Chapter 1

Introduction and overview

1.1. Introduction

The history[1] of number theory is replete with examples of problems which can be explained in simple language to an eager primary school student. However, finding solutions to many such problems have taken centuries of concerted efforts by a wider community of mathematicians (amateur as well as professional). Some of these problems are still unsolved. Often, a study of these problems has resulted in deep insights and path-breaking ideas which have revolutionized mathematics. Some of these questions, including those covered in this book, originate from a common source going back several centuries.

Diophantus of Alexandria was a scholar in ancient Greece. Although little is known about his life, extant references indicate that he was born in the early part of the third century CE. He wrote a series of thirteen books titled *Arithmetica*. The book series is considered the earliest text in Western European history in which mathematical ideas and questions were explained using symbols. They contain several algebraic equations to which Diophantus sought solutions in integers. These textbooks became obscure in Western Europe during the period of the Dark Ages,

[1]This chapter is a modified version of an article titled "Additive problems in number theory" by the second named author in Blackboard (Mathematics Teachers' Association, India), Issue 3, 2021.

but some of the books were preserved by Byzantine scholars and were rediscovered in Rome in the fifteenth century. The *Arithmetica* became available to European scholars when Claude Bachet published a Latin translation of the six surviving books.

Bachet's translation soon gained the attention of mathematics lovers, among whom was a young French lawyer by the name of Pierre de Fermat. Fermat was a lawyer who pursued mathematics as a hobby in his free time, and made significant contributions to the subject. Some of his pertinent observations and insights were written on the margins of his copy of Bachet's translation and were rediscovered by his son a few years after Fermat passed away. An English translation of one such observation ([**59**, Page 3]) is as follows: *"Every number is a triangular number or the sum of two or three triangular numbers;* **every number is a square or the sum of two, three or four squares***; every number is a pentagonal number or the sum of two, three, four or five pentagonal numbers; and so on .... The precise statement of this very beautiful and general theorem depends on the number of angles. The theorem is based on the most diverse and abstruse mysteries of numbers, but I am not able to include the proof here."*

The general theorem that Fermat is referring to is about what are called polygonal numbers. The note implies that Fermat had a proof, and it does seem plausible that he did. This theorem was proved in its entirety by Augustin-Louis Cauchy in 1813. Our focus, however, will be on the highlighted part of Fermat's note above, namely the conjecture that every natural number can be written as a sum of at most four squares. It is possible that Diophantus was familiar with this conjecture. But, we find the first recorded statement by Bachet in 1621 (in his translation of *Arithmetica*), which is how Fermat became familiar with it. Bachet also verified it for every number less than 326. In 1748, Leonhard Euler wrote a letter to Christian Goldbach, which contains a fundamental step in the proof of the four square conjecture. This refers to an explicit identity which shows that a product of two numbers—each of which is a sum of at most four squares—is also a sum of at most four squares. Thus, it is sufficient to prove that every prime number can be written as a sum of at most four squares. This was done by Joseph Louis Lagrange in 1770 and the four square theorem is now named after him.

Theorem 1.1 (Lagrange's four square theorem)**.** *Every natural number is a sum of the squares of at most four natural numbers.*

Around the same time, the mathematician Edward Waring, in his book *Meditationes Algebraicae* conjectured a generalization of the four square theorem. He stated that every nonnegative integer is the sum of four squares, nine cubes, nineteen fourth powers *and so on*. The phrase "and so on" has the following precise expression.

Conjecture 1.2 (Waring's problem, 1770)**.** *For each positive integer $k \geq 2$, there exists a positive integer $g = g(k) \geq 2$ such that for any positive integer n, there exist g nonnegative integers $x_1, x_2, \ldots, x_g$ such that*

$$n = x_1^k + x_2^k + \cdots + x_g^k.$$

We note here that $g(k)$ is chosen to be the minimal positive integer with the above property. That is, there exists a natural number n which cannot be written as a sum of $[g(k) - 1]$ kth powers. Lagrange's theorem is the assertion that $g(2) = 4$. Moreover, as per Waring's conjecture, $g(3) = 9$ and $g(4) = 19$. As this book proceeds, we will be able to state and interpret Waring's problem in various elegant ways.

Waring's problem leads us to ask two questions: firstly, does $g(k)$ exist for every k? Secondly, can we find a precise formula for $g(k)$ for all k?

In a parallel correspondence, L. Euler and Goldbach also discussed fundamental questions about expressing all natural numbers > 1 as sums of finitely many primes. In this direction, Goldbach wrote a letter to L. Euler in 1742, in which he made the following conjectures.

Conjecture 1.3 (Goldbach's binary (strong) conjecture)**.** *Every even number $n \geq 4$ can be written as a sum of two primes.*

Conjecture 1.4 (Goldbach's ternary (weak) conjecture)**.** *Every odd number $n > 5$ can be written as a sum of three primes.*

One sees immediately that the strong conjecture implies the weak one. This follows from the observation that an odd $n > 5$ can be written as $3 + k$, where k is even and > 2.

The ternary Goldbach conjecture is essentially a theorem due to the pioneering work of Ivan M. Vinogradov who showed that the assertion is true for n sufficiently large. In one of the most interesting developments in the last decade, the full Goldbach ternary conjecture has been proved by Harald Helfgott, a mathematician at the University of Göttingen. However, the binary conjecture is still open.

The Goldbach conjectures present an interesting contrast between the additive and multiplicative properties of primes. By the Fundamental Theorem of Arithmetic, any natural number $n > 1$ can be written uniquely as a product of powers of primes,

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},\ a_i \geq 1.$$

We now consider a number c. Can we write **any** $n > 1$ as a product of at most c primes? The answer to this question is no. To see this, we note that there are infinitely many primes. Let us denote the nth prime number by p_n. Now, for any c, we have a number

$$n = p_1 p_2 \cdots p_{c+1},$$

which, by the Fundamental Theorem of Arithmetic, cannot be written as a product of at most c primes.

We now give an additive twist to the above question. Can we write any $n > 1$ as a *sum* of at most c primes? Goldbach's conjectures predict that not only do we have an affirmative answer to this question, but also that the value of c is as small as 3.

The problems of Goldbach and Waring are often combined into a single question called the Goldbach-Waring problem which asks: when can we write a natural number n as a sum

$$n = m_1^k + m_2^k + \cdots + m_g^k,$$

where the m_i belong to a prescribed set S. If $k = 1$ and S is the set of primes, we have the Goldbach problem. If $k \geq 2$ and S is the set of natural numbers, we have the Waring problem. This perspective opens the door to a vista of new questions to which the methods of this book can be applied and the limitations of these methods explored.

This book is meant to be a survey of various additive problems in number theory related to Waring's problem and the conjectures of Goldbach. It is aimed at undergraduate students eager to acquire a knowledge of these problems. Our endeavour is to introduce students to fundamental concepts in number theory and to familiarise them with important techniques in additive number theory such as the circle method in a self-contained manner. As such, this book will be accessible to a student who has had introductory courses in real and complex analysis, but who is learning number theory for the first time. This book is organized into the following chapters.

1.2. Preparatory chapters

1.2.1. Elementary number theory. Since our aim is to be as self-contained as possible, we start with a review of basic notions in number theory from Chapters 2–4.

In Chapter 2, we introduce the student to fundamental notions at the heart of the study of numbers, such as divisibility, the Euclidean algorithm for finding the greatest common divisor of two integers, prime numbers and the Fundamental Theorem of Arithmetic.

In Chapter 3, we introduce the notion of arithmetic functions, that is, complex-valued functions defined on the set of natural numbers. We introduce tools from analysis to study the behavior of various arithmetic functions which are relevant in additive number theory.

In Chapter 4, we review basic notions and properties of congruence arithmetic. After learning the basic language of congruence arithmetic to express important divisibility properties of integers, the reader will learn important techniques to find solutions of what are called congruence equations. The contents of this chapter form a vital and foundational component of any study in number theory: in the context of this textbook, we will also provide details of specific theorems in congruence arithmetic which are necessary to address the questions of Waring and Goldbach.

1.2.2. Analytic number theory. In Chapter 5, we approach the study of prime numbers from an "analytic" viewpoint. We start by interpreting properties of prime numbers covered in the previous chapters in the language of infinite series. For example, the divergence of the series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

implies that there are infinitely many prime numbers. In this chapter, we cover mathematical tools which have been carefully developed over many centuries to understand prime numbers. One such tool is the well-known Riemann zeta function. The zeta function is defined as

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

for a complex number $s \in \mathbb{C}$ with real part $\Re(s) > 1$. Much of the early work on the zeta function viewed this function for real numbers $s > 1$.

The study of the zeta function as a real-valued function has immediate connections with classical properties of prime numbers. For example, the fundamental theorem of arithmetic is equivalent to the assertion that for any real number $s > 1$,

$$\zeta(s) = \prod_p \left(\sum_{k=0}^{\infty} \frac{1}{p^{ks}} \right) = \prod_p \left(1 - \frac{1}{p^s} \right)^{-1}.$$

In a breakthrough paper written in 1859 [**63**], Bernhard Riemann studied the zeta function $\zeta(s)$ as a function of a *complex* variable s and outlined a detailed program linking the complex-analytic properties of $\zeta(s)$ with the distribution properties of prime numbers. He made two important observations. Firstly, the zeta function can be analytically continued to the entire complex plane except the point $s = 1$. Secondly, the zero-free regions of this function (that is, the regions where $\zeta(s) \neq 0$) in the half-plane $\Re(s) > 0$ have a direct bearing on estimates for the prime-counting function $\pi(x)$, defined as the number of primes up to x for large values of x.

In this context, Riemann made a conjecture, the well-known Riemann hypothesis, which predicts that any nonreal zero of $\zeta(s)$ have real part equal to $1/2$. This conjecture still remains unproved and has motivated a good deal of mathematics over the last 160 years.

The theme outlined by Riemann can be generalized to series of the form

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

for various interesting arithmetic functions $f(n)$. In particular, we are interested in L-functions of the form

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a special periodic complex-valued function called a Dirichlet character. L-functions were defined by Peter G. L. Dirichletin order to study the distribution properties of primes in arithmetic progressions. As with the classical zeta function of Riemann, the study of zero-free regions of these L-functions has direct applications to the function $\pi(x, q, a)$ which counts the number of primes up to x lying in the arithmetic progression $\{kq + a : k \in \mathbb{Z}\}$. Here, $\mathbb{Z}$ is the set of integers.

This analytic perspective is described in Chapter 5. More precisely, we discuss the following topics:

- The Riemann zeta function and more generally, the Dirichlet series associated to suitable arithmetic functions. We derive their complex-analytic properties and how these properties lead to estimates for the partial sums $\sum_{n\leq x} f(n)$.
- A sharp version of the prime number theorem states that

$$\pi(x) = \operatorname{li} x + \mathrm{O}\Big(\frac{x}{(\log x)^C}\Big)$$

for any $C > 1$ and $\operatorname{li} x$ is the logarithmic integral defined by

$$\operatorname{li} x := \int_2^x \frac{dt}{\log t}.$$

We review a classical proof for the error term in the above asymptotic using information about the zero-free regions of the Riemann zeta function.

- Fundamental properties of Dirichlet characters and L-functions associated to them.
- A classical theorem of Carl L. Siegel and Arnold Walfisz which states that if a and q are coprime integers, then

$$\pi(x, q, a) = \frac{1}{\phi(q)} \operatorname{li} x + \mathrm{O}\Big(\frac{x}{(\log x)^C}\Big)$$

for any $C > 1$. Here, $\phi(q)$ denotes the number of integers $1 \leq n \leq q-1$ which are coprime to q. The main idea in the proof of the Siegel–Walfisz theorem is an extension of the argument to prove the (sharp) prime number theorem stated above and requires a discussion of zero-free regions of Dirichlet L-functions.

The above topics have been covered in several expositions (see [**16**], [**39**], [**43**], [**53**], [**54**]). Our aim is to provide to the reader a selective review of essential topics required in the study of additive problems covered in this textbook.

1.3. Early developments in the study of Waring's problem

With the preliminaries in place, we move to the first additive problem of interest to us, namely Waring's problem.

1.3.1. Introduction to Waring's problem. In Chapter 6, we put together theorems learned in the earlier chapters on elementary number theory to prove Lagrange's four square theorem (Theorem 1.1). We then introduce Waring's problem (Conjecture 1.2) and the interesting questions that it leads to. After a brief review of early developments in the study of Waring's problem, we discuss a conjecture of Johann Albrecht Euler regarding the value of $g(k)$ and interesting developments around it.

1.3.2. Additive problems and Schnirelmann density. In the 1930s, the Russian mathematician Lev Schnirelmann introduced a new perspective to study additive problems in number theory. Let us take a subset B of the set $\mathbb{N}$ of natural numbers. For $m \in \mathbb{N}$, Schnirelmann defined the "sumset"

$$mB = \left\{ \sum_{i=1}^{m} b_i \ : \ b_i \in B \cup \{0\} \right\}.$$

He also defined a new notion of density of subsets of $\mathbb{N}$, called the Schnirelmann density and showed that if B has positive Schirelmann density, then $mB = \mathbb{N}$ for some some $m \in \mathbb{N}$. In other words, every natural number can be written as a sum of at most m elements from the set B. His ideas lead to neat expressions for additive problems such as Waring's problem and the Goldbach conjectures. In the context of Waring's problem, we are interested in the sets

$$A_k := \{n^k \ : \ n \in \mathbb{N}\}, \tag{1.1}$$

where $k \geq 2$ is a fixed positive integer. Waring's problem asks if, for each k, one can find a natural number $g = g(k)$ such that $gA_k = \mathbb{N}$. Schnirelmann's observation is not directly applicable to A_k since it has Schnirelmann density 0. Instead, one first shows that there exists $l \in \mathbb{N}$ such that $\delta(lA_k) > 0$. Applying Schnirelmann's observation to the set lA_k, there exists $m \in \mathbb{N}$ such that $mlA_k = \mathbb{N}$. The existence of $l \in \mathbb{N}$ such that $\delta(lA_k) > 0$ was shown by Linnik [**47**] in 1943. This solves Waring's problem (Conjecture 1.2) as we can now take $g = ml$. Linnik's

method was further simplified by Loo Keng Hua [**40**, Chapters 18 and 19].

In Chapter 7, we learn about the Schnirelmann density of subsets of $\mathbb{N}$. We study the properties of the Schnirelmann density and its connection with sumsets. Finally, we outline Linnik's solution of Waring's problem combined with a theorem of Hua on exponential sums.

1.4. The method of exponential sums

The additive properties of a subset of natural numbers are intricately connected to certain associated exponential sums. This connection lies at the heart of most of the work done on the Goldbach conjectures as well as Waring's problem.

For a real number α, let

$$e(\alpha) := e^{2\pi i\alpha} = \cos 2\pi\alpha + i \sin 2\pi\alpha.$$

The method of exponential sums originates in the following integral identity: for an integer m,

$$\int_0^1 e(m\alpha)d\alpha = \begin{cases} 1 & \text{if } m = 0 \\ 0 & \text{if } m \neq 0. \end{cases} \tag{1.2}$$

To use this identity for our purposes, let us take a set $\mathcal{A} \subset \mathbb{N} \cup \{0\}$. For a natural number n, we define the exponential sum

$$f(\alpha) := \sum_{r\in\mathcal{A}, r\leq n} e(r\alpha).$$

Then,

$$f^g(\alpha) = \sum_{r_1,r_2\ldots,r_g\in\mathcal{A}, r_i\leq n} e((r_1 + r_2 + \cdots + r_g)\alpha).$$

Using the integral identity (1.2), we deduce that

$$\int_0^1 f^g(\alpha)e(-n\alpha)d\alpha = \#\{(r_1, r_2 \ldots, r_g) \in \mathcal{A}^g \,:\, r_1 + r_2 + \cdots + r_g = n\}.$$

A question about expressing n as a sum of m elements of $\mathcal{A}$ now reduces to the following question.

Question 1.5. *Does there exist a positive number m such that*

$$\int_0^1 f^m(\alpha)e(-n\alpha)d\alpha > 0$$

for all n, or at least for all sufficiently large n ?

Clearly, the above integral depends on the exponential sum $f(\alpha)$ and in Chapter 8, we learn techniques to evaluate such sums corresponding to sets $\mathcal{A}$ connected with Waring's problem as well as the Goldbach conjectures. We also learn how the values of these sums at an irrational number α are influenced by the Diophantine approximation properties of α. This connection proves extremely useful in the evaluation of the above integral.

1.5. Origins of the circle method and applications to additive problems

As in the previous section, let us consider a subset $\mathcal{A} \subset \mathbb{N} \cup \{0\}$. Additive questions described in this article can be modified into the following general form.

Question 1.6. *Does there exist $g \in \mathbb{N}$ such that every $n \in \mathbb{N}$ can be written as a sum of g elements in $\mathcal{A}$?*

More precisely, let $r_{\mathcal{A},g}(n)$ be defined as

$$r_{\mathcal{A},g}(n) := \#\left\{(x_1, x_2, \dots, x_g) : x_i \in \mathcal{A}, \sum_{i=1}^{g} x_i = n\right\}.$$

That is,

$$r_{\mathcal{A},g}(n) = \int_0^1 (f(\alpha))^g e(-n\alpha) d\alpha, \qquad f(\alpha) = \sum_{m\in\mathcal{A},\, m\le n} e(m\alpha).$$

Does there exist a natural number g such that $r_{\mathcal{A},g}(n) > 0$ for each $n \in \mathbb{N}$ or, at least, for sufficiently large values of n?

A related question to ask is if we can find an exact formula for $r_{\mathcal{A},g}(n)$ for given g, $n \in \mathbb{N}$. Alternatively, for each g, can we determine the asymptotic growth of $r_{\mathcal{A},g}(n)$ as $n \to \infty$?

In 1918, Hardy and Ramanujan studied the above question through a complex-analytic approach which is referred to as the circle method. This method was originally developed in an epoch-making 1918 paper of Hardy and Ramanujan [**31**], in which they derived an asymptotic formula for the partition function $p(n)$, which denotes the number of representations of n as a sum of natural numbers less than or equal to n. The roots of their work go back further to one of the letters that Ramanujan had written to Hardy from India, which indicates that Ramanujan had a

rudimentary form of the circle method in mind. The reader can find the historical details in Chapter 5 of [**55**]. For the partition function studied by Hardy and Ramanujan, formulated in the language of Question 1.6, one considers $\mathcal{A} = \mathbb{N}$.

For Waring's problem, we take $\mathcal{A} = A_k \cup \{0\}$. Here, A_k is as defined in Equation (1.1). Let $\mathbb{P}$ denote the set of prime numbers. For the conjectures of Goldbach, we take $\mathcal{A} = \mathbb{P}$. For the binary conjecture, we take $g = 2$ and n is an even integer ≥ 4, whereas for the ternary conjecture, we take $g = 3$ and n is an odd integer ≥ 7. Further questions of Goldbach type could be asked for larger values of g.

After Ramanujan's early demise, Hardy and John E. Littlewood developed the method to derive asymptotic formulas in Waring's problem. They also treated questions of Goldbach type by the circle method. Later, Vinogradov [**77**] introduced new methods (most notably the method of exponential sums) that allowed for an unconditional treatment of the Goldbach conjectures.

The most fundamental observation in the application of the circle method to Waring's problem as well as the Goldbach conjectures is that the function $f(\alpha) = \sum_{m\in\mathcal{A},\, m\leq n} e(m\alpha)$ takes unusually large values at rational numbers $\alpha = a/q$ with suitably bounded denominators. So, we partition the interval $[0,1]$ into two parts: the **major arcs** $\mathfrak{M}$, which are unions of very tiny intervals around the rational numbers at which the function peaks and the **minor arcs**

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M},$$

which are the portions left behind in the unit interval after taking away the major arcs.

1.5.1. The circle method and Waring's problem. Between 1920 and 1928, Hardy and Littlewood applied the circle method to the evaluation of

$$\int_0^1 (f(\alpha))^g e(-n\alpha)d\alpha, \qquad f(\alpha) = \sum_{m\in A_k\cup\{0\},\, m\leq n} e(m\alpha).$$

They wrote a series of papers culminating in [**30**], in which they showed that for $g > 2^k$, one can obtain asymptotics for the above integral as $n \to \infty$. For this, one has to isolate the major and minor arcs and evaluate the integral $\int (f(\alpha))^g e(-n\alpha)d\alpha$ over each of them. One then obtains lower

bounds for $g = g(k)$ such that the main term will dominate the error term, leading to a positive value for $r_{A_k \cup \{0\},g}(n)$ for all $n \in \mathbb{N}$.

We describe the above work of Hardy and Littlewood on the application of the circle method to Waring's problem in Chapter 9.

1.5.2. The circle method and the Goldbach conjectures. In 1923, Hardy and Littlewood used the circle method to prove the ternary Goldbach conjecture for "sufficiently large" odd values of $n \geq C$ (under the assumption of the generalized Riemann hypothesis (GRH)). That is, under the condition that the GRH holds, any sufficiently large odd number n can be written as a sum of three primes. This was the first major development in the study of Goldbach conjectures since 1742.

In 1937, Russian mathematician Vinogradov introduced some remarkably new and beautiful ideas which circumvented the assumption of the generalised Riemann hypothesis to prove the result of Hardy and Littlewood. He proved the ternary Goldbach conjecture *unconditionally* for "sufficiently large" odd values $n \geq C$. Only recently did Helfgott show that we can assert this for $n > 5$.

Before we proceed further, we make some remarks about the use of the phrase "sufficiently large". The theorems of Hardy–Littlewood and Vinogradov were not able to specify an explicit value of C such that the ternary Goldbach conjecture would hold for all odd $n \geq C$. What they showed was that such a C exists. If one could provide an explicit value of C, then one can verify the conjecture for odd $n < C$ through computations and derive a complete proof of the ternary Goldbach conjecture (or disprove it if counterexamples exist). Therefore, three main challenges needed to be overcome before one could complete the treatment of Goldbach's conjectures.

(1) Make Vinogradov's theorem effective by establishing an explicit number C such that the ternary Goldbach conjecture holds for $n \geq C$.

(2) Verify the conjecture for $n < C$ case-by-case.

(3) If C is too large for our current computational resources, then refine C down to a value for which computational verification of $n < C$ is feasible.

These challenges were overcome through multiple developments which are encapsulated below.

- In 1956, K. G. Borodzkin [**7**] showed that the ternary Goldbach conjecture holds for all
$$n \geq C = 10^{4008659}.$$
- In 1989, Jing Run Chen and Tian Ze Wang [**12**] reduced C to 10^{43000} and in 1996, to 10^{7194} [**13**].
- In 1997, Jean-Marc Deshouillers, Gove W. Effinger, Herman te Riele and Dmitrii Zinoviev [**20**] proved the ternary Goldbach conjecture for **all** odd numbers $n > 5$, but conditionally on GRH.
- $C = 2 \cdot 10^{1346}$ was obtained by Ming-Chit Liu and Wang [**48**] in 2002. Until 2013, this remained the lowest known unconditional value for C.
- On the most powerful computers, computer verification of the conjecture can be done up to the order of 10^{30}. In fact, in 2013, Helfgott and David J. Platt [**37**] verified the conjecture for odd $n \leq 8.875 \cdot 10^{30}$.
- In 2013, Helfgott ([**34**], [**35**]) proved that the ternary Goldbach conjecture holds for odd $n \geq 10^{27}$. Since the conjecture had already been verified for $n \leq 10^{27}$ [**37**], Helfgott's result was the proverbial last nail in the coffin that led to a complete proof of the ternary Goldbach conjecture.

All the above results use the circle method.

In Chapter 10, we learn the application of the circle method to prove Vinogradov's assertion that the ternary Goldbach conjecture holds for sufficiently large odd values of n. We also make remarks about the limitations of the circle method in addressing the binary Goldbach conjecture.

Finally, in Chapter 11, we provide the reader a lightning tour of the circle method, and describe the underlying philosophy of this method. We mention references where the interested reader can further explore the circle method in greater depth. We also briefly indicate contemporary applications and generalizations of the circle method.

Chapter 7

Waring's problem

A fundamental contribution to additive number theory was made by Schnirelmann in the 1930s. Schnirelmann was motivated by the conjecture of Goldbach that every $n > 2$ can be written as a sum of at most two primes numbers if n is even and at most three primes if n is odd. Before the advent of sieve theory, Edmund Landau in 1912 challenged the mathematical community to show that there exists a positive integer C such that every natural number greater than 1 can be written as the sum of at most C prime numbers. Responding to this challenge, Schnirelmann was able to show that $C < 800,000$. In order to obtain his theorem, he related the existence of such a constant C to a new way of interpreting the density of the set of primes. This new notion of density, different from the notion of "natural" density, can be generalized to subsets of natural numbers and is amenable to several additive problems including the one posed by Waring. In this chapter, we introduce the notion of Schnirelmann density and show how it leads to a solution of Waring's problem following an approach used by Linnik.

7.1. Schnirelmann density

Let $A \subseteq \mathbb{N}$ and for every $n \geq 1$, let $A(n) = \#\{a \in A : a \leq n\}$. The **Schnirelmann density of** A**,** denoted by $\delta(A)$ is defined as

$$\delta(A) := \inf_{n \geq 1} \frac{A(n)}{n}.$$

We observe that $A(n) \geq \delta(A)n$ for all $n \geq 1$. We also observe that $0 \leq \delta(A) \leq 1$ and $\delta(A) = 1$ if and only if $A = \mathbb{N}$.

The Schnirelmann density is different from the **natural density** or **asymptotic density** $\sigma(A)$ defined as

$$\sigma(A) = \lim_{n\to\infty} \frac{A(n)}{n}.$$

While $\sigma(A)$ measures the asymptotic behavior of $\frac{A(n)}{n}$ for arbitrarily large values of n, the Schnirelmann density $\delta(A)$ is sensitive to all values of n. For example, if $\mathbb{E}$ and $\mathbb{O}$ denote the set of even and odd natural numbers respectively, then $\sigma(\mathbb{E}) = \sigma(\mathbb{O}) = 1/2$. On the other hand, $\delta(\mathbb{E}) = 0$ and $\delta(\mathbb{O}) = 1/2$.

Given two sets A and B of integers, let $A + B$ denote the sumset of A and B, that is, $A + B = \{a + b : a \in A,\ b \in B\}$. If A and B are subsets of $\mathbb{N}$, let $A \oplus B$ denote the set

$$A \oplus B := A \cup \{0\} + B \cup \{0\}.$$

More generally, let $A_1, A_2, \cdots, A_t \subseteq \mathbb{N}$. For any $i \geq 2$, let us define $\oplus_{i=1}^{t} A_i$ recursively as follows:

$$\oplus_{i=1}^{t} A_i := \left(\oplus_{i=1}^{t-1} A_i\right) \oplus A_t.$$

Furthermore, for any $m \in \mathbb{N}$ and $A \subseteq \mathbb{N}$, we denote

$$mA := \oplus_{i=1}^{m} A_i, \quad A_i = A \quad \text{for each } 1 \leq i \leq m.$$

The above concept of sums of sets helps us to restate Waring's conjecture (which we also call Waring's problem) in a simple and elegant manner. For $k \geq 2$, let us consider

$$A_k = \{n^k : n \in \mathbb{N}\}.$$

Waring's problem posits the existence of $g = g(k) \in \mathbb{N}$ such that $gA_k = \mathbb{N}$. In this sense, Lagrange's four square theorem is simply the assertion that $4A_2 = \mathbb{N}$.

One can reformulate the Goldbach problem also in a similar framework which was the original motivation for Schnirelmann. In order to understand his treatment of such problems, we start with some fundamental properties of $\delta(A)$ proved by him in 1936.

Theorem 7.1 (Schnirelmann, 1936)**.** *For any two subsets A and B of $\mathbb{N}$,*

$$\delta(A \oplus B) \geq \delta(A) + \delta(B) - \delta(A)\delta(B).$$

Proof. Suppose $A(n) = r$. We order the elements $a_i \leq n$ of A as $1 \leq a_1 < a_2 < a_3 \cdots < a_r \leq n$.

Let

$$B_1 := \{b \in B : b < a_1\}.$$

For $2 \leq i \leq r$, let

$$B_i := \{b \in B : a_{i-1} + b < a_i\}.$$

Finally, let

$$B_{r+1} := \{b \in B : a_r + b \leq n\}.$$

We denote $a_0 = 0$.

Observe that the sets $\{a_1, a_2, \cdots a_r\}$ and the sets $a_{i-1} + B_i$, $1 \leq i \leq r+1$ are disjoint subsets of $(A \oplus B)$, and each element in these sets is $\leq n$. For notational convenience, let us define $B(0) = 0$. From above, we have

$$(A \oplus B)(n) \geq A(n) + \sum_{i=1}^{r+1} |B_i|$$

$$\geq A(n) + B(a_1 - 1) + \sum_{i=2}^{r} B(a_i - a_{i-1} - 1) + B(n - a_r).$$

Combining the above inequality with the property that $B(n) \geq \delta(B)n$, we get that for every $n \geq 1$,

$$\begin{aligned}
(A \oplus B)(n) &\geq A(n) + \delta(B)\{(a_1 - 1) + \sum_{i=2}^{r}(a_i - a_{i-1} - 1) + (n - a_r)\} \\
&= A(n) + \delta(B)(n - r) \\
&= A(n) + \delta(B)(n - A(n)) \\
&= A(n)(1 - \delta(B)) + \delta(B)n \\
&\geq \delta(A)n(1 - \delta(B)) + \delta(B)n \\
&= n\left(\delta(A) + \delta(B) - \delta(A)\delta(B)\right).
\end{aligned}$$

This proves Theorem 7.1.

□

A more general version of Schnirelmann's theorem can be stated as follows:

Theorem 7.2. *For $A_1, A_2, \cdots, A_t \subseteq \mathbb{N}$,*

$$\delta(\oplus_{i=1}^{t} A_i) \geq 1 - \prod_{i=1}^{t}(1 - \delta(A_i)).$$

Proof. By Theorem 7.1,

$$\delta(A_1 \oplus A_2) \geq \delta(A_1) + \delta(A_2) - \delta(A_1)\delta(A_2) = 1 - (1 - \delta(A_1))(1 - \delta(A_2)).$$

This proves the theorem for $t = 2$. We now apply induction. We have,

$$\delta\left(\oplus_{i=1}^{t} A_i\right) = \delta\left(\oplus_{i=1}^{t-1} A_i \oplus A_t\right) \geq 1 - \left(1 - \delta\left(\oplus_{i=1}^{t-1} A_i\right)\right)(1 - \delta(A_t)).$$

By the induction hypothesis for $i = t - 1$,

$$\delta\left(\oplus_{i=1}^{t-1} A_i\right) \geq 1 - \prod_{i=1}^{t-1}(1 - \delta(A_i)),$$

that is,

$$1 - \delta\left(\oplus_{i=1}^{t-1} A_i\right) \leq \prod_{i=1}^{t-1}(1 - \delta(A_i)).$$

Therefore,

$$\begin{aligned}\delta\left(\oplus_{i=1}^{t} A_i\right) &\geq 1 - \left(1 - \delta\left(\oplus_{i=1}^{t-1} A_i\right)\right)(1 - \delta(A_t)) \\ &\geq 1 - (1 - \delta(A_t)) \prod_{i=1}^{t-1}(1 - \delta(A_i)).\end{aligned}$$

This proves the theorem for any $t \geq 2$. □

The Schnirelmann density of a subset B of $\mathbb{N}$ measures the "closeness" of B to $\mathbb{N}$. For example, $\delta(B) = 1$ if and only if $B = \mathbb{N}$. We now show that if $\delta(B)$ is greater than $1/2$, then $2B = \mathbb{N}$.

Lemma 7.3. *If $\delta(B) > 1/2$ for some $B \subseteq \mathbb{N}$, then $\delta(2B) = 1$. In other words, $2B = \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$. We will show that $n \in 2B$. If $n \in B$, then we are done. If $n \notin B$, let $B_n = \{b \in B : b < n\}$ and $B'_n = \{n - b : b \in B_n\}$. Clearly, $\#B_n = \#B'_n$. Also, $\#B_n = B(n)$, as $n \notin B$. Since $B_n \cup B'_n \subseteq \{1, 2, \cdots, n\}$, it is clear that $\#(B_n \cup B'_n) \leq n$.

Since $\delta(B) > 1/2$, we get

$$\#B_n = \#B'_n = B(n) > \frac{n}{2}.$$

Let us assume that B_n and B'_n are disjoint. This implies, $n < \#(B_n \cup B'_n)$, which contradicts the fact that $\#(B_n \cup B'_n) \leq n$. Hence, our assumption is false and B_n and B'_n are not disjoint. In other words, there exist $b_1, b_2 \in B$, with $b_1, b_2 < n$, such that $b_1 = n - b_2$, that is, $b_1 + b_2 = n$. This proves that $n \in 2B$.

This proves Lemma 7.3.

□

Theorem 7.4 connects the concept of Schnirelmann density with additive problems:

Theorem 7.4 (Schnirelmann, 1936). *If A is a subset of $\mathbb{N}$ such that $\delta(A) > 0$, then there exists $m \in \mathbb{N}$ such that $\delta(mA) = 1$, and therefore, $mA = \mathbb{N}$.*

Proof. If $\delta(A) = 1$, we are done. If not, we have $0 < \delta(A) < 1$. Since $0 < 1 - \delta(A) < 1$, we may choose t large enough so that

$$(1 - \delta(A))^t < \frac{1}{2}.$$

By Theorem 7.2, we see that

$$\delta(tA) \geq 1 - (1 - \delta(A))^t > \frac{1}{2}.$$

The theorem follows as a quick application of Lemma 7.3.

□

In 1940, Linnik noticed how Schnirelmann's theorem can be applied to solve Waring's problem. Let $k \geq 2$ and

$$A_k := \{n^k \ : \ n \in \mathbb{N}\}.$$

Theorem 7.4 reduces Waring's problem to showing the existence of a natural number m such that $\delta(mA_k) > 0$. This is done in the next section. In other words, Waring's problem is reduced to the "easier problem" of showing that a positive Schnirelmann density of natural numbers can be written as a sum of a bounded number of kth powers.

Theorem 7.1 of Schnirelmann has been improved by various authors culminating in the work of Henry Berthold Mann who showed in 1942 that if $0 \in A \cap B$, then

$$\delta(A + B) \geq \min(1, \delta(A) + \delta(B)).$$

Students can find a simple proof of Theorem 7.4 in the combinatorial classic of Heini Halberstam and Klaus Friedrich Roth [**29**].

7.1.1. Exercises.

Exercise 7.1.1.1. Let $m > 1$. Prove that the Schnirelmann density of the set of natural numbers $\equiv 1 \pmod{m}$ is equal to $1/m$.

Exercise 7.1.1.2. Show that Theorem 7.4 is false if we replace Schnirelmann density by natural density.

Exercise 7.1.1.3. Let $A \subseteq \mathbb{N}$ with Schnirelmann density δ. Then, $A(n) \geq \delta n$. Show that this inequality is false if δ is replaced by natural density.

Exercise 7.1.1.4. Let $A \subseteq \mathbb{N}$ be a subset with Schnirelmann density ω with $0 < \omega < 1$. Show that every natural number can be written as a sum of at most

$$2\left(1 + \left[-\frac{\log 2}{\log(1-\omega)}\right]\right)$$

elements from A.

Exercise 7.1.1.5.

(1) Show that

$$\sum_p \frac{1}{p^2} < \frac{1}{2},$$

where the sum is over all prime numbers p.

(2) Show that the set of squarefree numbers has Schnirelmann density $> 1/2$. Deduce that every natural number can be written as a sum of at most two squarefree numbers.

7.2. Schnirelmann density and Waring's problem

In 1940 Linnik [**47**] used Schnirelmann's theorem (Theorem 7.4) to provide a solution of Waring's problem through elementary number-theoretic techniques. We outline Linnik's arguments in this section.

Let $k \geq 2$ and $A_k = \{x^k : x \in \mathbb{N}\}$. We observe that

$$\frac{1}{n} \leq \frac{A_k(n)}{n} \leq \frac{n^{1/k}}{n} \text{ for every } n \geq 1.$$

Thus,

$$\delta(A_k) \leq \sigma(A_k) \leq \lim_{n\to\infty} \frac{n^{1/k}}{n} = 0.$$

Hence, $\delta(A_k) = 0$. In view of Theorem 7.4 of Schnirelmann, showing that $\delta(sA_k) > 0$ for some $s \geq 2$ would solve Waring's problem.

For integers $s \geq 1$ and $m \geq 0$, let $r_{s,k}(m)$ denote the number of nonnegative integral solutions of the equation $x_1^k + x_2^k + \cdots x_s^k = m$. That is,

$$r_{s,k}(m) = \#\left\{(x_1, x_2, \ldots, x_s) : x_i \in \mathbb{N} \cup \{0\},\ x_1^k + x_2^k + \cdots x_s^k = m\right\}.$$

Observe that if $x_1^k + x_2^k + \cdots x_s^k = m$, then $0 \leq x_i \leq m^{1/k}$ for each $1 \leq i \leq s$. Thus, for $m \geq 1$,

$$r_{s,k}(m) \leq \left(\left[m^{1/k}\right] + 1\right)^s = \sum_{j=0}^{s} \binom{s}{j} \left(\left[m^{1/k}\right]\right)^j \ll_s m^{s/k}.$$

Linnik's fundamental observation, which we will prove in Section 7.3, was that we can find a sufficiently large natural number s for which the above estimate for $r_{s,k}(m)$ can be sharpened. He proved Theorem 7.5.

Theorem 7.5 (Linnik, 1943)**.** *For a natural number $k \geq 2$ there exists $s \in \mathbb{N}$ and a constant $c(k)$ depending only on k such that*

$$r_{s,k}(m) \leq c(k) m^{\frac{s}{k}-1}$$

for all $m \geq 1$.

Before proving Linnik's theorem, we prove Corollary 7.6.

Corollary 7.6. *For any natural number $k \geq 2$, there exists $s \in \mathbb{N}$ such that $\delta(sA_k) > 0$.*

Proof. By Theorem 7.5, there exists $s \in \mathbb{N}$ such that

$$\sum_{\substack{m=0 \\ r_{s,k}(m)\neq 0}}^{n} r_{s,k}(m) \leq 1 + \sum_{\substack{m=1 \\ r_{s,k}(m)\neq 0}}^{n} c(k) m^{\frac{s}{k}-1} \leq c'(k) n^{\frac{s}{k}-1} \sum_{\substack{m=0 \\ r_{s,k}(m)\neq 0}}^{n} 1, \tag{7.1}$$

where $c'(k) = \max\{1, c(k)\}$.

We also observe that if

$$0 \leq x_i \leq \frac{n^{1/k}}{s^{1/k}} \text{ for each } i,$$

then,

$$\sum_{i=1}^{s} x_i^k \leq n.$$

Thus,

$$\sum_{\substack{(x_1,x_2,\cdots,x_s)\\ 0\le x_i\le \frac{n^{1/k}}{s^{1/k}}}} 1 \le \sum_{\substack{m=0\\ r_{s,k}(m)\neq 0}}^{n} r_{s,k}(m). \tag{7.2}$$

Observe that

$$(sA_k)(n) = \sum_{\substack{(x_1,x_2,\cdots,x_s)\\ 0\le x_i\le \frac{n^{1/k}}{s^{1/k}}}} 1 = \left(\left[\frac{n^{1/k}}{s^{1/k}}\right]+1\right)^s \ge \left(\frac{n^{1/k}}{s^{1/k}}\right)^s. \tag{7.3}$$

Combining equation (7.3) with the inequalities in equations (7.1) and (7.2), we get a positive constant $c'(k)$ such that

$$\left(\frac{n^{1/k}}{s^{1/k}}\right)^s \le c'(k)n^{\frac{s}{k}-1}(sA_k)(n) \text{ for every } n \ge 1.$$

Thus,

$$\frac{(sA_k)(n)}{n} \ge \frac{1}{c'(k)s^{\frac{s}{k}}} \text{ for every } n \ge 1.$$

Hence, by Theorem 7.5, we can find $s \in \mathbb{N}$ and $d(k) > 0$ such that

$$\delta(sA_k) \ge \frac{1}{c'(k)s^{\frac{s}{k}}},$$

and therefore, $\delta(sA_k) > 0$. □

Thus, by Theorem 7.4, Corollary 7.6 solves Waring's problem. We now prove Linnik's Theorem 7.5 in Section 7.3.

7.3. Proof of Linnik's theorem

We start this section with an observation about exponential functions which helps us to express the term $r_{s,k}(m)$ with the help of suitable exponential sums. This helps us to prove Linnik's theorem and will also enable us later to invoke the circle method.

Let $n \in \mathbb{Z}$. We observe that

$$\int_0^1 e^{2\pi i n\alpha} d\alpha = \begin{cases} 1 & \text{if } n = 0,\\ 0 & \text{otherwise.}\end{cases} \tag{7.4}$$

Let $P = m^{1/k}$ and set

$$f(\alpha) := \sum_{0\le x\le P} e(x^k\alpha), \quad e(x) := e^{2\pi i x}.$$

As an immediate application of (7.4), we deduce that for any $s \in \mathbb{N}$ and for a nonnegative integer $m \ge 0$,

$$\begin{aligned}
&\int_0^1 (f(\alpha))^s e(-m\alpha)d\alpha \\
&= \int_0^1 \sum_{\substack{(x_1,x_2,\dots,x_s)\\ 0\le x_1,x_2,\dots,x_s\le P}} e\left(\left(x_1^k + x_2^k + \cdots + x_s^k\right)\alpha\right) e(-m\alpha)d\alpha \\
&= \sum_{\substack{(x_1,x_2,\dots,x_s)\\ 0\le x_1,x_2,\dots,x_s\le P}} \int_0^1 e\left(\left(x_1^k + x_2^k + \cdots + x_s^k - m\right)\alpha\right) d\alpha \qquad (7.5)\\
&= \sum_{\substack{(x_1,x_2,\dots,x_s)\\ 0\le x_1,x_2,\dots,x_s\le P}} \begin{cases} 1 & \text{if } x_1^k + x_2^k + \cdots + x_s^k = m \\ 0 & \text{otherwise.}\end{cases} \\
&= r_{s,k}(m).
\end{aligned}$$

Thus,

$$\begin{aligned}
r_{s,k}(m) = |r_{s,k}(m)| &= \left|\int_0^1 (f(\alpha))^s e(-m\alpha)d\alpha\right| \qquad (7.6)\\
&\le \int_0^1 \left|\sum_{0\le x\le P} e(x^k\alpha)\right|^s d\alpha.
\end{aligned}$$

Linnik proved Theorem 7.7 with respect to the above exponential sum.

Theorem 7.7. *For any natural number $k \ge 2$ and for $P \ge 1$,*

$$\int_0^1 \left|\sum_{0\le x\le P} e(x^k\alpha)\right|^{8^{k-1}} d\alpha \le c(k)P^{8^{k-1}-k},$$

where $c(k)$ is a real number depending on k.

Let $m \ge 1$. Choosing

$$P = m^{\frac{1}{k}} \text{ and } s = 8^{k-1},$$

we get, by equation (7.6),

$$r_{s,k}(m) \leq c(k)m^{\frac{s}{k}-1},$$

which proves Theorem 7.5 and consequently, Corollary 7.6. For the rest of this section, therefore, we focus our attention to proving Theorem 7.7.

We now prove a basic lemma on linear equations.

Lemma 7.8. *For a nonnegative integer n, let $q(n)$ denote the number of integer solutions (x_1, x_2, y_1, y_2) of the equation*

$$x_1y_1 + x_2y_2 = n \tag{7.7}$$

such that $|x_i| \leq X$ and $|y_i| \leq Y$. Then

$$q(0) \ll (XY)^{3/2}$$

and

$$q(n) \ll \left(XY \sum_{d|n} \frac{1}{d}\right) \quad \text{for } n \geq 1.$$

Proof. We first consider the case when $n = 0$. Clearly, x_1, x_2 and y_1 can take at most $2X + 1$, $2X + 1$ and $2Y + 1$ values respectively. Once these are chosen, y_2 can take at most one value. Thus,

$$q(0) \leq (2X + 1)^2(2Y + 1) \ll X^2Y.$$

Similarly, $q(0) \ll XY^2$. Thus,

$$q(0) \ll \min\{X^2Y, XY^2\} \ll \sqrt{X^2Y.XY^2} \ll (XY)^{3/2}.$$

We can do better when $n \neq 0$. We assume, without loss of generality, that $X \leq Y$. Let $q_1(n)$ be the number of integer solutions to $x_1y_1 + x_2y_2 = n$, such that $|x_2| \leq |x_1| \leq X$ and $|y_i| \leq Y$ for $i = 1, 2$. This ensures that $x_1 \neq 0$. Otherwise, we would get $x_2 = 0$ which implies that $n = 0$.

Let us start by fixing x_1 and x_2 and assume that $(x_1, x_2) = 1$. Let $q(n; x_1, x_2)$ be the number of integral solutions of equation (7.7). Clearly, $q(n; x_1, x_2) > 0$. Given a particular solution (y_1', y_2'), all solutions of equation (7.7) are of the form

$$y_1 = y_1' + tx_2,\ y_2 = y_2' - tx_1,\ t \in \mathbb{Z}.$$

We observe that

$$|t| = \frac{|y_2' - y_2|}{|x_1|} \leq \frac{2Y}{|x_1|}.$$

We conclude that

$$\begin{aligned} q_1(n) &\leq \sum_{1\leq|x_1|\leq X}\sum_{|x_2|\leq|x_1|}\left(2\frac{2Y}{|x_1|}+1\right) \\ &\leq \sum_{1\leq|x_1|\leq X}\sum_{|x_2|\leq|x_1|}\left(\frac{4Y+|x_1|}{|x_1|}\right) \\ &\leq 5Y\sum_{1\leq|x_1|\leq X}\frac{2|x_1|+1}{|x_1|} \ll XY. \end{aligned}$$

Thus, equation (7.7) has $\ll XY$ integer solutions.

If $(x_1, x_2) = d > 1$, equation (7.7) has an integer solution provided $d|n$. In this case, we take

$$x_1' = \frac{x_1}{d},\ x_2' = \frac{x_2}{d}.$$

From above, the number of integer solutions to the equation

$$x_1'y_1 + x_2'y_2 = \frac{n}{d}$$

is $\ll \frac{XY}{d}$. We conclude that

$$q_1(n) \ll XY\sum_{d|n}\frac{1}{d}.$$

It immediately follows that

$$q(n) \ll XY\sum_{d|n}\frac{1}{d}.$$

□

From Lemma 7.8, we deduce the following:

Lemma 7.9. *Let $f(x)$ be a polynomial of degree 2 with integer coefficients, say, $f(x) = a_2x^2 + a_1x + a_0$, with $a_2 = \mathrm{O}(1)$, $a_1 = \mathrm{O}(P)$ and $a_0 = \mathrm{O}(P^2)$. The number of solutions in the variables x_i's and y_i's such that $0 \leq x_i, y_i \leq P$ for $1 \leq i \leq 4$ to the equation*

$$f(x_1) + f(x_2) + f(x_3) + f(x_4) = f(y_1) + f(y_2) + f(y_3) + f(y_4) \tag{7.8}$$

is $\ll P^6$.

Proof. We observe that

$$f(x_i) - f(y_i) = (x_i - y_i)[a_2(x_i + y_i) + a_1].$$

We put $z_i = x_i - y_i$ and $w_i = a_2(x_i + y_i) + a_1$.

The number of solutions of equation (7.8) is less than or equal to the number of solutions of the equation

$$z_1 w_1 + z_2 w_2 = -z_3 w_3 - z_4 w_4,$$

where $z_i \ll P$ and $w_i \ll P$. By Lemma 7.8, we see that for a fixed $n \geq 0$, the number $q(n)$ of solutions of $z_1 w_1 + z_2 w_2 = n$ is

$$\ll P^3 \text{ if } n = 0,$$

and

$$\ll P^2 \sum_{d|n} \frac{1}{d} \text{ if } n \geq 1.$$

Thus, the number of solutions of the equation

$$z_1 w_1 + z_2 w_2 = -z_3 w_3 - z_4 w_4,$$

where $z_i \ll P$ and $w_i \ll P$ is

$$\begin{aligned}\sum_{|n| \ll P^2} q(n)^2 &\ll P^6 + \sum_{1 \leq n \leq cP^2} \left(P^2 \sum_{d|n} \frac{1}{d} \right)^2 \\ &\ll P^6 + P^4 \sum_{1 \leq n \leq P^2} \sum_{\substack{d_1|n \\ d_2|n}} \frac{1}{d_1 d_2}.\end{aligned}$$

We now observe that

$$\begin{aligned}\sum_{1 \leq n \leq P^2} \sum_{\substack{d_1|n \\ d_2|n}} \frac{1}{d_1 d_2} &= \sum_{\substack{1 \leq d_1 \leq P^2 \\ 1 \leq d_2 \leq P^2}} \frac{1}{d_1 d_2} \sum_{\substack{1 \leq n \leq P^2 \\ d_1|n, d_2|n}} 1 \\ &= \sum_{\substack{1 \leq d_1 \leq P^2 \\ 1 \leq d_2 \leq P^2}} \frac{1}{d_1 d_2} \sum_{\substack{1 \leq n \leq P^2 \\ d_1|n, d_2|n}} 1 \\ &\sum_{\substack{1 \leq d_1 \leq P^2 \\ 1 \leq d_2 \leq P^2}} \frac{1}{d_1 d_2} \sum_{\substack{1 \leq n \leq P^2 \\ [d_1, d_2]|n}} 1 \\ &\sum_{\substack{1 \leq d_1 \leq P^2 \\ 1 \leq d_2 \leq P^2}} \frac{1}{d_1 d_2} \left(\frac{P^2}{[d_1, d_2]} + O(1) \right),\end{aligned}$$

where $[d_1, d_2]$ denotes the least common multiple of d_1 and d_2. Using the elementary identity $[d_1, d_2](d_1, d_2) = d_1 d_2$, we have,

$$\begin{aligned}
\sum_{|n|\ll P^2} q(n)^2 &\ll P^6 + \sum_{1\le n\le cP^2} \left(P^2 \sum_{d|n} \frac{1}{d} \right)^2 \\
&\ll P^6 + P^4 \sum_{\substack{1\le d_1\le P^2 \\ 1\le d_2\le P^2}} \frac{1}{d_1 d_2} \frac{P^2}{[d_1, d_2]} \\
&\ll P^6 + P^6 \sum_{\substack{1\le d_1\le P^2 \\ 1\le d_2\le P^2}} \frac{(d_1, d_2)}{(d_1 d_2)^2} \\
&\ll P^6 + P^6 \sum_{d_1=1}^{\infty} \sum_{d_2=1}^{\infty} \frac{1}{(d_1 d_2)^{3/2}} \\
&\ll P^6.
\end{aligned}$$

In the above, we have used the trivial estimate $(d_1, d_2) \le \sqrt{d_1 d_2}$. This proves Lemma 7.9.

□

We now prove the following general version of Linnik's theorem, due to Hua [**40**]. Though elementary, the proof will require some intellectual stamina on the part of the reader.

Theorem 7.10. *Let $k \ge 2$ and $f(x)$ be a polynomial of degree k with integer coefficients, say,*

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots a_1 x_1 + a_0$$

such that

$$a_k = \mathrm{O}(1),\ a_{k-1} = \mathrm{O}(P), \cdots, a_1 = \mathrm{O}(P^{k-1}),\ a_0 = \mathrm{O}(P^k).$$

Then, there exists a positive real number $c = c(k)$ such that for all $P \ge 1$,

$$\int_0^1 \left| \sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right|^{8^{k-1}} d\alpha \le c(k)(P^{8^{k-1}-k}). \tag{7.9}$$

Proof. Let us start with $k = 2$. Observe that

$$\int_0^1 \left| \sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right|^8 d\alpha = \int_0^1 \left(\sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right)^4 \left(\sum_{x=0}^{P} e^{-2\pi i f(x)\alpha} \right)^4 d\alpha$$

$$= \int_0^1 \left(\sum_{\substack{0\le x_1,x_2,x_3,x_4\le P \\ 0\le y_1,y_2,y_3,y_4\le P}} e^{2\pi i(f(x_1)+f(x_2)+f(x_3)+f(x_4)-f(y_1)-f(y_2)-f(y_3)-f(y_4))\alpha} \right) d\alpha.$$

By equation (7.4), the integral in question is equal to the number of integer solutions $(x_1, \dots, x_4, y_1, \dots, y_4)$ to equation (7.8) such that $0 \le x_i, y_i \le P$. Thus, this integral is $\ll P^6$ by Lemma 7.9. This proves Theorem 7.10 for $k = 2$. We now proceed by mathematical induction and assume that equation (7.9) holds when we replace k by $k-1$.

Observe that

$$\begin{aligned}\left| \sum_{x=0}^{P} e^{2\pi i f(x)\alpha} \right|^2 &= \sum_{x_1=0}^{P} \sum_{x_2=0}^{P} e^{2\pi i(f(x_1)-f(x_2))\alpha} \\ &= \sum_{x=0}^{P} e^{-2\pi i f(x)\alpha} \sum_{h=-x}^{P-x} e^{2\pi i f(x+h)\alpha} \\ &= P + 1 + \sum_{h\neq 0}{}' \sum_{x}{}' e^{2\pi i(f(x+h)-f(x))\alpha},\end{aligned}$$

where the dash on top of the summations refers to all those integers h lying between $-P$ and P and those integers x such that both $x+h$ and x lie between 0 and P. Now,

$$\begin{aligned} f(x+h) - f(x) &= \sum_{j=0}^{k} a_j((x+h)^j - x^j) \\ &= \sum_{j=0}^{k} a_j \sum_{i=0}^{j-1} \binom{j}{i} x^i h^{j-i}. \end{aligned}$$

Thus, $f(x+h) - f(x) = h\phi(x,h)$, where

$$\phi(x,h) = h \sum_{i=0}^{k-1} b_i(h) x^i,$$

and $b_i(h) = \sum_{j=i+1}^{k} \binom{j}{i} h^{j-i-1}$. Thus, $\phi(x,h)$ is a polynomial whose degree in x is at most $k-1$. Moreover, the coefficient $b_i(h)$ of x^i for each $0 \le i \le k-1$ satisfies the bound

$$|b_i(h)| \ll \sum_{j=i+1}^{k} \binom{j}{i} |h|^{j-i-1} \le \sum_{j=i+1}^{k} \binom{j}{i} P^{j-i-1} \ll_k P^{k-1-i}. \tag{7.10}$$

Let us define

$$a_h = \sum_x{}' e^{2\pi i h\phi(x,h)\alpha}.$$

Then, we have

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^2 = P + 1 + \sum_{h\neq 0}{}' a_h.$$

Raising both sides by the power 8^{k-2}, we have

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2.8^{k-2}} = \left(P + 1 + \sum_{h\neq 0}{}' a_h\right)^{8^{k-2}} \leq 2^{8^{k-2}} \max\left(P^{8^{k-2}}, \left|\sum_{h\neq 0}{}' a_h\right|^{8^{k-2}}\right). \tag{7.11}$$

We now consider two cases.

Case 1. If

$$\left|\sum_{h\neq 0}{}' a_h\right| \leq P,$$

then

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2.8^{k-2}} \ll P^{8^{k-2}}.$$

Hence, raising the above equation to the fourth power,

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll P^{4.8^{k-2}} \ll P^{8^{k-1}-k},$$

since $4.8^{k-2} \leq 8^{k-1} - k$ for all $k \geq 2$. This proves the theorem, provided

$$\left|\sum_{h\neq 0}{}' a_h\right| \leq P.$$

Case 2. Suppose now that

$$\left|\sum_{h\neq 0}{}' a_h\right| \geq P.$$

Then, by equation (7.11),

$$\left|P+1+\sum_{h\neq 0}{}' a_h\right|^{8^{k-2}} \ll \left|\sum_{0<|h|\leq P}{}' a_h\right|^{8^{k-2}}.$$

We now apply Hölder's inequality (see Section 3.7). Choosing

$$p=\frac{8^{k-2}}{8^{k-2}-1},\ q=8^{k-2},$$

we observe that

$$\frac{1}{p}+\frac{1}{q}=1.$$

Thus, we have

$$\left|\sum_{h\neq 0}{}' 1.a_h\right| \leq \left(\sum_{h\neq 0}{}' 1^p\right)^{\frac{1}{p}} \left(\sum_{h\neq 0}{}' |a_h|^q\right)^{\frac{1}{q}}.$$

Raising to the power 8^{k-2},

$$\begin{aligned}\left|\sum_{h\neq 0}{}' 1.a_h\right|^{8^{k-2}} &= \left(\sum_{h}{}' 1\right)^{\frac{1}{p}.8^{k-2}} \left(\sum_{h\neq 0}{}' |a_h|^q\right)^{\frac{1}{q}.8^{k-2}} \\ &\ll P^{8^{k-2}-1}\sum_{h\neq 0}{}' |a_h|^{8^{k-2}}.\end{aligned}$$

Thus,

$$\left|\sum_{h\neq 0}{}' a_h\right|^{8^{k-2}} \ll P^{8^{k-2}-1}\sum_{h\neq 0}{}' |a_h|^{8^{k-2}}. \tag{7.12}$$

Putting it all together,

$$\begin{aligned}\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2.8^{k-2}} &= \left|P+1+\sum_{h\neq 0}{}' a_h\right|^{8^{k-2}} \\ &\ll \left|\sum_{0<|h|\leq P}{}' a_h\right|^{8^{k-2}} \\ &\ll P^{8^{k-2}-1}\sum_{h\neq 0}{}' |a_h|^{8^{k-2}},\end{aligned}$$

by Hölder's inequality. By raising equation (7.12) to the fourth power, we immediately deduce,

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll P^{4(8^{k-2}-1)} \int_0^1 \left(\sum_{h\neq 0}{}' |a_h|^{8^{k-2}}\right)^4 d\alpha. \tag{7.13}$$

We write

$$\left|\sum_{x=0}^{P}{}' e^{2\pi i h\phi(x,h)\alpha}\right|^{8^{k-2}} = \sum_n A(n) e^{2\pi i h n\alpha}, \tag{7.14}$$

where, by Exercise 7.3.1.1,

$$n \ll \max_{0\leq x\leq P} |\phi(x,h)| \ll P^{k-1}.$$

This gives us

$$\begin{aligned} |A(n)| &= \left|\int_0^1 \left|\sum_{x=0}^{P}{}' e^{2\pi i h\phi(x,h)\alpha}\right|^{8^{k-2}} e^{-2\pi i h n\alpha} d\alpha\right| \\ &\leq \int_0^1 \left|\sum_{x=0}^{P}{}' e^{2\pi i h\phi(x,h)\alpha}\right|^{8^{k-2}} d\alpha, \end{aligned}$$

which, by induction hypothesis is

$$\ll P^{8^{k-2}-(k-1)}.$$

The induction hypothesis is applicable to the above equation by virtue of equation (7.10).

Thus, by equation (7.13) and the above bound,

$$|A(n)| \ll P^{8^{k-2}-(k-1)},$$

we get from (7.14)

$$\begin{aligned} &\int_0^1 \left|\sum_{x=0}^{P}{}' e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll P^{4(8^{k-2}-1)} \int_0^1 \left(\sum_{h\neq 0}{}' |a_h|^{8^{k-2}}\right)^4 d\alpha \\ &\ll P^{4(8^{k-2}-1)} \sum_{(\underline{n},\underline{h})\in S} A(n_1)A(n_2)A(n_3)A(n_4) \\ &\ll P^{4(8^{k-2}-1)} P^{4.8^{k-2}-4(k-1)} |S|, \end{aligned}$$

where

$$S := S(n_1, n_2, n_3, n_4, h_1, h_2, h_3, h_4) =$$
$$\{(\underline{n}, \underline{h}) = (n_1, n_2, n_3, n_4, h_1, h_2, h_3, h_4) \in \mathbb{Z}^8 \ : \ n_i \ll P^{k-1}, \ |h_i| \leq P,$$
$$n_1 h_1 + n_2 h_2 = -n_3 h_3 - n_4 h_4\},$$

By Exercise 7.3.1.2, we see that

$$|S| \ll P^{3k}.$$

Thus,

$$\int_0^1 \left| \sum_{x=0}^{P}{}' e^{2\pi i f(x)\alpha} \right|^{8^{k-1}} d\alpha \ll P^{4(8^{k-2}-1)} \int_0^1 \left(\sum_{h \neq 0}{}' |a_h|^{8^{k-2}} \right)^4 d\alpha$$
$$\ll P^{4(8^{k-2}-1)} P^{4.8^{k-2}-4(k-1)} P^{3k}$$
$$\ll P^{8^{k-1}-k}.$$

This proves Theorem 7.10 since in all the above inequalities, the implied constants only depend on k. □

We immediately deduce Theorem 7.7 by taking $f(x) = x^k$ in Theorem 7.10.

7.3.1. Exercises.

Exercise 7.3.1.1. Let h be a nonzero integer such that $|h| \leq P$. Let $\phi(x, h)$ be a polynomial of the form

$$\sum_{i=0}^{k-1} b_i(h) x^i, \text{ such that } |b_i(h)| \ll_k h^{k-1-i}.$$

Show that we can write

$$\left| \sum_{\substack{x=0 \\ 0 \leq x+h \leq P}}^{P} e^{2\pi i h \phi(x,h)\alpha} \right|^{8^{k-2}} = \sum_n A(n) e^{2\pi i h n \alpha},$$

where,

$$n \ll \max_{0 \leq x \leq P} |\phi(x, h)| \ll_k P^{k-1}.$$

Exercise 7.3.1.2. Show that

$$\#\{(n_1,n_2,n_3,n_4,h_1,h_2,h_3,h_4)\in\mathbb{Z}^8 \,:\, n_i \ll P^{k-1},\\ |h_i|\le P,\ n_1h_1+n_2h_2=-n_3h_3-n_4h_4\}\\ \ll P^{3k}.$$

Exercise 7.3.1.3. For a nonzero integer h, let $G(\alpha)$ be a function defined as

$$G(\alpha) := \sum_{|n|\le N} a_n e^{2\pi i n h\alpha}.$$

Show that

$$a_n = \int_0^1 G\Big(\frac{\alpha}{h}\Big)e^{-2\pi i n\alpha}d\alpha.$$

Exercise 7.3.1.4. Let $r_{g,k}(m)$ be the number of solutions of

$$x_1^k+\cdots+x_g^k=m, \qquad 0\le x_i\le m^{1/k}.$$

(a) Show that

$$\sum_{m\le n} r_{g,k}(m)\le 2^g n^{g/k}.$$

(b) Show that there is a constant $c(g,k)>0$ such that

$$r_{g,k}(n)\ge c(g,k)n^{g/k-1},$$

for infinitely many n. This shows that Linnik's theorem is essentially best possible.