac{(2b+3)c_1}{\lambda\log z}} + O\left(Lz^{-\alpha u+2b+\frac{2.01}{e^{2\lambda/\kappa}-1}}u^{C_0+1}\log^{C_0+\kappa+1}z\right)+O_U\left(u^{-\kappa}\log^{-U}X\right)\Bigg\}$$

and

$$S(\mathcal{A},z) \geq XW(z)\Bigg\{1-2\frac{\lambda^{2b}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{\frac{(2b+2)c_1}{\lambda\log z}} + O\left(Lz^{-\alpha u+2b-1+\frac{2.01}{e^{2\lambda/\kappa}-1}}u^{C_0+1}\log^{C_0+\kappa+1}z\right)+O_U\left(u^{-\kappa}\log^{-U}X\right)\Bigg\},$$

where κ, C_0, α, and U are constants.

One can read pages 66 and 67 of [11] to see that Theorem 2.2.5 implies every sufficiently large even integer can be written as a sum of a prime and a number having at most 7 prime divisors, and there are infinitely many primes p such that $p+2$ have at most 7 prime divisors, i.e., Theorem 2.2.5 implies "$1+7$" for sufficiently large even integers and "$1-7$" for every even integer.

Finally, Selberg's sieve, i.e., Theorem 2.5.2, is used to prove "$1+2$" and "$1-2$" in Chen's paper [5]. We will apply the same theorem to prove our main results, so Theorem 2.5.2 will be introduced later in Section 2.5.

A good reference for Goldbach's conjecture is the book by Wang [27], which is a collection of papers on the weak Goldbach conjecture and the strong Goldbach conjecture. In particular, one can read the third section of the book to see Rényi's paper on "$1+c$" [27, Pages 185-191], Wang's paper on "$1+3$" under the grand Riemann hypothesis [27, Pages 192-213], Pan's paper on "$1+5$" [27, Pages 214-226], Barban's paper on "$1+4$" [27, Pages 227-237], Buchstab and Vinogradov's papers on "$1+3$" [27, Pages 238-248], and Chen's paper on "$1+2$" [27, Pages 275-294].

2.3 Main Results

We say that a positive natural number is square-free if it is not divisible by the square of any prime. Estermann proved that every sufficiently large positive integer can be written as a sum of a prime and a square-free number in 1931 [10]. Dudek recently proved that every positive integer

greater than two can be written as a sum of a prime and a square-free number [9].

Chen proved in [4, 5] that every sufficiently large even integer can be represented as the sum of two primes or the sum of a prime and the product of two primes in 1966. Ross simplified Chen's proof in 1975 [23], and he pointed out that every sufficiently large even integer can be represented as the sum of a prime and a square-free number with at most two prime divisors.

In this thesis, we prove that every sufficiently large odd integer can be written as a sum of a prime and 2 times the product of at most two distinct odd primes. Together with Chen's theorem and Ross's work, we know that every sufficiently large integer can be written as a sum of a prime and a square-free number with at most three prime divisors. This answers the question at the end of the introduction of [9], for sufficiently large integers.

Goldbach's strong conjecture states that every even integer greater than 2 can be written as the sum of two primes. The analogous conjecture for odd numbers is Lemoine's conjecture, also known as the Levy's conjecture, which states that every odd integer greater than 5 can be written as a sum of a prime and twice a prime. Lemoine's conjecture has been verified up to 10^9 by Corbit [6]. One can easily see that Lemoine's conjecture implies Goldbach's weak conjecture. If we count the largest number of prime divisors of each term in the decomposition of even numbers, then Goldbach's strong conjecture can be denoted as "$1+1$", and Chen's theorem asserts "$1+2$", for sufficiently large even integers. For the decomposition of odd numbers, if we denote Lemoine's conjecture as "$1+2$", then we prove in this chapter that "$1+3$" is true for sufficiently large odd integers. See the table below that represents integers from 4 to 50 as the sum of a prime and a square-free number with at most two prime divisors.

			$4=2+2$	$5=3+2\times 1$
$6=3+3$	$7=5+2\times 1$	$8=3+5$	$9=7+2\times 1$	$10=3+7$
$11=5+2\times 3$	$12=5+7$	$13=3+2\times 5$	$14=3+11$	$15=13+2\times 1$
$16=3+13$	$17=3+2\times 7$	$18=5+13$	$19=5+2\times 7$	$20=3+17$
$21=11+2\times 5$	$22=3+19$	$23=13+2\times 5$	$24=5+19$	$25=3+2\times 11$
$26=3+23$	$27=5+2\times 11$	$28=5+23$	$29=3+2\times 13$	$30=7+23$
$31=5+2\times 13$	$32=3+29$	$33=7+2\times 13$	$34=3+31$	$35=13+2\times 11$
$36=5+31$	$37=3+2\times 17$	$38=7+31$	$39=5+2\times 17$	$40=3+37$
$41=3+2\times 19$	$42=5+37$	$43=5+2\times 19$	$44=3+41$	$45=5+2\times 19$
$46=3+43$	$47=37+2\times 5$	$48=5+43$	$49=3+2\times 23$	$50=3+47$

Table 2.5: "$1+2$" for Integers from 4 to 50

Moreover, Chen proved in [5] that every even integer can be represented as the difference

of a prime and a number with at most two prime divisors infinitely often. Similarly, we show that every odd integer can be written as the difference of a prime and a square-free number with at most three prime divisors infinitely often, one of which is 2. Therefore, every integer can be represented as the difference of a prime and a square-free number with at most three prime divisors.

It was conjectured by Polignac in 1849 that, for every even number N, there are infinitely many pairs of consecutive primes which differ by N. The analogous conjecture for odd integers should be the following: for every odd integer M, there are infinitely many pairs of primes (p, q) such that $p - 2q = M$. An easy application of [26, Exercise 3.3.2] shows that every odd integer can be represented as a prime minus the sum of two primes infinitely often, and this proposition will be an easy corollary if the analogous Polignac's conjecture holds. For even integers, if we denote Polignac's conjecture by "$1-1$", then Chen's theorem asserts "$1-2$". For odd integers, if we denote the analogous Polignac's conjecture by "$1-2$", then we prove "$1-3$" in this chapter. See the table below that represents integers from 1 to 50 as the difference of a prime and a square-free number with at most two prime divisors.

$1 = 7 - 2 \times 3$	$2 = 5 - 3$	$3 = 13 - 2 \times 5$	$4 = 7 - 3$	$5 = 11 - 2 \times 3$
$6 = 11 - 5$	$7 = 13 - 2 \times 3$	$8 = 11 - 3$	$9 = 19 - 2 \times 5$	$10 = 13 - 3$
$11 = 17 - 2 \times 3$	$12 = 17 - 5$	$13 = 19 - 2 \times 3$	$14 = 17 - 3$	$15 = 37 - 2 \times 11$
$16 = 19 - 3$	$17 = 23 - 2 \times 3$	$18 = 23 - 5$	$19 = 29 - 2 \times 5$	$20 = 23 - 3$
$21 = 31 - 2 \times 5$	$22 = 29 - 7$	$23 = 29 - 2 \times 3$	$24 = 29 - 5$	$25 = 31 - 2 \times 3$
$26 = 29 - 3$	$27 = 37 - 2 \times 5$	$28 = 31 - 3$	$29 = 43 - 2 \times 7$	$30 = 37 - 7$
$31 = 37 - 2 \times 3$	$32 = 37 - 5$	$33 = 43 - 2 \times 5$	$34 = 37 - 3$	$35 = 41 - 2 \times 3$
$36 = 41 - 5$	$37 = 43 - 2 \times 3$	$38 = 41 - 3$	$39 = 53 - 2 \times 7$	$40 = 47 - 7$
$41 = 47 - 2 \times 3$	$42 = 47 - 5$	$43 = 53 - 2 \times 5$	$44 = 47 - 3$	$45 = 59 - 2 \times 7$
$46 = 53 - 7$	$47 = 53 - 2 \times 3$	$48 = 53 - 5$	$49 = 59 - 2 \times 5$	$50 = 53 - 3$

Table 2.6: "$1-2$" for Integers from 1 to 50

Let M be a large odd integer, let N be a large integer and let h be any odd integer. Let $R(M)$ be the number of primes $p \leq M - 2$ for which $M - p$ is 2 times the product of at most two distinct odd primes. Let $r_h(N)$ be the number of primes $p \leq N$ for which $p - h$ is 2 times the product of at most two distinct odd primes. For any odd integer n, we write

$$\mathfrak{S}_n = \left(\prod_{p|n} \frac{p-1}{p-2} \right) \prod_{p>2} \frac{p(p-2)}{(p-1)^2}.$$

The main results of this chapter are the following two theorems:

Theorem 2.3.1. *For every sufficiently large odd integer M, we have*

$$R(M) \geq \frac{0.32M\mathfrak{S}_M}{(\log M)^2}.$$

Theorem 2.3.2. *For every sufficiently large integer N and an arbitrary odd integer h, we have*

$$r_h(N) \geq \frac{0.32N\mathfrak{S}_h}{(\log N)^2}.$$

We give a detailed proof of Theorem 2.3.1; Theorem 2.3.2 follows from the same method, and the following corollaries follow immediately:

Corollary 2.3.3. *Every sufficiently large integer can be written as a sum of a prime and a square-free number with at most three prime divisors.*

Corollary 2.3.4. *Every integer can be written as the difference of a prime and a square-free number with at most three prime divisors infinitely often.*

It is easy to see that Theorem 2.3.1 improves the following result by Wang:

Theorem 2.3.5 ([27, Theorem 3, Page 192])**.** *Under the truth of the following implication of the grand Riemann hypothesis:*

$$\pi(x;k,l) = \sum_{\substack{p\leq x \\ p\equiv l \pmod k}} 1 = \frac{li(x)}{\phi(k)} + O(x^{1/2}\log x),$$

where $(l,k)=1$ and $li(x) = \int_2^x \frac{dt}{\log t}$, we know every sufficiently large odd integer M can be represented as $M = p + 2P_3$, where p is a prime number and P_3 is an almost prime of not more than 3 prime prime divisors.

The main idea of the proof in the odd number case mimics the proof in [5]. For the decomposition of odd numbers, we make adjustments to the set we sieve from the even number case. To estimate the main terms, we still use the linear sieve from [11]. To bound the error terms, we use Bombieri's theorem [8, Chapter 24] and a theorem by Ding, Pan, and Wang [20, Theorem 2].

2.4 The Sets We Sieve

In this section, we consider the sets we sieve. Let

$$\mathcal{A} = \{(M-p)/2 : p \text{ is prime}, p < M, p \nmid M, M - p \equiv 2 \pmod 4\}$$

and

$$\mathcal{B} = \Big\{ M - 2p_1p_2p_3 : p_1, p_2, p_3 \text{ are all prime}, p_1p_2p_3 \le M/2, (p_1p_2p_3, M) = 1, \\ (M/2)^{1/10} \le p_1 \le (M/2)^{1/3} \le p_2 \le (M/(2p_1))^{1/2} \Big\}.$$

In the set $\mathcal{B}$, if $(M/2)^{1/10} \le p_3 \le (M/2)^{1/3}$ with $p_3 \ne p_1$ or $(M/2)^{1/3} \le p_3 \le (M/2p_1)^{1/2}$ with $p_3 \ne p_2$, then elements $M-2p_1p_2p_3$ and $M-2p_3p_2p_1$ or $M-2p_1p_2p_3$ and $M-2p_1p_3p_2$ are considered distinct. To ease notation, we let

$$I(M) = \left\{ p : p \text{ is prime}, (M/2)^{1/10} \le p \le (M/2)^{1/3}, p \nmid M \right\},$$

and for a prime $p_1 \in I(M)$, we let

$$I(M, p_1) = \left\{ p : p \text{ is prime}, (M/2)^{1/3} \le p \le (M/(2p_1))^{1/2}, p \nmid M \right\}.$$

With a straight forward argument, we have the following proposition, which gives a lower bound for $R(M)$ in terms of $S_M(\mathcal{A}, q, x)$ and $S_M(\mathcal{B}, q, x)$. An analogous result for the even numbers case is given in [5, (34)] and [23, (2.5)] without a proof. We include a proof here for the reader's convenience:

Proposition 2.4.1. *For some constants $B, C > 0$ and a sufficiently large odd integer M, we have*

$$R(M) \ge S_M(\mathcal{A}, (M/2)^{1/10}) - \frac{1}{2} \sum_{p \in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) \\ - \frac{1}{2} S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}) - CM^{9/10}. \tag{2.1}$$

Proof. Inequality (2.1) holds because

1. The number of prime divisors of M is $O(\log M)$, which is much less than the main term of $R(M)$ in Theorem 2.3.1. Thus, we can only count primes less than M that do not divide M.

2. We only count those $(M-p)/2 \in \mathcal{A}$ that are odd, whose odd prime divisors are all greater than $(M/2)^{1/10}$, i.e., we sieve from the set $S_M(\mathcal{A}, (M/2)^{1/10})$. With the lower bound on the odd prime divisors of $(M-p)/2$, for a prime $p < M$ such that $(M-p)/2 \in S_M(\mathcal{A}, (M/2)^{1/10})$, we know $(M-p)/2$ has at most 9 prime divisors with multiplicity.

3. From $S_M(\mathcal{A}, (M/2)^{1/10})$, we sieve those $(M-p)/2$ that are not square-free and those $(M-p)/2$ that are square-free with 3 or more prime divisors. This is why we subtract the last three terms. The term

$$\frac{1}{2}\sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10})$$

contains all $(M-p)/2 \in S_M(\mathcal{A}, p, (M/2)^{1/10})$ with two or more distinct prime divisors between $(M/2)^{1/10}$ and $(M/2)^{1/3}$. For those $(M-p)/2 \in S_M(\mathcal{A}, p, (M/2)^{1/10})$ with three or more distinct prime divisors but with only one prime divisor between $(M/2)^{1/10}$ and $(M/2)^{1/3}$, they are counted half of the time in the above summation. Since their other prime divisors are all greater than $(M/2)^{1/3}$, these $(M-p)/2$ have exactly three prime divisors, and the corresponding primes p are counted half of the time in $\frac{1}{2}S_M(\mathcal{B}, M^{1/2}(\log M)^{-B})$.

4. We claim that the number of integers of the form $(M-p)/2$ that are not square-free in

$$S_M(\mathcal{A}, (M/2)^{1/10}) - \frac{1}{2}\sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) - \frac{1}{2}S_M(\mathcal{B}, M^{1/2}(\log M)^{-B})$$

is $O(M^{9/10})$. This is true since if $(M-p)/2 \in S_M(\mathcal{A}, (M/2)^{1/10})$ is not square-free and it is not sieved from the second and the third term, by the argument above, it must has the form $(M-p)/2 = p_1^{n_1}$, $2 \le n_1 \le 9$, or $(M-p)/2 = p_1^{n_2}p_2$, $2 \le n_2 \le 6$, or $(M-p)/2 = p_1^{n_3}p_2^2$, $1 \le n_3 \le 3$, or $(M-p)/2 = p_1^{n_4}p_2p_3$, $2 \le n_4 \le 3$, where $(M/2)^{1/10} \le p_1 \le (M/2)^{1/3} \le p_2 < p_3$. Note that such integers are relatively rare, in fact, the total number is $O(M^{9/10})$ by the prime number theorem.

Therefore, Inequality (2.1) holds. □

2.5 Selberg's Sieve with Weight

In this section, we introduce Selberg's linear sieve theorem. Let $\mathcal{C}$ be a finite set of integers. Let $A_1, A_2, L \geq 1$ be constants. Let $\gamma(d)$ be a multiplicative function satisfying

$$0 \leq \gamma(p) \leq \left(1 - \frac{1}{A_1}\right)$$

if $p \nmid M$ and

$$-L \leq \sum_{v \leq p < \omega} \frac{\gamma(p)}{p} \log p - \log\left(\frac{\omega}{v}\right) \leq A_2$$

for any $2 \leq v \leq \omega$. Let μ be the Möbius function. For $\mu(n) \neq 0$ and $(n, M) = 1$, we choose $\gamma(n)$ and $X > 1$ so that the numbers

$$\eta(X, n) = \left| \sum_{\substack{a \in \mathcal{C} \\ a \equiv 0 \pmod{n}}} 1 - \frac{\gamma(n)}{n} X \right|$$

are in the nature of error terms, i.e., their sum should be small. For $z \geq 2$, we introduce the function

$$\Gamma_M(z) = \prod_{\substack{p < z \\ p \nmid M}} \left(1 - \frac{\gamma(p)}{p}\right).$$

We will make use of the following lemma and theorem in our proof:

Lemma 2.5.1 ([22, Lemma 2])**.** *We have*

$$\Gamma_M(z) = \frac{M}{\phi(M)} \prod_{p \nmid M} \frac{1 - \gamma(p)/p}{1 - 1/p} \frac{e^{-\gamma_0}}{\log z} \left\{1 + O\left(\frac{1}{\log z}\right)\right\} \tag{2.2}$$

for $\log M \leq z^{1/2}$*, where* ϕ *is the Euler's totient function and* γ_0 *is the Euler's constant.*

Theorem 2.5.2 ([11, Theorem 8.3])**.** *For* $z \ll \xi^{\lambda}$ *with a positive constant* λ *and* $X \sim |\mathcal{C}|$*, we have for some constant* B_1 *that depends on* A_1*,* A_2 *and some constant* $B(\lambda)$ *that depends on* A_1*,* A_2*, and* λ*, the following inequalities hold,*

$$S_M(\mathcal{C}, q, z) \leq \frac{\gamma(q)}{q} X \Gamma_M(z) \left\{F\left(\frac{\log(\xi^2)}{\log z}\right) + B(\lambda) \frac{L}{(\log \xi)^{1/14}}\right\} + \sum_{\substack{n \leq \xi^2 \\ n | P_M(z)}} 3^{\nu(n)} \eta(X, qn), \tag{2.3}$$

$$S_M(\mathcal{C},q,z) \geq \frac{\gamma(q)}{q} X\Gamma_M(z)\left\{f\left(\frac{\log(\xi^2)}{\log z}\right) - B_1\frac{L}{(\log\xi)^{1/14}}\right\} - \sum_{\substack{n\leq\xi^2\\ n|P_M(z)}} 3^{\nu(n)}\eta(X,qn), \tag{2.4}$$

where $\nu(n)$ is the number of distinct prime divisors of n. Here, the functions $F(u)$ and $f(u)$ can be defined by

$$F(u) = 2e^{\gamma_0}/u,\ f(u) = 0,\ 0 < u \leq 2,$$

$$(uF(u))' = f(u-1),\ (uf(u))' = F(u-1),\ u \geq 2.$$

2.6 First Two Terms

Now we consider the first two terms on the right hand side of (2.1), namely,

$$S_M(\mathcal{A},(M/2)^{1/10}) - \frac{1}{2}\sum_{p\in I(M)} S_M(\mathcal{A},p,(M/2)^{1/10}).$$

We put $\mathcal{C} = \mathcal{A}$, $\gamma(2) = 0$, $\gamma(p) = \frac{p}{p-1}$ for primes $p > 2$ and $z = (M/2)^{1/10}$. Then by (2.2), for any sufficiently large odd integer M, we have

$$\begin{aligned}
\Gamma_M(z) =& \frac{M}{\phi(M)}\prod_{p\nmid M}\frac{1-\gamma(p)/p}{1-1/p}\frac{e^{-\gamma_0}}{\log z}\left\{1+O\left(\frac{1}{\log z}\right)\right\}\\
=& \frac{M}{\phi(M)}\frac{1-0/2}{1-1/2}\prod_{2<p\nmid M}\frac{1-1/(p-1)}{1-1/p}\frac{e^{-\gamma_0}}{\log z}\left\{1+O\left(\frac{1}{\log z}\right)\right\}\\
=& \frac{20M}{\phi(M)}\prod_{2<p\nmid M}\frac{p(p-2)}{(p-1)^2}\frac{e^{-\gamma_0}}{\log(M/2)}\left\{1+O\left(\frac{1}{\log M}\right)\right\}\\
=& \frac{20e^{-\gamma_0}\mathfrak{S}_M}{\log M}\left\{1+O\left(\frac{1}{\log M}\right)\right\},
\end{aligned}$$

Note that the elements in $\mathcal{A}$ are in one-to-one correspondence with elements in the set

$$\mathcal{A}' = \{p:\ p \text{ is prime}, p < M, p\nmid M, M-p \equiv 2 \pmod 4\},$$

under the map $p \leftrightarrow \frac{M-p}{2}$, if we set $\pi(x;q,b)$ to be the number of primes less than x that are congruent to b modulo q, since the number of prime divisors of M is $O(\log M)$, we know that $|\mathcal{A}| = |\mathcal{A}'| \sim \frac{\pi(M;1,1)}{2} \sim \frac{M}{2\log M}$.

For the term $S_M(\mathcal{A}, (M/2)^{1/10})$, we put $q = 1$, $X = \frac{\pi(M;1,1)}{2} \sim |\mathcal{A}|$, $0 < \epsilon < 0.000001$, $\xi^2 = (M/2)^{1/2}(\log(M/2))^{-B'}$, where B' is a positive constant, and let M be sufficiently large such that

$$\begin{aligned}
&X\Gamma_M(z)\left\{f\left(\frac{\log(\xi^2)}{\log z}\right) - B_1\frac{L}{(\log\xi)^{1/14}}\right\}\\
=&X\Gamma_M(z)\left\{f\left(5 - \frac{10B'\log(\log(M/2))}{\log(M/2)}\right) - B_1\frac{L}{(\log\xi)^{1/14}}\right\}\\
\geq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1-\epsilon)}{(\log M)^2}f(5).
\end{aligned}$$

Then by (2.4) of Theorem 2.5.2, we have

$$S_M(\mathcal{A}, (M/2)^{1/10}) \geq \frac{10Me^{-\gamma_0}\mathfrak{S}_M(1-\epsilon)}{(\log M)^2}f(5) - E_1,$$

where

$$E_1 = \sum_{\substack{n\leq(M/2)^{1/2}(\log(M/2))^{-B'}\\ n|P_M(z)}} 3^{\nu(n)}\eta(X,n).$$

For the terms $S_M(\mathcal{A}, p, (M/2)^{1/10})$, where $p \in I(M)$, we put $q = p$, X and ϵ same as above, $\xi^2 = (M/2)^{1/2}(\log(M/2))^{-B''}/p$, where B'' is a positive constant, $\lambda = 2$ in $B(\lambda)$, and let M be sufficiently large such that

$$\begin{aligned}
&X\Gamma_M(z)\left\{F\left(\frac{\log(\xi^2)}{\log z}\right) + B(\lambda)\frac{L}{(\log\xi)^{1/14}}\right\}\\
=&X\Gamma_M(z)\left\{F\left(5 - \frac{10B''\log(\log(M/2))}{\log(M/2)} - \frac{10\log p}{\log(M/2)}\right) + B(\lambda)\frac{L}{(\log\xi)^{1/14}}\right\}\\
\leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+\epsilon)}{(\log M)^2}F\left(5 - \frac{10\log p}{\log(M/2)}\right).
\end{aligned}$$

Then by (2.3) of Theorem 2.5.2, we have

$$\begin{aligned}
S_M(\mathcal{A}, p, (M/2)^{1/10}) \leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+\epsilon)}{(\log M)^2}\frac{1}{p-1}F\left(5 - \frac{10\log p}{\log(M/2)}\right)\\
&+ \sum_{\substack{n\leq(M/2)^{1/2}(\log(M/2))^{-B''}/p\\ n|P_M(z)}} 3^{\nu(n)}\eta(X,pn).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&\sum_{p\in I(M)} S_M(\mathcal{A},p,(M/2)^{1/10})\\
\leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+\epsilon)}{(\log M)^2}\sum_{p\in I(M)}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)\\
&+\sum_{p\in I(M)}\sum_{\substack{n\leq(M/2)^{1/2}(\log(M/2))^{-B''}/p\\ n\mid P_M(z)}} 3^{\nu(n)}\eta(X,pn)\\
\leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+\epsilon)}{(\log M)^2}\sum_{p\in I(M)}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)+E_2,
\end{aligned}$$

where

$$E_2=\sum_{\substack{n\leq(M/2)^{1/2}(\log(M/2))^{-B''}\\ (n,M)=1}}\mu^2(n)3^{\nu(n)}\eta(X,n).$$

The $\mu^2(n)$ term is in E_2 since np is square-free for $p\in I(M)$ and $n\mid P_M(z)$.

Now, we look at the error terms E_1 and E_2. Recall that we take $X=\frac{\pi(M;1,1)}{2}$, $\gamma(2)=0$, and $\gamma(p)=\frac{p}{p-1}$ for primes $p>2$. When n is even, since all integers of the form $(M-p)/2\in\mathcal{A}$ are odd and $\gamma(n)=0$, we have

$$\eta(X,n)=\left|\sum_{\substack{a\in\mathcal{A}\\ a\equiv 0 \pmod n}}1-\frac{\gamma(n)}{n}X\right|=|0-0|=0.$$

Therefore, since $P_M(z)$ is square-free, we only need to count the $3^{\nu(n)}\eta(X,n)$ terms for odd square-free integers $n<(M/2)^{1/2}(\log(M/2))^{-B'}$ in E_1. Since $\mu(n)=0$ if n is not square-free, we also only need to count the $3^{\nu(n)}\eta(X,n)$ terms for odd square-free integers $n<(M/2)^{1/2}(\log(M/2))^{-B''}$ in E_2. For such an integer n, since $(M-p)/2\in\mathcal{A}$ and $n\mid(M-p)/2$ if and only if $p<M$ and $p\equiv M-2n \pmod{4n}$, we have $(M-2n,4n)=1$ and

$$\begin{aligned}
\eta(X,n)&=\left|\sum_{\substack{a\in\mathcal{A}\\ a\equiv 0 \pmod n}}1-\frac{\gamma(n)}{n}X\right|\\
&=\left|\pi(M;4n,M-2n)-\frac{X}{\phi(n)}\right|
\end{aligned}$$

$$= \left| \pi(M; 4n, M-2n) - \frac{\pi(M;1,1)}{2\phi(n)} \right|$$
$$= \left| \pi(M; 4n, M-2n) - \frac{\pi(M;1,1)}{\phi(4n)} \right|.$$

Now, we apply the following theorem of Bombieri to estimate the error terms E_1 and E_2:

Theorem 2.6.1 ([8, Chapter 24], [22, equation (4.18)]). *For any given positive $A_3 > 0$, there exists a positive constant B_2 such that*

$$\sum_{n \le Y^{1/2}(\log Y)^{-B_2}} \max_{y \le Y} \max_{(l,n)=1} \left| \pi(y; n, l) - \frac{\pi(y;1,1)}{\phi(n)} \right| \ll Y(\log Y)^{-A_3}.$$

Let $A_3 = 15$ and $Y = M$ in Theorem 2.6.1. Then, there exists a positive constant B_2 such that

$$\sum_{n \le M^{1/2}(\log M)^{-B_2}} \max_{y \le M} \max_{(l,n)=1} \left| \pi(y; n, l) - \frac{\pi(y;1,1)}{\phi(n)} \right| \ll M(\log M)^{-15}.$$

Therefore, if we choose $B' = B'' > B_2$ such that $4n \le M^{1/2}(\log M)^{-B_2}$ for all $n \le (M/2)^{1/2}(M/2)^{-B'}$, and let M be large enough, we have

$$\begin{aligned}
&\sum_{\substack{n \le (M/2)^{1/2}(\log(M/2))^{-B'} \\ n | P_M(z)}} \eta(X, n) \\
\le &\sum_{\substack{4n \le M^{1/2}(\log M)^{-B_2} \\ n | P_M(z)}} \left| \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0 \pmod{n}}} 1 - \frac{\gamma(n)}{n} X \right| \\
= &\sum_{\substack{4n \le M^{1/2}(\log M)^{-B_2} \\ n | P_M(z)}} \left| \pi(M, 4n, M-2n) - \frac{\pi(M;1,1)}{\phi(4n)} \right| \\
\ll &M(\log M)^{-15}. \qquad (2.5)
\end{aligned}$$

Similarly, we can obtain

$$\sum_{\substack{n \le (M/2)^{1/2}(\log(M/2))^{-B''} \\ (n,M)=1}} \mu^2(n)\eta(X, n) \ll M(\log M)^{-15}. \qquad (2.6)$$

Note that, trivially, for all $n \le (M/2)^{1/2}(\log(M/2))^{-B'} = (M/2)^{1/2}(\log(M/2))^{-B''}$, we have $\eta(X, n) \le$

$\left\lfloor \frac{M}{n} + 1 \right\rfloor < 2M/n$, which implies

$$\eta(X,n)^{1/2} \leq \sqrt{2M}/\sqrt{n},$$

i.e.,

$$\sqrt{n}\eta(X,n)^{1/2} \leq \sqrt{2}M^{1/2}. \tag{2.7}$$

We apply the following lemma from [22]:

Lemma 2.6.2 ([22, Lemma 3])**.** *For any real number $x \geq 1$ and for any natural number h we have*

$$\sum_{n \leq x} \frac{\mu^2(n)}{n} h^{\nu(n)} \leq (\log x + 1)^h.$$

Taking $h = 9$ and $x = (M/2)^{1/2}$ in Lemma 2.6.2, we obtain

$$\sum_{n \leq (M/2)^{1/2}} \frac{\mu^2(n)}{n} 9^{\nu(n)} \ll (\log((M/2)^{1/2} + 1))^9 \ll (\log M)^9. \tag{2.8}$$

Now, by Inequalities (2.5), (2.7), and (2.8), and the Cauchy-Schwarz inequality, we have

$$\begin{aligned}
E_1 = & \sum_{\substack{n \leq (M/2)^{1/2} (\log(M/2))^{-B'} \\ n | P_M(z)}} 3^{\nu(n)} \eta(X,n) \\
= & \sum_{\substack{n \leq (M/2)^{1/2} (\log(M/2))^{-B'} \\ n | P_M(z)}} \frac{3^{\nu(n)}}{\sqrt{n}} \times \sqrt{n}\eta^{1/2}(X,n) \times \eta^{1/2}(X,n) \\
\leq & \sqrt{2}M^{1/2} \sum_{\substack{n \leq (M/2)^{1/2} (\log(M/2))^{-B'} \\ n | P_M(z)}} \frac{3^{\nu(n)}}{\sqrt{n}} \times \eta^{1/2}(X,n) \\
\leq & \sqrt{2}M^{1/2} \sqrt{\sum_{\substack{n \leq (M/2)^{1/2} (\log(M/2))^{-B'} \\ n | P_M(z)}} \left(\frac{3^{\nu(n)}}{\sqrt{n}} \right)^2 \times \sum_{\substack{n \leq (M/2)^{1/2} (\log(M/2))^{-B'} \\ n | P_M(z)}} \eta(X,n)} \\
\ll & M^{1/2} \sqrt{(\log M)^9 \times M(\log M)^{-15}} \\
\ll & M(\log M)^{-3}.
\end{aligned}$$

Similarly, by Inequalities (2.6), (2.7), and (2.8), and the Cauchy-Schwarz inequality, we have

$$E_2 \ll M(\log M)^{-3}.$$

Therefore, we can choose large enough M so that

$$S_M(\mathcal{A}, (M/2)^{1/10}) \geq \frac{10Me^{-\gamma_0}\mathfrak{S}_M(1-2\epsilon)}{(\log M)^2} f(5)$$

and

$$\sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) \leq \frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+2\epsilon)}{(\log M)^2} \sum_{p\in I(M)} \frac{1}{p-1} F\left(5 - \frac{10\log p}{\log(M/2)}\right).$$

Next, we estimate the main terms. By the definition of $f(u)$ and $F(u)$, we know [5, Page 173]

$$f(u) = \frac{\int_2^u F(t-1)dt}{u} = \frac{2e^{\gamma_0}\log(u-1)}{u},\ 2 \leq u \leq 4,$$

$$5f(5) = 2e^{\gamma_0}\left(\log 4 + \int_3^4 \frac{du}{u}\int_2^{u-1} \frac{\log(t-1)}{t}dt\right) \geq 2e^{\gamma_0}(\log 4 + 0.0148),$$

$$F(u) = \frac{2e_0^{\gamma}}{u},\ 0 < u \leq 3,$$

and

$$F(u) = \frac{2e^{\gamma_0} + \int_3^u f(t-1)dt}{u} = \frac{2e^{\gamma_0}\left(1 + \int_2^{u-1} \frac{\log(t-1)}{t}dt\right)}{u},\ 3 \leq u \leq 4.$$

Therefore, for any sufficiently large odd integer M, we have

$$S_M(\mathcal{A}, (M/2)^{1/10}) \geq \frac{4M\mathfrak{S}_M(1-2\epsilon)}{(\log M)^2}(\log 4 + 0.0148) \geq \frac{5.6043M\mathfrak{S}_M(1-2\epsilon)}{(\log M)^2}.$$

Moreover, we split the interval $\left[(M/2)^{1/10}, (M/2)^{1/3}\right]$ into two subintervals I_1 and I_2 due to the behavior of $F(u)$, where

$$I_1 = \left[(M/2)^{1/10}, (M/2)^{1/5}\right]$$

and

$$I_2 = \left[(M/2)^{1/5}, (M/2)^{1/3}\right].$$

Thus,

$$\begin{aligned}
&\sum_{p\in I(M)} S_M(\mathcal{A},p,(M/2)^{1/10})\\
\leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+2\epsilon)}{(\log M)^2}\sum_{p\in I(M)}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)\\
\leq&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+2\epsilon)}{(\log M)^2}\left(\sum_{p\in I_1}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)+\sum_{p\in I_2}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)\right).
\end{aligned}$$

For a prime $p\in I_1$, we have $3\leq 5-\frac{10\log p}{\log(M/2)}\leq 4$. Therefore,

$$\begin{aligned}
&\sum_{p\in I_1}\frac{1}{p-1}F\left(5-\frac{10\log p}{\log(M/2)}\right)\\
=&\sum_{p\in I_1}\frac{2e^{\gamma_0}}{(p-1)\left(5-\frac{10\log p}{\log(M/2)}\right)}\times\left(1+\int_2^{4-\frac{10\log p}{\log(M/2)}}\frac{\log(t-1)}{t}dt\right)\\
\leq&\frac{e^{\gamma_0}\log(M/2)(1+\epsilon)}{5}\int_{(M/2)^{1/10}}^{(M/2)^{1/5}}\frac{ds}{(s-1)\log s(1/2\times\log(M/2)-\log s)}\\
&\qquad\times\left(1+\int_2^{4-\frac{10\log s}{\log(M/2)}}\frac{\log(t-1)}{t}dt\right).
\end{aligned}$$

Taking $\alpha=\frac{\log s}{\log(M/2)}$, we know $s=(M/2)^\alpha$, $\log s=\log(M/2)\times\alpha$, and $ds=\log(M/2)\times s\,d\alpha=\log(M/2)\times(M/2)^\alpha\,d\alpha$. Therefore, for sufficiently large M, we have

$$\begin{aligned}
&\frac{e^{\gamma_0}\log(M/2)(1+\epsilon)}{5}\int_{(M/2)^{1/10}}^{(M/2)^{1/5}}\frac{ds}{(s-1)\log s(1/2\times\log(M/2)-\log s)}\\
&\qquad\times\left(1+\int_2^{4-\frac{10\log s}{\log(M/2)}}\frac{\log(t-1)}{t}dt\right)\\
=&\frac{e^{\gamma_0}(1+\epsilon)}{5}\int_{1/10}^{1/5}\frac{(M/2)^\alpha}{(M/2)^\alpha-1}\times\frac{d\alpha}{\alpha(1/2-\alpha)}\times\left(1+\int_2^{4-10\alpha}\frac{\log(t-1)}{t}dt\right)\\
\leq&\frac{e^{\gamma_0}(1+2\epsilon)}{5}\left(\int_{1/10}^{1/5}\frac{d\alpha}{\alpha(1/2-\alpha)}+\int_{1/10}^{1/5}\frac{d\alpha}{\alpha(1/2-\alpha)}\times\int_2^{4-10\alpha}\frac{\log(t-1)}{t}dt\right).
\end{aligned}$$

For a prime $p \in I_2$, we have $5/3 \le 5 - \frac{10\log p}{\log(M/2)} \le 3$. Therefore,

$$\begin{aligned}
&\sum_{p\in I_2} \frac{1}{p-1} F\left(5 - \frac{10\log p}{\log(M/2)}\right) \\
=&\sum_{p\in I_2} \frac{2e^{\gamma_0}}{(p-1)\left(5 - \frac{10\log p}{\log(M/2)}\right)} \\
\le&\frac{e^{\gamma_0}\log(M/2)(1+\epsilon)}{5} \int_{(M/2)^{1/5}}^{(M/2)^{1/3}} \frac{ds}{(s-1)\log s(1/2\times\log(M/2) - \log s)} \\
=&\frac{e^{\gamma_0}(1+\epsilon)}{5} \int_{1/10}^{1/5} \frac{(M/2)^{\alpha}}{(M/2)^{\alpha}-1} \times \frac{d\alpha}{\alpha(1/2-\alpha)} \\
\le&\frac{e^{\gamma_0}(1+2\epsilon)}{5} \int_{1/5}^{1/3} \frac{d\alpha}{\alpha(1/2-\alpha)}.
\end{aligned}$$

We combine them together and obtain

$$\begin{aligned}
&\sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) \\
\le&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+2\epsilon)}{(\log M)^2} \sum_{p\in I(M)} \frac{1}{p-1} F\left(5 - \frac{10\log p}{\log(M/2)}\right) \\
\le&\frac{10Me^{-\gamma_0}\mathfrak{S}_M(1+2\epsilon)}{(\log M)^2} \left(\sum_{p\in I_1} \frac{1}{p-1} F\left(5 - \frac{10\log p}{\log(M/2)}\right) + \sum_{p\in I_2} \frac{1}{p-1} F\left(5 - \frac{10\log p}{\log(M/2)}\right)\right) \\
\le&\frac{2M\mathfrak{S}_M(1+2\epsilon)^2}{(\log M)^2} \left(\int_{1/10}^{1/3} \frac{d\alpha}{\alpha(1/2-\alpha)} + \int_{1/10}^{1/5} \frac{d\alpha}{\alpha(1/2-\alpha)} \times \int_2^{4-10\alpha} \frac{\log(t-1)}{t} dt\right) \\
\le&\frac{2M\mathfrak{S}_M(1+5\epsilon)}{(\log M)^2} \left(\int_{1/10}^{1/3} \frac{d\alpha}{\alpha(1/2-\alpha)} + \int_{1/10}^{1/5} \frac{d\alpha}{\alpha(1/2-\alpha)} \times \int_2^{4-10\alpha} \frac{\log(t-1)}{t} dt\right) \\
\le&\frac{2M\mathfrak{S}_M(1+5\epsilon)}{(\log M)^2} (4.1589 + 0.1191) \\
\le&\frac{8.556M\mathfrak{S}_M(1+5\epsilon)}{(\log M)^2}.
\end{aligned}$$

Since ϵ is chosen to be small enough, we have

$$S_M(\mathcal{A}, (M/2)^{1/10}) - \frac{1}{2} \sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) \ge \frac{(1.3263 - 33\epsilon)M\mathfrak{S}_M}{(\log M)^2} \ge \frac{1.326M\mathfrak{S}_M}{(\log M)^2}. \quad (2.9)$$

2.7 The Third Term

Now, we consider the third term on the right hand side of (2.1), namely,

$$S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}).$$

We substitute $\mathcal{C} = \mathcal{B}$, $\gamma(2) = 0$, $\gamma(p) = \frac{p}{p-1}$ for primes $p > 2$, and $z = (M/2)^{1/2}$ in Lemma 2.5.1. For any sufficiently large odd integer M we have

$$\Gamma_M(z) = \frac{4e^{-\gamma_0}\mathfrak{S}_M}{\log M}\left\{1 + O\left(\frac{1}{\log M}\right)\right\}.$$

Let $X = |\mathcal{B}'|$, where

$$\mathcal{B}' = \{(p_1, p_2, p_3) : p_1, p_2, p_3 \text{ are all prime}, p_1p_2p_3 \le M/2, p_1 \in I(M), p_2 \in I(M, p_1)\}.$$

It is easy to see $|\mathcal{B}| \sim |\mathcal{B}'|$ since the only difference of the restrictions on p_3 in $\mathcal{B}$ and $\mathcal{B}'$ is whether p_3 could be a prime divisor of M or not, and the number of prime divisors of M is $O(\log M)$. We put $q = 1$, $\xi^2 = M^{1/2}(\log M)^{-B}$ where B is a positive constant, and $\lambda = 1$ in $B(\lambda)$ in Inequality (2.3) of Theorem 2.5.2. Then, for any sufficiently large odd integer M, we have

$$\begin{aligned} S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}) \le& \frac{8\mathfrak{S}_M X}{\log M}\left\{1 + B(\lambda)\frac{L}{(\log(M^{1/2}(\log M)^{-B}))^{1/14}}\right\} + E_3 \\ \le& \frac{8\mathfrak{S}_M X(1+\epsilon)}{\log M} + E_3, \end{aligned}$$

where

$$E_3 = \sum_{\substack{n \le M^{1/2}(\log M)^{-B} \\ n | P_M(z)}} 3^{\nu(n)}\eta(X, n).$$

Next, we estimate $X = |\mathcal{B}'|$. By the definitions of $\mathcal{B}$ and $\mathcal{B}'$, we can apply the prime number theorem and estimate X analogously to [23, Inequalities (3.9) and (3.10)],

$$\begin{aligned} X \le& (1+\epsilon)\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{\log u}\int_{(M/2)^{1/3}}^{(M/2u)^{1/2}} \frac{M/(2uv)}{\log(M/(2uv))} \times \frac{dv}{\log v} \\ =& (1+\epsilon)(M/2)\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u}\int_{(M/2)^{1/3}}^{(M/2u)^{1/2}} \frac{dv}{v(\log v)\log(M/(2uv))}. \end{aligned}$$

To deal with the double integral, we substitute $t = \log v$ and $w = \frac{\log u}{\log(M/2)}$ to obtain the integral with variable w:

$$\begin{aligned}
&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u} \int_{(M/2)^{1/3}}^{(M/2u)^{1/2}} \frac{dv}{v(\log v)\log(M/(2uv))} \\
=&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u} \int_{\frac{\log(M/2)}{3}}^{\frac{\log(M/2u)}{2}} \frac{dt}{t(\log(M/2u)-t)} \\
=&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u} \int_{\frac{\log(M/2)}{3}}^{\frac{\log(M/2u)}{2}} \frac{1}{\log(M/2u)}\left(\frac{1}{\log(M/2u)-t}+\frac{1}{t}\right)dt \\
=&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u\log(M/2u)} \times \left((-\log(\log(M/2u)-t)+\log t)\Big|_{\frac{\log(M/2)}{3}}^{\frac{\log(M/2u)}{2}}\right) \\
=&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u\log(M/2u)} \times \left(\log\left(\log(M/2u)-\frac{\log(M/2)}{3}\right)-\log\left(\frac{\log(M/2)}{3}\right)\right) \\
=&\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u\log(M/2u)} \times \log\left(\frac{3\log(M/2u)}{\log(M/2)}-1\right) \\
=&\int_{1/10}^{1/3} \frac{\log(M/2)dw}{\log(M/2)w\times\log(M/2)(1-w)} \times \log\left(3(1-w)-1\right) \\
=&\frac{1}{\log(M/2)}\int_{1/10}^{1/3}\frac{\log(2-3w)}{w(1-w)}dw.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
X \leq&(1+\epsilon)(M/2)\int_{(M/2)^{1/10}}^{(M/2)^{1/3}} \frac{du}{u\log u} \int_{(M/2)^{1/3}}^{(M/2u)^{1/2}} \frac{dv}{v(\log v)\log(M/(2uv))} \\
=&(1+\epsilon)\frac{M/2}{\log(M/2)}\int_{1/10}^{1/3}\frac{\log(2-3w)}{w(1-w)}dw \\
\leq&(1+2\epsilon)\frac{M/2}{\log M}\times 0.5024.
\end{aligned}$$

Therefore, for any sufficiently large odd integer M we have

$$S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}) < \frac{2.0096M\mathfrak{S}_M(1+\epsilon)(1+2\epsilon)}{(\log M)^2} + E_3.$$

Finally, we look at the error term E_3. If n is even, we note that all numbers of the form

$M - 2p_1p_2p_3 \in \mathcal{B}$ are odd and $\gamma(n) = 0$, so we have

$$\eta(X,n) = \left| \sum_{\substack{a \in \mathcal{B} \\ a \equiv 0 \pmod{n}}} 1 - \frac{\gamma(d)}{d} X \right| = |0 - 0| = 0.$$

Since $P_M(z)$ is square-free, we only need to count the $3^{\nu(n)}\eta(X,n)$ terms for odd square-free integers $n \le M^{1/2}(\log M)^{-B}$ in E_3. For such an integer n, by the definition of $\gamma(n)$, we have

$$\eta(X,n) = \left| \sum_{\substack{a \in \mathcal{B} \\ a \equiv 0 \pmod{n}}} 1 - \frac{\gamma(n)}{n} X \right| = \left| \sum_{\substack{a \in \mathcal{B} \\ a \equiv 0 \pmod{n}}} 1 - \frac{X}{\phi(n)} \right|.$$

Now, we apply the following theorem by Ding, Pan, and Wang to bound the error term E_3:

Theorem 2.7.1 ([27, Theorem 3, Page 295], [20, Theorem 2])**.** *Let*

$$\pi(Y; a, n, l) = \sum_{\substack{ap \le Y \\ ap \equiv l \pmod{n}}} 1$$

and let $f(a)$ be a real function with $f(a) \ll 1$. For any given $A_4 > 0$, we have

$$\sum_{n \le Y^{1/2}(\log Y)^{-B_3}} \max_{y \le Y} \max_{(l,n)=1} \left| \sum_{\substack{a \le Y^{1-\delta} \\ (a,n)=1}} f(a) \left(\pi(y; a, n, l) - \frac{\pi(y; a, 1, 1)}{\phi(n)} \right) \right| \ll Y(\log Y)^{-A_4},$$

where $B_3 = 3A_4/2 + 17$ and $0 < \delta < 1$.

Let $A_4 = 15$, $Y = M$, and let $\delta < 1/6$ so that $2p_1p_2 \le M^{1-\delta}$ for all $p_1 \in I(M)$ and $p_2 \in I(M, p_1)$. Let

$$f(a) = \begin{cases} 1 & \text{if } a = 2p_1p_2,\ p_1 \in I(M), p_2 \in I(M, p_1), \\ 0 & \text{otherwise.} \end{cases}$$

Then all conditions of Theorem 2.7.1 are satisfied.

Note that, when $n \mid P_M(z)$, $p_1p_2 \mid P_M(z)$, and $2p_1p_2p \equiv M \pmod{n}$, we have $(n, M) = 1$

and $(2p_1p_2, n) = 1$. By the definition of X, $\mathcal{B}'$, and $\eta(X, n)$, we see

$$\begin{aligned}\eta(X,n) &= \left| \sum_{\substack{a\in\mathcal{B}\\ a\equiv 0 \pmod n}} 1 - \frac{X}{\phi(n)} \right| \\ &= \left| \sum_{\substack{p_1\in I(M)\\ p_2\in I(M,p_1)}} \left(\pi(M; 2p_1p_2, n, M) - \frac{\pi(M; 2p_1p_2, 1, 1)}{\phi(n)} \right) \right|.\end{aligned}$$

Therefore,

$$\begin{aligned}\eta(X,n) &\le \max_{y\le M} \left| \sum\nolimits_{p_2\in I(M,p_1)}^{p_1\in I(M)} \left(\pi(y; 2p_1p_2, n, M) - \frac{\pi(y; 2p_1p_2, 1, 1)}{\phi(n)} \right) \right| \\ &\le \max_{y\le M} \max_{(l,n)=1} \left| \sum_{\substack{p_1\in I(M)\\ p_2\in I(M,p_1)\\ (2p_1p_2,n)=1}} \left(\pi(y; 2p_1p_2, n, l) - \frac{\pi(y; 2p_1p_2, 1, 1)}{\phi(n)} \right) \right|.\end{aligned}$$

Therefore, we can take $B > B_3 = 45/2 + 7$ so that

$$\begin{aligned}\sum_{\substack{n\le M^{1/2}(\log M)^{-B}\\ n|P_M(z)}} \eta(X,n) &= \sum_{\substack{n\le M^{1/2}(\log M)^{-B}\\ n|P_M(z),\, n \text{ is odd}}} \eta(X,n) \\ &\le \sum_{\substack{n\le M^{1/2}(\log M)^{-B}\\ n|P_M(z), n \text{ is odd}}} \max_{y\le M} \max_{(n,l)=1} \left| \sum_{\substack{p_1\in I(M)\\ p_2\in I(M,p_1)\\ (2p_1p_2,n)=1}} \left(\pi(y; 2p_1p_2, n, l) - \frac{\pi(y; 2p_1p_2, 1, 1)}{\phi(n)} \right) \right| \\ &\le \sum_{n\le M^{1/2}(\log M)^{-B_3}} \max_{y\le M} \max_{(n,l)=1} \left| \sum_{\substack{a\le M^{1-\delta}\\ (a,n)=1}} f(a) \left(\pi(y; a, n, l) - \frac{\pi(y; a, 1, 1)}{\phi(n)} \right) \right| \\ &\ll M(\log M)^{-15}. \end{aligned} \tag{2.10}$$

In this case, we also, trivially, have $\eta(X, n) \le \left\lfloor \frac{M}{n} + 1 \right\rfloor < 2M/n$ for all $n \le M^{1/2}(\log M)^{-B}$. Then,

$$\eta(X,n)^{1/2} \le \sqrt{2M}/\sqrt{n},$$

i.e.,

$$\sqrt{n}\eta(X,n)^{1/2} \leq \sqrt{2}M^{1/2}. \tag{2.11}$$

Taking $h = 9$ and $x = M^{1/2}$ in Lemma 2.6.2, we obtain

$$\sum_{n\leq M^{1/2}} \frac{\mu^2(n)}{n} 9^{\nu(n)} \ll (\log(M^{1/2})+1)^9 \ll (\log M)^9. \tag{2.12}$$

By Inequalities (2.10), (2.11), and (2.12), and the Cauchy-Schwarz inequality, we have

$$E_3 \ll M(\log M)^{-3}.$$

Therefore, for any sufficiently large odd integer M we have

$$S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}) \leq \frac{2.0096M\mathfrak{S}_M(1+\epsilon)(1+2\epsilon)}{(\log M)^2} + E_3 \leq \frac{2.01M\mathfrak{S}_M}{(\log M)^2}. \tag{2.13}$$

2.8 Main Results

Now we perform some easy calculation and prove our main theorems. By Inequalities (2.1), (2.9), and (2.13), for any sufficiently large odd integer M, we have

$$\begin{aligned} R(M) \geq & S_M(\mathcal{A}, (M/2)^{1/10}) - \frac{1}{2}\sum_{p\in I(M)} S_M(\mathcal{A}, p, (M/2)^{1/10}) \\ & - \frac{1}{2}S_M(\mathcal{B}, M^{1/2}(\log M)^{-B}) - CM^{9/10} \\ \geq & \frac{1.326M\mathfrak{S}_M}{(\log M)^2} - \frac{1}{2}\frac{2.01M\mathfrak{S}_M}{(\log M)^2} - CM^{9/10} \\ \geq & \frac{0.32M\mathfrak{S}_M}{(\log M)^2}. \end{aligned}$$

This completes the proof of Theorem 2.3.1.

By the same method used in estimating $R(M)$, instead of considering

$$\mathcal{A} = \{(M-p)/2 : p \text{ is prime}, p < M, p \nmid M, M - p \equiv 2 \pmod 4\}$$

and

$$\mathcal{B}=\Big\{M-2p_1p_2p_3:\ p_1,p_2,p_3 \text{ are all prime}, p_1p_2p_3\le M/2, (p_1p_2p_3,M)=1,\\ (M/2)^{1/10}\le p_1\le (M/2)^{1/3}\le p_2\le (M/(2p_1))^{1/2}\Big\},$$

for a sufficiently large integer N, we consider

$$\mathcal{A}_h=\{(p-h)/2:\ p \text{ is prime}, p<N, p\nmid h, p-h\equiv 2 \pmod 4\}$$

and

$$\mathcal{B}_h=\Big\{h+2p_1p_2p_3:\ p_1,p_2,p_3 \text{ are all prime}, p_1p_2p_3\le (N-h)/2, (p_1p_2p_3,h)=1,\\ (N/2)^{1/10}\le p_1\le (N/2)^{1/3}\le p_2\le (N/(2p_1))^{1/2}\Big\}.$$

We define

$$I_h(N)=\left\{p:\ p \text{ is prime}, (N/2)^{1/10}\le p\le (N/2)^{1/3},\ p\nmid h\right\}.$$

The same argument shows that

$$\begin{aligned} r_h(N)\ge& S_h(\mathcal{A}_h,(N/2)^{1/10})-\frac{1}{2}\sum_{p\in I_h(N)}S_h(\mathcal{A}_h,p,(N/2)^{1/10})\\ &-\frac{1}{2}S_h(\mathcal{B}_h,N^{1/2}(\log N)^{-B})-CN^{9/10}\\ \ge&\frac{1.326N\mathfrak{S}_h}{(\log N)^2}-\frac{1}{2}\frac{2.01N\mathfrak{S}_h}{(\log N)^2}-CN^{9/10}\\ \ge&\frac{0.32N\mathfrak{S}_h}{(\log N)^2}, \end{aligned}$$

and Theorem 2.3.2 follows.

Corollaries 2.3.3 and 2.3.4 are obvious.

2.9 Future Projects

In the past 50 years, there have been a lot of improvements on Chen's theorem. For example, in 2008 Cai improved the constant 0.67 in Chen's theorem in [2]. In 2015 Chen's theorem with a

small prime in the representation was proved by Cai in [3]. Also in 2015 the explicit Chen's theorem was proved by Yamada in [28] that every even integer greater than $e^{e^{36}}$ is a sum of a prime and an almost prime with at most two prime divisors.

Since Chen's theorem deals with large even integers and Theorem 2.3.1 deals with large odd integers, we can try to make the constant 0.32 in Theorem 2.3.1 larger, try to prove the representation exists with a small prime, and try to make Theorem 2.3.1 explicit.

An upper bound on the exceptional set of Goldbach numbers is given in [16]. Thus, we can look at the exceptional set of "Lemoine numbers", i.e., the odd integers that are not the sum of a prime and twice a prime.

Furthermore, we can try to combine Chen's theorem and Theorem 2.3.1 to obtain a more general result. Instead of looking at numbers represented by $p \pm q$ or $p \pm qr$ and $p \pm 2q$ or $p \pm 2qr$, we can look at numbers represented by $ap \pm bq$ or $ap \pm bqr$ for integers a and b, and prime numbers p, q, and r. Moreover, we can try to obtain similar types of results as presented above on such linear combinations.

In the twin primes conjectures setting, by Theorem 2.3.2 we know $p - 2q$ or $p - 2qr$ is bounded infinitely often by 1. Inspired by the recent breakthrough on the bounded gaps between primes, we can try to bound $p - 2q$ infinitely often, where p, q, and r are prime numbers.

Primes of the form $2p + 1$ are called safe primes. We can try to prove there are infinitely many safe primes. Primes that are 6 apart are called sexy primes, which may give us a pair of "safe sexy primes" that are 12 apart. We can try to prove there are infinitely many pairs of safe sexy primes.

Chapter 3

On Some Conjectures by Sun

In [24], Sun stated the following conjectures: we have

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} b_p} = 1+\sqrt{2},$$

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} a_p^2}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} b_p^2} = 4.5,$$

and

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\le x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\le x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} b_p} = 1+\sqrt{3}.$$

In this chapter, we prove some results that verify his first and third conjecture, and prove a modified version of the second conjecture.

The structure of this chapter is as follows. In Section 3.1, we discuss primes in arithmetic

progressions that are represented by quadratic forms. In Section 3.2, we state our main results. In Section 3.3, we prove the main theorems. We discuss future work in Section 3.4.

3.1 Representations of Primes in Arithmetic Progressions by Quadratic Forms

3.1.1 Fermat's theorem on sums of two squares

Fermat's theorem on sums of two squares states that an odd prime p can be written as a sum of two integer squares if and only if $p \equiv 1 \pmod 4$. Fermat described his observation in a letter to Mersenne dated December 25, 1640, so this theorem is also known as the Fermat's Christmas Theorem. This is the first theorem on representing primes in arithmetic progressions by quadratic forms. We will discuss other theorems of the same flavor later in this section.

There are many interesting proofs of Fermat's theorem on sums of two squares. One direction is easy, i.e., if an odd prime is a sum of two squares, then it is congruent to 1 modulo 4. For the other direction, Euler's proof in 1749 used infinite descent. We can briefly describe his proof in the following 5 steps:

1. Show that the product of two numbers, each of which is a sum of two squares, is itself a sum of two squares, i.e.,
$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2.$$

2. Show that if a number which is a sum of two squares is divisible by a prime which is a sum of two squares, then the quotient is a sum of two squares, i.e.,
$$\frac{a^2 + b^2}{p^2 + q^2} = \left(\frac{ap + bq}{p^2 + q^2}\right)^2 + \left(\frac{aq - bp}{p^2 + q^2}\right)^2.$$

3. Suppose $a^2 + b^2$ is divisible by x which is not a sum of two squares, then show their quotient $\frac{a^2+b^2}{x} = p_1 p_2 \cdots p_n$ has a prime divisor p_i that is not a sum of two squares. This follows from the previous two steps.

4. Show that if a and b are relatively prime, then every factor of $a^2 + b^2$ is a sum of two squares.

Suppose $x \mid a^2 + b^2$ is not a sum of two squares, then we can write

$$a = mx \pm c, b = nx \pm d, |c| \leq x/2, |d| \leq x/2, (c, d, x) = 1,$$

where c and d are at most half of x in absolute value. Then we have

$$a^2 + b^2 = m^2x^2 \pm 2mxc + c^2 + n^2x^2 \pm 2nxd + d^2 = Ax + (c^2 + d^2).$$

Therefore, x divides $c^2 + d^2$, say $c^2 + d^2 = xy$. Let g be the greatest common divisor of c and d, $c = ge$, and $d = gf$, for some $e, f \in \mathbb{Z}$. Then we can easily show g and x are relatively prime, and thus $g^2 \mid y$. Let $y = g^2z$, then

$$e^2 + f^2 = zx \leq c^2 + d^2 \leq x^2/2,$$

where $(e, f) = 1$ and $z \leq x/2$. If x is not the sum of two squares, by Step 3, there exists a factor of z that is not a sum of two squares. Since $\omega \mid z$, we have $\omega < x$, both not the sum of of two squares. Since an infinite descent is impossible, we complete the proof of Step 4.

5. Complete the proof. For $1 \leq a \leq 4n - 1$, by Fermat's Little Theorem we have

$$p \mid (a+1)^{4n} - a^{4n} = \left((a+1)^{2n} + a^{2n}\right)\left((a+1)^{2n} - a^{2n}\right).$$

Since $a + 1$ and a are relatively prime, by Step 4, we know p itself is a sum of two squares. If $p \mid \left((a+1)^{2n} - a^{2n}\right)$ for all $1 \leq a \leq 4n - 1$, then it would divide all $4n - 2$ differences of successive terms, all $4n - 3$ differences of the differences, and so force, which implies $p \mid (2n)!$, which is a contradiction. This completes the proof.

Zagier gave a beautiful one-sentence proof of Fermat's theorem on sums of two squares. If $p = 4n+1$ is prime, then the set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ is finite and has two involutions: an obvious one $(x, y, z) \to (x, z, y)$, whose fixed points, (x, y, y), correspond to representations of p

as a sum of two squares, and a more complicated one,

$$(x,y,z) \mapsto \begin{cases} (x+2z,\ z,\ y-x-z), & \text{if } x < y-z, \\ (2y-x,\ y,\ x-y+z), & \text{if } y-z < x < 2y, \\ (x-2y,\ x-y+z,\ y), & \text{if } x > 2y, \end{cases}$$

which has exactly one fixed point, $(1,1,n)$.

If we look at the ring of Gaussian integers, Fermat's theorem on sums of two squares can be stated as follows: a rational prime $p > 2$ splits in $\mathbb{Q}(i)$ if and only if $p \equiv 1 \pmod 4$. Dedekind gave a proof of the Fermat's theorem on sums of two squares using Gaussian integers, and this will be relevant to our main results.

Here is the main idea of his proof. Suppose $p \mid m^2+1$ for the prime $p = 4n+1$ and some integers m and n. Then $p \mid (m+i)(m-i)$ in $\mathbb{Z}[i]$, the ring of integers of $\mathbb{Q}(i)$. Since $p \nmid m+i$ and $p \nmid m-i$, and it has norm $N(p) = p^2$ in $\mathbb{Z}[i]$, which is a unique factorization domain, we know $p = (x+yi)(x-yi)$ for some integers x and y. Therefore, $p = x^2+y^2$ is a sum of two squares. Such an integer m exists since $\mathbb{F}_p^\times$ is a cyclic group consisting of the roots of the polynomial $z^{4n}-1 = \left(z^{2n}-1\right)\left(z^{2n}+1\right)$, we can pick a root z of the polynomial $z^{2n}+1$ in $\mathbb{F}_p^\times$. Then $m = z^n$ satisfies $p \mid m^2+1$.

Now we know that any odd prime $p \equiv 1 \pmod 4$ can be written as $p = a_p^2 + b_p^2$ for integers a_p and b_p. Note that if we restrict $0 < b_p < a_p$, such representations will be unique. Suppose for a prime $p \equiv 1 \pmod 4$ we have $p = a_p^2 + b_p^2$ and $p = a_p'^2 + b_p'^2$ with positive integers $a_p > b_p$ and $a_p' > b_p'$, then $\mathfrak{p} = a_p + b_p i$ and $\mathfrak{p}' = a_p' + b_p' i$ are both Gaussian primes with $0 < \arg(\pi) < \frac{\pi}{4}$ and $0 < \arg(\pi') < \frac{\pi}{4}$. Since the only Gaussian primes with norm p are $\mathfrak{p}$, $\mathfrak{p}i$, $-\mathfrak{p}$, and $-\mathfrak{p}i$. With the restriction on $\arg(\mathfrak{p})$ and $\arg(\mathfrak{p}')$, we must have $\mathfrak{p}' = \mathfrak{p}$.

3.1.2 Primes congruent to 1 modulo 3

There is a classical result in number theory, which is similar to Fermat's theorem on sums of two squares: a prime $p > 3$ can be written in the form $a_p^2 + a_p b_p + b_p^2$ for integers a_p and b_p if and only if $p \equiv 1 \pmod 3$. Moreover, if we restrict $0 < b_p < a_p$, such representations are unique.

One direction of the proof is easy. Suppose $p = x^2 + xy + y^2 > 3$ is a prime. Suppose $3 \mid xy$, without loss of generality let $3 \mid x$, then $3 \nmid y$, otherwise $3 \mid p$, and we would have a contradiction.

Therefore, we know $y^2 \equiv 1 \pmod 3$, and thus $p = x^2 + xy + y^2 \equiv 1 \pmod 3$. Suppose $3 \nmid xy$, then $p \equiv 1 + xy + 1 \equiv 2 + xy \pmod 3$. Since $3 \nmid p$, we know $xy \equiv 0 \pmod 3$ or $xy \equiv 2 \pmod 3$, and by assumption, we have $xy \equiv 2 \pmod 3$. Therefore, we have $p \equiv 2 + xy \equiv 1 \pmod 3$.

For the other direction, let us first show the existence of such a representation. There are elementary number theory proofs as in the previous case. Here I give a proof using algebraic number theory.

Let $p \equiv 1 \pmod 3$ be a prime. Consider the number field $\mathbb{Q}(\sqrt{-3})$ with discriminant 3. We know its ring of integers is $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$, where $\frac{-1+\sqrt{-3}}{2}$ is a primitive third root of unity. When $p \equiv 1 \pmod 3$, we know p does not divide the discriminant, thus p does not ramify in $\mathbb{Q}(\sqrt{-3})$. Note that $f(x) = x^2 + x + 1$ is the minimum polynomial of $\frac{-1+\sqrt{-3}}{2}$, so we only need to consider the factorization of the polynomial $f(x)$ modulo p. To show p splits in $\mathbb{Q}(\sqrt{-3})$, it suffices to show $x^2 + x + 1 = 0$ has a solution in $\mathbb{F}_p$. Note that $x = 1$ is not a solution, this is equivalent to $x^3 = 1$ has a solution in $\mathbb{F}_p$ other than $x = 1$. Note that when $p \equiv 1 \pmod 3$, the size of the group $\mathbb{F}_p^\times$ is divisible by 3, by Sylow's theorem we know the existence of a nontrivial solution. This shows all primes $p \equiv 1 \pmod 3$ split in $\mathbb{Q}(\sqrt{-3})$.

Since $p \equiv 1 \pmod 3$ splits in $\mathbb{Q}(\sqrt{-3})$, we know there exists $a_p + b_p\frac{-1+\sqrt{-3}}{2} \in \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ with $a_p, b_p \in \mathbb{Z}$, such that its norm $N\left(a_p + b_p\frac{-1+\sqrt{-3}}{2}\right) = (a_p - b_p/2)^2 + 3b_p^2/4 = a_p^2 - a_pb_p + b_p^2$ is equal to p. If $a_pb_p < 0$, without loss of generality, let $a_p > 0$ and $b_p < 0$, then $a_p^2 + a_p(-b_p) + (-b_p)^2 = p$ for positive integers a_p and $-b_p$. If $a_pb_p > 0$, without loss of generality let $a_p > 0$ and $b_p > 0$, because otherwise we can consider $-a_p$ and $-b_p$ instead. If $a_p > b_p$, we have $(a_p - b_p)^2 + (a_p - b_p)a_p + b_p^2 = a_p^2 - a_pb_p + b_p^2 = p$, where $a_p - b_p > 0$ and $b_p > 0$. If $b_p > a_p$, we have $(b_p - a_p)^2 + (b_p - a_p)a_p + a_p^2 = a_p^2 - a_pb_p + b_p^2 = p$, where $b_p - a_p > 0$ and $a_p > 0$. Changing the order if necessary, we know a prime $p \equiv 1 \pmod 3$ can be written in the form $a_p^2 + a_pb_p + b_p^2$ for positive integers $a_p > b_p$.

Next, we prove the uniqueness of such representations. Given a prime $p \equiv 1 \pmod 3$, suppose $p = a_p^2 + a_pb_p + b_p^2$ and $p = a_p'^2 + a_p'b_p' + b_p'^2$ for positive integers $a_p > b_p$ and $a_p' > b_p'$. We know $\mathfrak{p} = a_p + b_p\frac{1+\sqrt{-3}}{2}$ and $\mathfrak{p}' = a_p' + b_p'\frac{1+\sqrt{-3}}{2}$ are primes in $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ with norm p. Since $\Re(\mathfrak{p}) > 0$, $\Im(\mathfrak{p}) > 0$, and $\cot(\arg\mathfrak{p}) = \frac{a_p + \frac{1}{2}b_p}{\frac{\sqrt{3}}{2}b_p} > \sqrt{3}$, we know $0 < \arg(\mathfrak{p}) < \frac{\pi}{6}$. Similarly we have $0 < \arg(\mathfrak{p}') < \frac{\pi}{6}$. Since the only primes with norm p are of the form $\mathfrak{p}$, $\mathfrak{p}i$, $-\mathfrak{p}$, $-\mathfrak{p}i$, $\mathfrak{p}\frac{-1+\sqrt{-3}}{2}$, $\mathfrak{p}\left(\frac{-1+\sqrt{-3}}{2}\right)^2$, $-\mathfrak{p}\frac{-1+\sqrt{-3}}{2}$, $-\mathfrak{p}\left(\frac{-1+\sqrt{-3}}{2}\right)^2$, $\overline{\mathfrak{p}}$, $\overline{\mathfrak{p}i}$, $\overline{-\mathfrak{p}}$, $\overline{-\mathfrak{p}i}$, $\overline{\mathfrak{p}\frac{-1+\sqrt{-3}}{2}}$, $\overline{\mathfrak{p}\left(\frac{-1+\sqrt{-3}}{2}\right)^2}$, $\overline{-\mathfrak{p}\frac{-1+\sqrt{-3}}{2}}$, and $\overline{-\mathfrak{p}\left(\frac{-1+\sqrt{-3}}{2}\right)^2}$, we know $\mathfrak{p}'$ has to equal one of them. With the restrictions $0 < \arg(\mathfrak{p}) < \frac{\pi}{6}$ and $0 < \arg(\mathfrak{p}') < \frac{\pi}{6}$, we must have $\mathfrak{p}' = \mathfrak{p}$. This completes the proof of uniqueness.

3.1.3 Primes in arithmetic progressions represented by other symmetric quadratic forms

First, we recall the following definitions on quadratic forms in two variables from [7, Pages 24-30]:

Definition 3.1.1. *A quadratic form $f(x) = ax^2 + bxy + cy^2$ is* primitive *if its coefficients a, b, and c are relatively prime.*

Definition 3.1.2. *An integer m is* represented *by a quadratic form $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y. If the x and y in the solution are relatively prime, we say that m is* properly represented *by $f(x, y)$.*

Definition 3.1.3. *We say that two quadratic forms $f(x, y)$ and $g(x, y)$ are* equivalent *if there are integers α, β, γ, and δ such that*

$$f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$$

and $\alpha\delta - \beta\gamma = \pm 1$. We say that an equivalence is a proper equivalence *if $\alpha\delta - \beta\gamma = 1$, and it is an* improper equivalence *if $\alpha\delta - \beta\gamma = -1$.*

Definition 3.1.4. *We define the* discriminant *of $f(x, y) = ax^2 + bxy + cy^2$ to be $D = b^2 - 4ac$. If $D > 0$, then $f(x, y)$ represents both positive and negative integers, and we call the form* indefinite*; if $D < 0$ and $a > 0$, then $f(x, y)$ represents only positive integers, and we call the form* positive definite*; if $D < 0$ and $a < 0$, then $f(x, y)$ represents only negative integers, and we call the form* negative definite.

Definition 3.1.5. *A primitive positive definite quadratic form $ax^2 + bxy + cy^2$ is said to be* reduced *if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$.*

Note that both $x^2 + y^2$ and $x^2 + xy + y^2$ are reduced positive definite quadratic forms, and Sun's conjectures are based on primes in arithmetic progressions represented by those two positive definite symmetric quadratic forms. We want to explore primes in arithmetic progressions represented by other positive definite symmetric quadratic forms $ax^2 + bxy + ay^2$ with coefficients $a, b \in \mathbb{Z}$ and discriminant $b^2 - 4a^2$. We will study which primes are represented by such forms and try to solve the same type of questions as Sun's conjectures. We introduce the following

theorems to relate such positive definite symmetric quadratics forms to reduced forms $x^2 + ny^2$ and $x^2 + xy + \frac{1-D}{4}y^2$:

Theorem 3.1.6 ([7, Theorem 2.8]). *Every primitive positive definite quadratic form is properly equivalent to a unique reduced form.*

Theorem 3.1.7 ([7, Theorem 2.13]). *Let $D < 0$ be fixed. Then, the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and furthermore, $h(D)$ is equal to the number of reduced forms of discriminant D.*

Definition 3.1.8. *Let $f(x, y) = ax^2+bxy+cy^2$ and $g(x, y) = a'x^2+b'xy+c'y^2$ be primitive positive definite quadratic forms of discriminant $D < 0$ which satisfy $\gcd(a, a', (b + b')/2) = 1$. Then, the* Dirichlet composition *of $f(x, y)$ and $g(x, y)$ is the form*

$$F(x, y) = aa'x^2 + 2Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the nonnegative integer less than $2aa'$ satisfying $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$, and $B^2 \equiv D \pmod{4aa'}$.

Remark 3.1.9. *The existence and uniqueness of such an integer B is proved in Lemma 3.2 of [7].*

Theorem 3.1.10 ([7, Theorem 3.9]). *Let $D \equiv 0, 1 \pmod 4$ be negative, and let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D. Then, Dirichlet composition induces a well-defined binary operation on $C(D)$ which makes $C(D)$ into a finite Abelian group whose order is the class number $h(D)$.*

Furthermore, the identity element of $C(D)$ is the class containing the principal form *$x^2-\frac{D}{4}y^2$ if $D \equiv 0 \pmod 4$ and $x^2 + xy + \frac{1-D}{4}y^2$ if $D \equiv 1 \pmod 4$, and the inverse of the class containing the form $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.*

To make things easier, we only look at positive definite symmetric quadratic forms with discriminant D such that $h(D)$ is equal to 1, so we introduce the following theorem:

Theorem 3.1.11 ([7, Theorem 7.10]). *If $D \equiv 0, 1 \pmod 4$ is negative, then*

$$h(D) = 1 \iff D = -3, -4, -7, -8, -11, -12, -16,$$
$$-19, -27, -28, -43, -67, -163.$$

Let us list all of the positive definite symmetric quadratic forms $ax^2 + bxy + ay^2$ with discriminant -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, and -163, respectively.

When D is even, since $D = b^2 - 4a^2$, we know b is even. Therefore, we have $a^2 - (b/2)^2 = -D/4$.

1. Let $b^2 - 4a^2 = -4$, then we have $a^2 - (b/2)^2 = 1$, which implies $a = \pm 1$ and $b = 0$. Therefore, we have one positive definite symmetric quadratic form with discriminant -4, which is $x^2 + y^2$.

2. Let $b^2 - 4a^2 = -8$, which implies $a^2 - (b/2)^2 = 2$. There is no integer solution to the equation $x^2 - y^2 = 2$, therefore, we do not have any positive definite symmetric quadratic form with discriminant -8.

3. Let $b^2 - 4a^2 = -12$, which implies $a^2 - (b/2)^2 = 3$. Thus, $a = \pm 2$ and $b = \pm 2$. Therefore, we have two positive definite symmetric quadratic forms with discriminant -12, which are $2x^2 + 2xy + 2y^2$ and $2x^2 - 2xy + 2y^2$.

4. Let $b^2 - 4a^2 = -16$, which implies $a^2 - (b/2)^2 = 4$. Thus, $a = \pm 2$ and $b = 0$. Therefore, we have one positive definite symmetric quadratic form with discriminant -16, which is $2x^2 + 2y^2$.

5. Let $b^2 - 4a^2 = -28$, which implies $a^2 - (b/2)^2 = 7$. Thus $a = \pm 4$ and $b = \pm 6$. Therefore, we have two positive definite symmetric quadratic form with discriminant -28, which are $4x^2 + 6xy + 4y^2$ and $4x^2 - 6xy + 4y^2$.

Next we consider the odd discriminants.

1. Let $b^2 - 4a^2 = -3$, then $a = \pm 1$ and $b = \pm 1$. Therefore, we have two positive definite symmetric quadratic form with discriminant -3, which are $x^2 + xy + y^2$ and $x^2 - xy + y^2$.

2. Let $b^2 - 4a^2 = -7$, then $a = \pm 2$ and $b = \pm 3$. Therefore, we have two positive definite symmetric quadratic form with discriminant -7, which are $2x^2 + 3xy + 2y^2$ and $2x^2 - 3xy + 2y^2$.

3. Let $b^2 - 4a^2 = -11$, then $a = \pm 3$ and $b = \pm 5$. Therefore, we have two positive definite symmetric quadratic form with discriminant -11, which are $3x^2 + 5xy + 3y^2$ and $3x^2 - 5xy + 3y^2$.

4. Let $b^2 - 4a^2 = -19$, then $a = \pm 5$ and $b = \pm 9$. Therefore, we have two positive definite symmetric quadratic form with discriminant -19, which are $5x^2 + 9xy + 5y^2$ and $5x^2 - 9xy + 5y^2$.

5. Let $b^2 - 4a^2 = -27$, then $(a, b) = (\pm 7, \pm 13)$ or $(a, b) = (\pm 3, \pm 3)$. Therefore, we have four positive definite symmetric quadratic form with discriminant -27, which are $7x^2 + 13xy + 7y^2$, $7x^2 - 13xy + 7y^2$, $3x^2 + 3xy + 3y^2$, and $3x^2 - 3xy + 3y^2$.

6. Let $b^2 - 4a^2 = -43$, then $a = \pm 11$ and $b = \pm 21$. Therefore, we have two positive definite symmetric quadratic form with discriminant -43, which are $11x^2 + 21xy + 11y^2$ and $11x^2 - 21xy + 11y^2$.

7. Let $b^2 - 4a^2 = -67$, then $a = \pm 17$ and $b = \pm 33$. Therefore, we have two positive definite symmetric quadratic form with discriminant -67, which are $17x^2 + 33xy + 17y^2$ and $17x^2 - 33xy + 17y^2$.

8. Let $b^2 - 4a^2 = -163$, then $a = \pm 41$ and $b = \pm 81$. Therefore, we have two positive definite symmetric quadratic form with discriminant -163, which are $41x^2 + 81xy + 41y^2$ and $41x^2 - 81xy + 41y^2$.

We can study primes represented by the symmetric quadratic forms above, and make similar conjectures as Sun's conjectures.

In the thesis, we will explore one of the symmetric quadratic forms, the $f(x, y) = 2x^2 + 3xy + 2y^2$ with discriminant -7. Since $h(-7) = 1$, by Theorem 3.1.10 we know $C(-7)$, the set of classes of primitive positive definite forms of discriminant -7, is an Abelian group of order 1. Thus $f(x, y) = 2x^2 + 3xy + 2y^2$ is properly equivalent to the principal form $x^2 + xy + \frac{1-(-7)}{4}y^2 = x^2 + xy + 2y^2$, and thus, they represent the same numbers by [7, Page 24]. Thus, we only need to study primes represented by the reduced positive definite primitive quadratic form $x^2 + xy + 2y^2$.

We claim that an odd prime $p > 7$ can be written in the form $2a_p^2 + 3a_p b_p + 2b_p^2$ for integers a_p and b_p if and only if $p \equiv 1, 2, 4 \pmod 7$. Moreover, if we assume $0 < |b_p| < a_p$, such representations are unique.

One direction is easy, we only need to compute $2x^2 + 3xy + 2y^2$ modulo 7 for all possible x and y modulo 7. See Table 3.1 for the computation.

For the other direction, let p be an odd prime that is congruent to 1, 2, or 4 modulo 7. We want to show the existence of integers a'_p and b'_p such that $p = a'^2_p + a'_p b'_p + 2b'^2_p$. Note that since $a'^2_p + a'_p b'_p + 2b'^2_p = \left(a'_p + \frac{1}{2}b'_p\right)^2 + \left(\frac{\sqrt{7}}{2}b'_p\right)^2$, we see the norm of $\mathfrak{p} = a'_p - \frac{-1+\sqrt{-7}}{2}b'_p$ is equal to $a'^2_p + a'_p b'_p + 2b'^2_p$. Therefore, it suffices to prove the given odd prime p splits in $\mathbb{Q}(\sqrt{-7})$, whose ring

	0	1	2	3	4	5	6
0	0	2	1	4	4	1	2
1	2	0	2	1	4	4	1
2	1	2	0	2	1	1	4
3	4	2	2	0	4	1	4
4	4	1	1	4	0	2	1
5	1	4	1	1	2	0	2
6	2	1	4	4	1	2	0

Table 3.1: $2x^2 + 3xy + 2y^2 \pmod 7$

of integers is $\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$. We apply the following theorem to find which primes split in $\mathbb{Q}(\sqrt{-7})$:

Theorem 3.1.12 ([19, Theorem 9.29(3)]). *Let $\mathbb{Q}(\sqrt{m})$ have the unique factorization property. Then an odd rational prime p satisfying $(p, m) = 1$ is a product $\pi_1\pi_2$ of two primes in $\mathbb{Q}(\sqrt{m})$ if and only if m is congruent to a square modulo p.*

In particular, we know an odd prime $p > 7$ splits in $\mathbb{Q}(\sqrt{-7})$ if and only if -7 is congruent to a square modulo p. We will apply the law of quadratic reciprocity:

Theorem 3.1.13 ([13, Theorem 1, Page 53]). *Let p and q be distinct odd primes. Then*

1. $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

2. $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

3. $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where for any integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ *has value 0 if $p \mid a$, 1 if a is congruent to a non-zero square modulo p, and -1 if a is not congruent to any non-zero square modulo p.*

Taking $q = 7$ in Theorem 3.1.13, we know

$$\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}\frac{7-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Since

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)$$

and

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

we know

$$\left(\frac{p}{7}\right)\left(\frac{-7}{p}\right) = 1.$$

Therefore, -7 is congruent to a square modulo p if and only if p congruent to a square modulo 7, i.e., if and only if p is congruent to 1, 2, or 4 modulo 7. Therefore, the given odd prime p splits in $\mathbb{Q}(\sqrt{-7})$, and thus, there exist integers a_p'' and b_p'' such that $p = a_p''^2 + a_p''b_p'' + 2b_p''^2$. Since $2x^2 + 3xy + 2y^2$ is properly equivalent to the reduced form $x^2 + xy + 2y^2$, p can be represented by $2a_p^2 + 3a_pb_p + 2b_p^2$ for integers a_p and b_p. Without loss of generality, we can assume that $0 < |b_p| < a_p$, since we can consider $-a_p$ and $-b_p$ instead, or change the order of a_p and b_p, if necessary.

Note that we can not assume that $0 < b_p < a_p$ in the representation. One example is when $p = 11 \equiv 4 \pmod 7$, it is easy to check there are no positive integers solutions to the equation $2x^2 + 3xy + 2y^2 = 11$, but we have $(x, y) = (3, -1)$ as a solution.

Finally, we prove the uniqueness of such representations. Suppose $p = 2a_p^2 + 3a_pb_p + 2b_p^2 = \frac{1}{4}(a_p - b_p)^2 + \frac{7}{4}(a_p + b_p)^2 = \left(\frac{a_p}{2} - \frac{b_p}{2}\right)^2 + 7\left(\frac{a_p}{2} + \frac{b_p}{2}\right)^2$ and $p = 2a_p'^2 + 3a_p'b_p' + 2b_p'^2 = \frac{1}{4}(a_p' - b_p')^2 + \frac{7}{4}(a_p' + b_p')^2 = \left(\frac{a_p'}{2} - \frac{b_p'}{2}\right)^2 + 7\left(\frac{a_p'}{2} + \frac{b_p'}{2}\right)^2$ with $0 < |b_p| < a_p$ and $0 < |b_p'| < a_p'$. Then, both $a_p + (a_p + b_p)\frac{-1+\sqrt{-7}}{2}$ and $a_p' + (a_p' + b_p')\frac{-1+\sqrt{-7}}{2}$ in $\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$ have norm p. Their ratio must be a unit in $\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$, which could only be 1 or -1, since $N\left(a + b\frac{-1+\sqrt{7}}{2}\right) = \left(a - \frac{b}{2}\right)^2 + \frac{7}{4}b^2 = 1$ if and only if $a = \pm 1$ and $b = 0$. With the restrictions on a_p, b_p, a_p', and b_p', we can see that $a_p = a_p'$ and $b_p = b_p'$. This completes the proof of uniqueness of the representations.

Now, we can consider the same type of questions as Sun's conjectures stated above. Let $c \geq 1$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1, 2, or 4 modulo 7, let a_p and b_p be integers such that $p = 2a_p^2 + 3a_pb_p + 2b_p^2$ and $0 < |b_p| < a_p$. Then, for the primes satisfying

$0 < c|b_p| < a_p$, we can ask for the value of

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\le x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\le x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n}.$$

Theorem 3.2.3 will answer this question.

3.1.4 Primes in arithmetic progressions represented by quadratic forms of the form $x^2 + ny^2$

Note that Sun's conjectures are about the sum of the larger terms over the sum of the smaller terms in certain representations, so we need symmetric quadratic forms $ax^2 + bxy + ay^2$ to form similar conjectures. We can consider a more general type of problems when the quadratic form is not symmetric. In this subsection we consider quadratic forms with the form $x^2 + ny^2$.

Primes of the form $x^2 + ny^2$ are very well studied in [7], here we quote a couple of results from the first three pages of the book:

$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8,$$

$$p = x^2 + 5y^2 \iff p \equiv 1 \text{ or } 9 \pmod{20},$$

$$p = x^2 + 27y^2 \iff p \equiv 1 \pmod 3 \text{ and } x^3 \equiv 2 \pmod p \text{ has an integer solution,}$$

$$p = x^2 + 27y^2 \text{ or } p = 4x^2 + 2xy + 7y^2 \iff p \equiv 1 \pmod 3,$$

$$p = x^2 + 14y^2 \iff$$

-14 is congruent to a square modulo p and $(x^2+1)^2 \equiv 8 \pmod p$ has an integer solution.

The main theorem of the book [7] characterizes which prime can be written of the form $x^2 + ny^2$.

Theorem 3.1.14 ([7, Theorem 9.2])**.** *Let $n > 0$ be an integer. Then, there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor the*

discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff$$

$-n$ is congruent to a square modulo p and $f_n(x) \equiv 0 \pmod{p}$ has an integer solution.

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the ring class field of order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$.

Finally, if $f_n(x)$ is any monic integer polynomial of degree $h(-4n)$ for which the above equivalence holds, then $f_n(x)$ is irreducible over $\mathbb{Z}$ and is the minimal polynomial of a primitive element of the ring class field.

We are not going into the details of the above theorem in the thesis, as it would take us too far afield. For a proof of the theorem and the definitions of the discriminant of a polynomial, the ring class field, the order of a number field, the primitive element of a ring class field, etc., please see Chapter 9 of [7].

Let us continue with Sun's conjectures and deal with the specific case

$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod{8}.$$

We claim that an odd prime p can be written in the form $a_p^2 + 2b_p^2$ for integers a_p and b_p if and only if $p \equiv 1$ or $3 \pmod{8}$. Moreover, if we assume a_p and b_p to be positive, such representations are unique.

One direction is easy, we only need to compute $x^2 + 2y^2$ modulo 8 for all possible x and y modulo 8. See Table 3.2 for the computation, where the even congruence classes are crossed off since we want $x^2 + 2y^2$ to be a prime number.

	0	1	2	3	4	5	6	7
0	~~0~~	1	~~4~~	1	~~0~~	1	~~4~~	1
1	~~2~~	3	~~6~~	3	~~2~~	3	~~6~~	3
2	~~0~~	1	~~4~~	1	~~0~~	1	~~4~~	1
3	~~2~~	3	~~6~~	3	~~2~~	3	~~6~~	3
4	~~0~~	1	~~4~~	1	~~0~~	1	~~4~~	1
5	~~2~~	3	~~6~~	3	~~2~~	3	~~6~~	3
6	~~0~~	1	~~4~~	1	~~0~~	1	~~4~~	1
7	~~2~~	3	~~6~~	3	~~2~~	3	~~6~~	3

Table 3.2: $x^2 + 2y^2 \pmod{8}$

For the other direction, let p be a prime that is congruent to 1 or 3 modulo 8. We want to show the existence of integers a_p and b_p such that $p = a_p^2 + 2b_p^2$. Note that since $a_p^2 + 2b_p^2 = \left(a_p + \sqrt{-2}b_p\right)\left(a_p - \sqrt{-2}b_p\right)$, we see the norm of $\mathfrak{p} = a_p + \sqrt{-2}b_p$ is equal to $a_p^2 + 2b_p^2$. Therefore, it suffices to prove the given prime p splits in $\mathbb{Q}(\sqrt{-2})$, whose ring of integers is $\mathbb{Z}[\sqrt{-2}]$. By Theorem 3.1.12, we know an odd prime p splits in $\mathbb{Q}(\sqrt{-2})$ if and only if -2 is a square modulo p. By Theorem 3.1.13, we have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p+5)(p-1)}{8}}.$$

Therefore, -2 is congruent to a square modulo p if and only if p is congruent to 1 or 3 modulo 8. Therefore, the given prime p splits in $\mathbb{Q}\left[\sqrt{-2}\right]$, and thus, there exist integers a_p and b_p such that $p = a_p^2 + 2b_p^2$. Without loss of generality, we can assume that $a_p > 0$ and $b_p > 0$, since otherwise we can consider $-a_p$ and $-b_p$ instead.

Finally, we prove the uniqueness of such representations. Suppose $p = a_p^2 + 2b_p^2 = a_p^2 + (\sqrt{2}b_p)^2$ and $p = a_p'^2 + 2b_p'^2 = a_p'^2 + (\sqrt{2}b_p')^2$ with positive integers a_p, b_p, a_p', and b_p'. Then, both $a_p + \sqrt{-2}b_p$ and $a_p' + \sqrt{-2}b_p'$ in $\mathbb{Z}[\sqrt{-2}]$ have norm p. Their ratio must be a unit in $\mathbb{Z}[\sqrt{-2}]$, which could only be 1 or -1, since $N\left(a + \sqrt{-2}b\right) = a^2 + 2b^2 = 1$ if and only if $a = \pm 1$ and $b = 0$. With the restrictions on a_p, b_p, a_p', and b_p', we can see that $a_p = a_p'$ and $b_p = b_p'$. This completes the proof of uniqueness of the representations.

Now, we can consider the same type of questions as Sun's conjectures. Let $c > 0$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1 or 3 modulo 8, let a_p and b_p be positive integers such that $p = a_p^2 + 2b_p^2$. Then, for the primes satisfying $0 < cb_p < a_p$, we can ask for the value of

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ p\leq x \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ p\leq x \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n}.$$

Theorem 3.2.4 will answer this question.

3.2 Main Results

In this chapter, we prove the following main theorems. For primes congruent to 1 modulo 4 represented by x^2+y^2, we have:

Theorem 3.2.1. *Let $c \geq 1$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1 modulo 4, let a_p and b_p be positive integers such that $p = a_p^2 + b_p^2$. Then, for the primes satisfying $0 < cb_p < a_p$, we have*

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt}.$$

In particular, for $c = 1$ and $n = 1$, we have

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} b_p} = 1+\sqrt{2},$$

and for $c = 1$ and $n = 2$, we have

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} a_p^2}{\sum\limits_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\leq x \\ p=a_p^2+b_p^2,\ 0<b_p<a_p}} b_p^2} = \frac{\pi+2}{\pi-2} \approx 4.5039.$$

Note that Sun conjectured the value of the limit for $c = 1$ and $n = 1$ to be $1+\sqrt{2}$, so this verifies his conjecture. In the case of $c = 1$ and $n = 2$ he conjectured the value of the limit to be 4.5, which is close to the actual value $\frac{\pi+2}{\pi-2}$.

For primes congruent to 1 modulo 3 represented by $x^2 + xy + y^2$, we have the following theorem:

Theorem 3.2.2. *Let $c \geq 1$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1 modulo 3, let a_p and b_p be positive integers such that $p = a_p^2 + a_p b_p + b_p^2$. Then, for the primes satisfying $0 < cb_p < a_p$, we have*

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\cos(t) - \frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt}.$$

In particular, for $c = 1$ and $n = 1$, we have

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} a_p}{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} b_p} = 1 + \sqrt{3},$$

and for $c = 1$ and $n = 2$, we have

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} a_p^2}{\displaystyle\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<b_p<a_p}} b_p^2} = \frac{2\pi}{2\pi - 3\sqrt{3}}.$$

Note that Sun conjectured the value of the limit for $c = 1$ and $n = 1$ to be $1 + \sqrt{3}$, so this verifies his conjecture.

For primes in arithmetic progressions represented by other symmetric quadratic forms, in particular for primes congruent to 1, 2, or 4 modulo 7 represented by $2x^2 + 3xy + 2y^2$, we have the following theorem:

Theorem 3.2.3. *Let $c \geq 1$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1, 2, or 4 modulo 7, let a_p and b_p be integers such that $p = 2a_p^2 + 3a_pb_p + 2b_p^2$ and $0 < |b_p| < a_p$. Then, for the primes satisfying $0 < c|b_p| < a_p$, we have*

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n}{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n} = \frac{\displaystyle\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}} + \cos(t)\right)^n dt}{\displaystyle\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}} - \cos(t)\right)^n dt}.$$

In particular, for $c = 1$ and $n = 1$, we have

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<|b_p|<a_p}} a_p}{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<|b_p|<a_p}} b_p} = \frac{1+\sqrt{7}}{1-\sqrt{7}},$$

and for $c = 1$ and $n = 2$, we have

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<|b_p|<a_p}} a_p^2}{\displaystyle\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<|b_p|<a_p}} b_p^2} = \frac{2\pi+\sqrt{7}}{2\pi-\sqrt{7}}.$$

For primes in arithmetic progressions represented by non-symmetric quadratic forms, in particular for primes congruent to 1 or 3 modulo 8 represented by $x^2 + 2y^2$, we have the following theorem:

Theorem 3.2.4. *Let $c > 0$ and $n \geq 1$ be constants. Given a prime p that is congruent to 1 or 3 modulo 8, let a_p and b_p be positive integers such that $p = a_p^2 + 2b_p^2$. Then, for the primes satisfying*

$0 < cb_p < a_p$, *we have*

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} (\cos(t))^n\, dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} \left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt}.$$

In particular, for $c = 1$ and $n = 1$, we have

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<b_p<a_p}} a_p}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<b_p<a_p}} b_p} = \sqrt{3}+1,$$

and for $c = 1$ and $n = 2$, we have

$$\lim_{x\to\infty} \frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<b_p<a_p}} a_p^2}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\le x\\ p=a_p^2+2b_p^2,\ 0<b_p<a_p}} b_p^2} = 2\times\frac{3\operatorname{arccot}\left(\frac{1}{\sqrt{2}}\right)+\sqrt{2}}{3\operatorname{arccot}\left(\frac{1}{\sqrt{2}}\right)-\sqrt{2}}.$$

3.3 Proof of the Theorems

3.3.1 Equidistribution of primes in imaginary quadratic fields

The key ingredient in the proof of the theorems is equidistribution of primes in imaginary quadratic fields. We introduce a modified version of Maknys's theorem [17].

Theorem 3.3.1 ([14, Prop 2])**.** *Let K be an imaginary quadratic field. Fix $\mu, \nu \in \mathcal{O}_K$ with $\mu \neq 0$ and with $\nu \pmod\mu$ an invertible residue class. Let $\eta = 0.735$. As $X \to \infty$,*

$$\sum_{\substack{N(\omega) \text{ prime}\\ X<N(\omega)\le X+X^\eta\\ \omega\equiv\nu \pmod\mu\\ \theta_1<\arg(\omega)<\theta_2}} 1 \sim \frac{w_K}{h_K\varphi(\mu)}\times\frac{\theta_2-\theta_1}{2\pi}\times\frac{X^\eta}{\log X},$$

when $X^{\eta-1} < \theta_2 - \theta_1 \leq 2\pi$, where $N(\omega)$ is the norm of ω in K, w_K is the number of units in K, h_K is the class number of K, and $\varphi(\mu)$ is the number of invertible residue classes modulo μ. Here the estimate is uniform in the θ_i's.

Remark 3.3.2 ([14, Remark, Page 3])**.** *Maknys claims that in place of the exponents 0.735 and -0.265, one can take any fixed constants larger than $\frac{11}{16}$ and $\frac{11}{16} - 1$, respectively. It was noted by Heath-Brown in Math Reviews that Maknys's argument is mistaken, and that, when corrected, $\frac{11}{16}$ becomes $(221 + \sqrt{201})/320 = 0.7349....$ We have used these corrected values above.*

3.3.2 Proof of Theorem 3.2.1

Let $c \geq 1$ be a constant. If a prime $p \equiv 1 \pmod 4$ satisfies $p = a_p^2 + b_p^2$ for positive integers a_p and b_p such that $0 < cb_p < a_p$, then $\omega = a_p + ib_p \in \mathbb{Z}[i]$ satisfies $0 < \arg\omega < \operatorname{arccot}(c)$.

Let $K = \mathbb{Q}(i)$, and let $\mu = \nu = 1$ in Theorem 3.3.1. Then, we have $h_K = 1$, $w_K = 4$, and $\varphi(\mu) = 1$. For a constant $c \geq 1$, we set

$$R(X) = \{z \in \mathbb{C} : 0 < \arg z \leq \operatorname{arccot}(c), X < |z|^2 \leq X + X^\eta\}.$$

Then, we have

$$\sum_{\substack{\omega = a_p + ib_p \in R(X) \\ N(\omega) \text{ prime} \\ \theta_1 < \arg(\omega) < \theta_2}} 1 = \sum_{\substack{p \equiv 1 \pmod 4 \text{ prime} \\ X < p \leq X + X^\eta \\ p = a_p^2 + b_p^2,\ 0 < cb_p < a_p \\ \theta_1 < \operatorname{arccot}(a_p/b_p) < \theta_2}} 1 \sim (\theta_2 - \theta_1) \times \frac{2X^\eta}{\pi \log X},$$

as $X \to \infty$, when $0 < \theta_1 < \theta_2 < \operatorname{arccot}(c)$ and $X^{\eta-1} < \theta_2 - \theta_1$.

Let $n_X = \left\lfloor \frac{\operatorname{arccot}(c)}{\theta_X} \right\rfloor + 1$ for $\theta_X = 2X^{\eta-1} > X^{\eta-1}$. We divide $R(X)$ into n_X smaller regions:

$$R(X)_j = \{z \in \mathbb{C} : (j-1)\theta_X < \arg z \leq j\theta_X, X < |z|^2 \leq X + X^\eta\}$$

for $1 \leq j \leq n_X - 1$, and

$$R(X)_{n_X} = \{z \in \mathbb{C} : (n_X - 1)\theta_X < \arg z \leq \operatorname{arccot}(c), X < |z|^2 \leq X + X^\eta\}.$$

See Figure 3.1 that explains how the region $R(X)$ is divided into smaller regions.

We denote the number of Gaussian primes in the region $R(X)_j$ by $m(X)_j$ for $1 \leq j \leq n_X$.

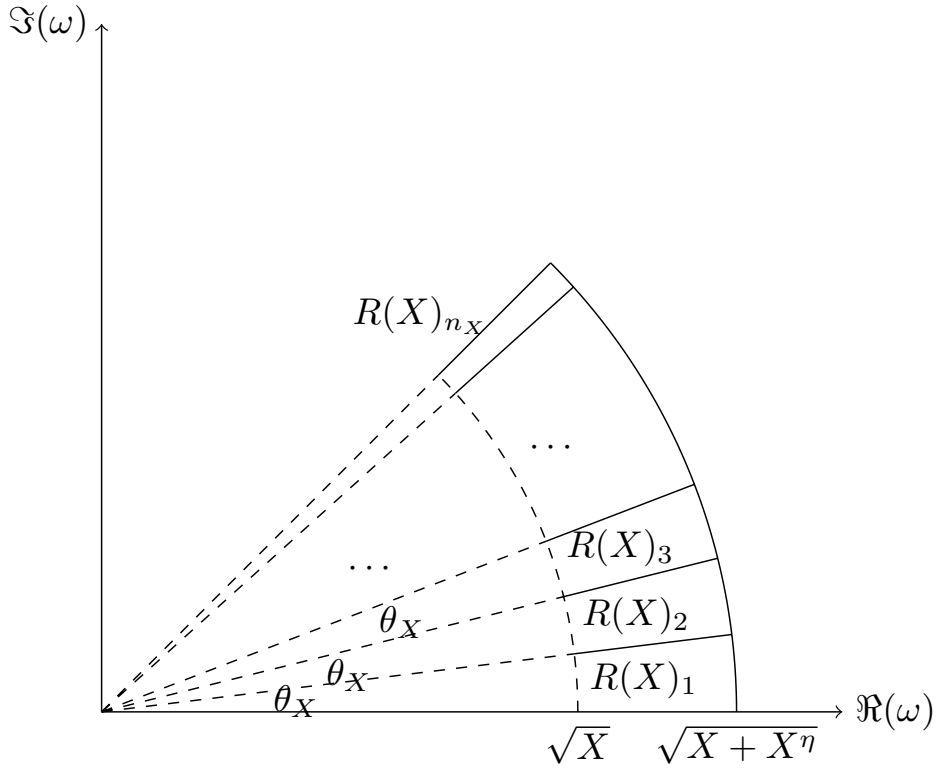

Figure 3.1: Split the Region $R(X)$

Let $m_X = \frac{2\theta_X X^\eta}{\pi \log X}$. Theorem 3.3.1 gives $m(X)_j = (1+o(X))m_X$ for $1 \le j \le n_X - 1$, and $m(X)_{n_X} \le (1+o(1))m_X$. For rational primes $X < p \le X + X^\eta$ that are congruent to 1 modulo 4, we know they correspond to Gaussian primes

$$\omega = a_p + b_p i \in R(X) = \bigsqcup_{j=1}^{n_X} R(X)_j.$$

As shown in Figures 3.2 and 3.3, if $\omega \in R(X)_j$ for $1 \le j \le n_X - 1$, there are upper and lower bounds on its real and imaginary parts:

$$\sqrt{X}\cos(j\theta_X) \le a_p = \Re(\omega) < \sqrt{X+X^\eta}\cos((j-1)\theta_X),$$

$$\sqrt{X}\sin((j-1)\theta_X) < b_p = \Im(\omega) \le \sqrt{X+X^\eta}\sin(j\theta_X).$$

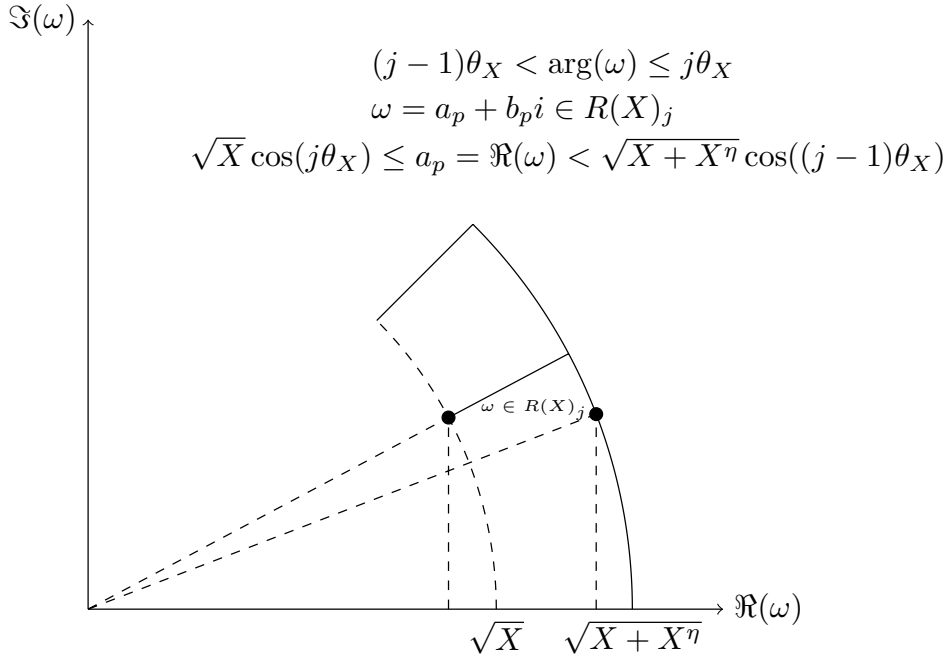

Figure 3.2: Bounds on the Real Parts of Gaussian Primes in $R(x)_j$

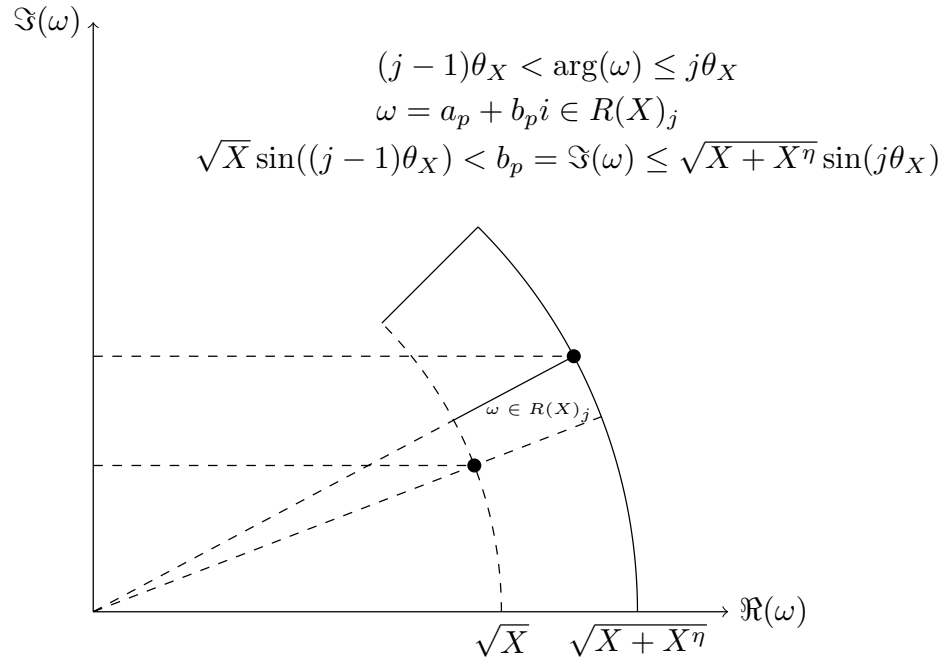

Figure 3.3: Bounds on the Imaginary Parts of Gaussian Primes in $R(x)_j$

Therefore, we know there exists an $o(1)$ term that only depends on X, such that

$$(1+o(1))m_X X^{\frac{n}{2}} \sum_{j=1}^{n_X-1} \cos^n(j\theta_X) \leq \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\leq X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n$$
$$\leq (1+o(1))m_X (X+X^\eta)^{\frac{n}{2}} \sum_{j=1}^{n_X} \cos^n((j-1)\theta_X),$$

and

$$(1+o(1))m_X X^{\frac{n}{2}} \sum_{j=1}^{n_X-1} \sin^n((j-1)\theta_X) \leq \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\leq X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n$$
$$\leq (1+o(1))m_X (X+X^\eta)^{\frac{n}{2}} \sum_{j=1}^{n_X} \sin^n(j\theta_X).$$

By the definition of n_X and θ_X, we know that $0 < (n_X-1)\theta_X \leq \operatorname{arccot}(c) \leq n_X\theta_X < \pi/2$ for all X. Therefore, we have

$$\begin{aligned}\sum_{j=1}^{n_X-1} \cos^n(j\theta_X) &\geq \frac{1}{\theta_X}\int_{\theta_X}^{n_X\theta_X} \cos^n(t)dt \\ &= \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt - \int_0^{\theta_X} \cos^n(t)dt + \int_{\operatorname{arccot}(c)}^{n_X\theta_X} \cos^n(t)dt\right) \\ &\geq \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt - \theta_X\right),\end{aligned}$$

and similarly,

$$\sum_{j=1}^{n_X} \cos^n((j-1)\theta_X) \leq \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt + \theta_X\right),$$

$$\sum_{j=1}^{n_X-1} \sin^n((j-1)\theta_X) \geq \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt - 2\theta_X\right),$$

and

$$\sum_{j=1}^{n_X} \sin^n(j\theta_X) \le \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt + 2\theta_X\right).$$

Therefore, we obtain

$$(1+o(1))m_X X^{\frac{n}{2}} \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt - \theta_X\right) \le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\le X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n$$
$$\le (1+o(1))m_X (X+X^\eta)^{\frac{n}{2}} \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt + \theta_X\right),$$

and

$$(1+o(1))m_X X^{\frac{n}{2}} \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt - 2\theta_X\right) \le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\le X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n$$
$$\le (1+o(1))m_X (X+X^\eta)^{\frac{n}{2}} \frac{1}{\theta_X}\left(\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt + 2\theta_X\right).$$

For sufficiently large X, since $\theta_X = o(1)$, we have

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\le X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n \le (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt + \theta_X}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt - 2\theta_X} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\le X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n$$
$$\le (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ X<p\le X+X^\eta \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n,$$

and

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X<p\le X+X^{\eta}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n \ge (1+o(1))(1-X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt - \theta_X}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt + 2\theta_X} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X<p\le X+X^{\eta}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n$$

$$\ge (1+o(1))(1-X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X<p\le X+X^{\eta}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n.$$

Next, we consider the region

$$R(x) = \{z \in \mathbb{C} : 0 < \arg z \le \operatorname{arccot}(c), 0 < |z|^2 \le x\}.$$

We split $R(x)$ as the union of smaller regions

$$R(X_i) = \{z \in \mathbb{C} : 0 < \arg z \le \operatorname{arccot}(c), X_i < |z|^2 \le X_i + X_i^{\eta}\},$$

where $1 \le i \le k$, $X_1 + X_1^{\eta} = x$, $X_i + X_i^{\eta} = X_{i-1}$ for $2 \le i \le k$, and $X_k < x^{1/2} \le X_{k-1}$, which implies $X_k = O(x^{1/2})$. See Figure 3.4 which illustrates how the region $R(x)$ is divided into smaller pieces.

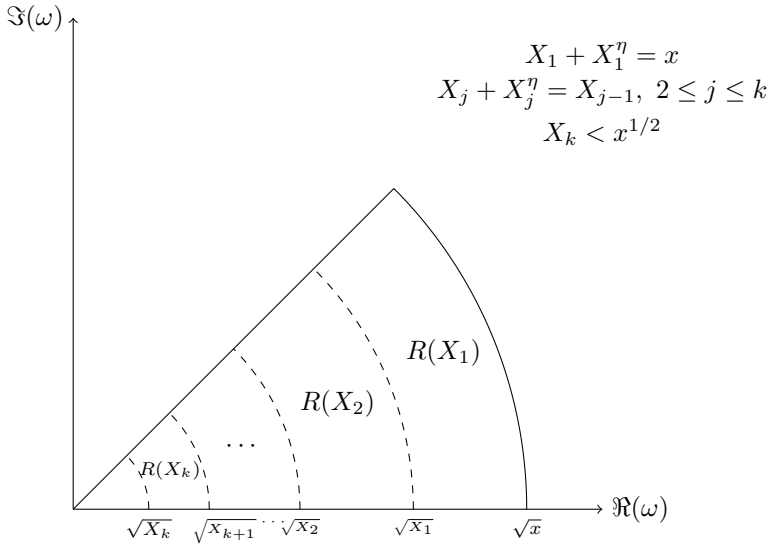

Figure 3.4: Split the Region $R(x)$

Then for sufficiently large x, we have

$$\begin{aligned}
&\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n\\
&= \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le X_k\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n + \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X_k<p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n\\
&\le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n + (1+o(1))\left(1+X_k^{\eta-1}\right)^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}(c)}\cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)}\sin^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X_k<p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n\\
&\le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n + (1+o(1))\left(1+O\left(x^{(\eta-1)/2}\right)\right)\\
&\qquad\qquad \times \frac{\int_0^{\operatorname{arccot}(c)}\cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)}\sin^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n,
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n\\
&= \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le X_k\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n + \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X_k<p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n\\
&\le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n + \frac{1}{(1+o(1))\left(1-X_k^{\eta-1}\right)^{\frac{n}{2}}} \times \frac{\int_0^{\operatorname{arccot}(c)}\sin^n(t)dt}{\int_0^{\operatorname{arccot}(c)}\cos^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ X_k<p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n\\
&\le \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n + \frac{1}{(1+o(1))\left(1+O\left(x^{(\eta-1)/2}\right)\right)}\\
&\qquad\qquad \times \frac{\int_0^{\operatorname{arccot}(c)}\sin^n(t)dt}{\int_0^{\operatorname{arccot}(c)}\cos^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n.
\end{aligned}$$

By the prime number theorem, we know

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n \le \sum_{p\le x^{1/2} \text{ prime}} p^{\frac{n}{2}} = (1+o(1))\frac{x^{1/2}}{\log x^{1/2}} x^{\frac{n}{4}} = o\left(x^{(2+n)/4}\right).$$

For large enough x, we have

$$\begin{aligned}
\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n &= \sum_{\substack{N(\omega)<x \text{ prime}\\ 0\le \arg\omega\le \operatorname{arccot}(c)}} b_p^n \\
&\ge \sum_{\substack{x-x^\eta<N(\omega)\le x-x^\eta+(x-x^\eta)^\eta \text{ prime}\\ \operatorname{arccot}(2c)<\arg(\omega)\le\operatorname{arccot}(c)}} b_p^n \\
&\ge \sin^n(\operatorname{arccot}(2c))(x-x^\eta)^{\frac{n}{2}} \sum_{\substack{x-x^\eta<N(\omega)\le x-x^\eta+(x-x^\eta)^\eta \text{ prime}\\ \operatorname{arccot}(2c)<\arg(\omega)\le\operatorname{arccot}(c)}} 1 \\
&= O\left(\frac{(x-x^\eta)^{(n/2+\eta)}}{\log(x-x^\eta)}\right) \\
&= O\left(\frac{x^{(n/2+\eta)}}{\log(x)}\right).
\end{aligned}$$

Therefore, for $n\ge 1$, note that $(2+n)/4-(n/2+\eta)=(2-n-4\eta)/4<0$, and so we have

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n = o\left(x^{(2-n-4\eta)/4}\log(x)\right) \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n = o(1) \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n.$$

Similarly, we obtain

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x^{1/2}\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n = o\left(x^{(2-n-4\eta)/4}\log(x)\right) \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n = o(1) \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n.$$

Therefore, noting that $(1+o(1))\left(1+O\left(x^{(\eta-1)/2}\right)\right)=1+o(1)$, we have

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n \le (1+o(1))\frac{\int_0^{\operatorname{arccot}(c)}\cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)}\sin^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime}\\ p\le x\\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n,$$

and

$$\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n \le \frac{1}{1+o(1)} \frac{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt} \sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n.$$

Therefore, for large enough x, we have

$$(1+o(1))\frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt} \le \frac{\displaystyle\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\displaystyle\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n} \le (1+o(1))\frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt}.$$

Now, letting $x \to \infty$, we have

$$\lim_{x\to\infty} \frac{\displaystyle\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\displaystyle\sum_{\substack{p\equiv 1 \pmod 4 \text{ prime} \\ p\le x \\ p=a_p^2+b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}(c)} \cos^n(t)dt}{\int_0^{\operatorname{arccot}(c)} \sin^n(t)dt}.$$

This completes the proof.

3.3.3 Proof of Theorem 3.2.2

The proof follows the same strategy as the proof of Theorem 3.2.1.

Let $c \ge 1$ be a constant. Suppose a prime $p \equiv 1 \pmod 3$ satisfies $p = a_p^2 + a_p b_p + b_p^2$ for positive integers a_p and b_p such that $0 < cb_p < a_p$. Let $\omega = a_p + b_p\frac{1+\sqrt{-3}}{2} = \cos(t) + \sin(t)i$. We have $a_p = \cos(t) - \frac{\sin(t)}{\sqrt{3}}$ and $b_p = \frac{2\sin(t)}{\sqrt{3}}$, which implies that $\omega = a_p + \frac{1+\sqrt{-3}}{2}b_p \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ satisfies $0 < \arg\omega < \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)$. In particular, when $c = 1$, we have $0 < \arg\omega < \frac{\pi}{6}$. We summarize the difference between the two situations in Table 3.2:

Let $K = \mathbb{Q}(\sqrt{-3})$, and let $\mu = \nu = 1$ in Theorem 3.3.1. Then, we have $h_K = 1$, $w_K = 8$,

$p \equiv 1 \pmod 4$	$p \equiv 1 \pmod 3$
$p = a_p^2 + b_p^2$	$p = a_p^2 + a_p b_p + b_p^2$
$\omega = a_p + b_p i$ is a prime in $\mathbb{Z}[i]$	$\omega = a_p + b_p \frac{1+\sqrt{-3}}{2}$ is a prime in $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$
$c = 1$ $0 < b_p < a_p$ $1 < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \frac{\pi}{4}$	$c = 1$ $0 < b_p < a_p$ $\sqrt{3} < \frac{a_p + \frac{b_p}{2}}{\frac{\sqrt{3}b_p}{2}} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \frac{\pi}{6}$
general c $0 < cb_p < a_p$, $c \geq 1$ $c < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}(c)$	general c $0 < cb_p < a_p$, $c \geq 1$ $\frac{2c+1}{\sqrt{3}} < \frac{a_p + \frac{b_p}{2}}{\frac{\sqrt{3}b_p}{2}} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)$

Table 3.3: $x^2 + y^2$ vs. $x^2 + xy + y^2$

and $\varphi(\mu) = 1$. For a constant $c \geq 1$, we denote

$$R(X) = \{z \in \mathbb{C} : 0 < \arg(z) < \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right), X < |z|^2 \leq X + X^\eta\}.$$

Then, we have

$$\sum_{\substack{\omega = a_p + b_p \frac{1+\sqrt{-3}}{2} \in R(X) \\ N(\omega) \text{ prime} \\ \theta_1 < \arg(\omega) < \theta_2}} 1 = \sum_{\substack{p \equiv 1 \pmod 3 \text{ prime} \\ X < p \leq X + X^\eta \\ p = a_p^2 + a_p b_p + b_p^2,\ 0 < cb_p < a_p \\ \theta_1 < \operatorname{arccot}\left(\frac{a_p + \frac{b_p}{2}}{\frac{\sqrt{3}b_p}{2}}\right) < \theta_2}} 1 \sim (\theta_2 - \theta_1) \times \frac{4X^\eta}{\pi \log X},$$

as $X \to \infty$, when $0 < \theta_1 < \theta_2 < \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)$ and $X^{\eta-1} < \theta_2 - \theta_1$.

Let $n_X = \left\lfloor \frac{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}{\theta_X} \right\rfloor + 1$ for $\theta_X = 2X^{\eta-1}$. Again, we divide $R(X)$ into n_X smaller regions:

$$R(X)_j = \{z \in \mathbb{C} : (j-1)\theta_X < \arg z \leq j\theta_X, X < |z|^2 \leq X + X^\eta\}$$

for $1 \leq j \leq n_X - 1$, and

$$R(X)_{n_X} = \left\{z \in \mathbb{C} : (n_X - 1)\theta_X < \arg z \leq \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right), X < |z|^2 \leq X + X^\eta\right\}.$$

For all primes inside the small region $R(X)_j$, we bound their real parts and imaginary parts accord-

ingly, sum them up and use Riemann sums to bound the sums from above and below. Arguing as before, we obtain

$$\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} a_p^n$$

$$\leq (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\cos(t)-\frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt} \sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} b_p^n,$$

and

$$\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} a_p^n$$

$$\geq (1+o(1))(1-X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\cos(t)-\frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)} \left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt} \sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} b_p^n.$$

Next, we consider the region

$$R(x)=\left\{z\in\mathbb{C}: 0<\arg z\leq \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right), 0<|z|^2\leq x\right\}.$$

We split $R(x)$ into the union of smaller regions

$$R(X_i)=\left\{z\in\mathbb{C}: 0<\arg z\leq \operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right), X_i<|z|^2\leq X_i+X_i^{\eta}\right\},$$

where $1\leq i\leq k$, $X_1+X_1^{\eta}=x$, $X_i+X_i^{\eta}=X_{i-1}$ for $2\leq i\leq k$, and $X_k<x^{1/2}\leq X_{k-1}$, which implies $X_k=O(x^{1/2})$.

Summing up the corresponding a_p^n and b_p^n from all small regions $R(X_i)$, and using the prime number theory to show that the inner most sector does not contain many primes, arguing as in the

previous section, we obtain that for large enough x,

$$(1+o(1))\frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\cos(t)-\frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt} \leq \frac{\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} b_p^n}$$
$$\leq (1+o(1))\frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\cos(t)-\frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt},$$

Now, letting $x\to\infty$, we have

$$\lim_{x\to\infty}\frac{\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum_{\substack{p\equiv 1 \pmod 3 \text{ prime} \\ p\leq x \\ p=a_p^2+a_pb_p+b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\cos(t)-\frac{\sin(t)}{\sqrt{3}}\right)^n dt}{\int_0^{\operatorname{arccot}\left(\frac{2c+1}{\sqrt{3}}\right)}\left(\frac{2\sin(t)}{\sqrt{3}}\right)^n dt}.$$

3.3.4 Proof of Theorem 3.2.3

We only give a sketch of the proof since the idea is the same as the previous two proofs.

Let $c\geq 1$ be a constant. Suppose a prime $p\equiv 1$, 2, or 4 $\pmod 7$ satisfies $p=2a_p^2+3a_pb_p+2b_p^2$ for integers a_p and b_p, such that $0<c|b_p|<a_p$. Let $\omega=a_p+\frac{-1+\sqrt{-7}}{2}(a_p+b_p)=\cos(t)+\sin(t)i$. We have $a_p=\cos(t)+\frac{\sin(t)}{\sqrt{7}}$ and $b_p=\frac{\sin(t)}{\sqrt{7}}-\cos(t)$, which implies that $\omega=a_p+\frac{-1+\sqrt{-7}}{2}(a_p+b_p)\in\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ satisfies $\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)<\arg\omega<\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)$. We summarize the difference between the two situations in Table 3.3.

Let $K=\mathbb{Q}(\sqrt{-7})$, and let $\mu=\nu=1$ in Theorem 3.3.1. Then, we have $h_K=1$, $w_K=2$, and $\varphi(\mu)=1$. For a constant $c\geq 1$, we denote the region

$$R(X)=\left\{z\in\mathbb{C}:\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)<\arg(\omega)<\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right),X<|z|^2\leq X+X^\eta\right\}.$$

$p \equiv 1 \pmod 4$	$p \equiv 1, 2, 4 \pmod 7$
$p = a_p^2 + b_p^2$	$p = 2a_p^2 + 3a_p b_p + 2b_p^2$
$\omega = a_p + b_p i$ is a prime in $\mathbb{Z}[i]$	$\omega = a_p + (a_p + b_p)\frac{-1+\sqrt{-7}}{2}$ is a prime in $\mathbb{Z}\left[\frac{-1+\sqrt{-7}}{2}\right]$
$c = 1$ $0 < b_p < a_p$ $1 < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \frac{\pi}{4}$	$c = 1$ $0 < \lvert b_p \rvert < a_p$ $0 < \frac{a_p - b_p}{\sqrt{7}(a_p + b_p)} = \cot(\arg(\omega)) < \infty$ $0 < \arg(\omega) < \frac{\pi}{2}$
general c $0 < cb_p < a_p$, $c \geq 1$ $c < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}(c)$	general c $0 < c\lvert b_p \rvert < a_p$, $c \geq 1$ $\frac{c-1}{\sqrt{7}(c+1)} < \frac{a_p - b_p}{\sqrt{7}(a_p + b_p)} = \cot(\arg(\omega)) < \frac{c+1}{\sqrt{7}(c-1)}$ $\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right) < \arg(\omega) < \operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)$

Table 3.4: $x^2 + y^2$ vs. $2x^2 + 3xy + 2y^2$

Then, we have

$$\sum_{\substack{\omega = a_p + (a_p+b_p)\frac{-1+\sqrt{-7}}{2} \in R(X) \\ N(\omega) \text{ prime} \\ \theta_1 < \arg(\omega) < \theta_2}} 1 = \sum_{\substack{p \equiv 1,2,4 \pmod 7 \text{ prime} \\ X < p \leq X + X^\eta \\ p = 2a_p^2 + 3a_p b_p + 2b_p^2,\ 0 < c\lvert b_p \rvert < a_p \\ \theta_1 < \operatorname{arccot}\left(\frac{a_p - b_p}{\sqrt{7}(a_p + b_p)}\right) < \theta_2}} 1 \sim (\theta_2 - \theta_1) \times \frac{X^\eta}{\pi \log X},$$

as $X \to \infty$, when $\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right) < \theta_1 < \theta_2 < \operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)$ and $X^{\eta-1} < \theta_2 - \theta_1$.

Let $n_X = \left\lfloor \frac{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right) - \operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}{\theta_X} \right\rfloor + 1$ for $\theta_X = 2X^{\eta-1}$. Again, we divide $R(X)$ into n_X smaller regions:

$$R(X)_j = \left\{ z \in \mathbb{C} : \operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right) + (j-1)\theta_X < \arg z \leq \operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right) + j\theta_X, \right.$$
$$\left. X < |z|^2 \leq X + X^\eta \right\}$$

for $1 \leq j \leq n_X - 1$, and

$$R(X)_{n_X} = \left\{ z \in \mathbb{C} : \operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right) + (n_X - 1)\theta_X < \arg z < \operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right), \right.$$
$$\left. X < |z|^2 \leq X + X^\eta \right\}.$$

For all primes inside the small region $R(X)_j$, we bound their real parts and imaginary parts accord-

ingly, sum them up and use Riemann sums to bound the sums from above and below. Arguing as before, we obtain

$$\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n$$
$$\leq (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}}+\cos(t)\right)^n dt}{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}}-\cos(t)\right)^n dt} \sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n,$$

and

$$\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n$$
$$\geq (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}}+\cos(t)\right)^n dt}{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)} \left(\frac{\sin(t)}{\sqrt{7}}-\cos(t)\right)^n dt} \sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n.$$

Next, we consider the region

$$R(x)=\left\{z\in\mathbb{C}:\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)\leq \arg z\leq \operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right), 0<|z|^2\leq x\right\}.$$

We split $R(x)$ as the union of smaller regions

$$R(X_i)=\left\{z\in\mathbb{C}:\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)\leq \arg z\leq \operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right), X_i<|z|^2\leq X_i+X_i^{\eta}\right\},$$

where $1\leq i\leq k$, $X_1+X_1^{\eta}=x$, $X_i+X_i^{\eta}=X_{i-1}$ for $2\leq i\leq k$, and $X_k<x^{1/2}\leq X_{k-1}$, which implies $X_k=O(x^{1/2})$.

Summing up the corresponding a_p^n and b_p^n from all small regions $R(X_i)$, and using the prime number theory to show the inner most sector does not contain many primes, arguing as in the

previous sections, we obtain that for large enough x,

$$(1+o(1))\frac{\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}+\cos(t)\right)^n dt}{\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}-\cos(t)\right)^n dt} \leq \frac{\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n}{\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n}$$
$$\leq (1+o(1))\frac{\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}+\cos(t)\right)^n dt}{\int_{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}^{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}-\cos(t)\right)^n dt}.$$

Now, letting $x \to \infty$, we have

$$\lim_{x\to\infty}\frac{\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} a_p^n}{\sum_{\substack{p\equiv 1,2,4 \pmod 7 \text{ prime} \\ p\leq x \\ p=2a_p^2+3a_pb_p+2b_p^2,\ 0<c|b_p|<a_p}} b_p^n} = \frac{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}+\cos(t)\right)^n dt}{\int_{\operatorname{arccot}\left(\frac{c-1}{\sqrt{7}(c+1)}\right)}^{\operatorname{arccot}\left(\frac{c+1}{\sqrt{7}(c-1)}\right)}\left(\frac{\sin(t)}{\sqrt{7}}-\cos(t)\right)^n dt}.$$

3.3.5 Proof of Theorem 3.2.4

Again we only give a sketch of the proof.

Let $c > 0$ be a constant. Suppose a prime $p \equiv 1$ or $3 \pmod 8$ satisfies $p = a_p^2 + 2b_p^2$ for positive integers a_p and b_p, such that $0 < cb_p < a_p$. Let $\omega = a_p + \sqrt{-2}b_p = \cos(t) + \sin(t)i$. We have $a_p = \cos(t)$ and $b_p = \frac{\sin(t)}{\sqrt{2}}$, which implies that $\omega = a_p + \sqrt{-2}b_p \in \mathbb{Z}\left[\sqrt{-2}\right]$ satisfies $0 < \arg(\omega) < \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)$. We summarize the difference of the two situations in Table 3.4.

Let $K = \mathbb{Q}(\sqrt{-2})$, and let $\mu = \nu = 1$ in Theorem 3.3.1. Then, we have $h_K = 1$, $w_K = 2$, and $\varphi(\mu) = 1$. For a constant $c \geq 1$, we denote the region

$$R(X) = \left\{ z \in \mathbb{C} : 0 < \arg(z) < \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right), X < |z|^2 \leq X + X^{\eta} \right\}.$$

$p \equiv 1 \pmod 4$	$p \equiv 1, 3 \pmod 8$
$p = a_p^2 + b_p^2$	$p = a_p^2 + 2b_p^2$
$\omega = a_p + b_p i$ is a prime in $\mathbb{Z}[i]$	$\omega = a_p + b_p\sqrt{-2}$ is a prime in $\mathbb{Z}\left[\sqrt{-2}\right]$
$c = 1$ $0 < b_p < a_p$ $1 < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \frac{\pi}{4}$	$c = 1$ $0 < b_p < a_p$ $\frac{1}{\sqrt{2}} < \frac{a_p}{\sqrt{2}b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}\left(\frac{1}{\sqrt{2}}\right)$
general c $0 < cb_p < a_p$, $c \geq 1$ $c < \frac{a_p}{b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}(c)$	general c $0 < cb_p < a_p$, $c > 0$ $\frac{c}{\sqrt{2}} < \frac{a_p}{\sqrt{2}b_p} = \cot(\arg(\omega))$ $0 < \arg(\omega) < \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)$

Table 3.5: $x^2 + y^2$ vs. $x^2 + 2y^2$

Then, we have

$$\sum_{\substack{\omega = a_p + \sqrt{-2}b_p \in R(X) \\ N(\omega) \text{ prime} \\ \theta_1 < \arg\omega < \theta_2}} 1 = \sum_{\substack{p \equiv 1,3 \pmod 8 \text{ prime} \\ X < p \leq X + X^\eta \\ p = a_p^2 + 2b_p^2,\ 0 < cb_p < a_p \\ \theta_1 < \operatorname{arccot}(a_p/\sqrt{2}b_p) < \theta_2}} 1 \sim (\theta_2 - \theta_1) \times \frac{X^\eta}{\pi \log X},$$

as $X \to \infty$, when $0 < \theta_1 < \theta_2 < \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)$ and $X^{\eta-1} < \theta_2 - \theta_1$.

Let $n_X = \left\lfloor \frac{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}{\theta_X} \right\rfloor + 1$ for $\theta_X = 2X^{\eta-1}$. Again, we divide $R(X)$ into n_X smaller regions:

$$R(X)_j = \{z \in \mathbb{C} : (j-1)\theta_X < \arg z \leq j\theta_X, X < |z|^2 \leq X + X^\eta\}$$

for $1 \leq j \leq n_X - 1$, and

$$R(X)_{n_X} = \left\{ z \in \mathbb{C} : (n_X - 1)\theta_X < \arg z \leq \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right), X < |z|^2 \leq X + X^\eta \right\}.$$

For all primes inside the small region $R(X)_j$, we bound their real parts and imaginary parts accordingly, sum them up and use Riemann sums to bound the sums from above and below. Similarly, we

obtain

$$\sum_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n$$

$$\leq (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} (\cos(t))^n\, dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} \left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt} \sum_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n,$$

and

$$\sum_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n$$

$$\geq (1+o(1))(1+X^{\eta-1})^{\frac{n}{2}} \frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} (\cos(t))^n\, dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)} \left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt} \sum_{\substack{p\equiv 1,3 \pmod 8 \text{ prime} \\ X<p\leq X+X^{\eta} \\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n.$$

Next, we consider the region

$$R(x) = \left\{ z\in\mathbb{C} : 0<\arg(z)\leq \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right), 0<|z|^2\leq x \right\}.$$

We split $R(x)$ as the union of smaller regions

$$R(X_i) = \left\{ z\in\mathbb{C} : 0<\arg z\leq \operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right), X_i<|z|^2\leq X_i+X_i^{\eta} \right\},$$

where $1\leq i\leq k$, $X_1+X_1^{\eta}=x$, $X_i+X_i^{\eta}=X_{i-1}$ for $2\leq i\leq k$, and $X_k<x^{1/2}\leq X_{k-1}$, which implies $X_k=O(x^{1/2})$.

Summing up the corresponding a_p^n and b_p^n from all small regions $R(X_i)$, and using the prime number theory to argue that the inner most sector does not contain many primes, arguing as in the

previous sections, we obtain that for large enough x,

$$(1+o(1))\frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}(\cos(t))^n\,dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}\left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt} \leq \frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\leq x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\leq x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n} \leq (1+o(1))\frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}(\cos(t))^n\,dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}\left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt}.$$

Now, letting $x\to\infty$, we have

$$\lim_{x\to\infty}\frac{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\leq x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} a_p^n}{\sum\limits_{\substack{p\equiv 1,3 \pmod 8 \text{ prime}\\ p\leq x\\ p=a_p^2+2b_p^2,\ 0<cb_p<a_p}} b_p^n} = \frac{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}(\cos(t))^n\,dt}{\int_0^{\operatorname{arccot}\left(\frac{c}{\sqrt{2}}\right)}\left(\frac{\sin(t)}{\sqrt{2}}\right)^n dt}.$$

3.4 Future Projects

The main theorems in this chapter are related to very specific quadratic forms, which are x^2+y^2, x^2+xy+y^2, $2x^2+3xy+2y^2$, and x^2+2y^2. We can generalize the results in many ways.

For symmetric quadratic forms $ax^2+bxy+ay^2$, we discussed in Section 3.1.3 symmetric quadratic forms with discriminant D such that $h(D)=1$. Those forms are easier to deal with. It is natural to ask whether we can deal with quadratic forms with discriminant D such that $h(D)\geq 2$. In that case, the primes might be harder to describe, but we can still try to evaluate the same type of ratios as in Sun's conjectures.

For non-symmetric quadratic forms, we discussed in Section 3.1.4 quadratic forms of the form x^2+ny^2, in particular, Theorem 3.2.4 is related to the quadratic form x^2+2y^2. We can try to prove a general result that deals with all quadratic forms x^2+ny^2. More generally, for primes in arithmetic progressions represented by $ax_p^2+bx_py_p+cy_p^2$, where $a\neq c$ and $b\neq 0$, we can again sum up all x_p, divide the sum by the sum of all y_p, and see whether the limit exists or not.

After we deal with all quadratic forms, we can move on to explore primes represented by cubic forms with two variables, and forms of higher degrees with two variables, and even with more than two variables. As they do not relate directly to quadratic forms, we will need to explore other avenues to solve the questions.

Bibliography

[1] J. Brown, K. James, and H. Li. Sun's conjecture on Gaussian primes. submitted, 2017.

[2] Y.C. Cai. A remark on Chen's theorem. II. *Chin. Ann. Math. Ser. B*, 29(6):687–698, 2008.

[3] Y.C. Cai. A remark on Chen's theorem with small primes. *Taiwanese J. Math.*, 19(4):1183–1202, 2015.

[4] J.R. Chen. On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Kexue Tongbao (Foreign Lang. Ed.)*, 17:385–386, 1966.

[5] J.R. Chen. On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica*, 16(2):151–176, 1973.

[6] D. Corbit. Conjecture on odd numbers. *sci.math posting*, Nov 19, 1999.

[7] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013.

[8] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000.

[9] A. W. Dudek. On the sum of a prime and a square-free number. *Ramanujan J.*, 42(1):233–240, 2017.

[10] T. Estermann. On the representations of a number as the sum of a prime and a quadratfrei number. *Journal of the London Mathematical Society*, s1-6(3):219–221, 1931.

[11] H. Halberstam and H. E. Richert. *Sieve methods*. Academic Press, London-New York, 1974.

[12] H. Helfgott. The ternary Goldbach conjecture. *Gac. R. Soc. Mat. Esp.*, 16(4):709–726, 2013.

[13] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[14] K. James and P. Pollack. Extremal primes for elliptic curves with complex multiplication. *Journal of Number Theory*, 172:383 – 391, 2017.

[15] H. Li. On the representation of a large integer as the sum of a prime and a square-free number with at most three prime divisors. *Ramanujan J.*, pages 1–18, May 16, 2018.

[16] W.C. Lu. Exceptional set of Goldbach number. *J. Number Theory*, 130(10):2359–2392, 2010.

[17] M. Maknys. On the distance between consecutive prime ideal numbers in sectors. *Acta Mathematica Hungarica*, 42(1):131–138, Mar 1983.

[18] J. Maynard. Small gaps between primes. *Ann. Math. (2)*, 181(1):383–413, 2015.

[19] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[20] C.D. Pan, X.X. Ding, and Y. Wang. On the representation of every large even integer as a sum of a prime and an almost prime. *Sci. Sinica*, 18(5):599–610, 1975.

[21] DHJ Polymath. Variants of the Selberg sieve, and bounded intervals containing many primes. *Research in the Mathematical Sciences*, 1(1):12, Oct 2014.

[22] H. E. Richert. Selberg's sieve with weights. *Mathematika*, 16:1–22, 1969.

[23] P. M. Ross. On Chen's theorem that each large even number has the form $p_1 + p_2$ or $p_1 + p_2p_3$. *J. London Math. Soc. (2)*, 10(4):500–506, 1975.

[24] Z.W. Sun. On Goldbach's conjecture. http://video.chaoxing.com/serie400051662.shtml, 2015.

[25] Z.W. Sun. Conjectures on representations involving primes. In *Combinatorial and additive number theory. II*, volume 220 of *Springer Proc. Math. Stat.*, pages 279–310. Springer, Cham, 2017.

[26] R. C. Vaughan. *The Hardy-Littlewood method*, volume 4 of *Cambridge Tracts in Mathematics*. Cambridge University Press, second edition, 1997.

[27] Y. Wang. The Goldbach conjecture. *Math. Medley*, 10(1):1–4, 1982.

[28] T. Yamada. Explicit Chen's theorem. *ArXiv e-prints*, November 2015.

[29] Y.T. Zhang. Bounded gaps between primes. *Ann. of Math.*, 179(3):1121–1174, 2014.