TURUN YLIOPISTO
UNIVERSITY OF TURKU

MODERN APPROACHES TO CLASSICAL ADDITIVE PROBLEMS

Juho Salmensuu

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. AI OSA – TOM. 667 | ASTRONOMICA – CHEMICA – PHYSICA – MATHEMATICA | TURKU 2022

TURUN YLIOPISTO
UNIVERSITY OF TURKU

MODERN APPROACHES TO CLASSICAL ADDITIVE PROBLEMS

Juho Salmensuu

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. AI OSA – TOM. 667 | ASTRONOMICA – CHEMICA – PHYSICA – MATHEMATICA | TURKU 2022

University of Turku

Faculty of Science
Department of Mathematics and Statistics
Mathematics
Doctoral Programme in Exact Sciences (EXACTUS)

Supervised by

Docent, Kaisa Matomäki
University of Turku

Reviewed by

Professor, Angel Kumchev
Towson University
United States

Lecturer, Sean Prendiville
Lancaster University
United Kingdom

Opponent

Assistant Professor, Sam Chow
University of Warwick
United Kingdom

ISBN 978-951-29-8824-2 (PRINT)
ISBN 978-951-29-8825-9 (PDF)
ISSN 0082-7002 (PRINT)
ISSN 2343-3175 (ONLINE)
Painosalama Oy, Turku, Finland, 2022

UNIVERSITY OF TURKU
Faculty of Science
Department of Mathematics and Statistics
Mathematics
SALMENSUU, JUHO: Modern approaches to classical additive problems
Doctoral dissertation, 138 pp.
Doctoral Programme in Exact Sciences (EXACTUS)
November 2022

ABSTRACT

In this thesis, we study additive problems using the transference principle and the Hardy-Littlewood circle method. The problems studied are related to Waring's prolem and Goldbach's conjecture. Waring's problem states that all natural numbers can be written as the sum of a bounded number of kth powers, for any fixed k. Goldbach's conjecture states that all even numbers greater than two can be written as the sum of two prime numbers. The thesis consists of three articles.

In the first article, we study the Waring-Goldbach problem with almost equal summands. In other words, we are interested when a natural number can be written as the sum of kth powers of prime numbers, where the prime numbers are as close to each other as possible. We considerably improve the existing results using the transference principle.

In the second article, we study a density version of Waring's problem. Particularly, we approach the problem: What is the smallest density θ such that any subset of kth powers with a relative density larger than θ forms an asymptotic additive basis. Here we say that a set $A \subseteq \mathbb{N}$ forms an asymptotic additive basis, when all sufficiently large natural numbers can be written as the sum of a bounded number of elements of A. We prove two results related to this problem. The main result is proved using the transference principle.

In the third article, we study the binary Goldbach conjecture in the case where the summands are restricted to arithmetic progressions with large moduli. We significantly improve the allowed size of moduli. The improvement is based on the suitable use of a Freiman isomorphism inside the circle method.

KEYWORDS: Waring's problem, Goldbach's conjecture, circle method, transference principle

TURUN YLIOPISTO
Matemaattis-luonnontieteellinen tiedekunta
Matematiikan ja tilastotieteen laitos
Matematiikka
SALMENSUU, JUHO: Modern approaches to classical additive problems
Väitöskirja, 138 s.
Eksaktien tieteiden tohtoriohjelma (EXACTUS)
Marraskuu 2022

TIIVISTELMÄ

Tässä väitöskirjasssa tutkitaan additiivisia ongelmia käyttäen transferenssiperiaatetta sekä Hardyn ja Littlewoodin ympyrämenetelmää. Tutkitut ongelmat liittyvät Waringin ongelmaan ja Goldbachin konjektuuriin. Waringin ongelman mukaan jokaiselle luonnolliselle luvulle k on olemassa sellainen luonnollinen luku s, että jokainen luonnollinen luku voidaan esittää s:n k:nnen potenssin summana. Goldbachin konjektuuri taas sanoo, että jokainen kahta suurempi parillinen luku voidaan esittää kahden alkuluvun summana. Väitöskirja koostuu kolmesta artikkelista.

Ensimmäisessä artikkelissa tutkitaan Waring-Goldbachin ongelmaa lyhyillä lukuväleillä. Toisin sanoen ollaan kiinnostuneita siitä milloin luonnollinen luku voidaan esittää alkulukujen k:nsien potenssien summana, missä alkuluvut ovat niin lähellä toisiaan kuin mahdollista. Artikkelissa saadaan merkittävä parannus aikaisempiin tuloksiin käyttäen transferenssiperiaatetta.

Toisessa artikkelissa tutkitaan Waringin ongelman tiheysversiota. Erityisesti ollaan kiinnostuneita seuraavasta ongelmasta: Mikä on pienin sellainen tiheys θ siten, että mikä tahansa k:nsien potenssien osajoukko, jonka suhteellinen tiheys on suurempi kuin θ, muodostaa asymptoottisen additiivisen kannan? Tässä joukon $A \subseteq \mathbb{N}$ sanotaan muodostavan asymptoottisen additiivisen kannan silloin, kun kaikki riittävän suuret luonnolliset luvut voidaan esittää s:n joukon A alkion summana, missä s on jokin rajoitettu luonnollinen luku. Artikkelissa todistetaan kaksi tulosta, jotka pyrkivät vastaamaan tähän kysymykseen. Artikkelin päätulos seuraa transferenssiperiaatteesta.

Kolmannessa artikkelissa tutkitaan binääristä Goldbachin konjektuuria tapauksessa, jossa summattavat on rajoitettu sellaisiin aritmeettisiin jonoihin, joilla on suuri moduuli. Artikkelissa merkittävästi parannetaan sallitun moduulin kokoa verrattuna aikaisempiin tuloksiin. Parannus perustuu ajatukseen käyttää sopivasti valittua Freimanin isomorfismia ympyrämenetelmän kanssa.

ASIASANAT: Waringin ongelma, Goldbachin konjektuuri, ympyrämenetelmä, transferenssiperiaate

Acknowledgements

I am deeply grateful to my supervisor, Prof. Kaisa Matomäki, for all the guidance during my PhD studies and the funding she has offered for my studies. Without her invaluable help, I wouldn't be able to finish the degree.

I am thankful to the reviewers of this thesis, Prof. Angel Kumchev and Prof. Sean Prendiville for carefully reading the dissertation and giving valuable comments. I am also thankful to Prof. Sam Chow for agreeing to act as the opponent at my doctoral defence.

I am grateful to Prof. Trevor Wooley for our weekly meetings during my visit to the University of Bristol in the Autumn semester of 2018. These conversations deepened my understanding of Waring's problem and the circle method. I am also thankful to my fellow doctoral students and colleagues for all the help and discussions during the journey.

I want to thank all my friends for making my life happy and for reminding me what are the most important values in life.

I am greatly in debt to my parents for all the love and support. I am also thankful to my brothers and sister for being an important part of my life.

During my PhD studies, I was supported by Academy of Finland project no. 293876 and by project funding from Emil Aaltonen foundation.

February 17, 2022
Juho Salmensuu

Table of Contents

List of Original Publications

This dissertation is based on the following original publications, which are referred to in the text by their Roman numerals:

I J. Salmensuu. On the Waring-Goldbach problem with almost equal summands. *Mathematika 66 (2020)*, no. 2, 255–296.

II J. Salmensuu. A density version of Waring's problem. *Acta Arith. 199 (2021)*, no. 4, 383–412.

III J. Salmensuu. The Goldbach conjecture with summands in arithmetic progressions. Preprint (2021). arXiv: 2106.00778

1 Notation

This section contains notations used in Sections 2 - 9.

1. **Sets**

   - $\mathbb{N}$ – the set of positive integers $\{1, 2, 3, \dots\}$.
   - $\mathbb{Z}$ – the set of all integers.
   - $\mathbb{P}$ – the set of all prime numbers.
   - Square-free integers – positive integers which are not divisible by square of any prime.
   - $\mathbb{T}$ – the set of all real numbers modulo 1 ($\mathbb{R}/\mathbb{Z}$).
   - $\mathbb{Z}_q$ – the ring of integers modulo q.
   - $\mathbb{Z}_q^*$ – $\{a \in \mathbb{Z}_q \mid (a, q) = 1\}$.
   - $A^{(k)}$ – $\{a^k \mid a \in A\}$.
   - A_q – $\{b \in \mathbb{Z}_q \mid \exists a \in A : b \equiv a \pmod{q}\}$.
   - $[N]$ – $\{1, 2, \dots, N\}$.

2. **Letters**

   - p, p_n – prime numbers.
   - a, b, c, d, n, m, k, s – natural numbers.
   - ϵ – a small positive constant.

3. **Functions**

   - $\Lambda(n)$ - von Mangoldt function, equals $\log p$, when $n = p^k$ for some prime p and integer $k \geq 1$, and 0 otherwise.
   - $\pi(x)$ – the number of prime numbers less than x.
   - $\phi(n)$ – Euler's totient function, $\phi(n) = |\mathbb{Z}_n^*|$.
   - $\omega(n)$ – the number of distinct prime factors of n.
   - $\mu(n)$ – Möbius function, equals $(-1)^{\omega(n)}$ if n is square-free, 0 otherwise.
   - $1_A(a)$ – indicator function of the set A.

- 1_A – indicator function of the statement A.
- $e(\alpha)$ – shorthand for $e^{2\pi i\alpha}$.
- $e_q(\alpha)$ – shorthand for $e^{2\pi i\alpha/q}$.

4. **Sums**

- $A+B$ – shorthand for the sumset $\{a+b \mid a \in A, b \in B\}$.
- sA – shorthand for the sumset $\{a_1+\cdots+a_s \mid a_i \in A\}$
- $\mathbb{E}_{a\in A}$ – shorthand for the mean value $\frac{1}{|A|}\sum_{a\in A}$.
- $f*g(n)$ – shorthand for the additive convolution $\sum_{a+b=n} f(a)g(b)$.

5. **Norms**

Let $f:\mathbb{N}\to\mathbb{C}$, $g:\mathbb{T}\to\mathbb{C}$, $h:\mathbb{T}\to\mathbb{C}$ and $t:X\to\mathbb{C}$ where X is a metric space with metric $d:X\times X\to\mathbb{R}_{\geq 0}$.

- $||f||_{l^p}$ – (l^p-norm) $\left(\mathbb{E}_{n\leq N}|f(n)|^p\right)^{1/p}$.
- $||g||_p$ – (L^p-norm) $\left(\int_{\mathbb{T}}|g(\alpha)|^p d\alpha\right)^{1/p}$.
- $||h||_\infty$ – (L^∞-norm) $\sup_\alpha |h(\alpha)|$.
- $||t||_{Lip}$ – (Lipschitz norm) $\inf\{K\in\mathbb{R} \mid \forall \mathbf{x},\mathbf{y}\in X : |t(\mathbf{x})-t(\mathbf{y})|\leq Kd(\mathbf{x},\mathbf{y})\}$
- $||f||_{U^2(N)}$ – (Gowers U^2-norm) $||f||_{U^2(N)} = ||f1_{[N]}||_{U^2(\mathbb{Z})}/||1_{[N]}||_{U^2(\mathbb{Z})}$, where

$$||f||_{U^2(\mathbb{Z})} = (\mathbb{E}_{x,h_1,h_2\in\mathbb{Z}}\, f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2))^{1/4}.$$

6. **Asymptotics**

Let $f:\mathbb{R}\to\mathbb{R}, g:\mathbb{R}\to\mathbb{R}_{\geq 0}$, $A,B\subseteq\mathbb{N}$.

- $f(x)=O(g(x))$ – for some constant $C>0$, we have $|f(x)|\leq Cg(x)$ for all $x\in\mathbb{R}$.
- $f(x)\ll g(x)$ – shorthand for $f(x)=O(g(x))$.
- $f(x)\gg g(x)$ – for some constant $C>0$, we have $f(x)\geq Cg(x)$ for all $x\in\mathbb{R}$.
- $f(x)\asymp g(x)$ – we have $f(x)\ll g(x)$ and $g(x)\ll f(x)$ for all $x\in\mathbb{R}$.
- $f(x)=o(g(x))$ – we have $\forall\epsilon>0:\exists x\in\mathbb{R}:\forall y\geq x:|f(y)|\leq\epsilon g(y)$.

- $f(x) \sim g(x)$ – we have $\lim_{x\to\infty} f(x)/g(x) = 1$.
- $A \simeq B$ – we have $A \setminus [N] = B \setminus [N]$ for some $N \geq 1$.

7. **Miscellaneous**

Let $A \subseteq B \subseteq \mathbb{N}$.

- $p^h || k$ – means that $p^h | k$, but $p^{h+1} \nmid k$.
- $\tau(k,p)$ – defined by $p^{\tau(k,p)} || k$.
- $\eta(k,p) := \begin{cases} \tau(k,p)+2 & \text{if } p = 2 \text{ and } \tau(k,p) > 0 \\ \tau(k,p)+1 & \text{otherwise} \end{cases}$
- $R_k := \prod_{(p-1)|k} p^{\eta(k,p)}$.
- $\delta_B(A)$ – relative density of A in B, $\delta_B(A) = \liminf_{N\to\infty} \frac{|A\cap[N]|}{|B\cap[N]|}$.
- $\widehat{f}(\alpha)$ – Fourier transform of function $f : \mathbb{Z} \to \mathbb{C}$, $\widehat{f}(\alpha) = \sum_n f(n)e(\alpha n)$.

2 Introduction

Additive number theory is a fascinating area of mathematics. Many of its problems are fairly easy to explain to the general public, but solving those problems is rather complex and usually requires machinery from multiple areas of mathematics. There are also numerous open problems in additive number theory. The most famous open problem is Goldbach's conjecture which states

Conjecture. *For all $n \in \mathbb{N}$ with $n \geq 2$, there exist primes p and q such that*

$$2n = p + q.$$

This problem was established in 1742 in an exchange of letters between mathematicians Christian Goldbach and Leonhard Euler. Despite the fact that Goldbach's conjecture is still open, there has been some remarkable progress towards the problem. In 1937, Ivan Matveevich Vinogradov proved that

Theorem. *[31] For all sufficiently large odd $n \in \mathbb{N}$, there exist primes p, q and r such that*

$$n = p + q + r.$$

The gap between "all" and "sufficiently large" was filled by Harald Helfgott in 2013 [17]. Another interesting result towards Goldbach's conjecture is from Jingrun Chen, who proved in 1966 that

Theorem. *[6] For all sufficiently large $n \in \mathbb{N}$, there exist a prime p and an almost prime[1] q such that*

$$2n = p + q.$$

Another classical additive problem is Waring's problem. It was proposed in 1770, by Edward Waring.

Problem. (Waring's problem) *For all natural numbers $k \geq 2$, there exists $s \in \mathbb{N}$ such that, for all $n \in \mathbb{N}$, we have*

$$n = a_1^k + \cdots + a_s^k,$$

for some $a_1, \ldots, a_s \in \mathbb{Z}_{\geq 0}$.

[1] Almost prime is either a prime or a product of two primes.

Waring's original problem was solved in 1909 by David Hilbert [18]. After Hilbert's solution attention has turned towards the modern version of Waring's problem.

Problem. (Modern Waring's problem) *For a given natural number $k \geq 2$, what is the smallest natural number $G(k)$ such that for all sufficiently large $n \in \mathbb{N}$, we have*

$$n = a_1^k + \cdots + a_{G(k)}^k,$$

for some $a_1, \ldots, a_{G(k)} \in \mathbb{Z}_{\geq 0}$.

The first explicit upper bound for $G(k)$, namely

$$G(k) < (k-2)2^{k-1} + 6,$$

was obtained by Godfrey Harold Hardy and John Edensor Littlewood in 1922 [15]. After Hardy and Littlewood, there has been considerable progress towards this problem. For example, Vinogradov [31] proved that

$$G(k) < 3k \log k + 11k.$$

The best upper bound currently known is

$$G(k) < k(\log k + \log\log k + 2 + O(\log\log k / \log k))$$

due to Trevor Wooley (1995) [32]. It is conjectured that $G(k) \leq 4k$ (See e.g. [30, Section 10]), but this bound is out of reach of current technologies.

The standard approach to studying these kinds of additive problems is to use the so-called circle method. The circle method was invented by Hardy and Littlewood and is centered around the identity

$$\sum_{\substack{n=a_1+\cdots+a_s \\ a_i \in A}} 1 = \int_0^1 \Big(\sum_{a \in A} e(\alpha a) \Big)^s e(-\alpha n) d\alpha.$$

The idea is that under certain conditions we can evaluate the integral on the right-hand side and thus give an asymptotic formula for the sum on the left-hand side. We discuss the circle method in more detail in Section 5.

Another approach is to use the so-called transference principle, which is a modern variant of the circle method. The transference principle was first used by Ben Green (2005) [12] to show that any positive density subset of the primes contains infinitely many three-term arithmetic progressions. The idea of the transference is the following. Assume that we want to solve an additive problem concerning sparse subsets of integers. Under certain conditions we can "replace" the sparse sets with positive density sets, making the problem much easier. We discuss the transference principle in more detail in Section 6.

In this thesis, we study different variants of Goldbach's conjecture and Waring's problem using the circle method and the transference principle.

In Article I, we study the Waring-Goldbach problem with almost equal summands. We prove that, for $k \geq 2$ and s large enough depending on k, all sufficiently large natural numbers n satisfying some congruence conditions can be written in the form $n = p_1^k + \cdots + p_s^k$, where $p_1, \ldots, p_s \in [x - x^\theta, x + x^\theta]$ are primes, $x = (n/s)^{1/k}$ and $\theta = 0.525 + \epsilon$. In our current understanding of primes in short intervals, this is the best that we can do in terms of θ. We use the transference principle to prove this result in Article I. We discuss Article I in more detail in Section 7.

In Article II, we study the density version of Waring's problem. Let $\delta_k = (1 - \mathcal{Z}_k^{-1}/2)^{1/k}$, where $\mathcal{Z}_k$ is a certain constant depending on k for which it holds that $\mathcal{Z}_k > 1$ for every k and $\lim_{k\to\infty} \mathcal{Z}_k = 1$. We prove that for any $A \subseteq \mathbb{N}^{(k)}$ with $\delta_{\mathbb{N}^{(k)}}(A) > \delta_k$ there exists a natural number s with $s \ll k^2$, such that $sA \simeq \mathbb{N}$. Again we use the transference principle to prove the result. We discuss Article II in more detail in Section 8.

In Article III, we study the binary Goldbach conjecture in the case where the summands are restricted to arithmetic progressions with large moduli. We prove that, for almost all $r \leq N^{1/2}/\log^{O(1)} N$, for any given $b_1 \pmod r$ with $(b_1, r) = 1$, and for almost all $b_2 \pmod r$ with $(b_2, r) = 1$, we have that almost all natural numbers $2n \leq N$ with $2n \equiv b_1 + b_2 \pmod r$ can be written in the form $2n = p_1 + p_2$, where $p_1 \equiv b_1 \pmod r$ and $p_2 \equiv b_2 \pmod r$ are prime numbers. The main improvement to the previous results comes from the suitable use of a Freiman isomorphism inside the circle method. We discuss Article III in more detail in Section 9.

Before turning to the circle method and the transference principle, we will briefly discuss primes and exponential sums.

3 Primes

The prime numbers belong to the most fascinating figures of all mathematics and their behaviour has attracted many mathematicians during the centuries. Even though a great deal of progress has been made towards our understanding of prime numbers, there are still numerous open problems concerning prime numbers.

The earliest significant modern breakthrough on prime numbers was the prime number theorem (PNT) proved independently by Jacques Hadamard [14] and Charles Jean de la Vallée Poussin [9] in 1896.

Theorem. (Prime number theorem) *For $x > 1$, we have*

$$\pi(x) = (1 + o(1))\frac{x}{\log x}.$$

A natural follow-up question is how the prime numbers are distributed on specific subsets of natural numbers. For example, on the short intervals, we are interested in the following problem.

Problem. *For large $x > 1$, what is the smallest $y \geq 1$ such that*

$$\pi(x + y) - \pi(x) = (1 + o(1))\frac{y}{\log x}$$

and what is the smallest $y \geq 1$ such that

$$\pi(x + y) - \pi(x) \gg \frac{y}{\log x}?$$

In heuristic studies of the distribution of the prime numbers, it is conjectured that every interval $[x, x + \log^{2+\epsilon} x]$ contains a prime, provided that x is large enough. However, this is far from an established fact. Huxley [21] and Heath-Brown [16] have proved that

$$\pi(x + x^{\theta}) - \pi(x) = (1 + o(1))\frac{x^{\theta}}{\log x},$$

for $\theta \geq 7/12 \approx 0.583$, which is currently the best known result if we require an asymptotic formula. If we relax the requirement for the asymptotic behaviour, then the best result is

$$\pi(x + x^{\theta}) - \pi(x) \gg \frac{x^{\theta}}{\log x},$$

for $\theta \geq 0.525$, by Baker, Harman and Pintz [2]. This result is close to what we can hope to currently achieve, since even assuming the Riemann Hypothesis, we only obtain the following

$$\pi(x + x^{1/2}\log^{2+\epsilon} x) - \pi(x) = (1 + o(1))x^{1/2}\log^{1+\epsilon} x,$$

for $\epsilon > 0$.

Another interesting topic is primes in arithmetic progressions. The classical result about primes in arithmetic progressions is the so-called Siegel-Walfisz theorem (See e.g. [26, Theorem 8.3]).

Theorem. ***(Siegel-Walfisz)*** *If $q \geq 1$ and $(a,q) = 1$, then, for any $C > 0$,*

$$\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \Lambda(n) = \frac{x}{\phi(q)} + O\Big(\frac{x}{\log^C x}\Big).$$

This is the best known unconditional result on primes in arithmetic progressions. Here the error term is suitably small as long as $q \leq \log^C x$ for some $C \geq 1$. If we take mean values over moduli q, then we obtain the expected asymptotic for almost all $q \leq x^{1/2}/\log^6 x$. This result is known as the Bombieri-Vinogradov theorem (See e.g. [11, Theorem 9.18]).

Theorem. ***(Bombieri-Vinogradov)*** *For any $A > 0$, we have*

$$\sum_{q\leq Q}\max_{(a,q)=1}\Big|\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \Lambda(n) - \frac{x}{\phi(q)}\Big| \ll \frac{x}{\log^A x},$$

where $Q = x^{1/2}/\log^B x$ for some $B = B(A) > 0$, and the implied constant depends only on A.

The Bombieri-Vinogradov theorem corresponds on average over q what the GRH (Generalized Riemann Hypothesis) gives conditionally. According to the GRH we have (See e.g. [22, (5.66)])

$$\max_{(a,q)=1}\Big|\sum_{\substack{n\leq x \\ n\equiv a \pmod q}} \Lambda(n) - \frac{x}{\phi(q)}\Big| \ll x^{1/2}\log x,$$

for $q \leq x$. The result is non-trivial when $q = o(x^{1/2}/\log x)$.

4 Exponential sums

The central issue of using the circle method to study additive problems concerning set A, is being able to evaluate the exponential sums of the form

$$\sum_{a\in A} e(\alpha a).$$

In this section, we present a few classical results on such exponential sums.

For the primes, we have the following theorem (See e.g. [26, Theorem 8.5]).

***Theorem* 4.1.** *Let* $a, q, N \in \mathbb{N}$ *and* $\alpha \in \mathbb{R}$ *be such that* $1 \le q \le N$, $(a,q) = 1$ *and* $|\alpha - a/q| \le q^{-2}$. *Then*

$$\sum_{n\le N} \Lambda(n)e(\alpha n) \ll \Big(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\Big)\log^4 N. \tag{4.1}$$

A standard strategy for tackling sums involving primes is to use so-called Vaughan's identity (See e.g. [22, Proposition 13.4]).

Theorem. (Vaughan's identity) *For any* $y \ge 1$, $n > y$, *we have*

$$\Lambda(n) = \sum_{\substack{b|n\\ b\le y}} \mu(b)\log\frac{n}{b} - \sum_{\substack{bc|n\\ b,c\le y}} \mu(b)\Lambda(c) + \sum_{\substack{bc|n\\ b,c>y}} \mu(b)\Lambda(c).$$

Using Vaughan's identity we can split the exponential sum on the left-hand side of (4.1) into Type I and Type II sums, which we evaluate separately. By Type I and Type II sums, we mean the sums of the following form:

$$\text{Type I: } \sum_{n,m} a_n e(\alpha nm),$$
$$\text{Type II: } \sum_{n,m} a_n b_m e(\alpha nm),$$

where a_n, b_m are complex sequences with $|a_n|, |b_m| \le 1$ that are supported on suitable intervals.

For the k-th powers we have the following result, known as Weyl's inequality (See e.g. [26, Theorem 4.3]).

Theorem. ***(Weyl's inequality)*** *Let f be a monic polynomial of degree $k \geq 2$ with real coefficients. Let $\alpha \geq 0$ and $a, q \in \mathbb{N}$ be such that $(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$. Then*

$$\sum_{n \leq N} e(\alpha f(n)) \ll N^{1+\epsilon}(N^{-1} + q^{-1} + N^{-k}q)^{1/K},$$

where $K > 0$ depending on k.

The original Weyl's inequality had $K = 2^{k-1}$, but the progress in Vinogradov's mean value theorem has improved this value tremendously. Due to the breaktrough by Bourgain, Demeter and Guth [5], we can now take $K = k(k-1)$ (See [4, Theorem 5]).

5 Circle method

The circle method is a strategy, developed by Hardy and Littlewood, to count solutions of linear equations. Particularly, the circle method gives an asymptotic formula for

$$\sum_{\substack{n=a_1+\cdots+a_s\\ a_i\in A}} 1, \tag{5.1}$$

when $A \subseteq \mathbb{N}$, $s, n \in \mathbb{N}$ are suitably chosen. In general, we fix set A, assume that s is large enough depending on A and prove that the asymptotic formula holds for all $n \in \mathbb{N}$ large enough.

For $n \in \mathbb{Z}$, we have

$$\int_0^1 e(\alpha n)d\alpha = \begin{cases} 1 & \text{if } n = 0,\\ 0 & \text{otherwise.}\end{cases}$$

Using the previous identity we can derive the basic identity of the circle method:

$$\sum_{\substack{n=a_1+\cdots+a_s\\ a_i\in A}} 1 = \int_0^1 \Big(\sum_{t\le n} 1_A(t)e(\alpha t)\Big)^s e(-\alpha n)d\alpha. \tag{5.2}$$

In order to evaluate the integral in (5.2), we divide the unit interval $[0,1]$ into two disjoint sets using the so-called Hardy-Littlewood decomposition. The idea of this decomposition is that, when α is close to a rational number with a small denominator, then we have a good approximation for

$$\sum_{t\le n} 1_A(t)e(\alpha t).$$

On the other hand, if α is not close to a rational number with a small denominator, then we can often prove that

$$\sum_{t\le n} 1_A(t)e(\alpha t) = o(A(n)),$$

where $A(n) = \sum_{t\le n} 1_A(t)$.

We define the Hardy-Littlewood decomposition in the following way. Let $Q, P \ge 1$. Define

$$\mathfrak{M}_{Q,P} := \bigcup_{\substack{1\le q\le Q\\ 0\le a<q\\ (a,q)=1}} \mathfrak{M}_P(q,a),$$

where

$$\mathfrak{M}_P(q,a) := \{\alpha \in [0,1] \mid |\alpha - a/q| \le P^{-1}\}.$$

In addition, define $\mathfrak{m}_{Q,P} := [0,1] \setminus \mathfrak{M}_{Q,P}$. We call $\mathfrak{M}_{Q,P}$ major arcs and $\mathfrak{m}_{Q,P}$ minor arcs. We also require that the intervals $\mathfrak{M}_P(q,a)$ are all disjoint, which holds when $2Q^2 < P$.

Our task is now to estimate the integral

$$\int_M \Big(\sum_{t\le n} 1_A(t)e(\alpha t)\Big)^s e(-\alpha n)d\alpha, \tag{5.3}$$

when $M \in \{\mathfrak{m}_{Q,P}, \mathfrak{M}_{Q,P}\}$. For $M = \mathfrak{m}_{Q,P}$ we usually need Q to be sufficiently large and P to be sufficiently small, both depending on n and A. Whereas, for $M = \mathfrak{M}_{Q,P}$, we usually need that Q is sufficiently small and P is close to n. A balanced choice for Q and P usually exists.

Typically, the main term comes from the major arcs and the error term comes from the minor arcs.

5.1 Major arcs

When trying to evaluate the integal over the major arcs, our first task is to find a good approximation for $\sum_{t\le n} 1_A(t)e(\alpha t)$.

Let $\alpha = a/q+\beta \in \mathfrak{M}(a,q)$ and $A_q = \{b \pmod q \mid \exists a \in A : a \equiv b \pmod q\}$ be the residue classes modulo q occupied by elements of A. Assume that A is equidistributed among these residue classes, that is for all $b \in A_q$ we have

$$\sum_{\substack{t\le n\\ t\equiv b \pmod q}} 1_A(t) = (1+o(1))\frac{A(n)}{|A_q|}.$$

Then

$$\sum_{t\le n} 1_A(t)e_q(at) = \frac{A(n)}{|A_q|}\sum_{\substack{h=1\\ h\in A_q}}^{q} e_q(ah) + o(A(n)).$$

Let $A'(t)$ be defined in a such way that $\sum_{1\le t\le y} A'(t) \approx A(y)$. Now using partial summation we can prove that

$$\sum_{t\le n} 1_A(t)e(\alpha t) = \frac{1}{|A_q|}\sum_{\substack{h=1\\ h\in A_q}}^{q} e_q(ah)\sum_{t\le n} A'(t)e(\beta t) + Error, \tag{5.4}$$

where the error term depends on q and β. One chooses Q and P in a such way that the error term is small enough, when $\alpha \in \mathfrak{M}_{Q,P}$.

Let

$$\mathfrak{S}(Q) := \sum_{1\le q\le Q} \sum_{\substack{1\le a\le q\\(a,q)=1}} \frac{1}{|A_q|^s} \sum_{\substack{h_1,\dots,h_s \pmod q\\ h_i\in A_q}} e_q(a(h_1+\cdots+h_s-n))$$

and

$$\mathfrak{I}(P) := \int_{-P^{-1}}^{P^{-1}} \Big(\sum_{t\le b} A'(t)e(\beta t)\Big)^s e(-\beta n).$$

We call $\mathfrak{S}(Q)$ a singular series and $\mathfrak{I}(P)$ a singular integral.

Using the approximation formula (5.4) we can now show that the integral over major arcs can be written as a product of the singular integral and the singular series:

$$\int_{\mathfrak{M}_{Q,P}} \Big(\sum_{t\le n} 1_A(t)e(\alpha t)\Big)^s e(-\alpha n) = \mathfrak{S}(Q)\mathfrak{I}(P) + Error.$$

Typically, when $A(n)^s > n$ and sA_q occupies all relevant residue classes modulo q for all $q \ge 1$, we have

$$0 < \mathfrak{S}(Q) \sim \lim_{Q\to\infty} \mathfrak{S}(Q) < \infty.$$

For the singular integral, we usually have

$$\mathfrak{I}(P) \sim CA(n)^s n^{-1},$$

for some contant $C > 0$.

5.2 Minor arcs

When evaluating the integral over minor arcs, we need to be able to show that

$$\max_{\alpha\in\mathfrak{m}_{Q,P}} \Big|\sum_{t\le n} 1_A(t)e(\alpha t)\Big| = o(A(n)). \tag{5.5}$$

In Section 4, we have already introduced a few of classical results of the form (5.5).

We approach the integral over minor arcs by noting that, for $2s' \le s$, we have

$$\begin{aligned}\int_{\mathfrak{m}_{Q,P}} \Big(\sum_{t\le n} 1_A(t)e(\alpha t)\Big)^s e(-\alpha n)d\alpha \le \max_{\alpha\in\mathfrak{m}_{Q,P}} \Big|\sum_{t\le n} 1_A(t)e(\alpha t)\Big|^{s-2s'}\\ \times \int_0^1 \Big|\sum_{t\le n} 1_A(t)e(\alpha t)\Big|^{2s'} d\alpha.\end{aligned} \tag{5.6}$$

Here
$$\int_0^1 \Big|\sum_{t\le n} 1_A(t)e(\alpha t)\Big|^{2s'} d\alpha = \sum_{\substack{a_1+\cdots+a_{s'}=b_1+\cdots+b_{s'} \\ a_i,b_i\le t \\ a_i,b_i\in A}} 1.$$

Assuming that A has a nice structure, we can usually prove that

$$\int_0^1 \Big|\sum_{t\le n} 1_A(t)e(\alpha t)\Big|^{2s'} d\alpha \ll A(n)^{2s'}n^{-1}, \tag{5.7}$$

for s' sufficiently large depending on A. Let s_A be the smallest such s'. Then, for all $s > 2s_A$, we have by (5.6), (5.5) and (5.7), that

$$\int_{\mathfrak{m}_{Q,P}} \Big(\sum_{t\le n} 1_A(t)e(\alpha t)\Big)^s e(-\alpha n)d\alpha = o(A(n)^s n^{-1}).$$

Major arc calculations usually hold for the heuristically expected number of required summands. Since we are often required to take absolute values in order to evaluate the integral over minor arcs, we usually need more summands than is heuristically expected.

5.3 Example

In this subsection, we give an example of how the circle method can be used to prove that the set of prime numbers contains infinitely many 3-term arithmetic progressions.

Let $Q = \log^B N$ and $P = N/\log^{4B} N$ for some $B > 1$ to be chosen later. Write $\mathfrak{M} := \mathfrak{M}_{Q,P}$ and $\mathfrak{m} := \mathfrak{m}_{Q,P}$. Let

$$f(\alpha) = \sum_{n\le N} \Lambda(n)e(\alpha n).$$

We have
$$\sum_{\substack{a+b=2c \\ a,b,c\le N}} \Lambda(a)\Lambda(b)\Lambda(c) = \int_0^1 f(\alpha)^2 f(-2\alpha)d\alpha.$$

Our aim is to evaluate the integral on the right-hand side in the major arcs and in the minor arcs.

Let us first deal with the minor arcs. Using Theorem 4.1 we find that

$$\sup_{\alpha\in\mathfrak{m}} |f(2\alpha)| \ll \frac{N}{\log^A N},$$

for any $A \geq 1$ provided that B is large enough. We also see that

$$\int_0^1 |f(\alpha)|^2 d\alpha = \sum_{n \leq N} \Lambda(n)^2 \leq N \log^2 N.$$

Hence, for any $C \geq 1$, we have

$$\int_{\mathfrak{m}} f(\alpha)^2 f(-2\alpha) d\alpha \leq \sup_{\alpha \in \mathfrak{m}} |f(2\alpha)| \int_0^1 |f(\alpha)|^2 d\alpha \ll \frac{N}{\log^C N},$$

provided that B is large enough.

Now we deal with the major arcs. Let $\alpha = a/q + \beta$. Using partial summation and the Siegel-Walfisz theorem we find that

$$f(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{t \leq N} e(\beta t) + O(q + q|\beta|N).$$

Denote $u(\beta) = \sum_{n \leq N} e(\beta n)$. We can now write

$$\begin{aligned}
\int_{\mathfrak{M}} f(\alpha)^2 f(-2\alpha) d\alpha &= \sum_{1 \leq q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \int_{\mathfrak{M}(q,a)} f(\alpha)^2 f(-2\alpha) d\alpha \\
&= \sum_{1 \leq q \leq Q} \frac{\mu(q)}{\phi(q)^2} \int_{-\log^B N/N}^{\log^B N/N} u(\beta)^2 u(-2\beta) d\beta + O\Big(\frac{N^2}{\log^C N}\Big),
\end{aligned}$$

for any $C \geq 1$, provided that B is large enough. We have

$$\sum_{1 \leq q \leq Q} \frac{\mu(q)}{\phi(q)^2} = \prod_p \Big(1 - \frac{1}{(p-1)^2}\Big) + O\Big(\frac{\log Q}{Q}\Big)$$

and

$$\int_{-\log^B N/N}^{\log^B N/N} u(\beta)^2 u(-2\beta) d\beta = \frac{N^2}{2} + O\Big(N^2/\log^{2B} N\Big).$$

Combining all these results we obtain the following

$$\sum_{\substack{a+b=2c \\ a,b,c \leq N}} \Lambda(a)\Lambda(b)\Lambda(c) = \prod_p \Big(1 - \frac{1}{(p-1)^2}\Big) \frac{N^2}{2} + O\Big(\frac{N^2}{\log^D N}\Big), \tag{5.8}$$

for any $D \geq 1$, provided that B is large enough. Since there are only N trivial solutions ($a = b = c$) to $a + b = 2c$, where $a, b, c \leq N$, the contribution of trivial solutions to the sum on the left-hand side of (5.8) is at most $N \log^3 N$. Hence the set of prime numbers contains infinitely many 3-term arithmetic progressions.

6 Transference principle

If we have limited information about the set $A \subset \mathbb{N}$ (e.g. we only know that it is a positive density subset of primes), then we can no longer calculate the solutions to (5.1) using the circle method, since we cannot directly analyse the exponential sum

$$\sum_{t \leq n} 1_A(t) e(\alpha t).$$

We can sometimes circumvent this problem by using the transference principle. The transference principle was originally developed by Ben Green [12] to show that any positive density subset of the primes contains infinitely many three-term arithmetic progressions. The idea of the transference principle is that under certain circumstances we can estimate (5.1) by "replacing" set A with some positive density subset of natural numbers. Additive problems concerning positive density sets are usually easier than additive problems concerning sparse sets. Next, we will provide a brief description of how the transference principle works.

6.1 Transference

We say that function $\nu : [N] \to \mathbb{R}_{\geq 0}$ is a *pseudorandom* if $|\widehat{\nu}(\alpha) - \widehat{1_{[N]}}(\alpha)| = o(N)$ for all $\alpha \in [0, 1]$. We also say that function $\nu : [N] \to \mathbb{R}$ is *a majorant function* of $f : [N] \to \mathbb{R}$ if $f(n) \leq \nu(n)$ for all $n \in [N]$.

The core of the transference principle is the following lemma: [1]

***Lemma* 6.1.** *Assume that $f : [N] \to \mathbb{R}_{\geq 0}$ has a pseudorandom majorant function. Then there exist functions $g : [N] \to \mathbb{R}_{\geq 0}$ and $h : [N] \to \mathbb{R}$ such that*

(i) $f(n) = g(n) + h(n)$ *for all* $n \in [N]$.

(ii) $0 \leq g(n) \leq 1 + o(1)$ *for all* $n \in [N]$.

(iii) $||\widehat{h}||_\infty = o(N)$.

(iv) $||\widehat{h}||_q, ||\widehat{g}||_q \leq ||\widehat{f}||_q$ *for all* $q \geq 1$.

[1] For the precise form of Lemma 6.1 see Article II, Lemma 3.7.

Let $f_1, \dots, f_s : [N] \to \mathbb{R}_{\geq 0}$ be such that they all have a pseudorandom majorant function. By symmetry we can assume that $||\widehat{f_i}||_{s-\frac{1}{2}} \leq ||\widehat{f_1}||_{s-\frac{1}{2}}$ for all $i = 1, \dots, s$.

Using Lemma 6.1 and Hölder's inequality we can show that

$$\sum_{a_1+\cdots+a_s=n} f_1(a_1)\cdots f_s(a_s) = \sum_{a_1+\cdots+a_s=n} g_1(a_1)\cdots g_s(a_s) + o(N^{\frac{1}{2}}||\widehat{f_1}||_{s-\frac{1}{2}}^{s-\frac{1}{2}}). \tag{6.1}$$

Let $G_\epsilon^i = \{n \leq N \mid g_i(n) > \epsilon\}$, where $\epsilon > 0$. Then

$$\sum_{a_1+\cdots+a_s=n} g_1(a_1)\cdots g_s(a_s) \geq \epsilon^s \sum_{a_1+\cdots+a_s=n} 1_{G_\epsilon^1}(a_1)\cdots 1_{G_\epsilon^s}(a_s). \tag{6.2}$$

Assume that $\sum_{n\leq N} f_i(n) \gg N$ for each $i = 1, \dots, s$. Then it follows from (i) and (iii) that $|G_\epsilon^i| \gg N$ for each $i = 1, \dots, s$, provided that ϵ is sufficiently small. Typically, we can define g_i in such a way that we can transfer a sufficient amount of arithmetic information from f_i to g_i so that the right-hand side of (6.2) is positive. If we can prove that

$$\sum_{a_1+\cdots+a_s=n} 1_{G_\epsilon^1}(a_1)\cdots 1_{G_\epsilon^s}(a_s) \gg N^{s-1}, \tag{6.3}$$

then we obtain from (6.1) and (6.2) that

$$\sum_{a_1+\cdots+a_s=n} f_1(a_1)\cdots f_s(a_s) \gg N^{s-1}, \tag{6.4}$$

provided that

$$||\widehat{f_1}||_{s-\frac{1}{2}}^{s-\frac{1}{2}} \ll N^{s-\frac{3}{2}}. \tag{6.5}$$

We call inequality (6.3) a **dense problem**. The restriction estimate (6.5) is usually rather straight-forward to calculate using the standard circle method machinery. The restriction estimate often gives the strictest condition for the number of required summands.

Assume, for simplicity, that functions $f_1, \dots, f_s$ all are 1_A (In general, they are shifted and weighted versions of 1_A). Then we can see that the ideas presented above provide a lower bound for (5.1).

6.2 Pseudorandomness

One of the problems of using the transference principle is to find a suitable pseudorandom majorant function for $f \approx 1_A$. In this section, we explain the common strategy for defining a pseudorandom function.

6.2.1 The problem with the characteristic function

A natural candidate for the pseudorandom function is $w1_A$, where w is a suitable weight function with $\mathbb{E}_{n\in[N]}\, w(n)1_A(n) = 1 + o(1)$. In this subsection, we demonstrate why $w1_A$ is often not pseudorandom.

For example, by the prime number theorem, we have $\mathbb{E}_{n\in[N]}\,\Lambda(n) = 1 + o(1)$. However, $\Lambda(n)$ is not pseudorandom, as we will see from the following lemma.

***Lemma* 6.1.** *There exists $\alpha \in \mathbb{R}$ such that*

$$\Big|\sum_{n\le N}\Lambda(n)e(\alpha n) - \sum_{n\le N} e(\alpha n)\Big| \gg N.$$

Proof. For prime p, let $\alpha = 1/p$. Then

$$\begin{aligned}\sum_{n\le N}\Lambda(n)e(\alpha n) - \sum_{n\le N} e(\alpha n) &\sim \sum_{1\le a<p} e_p(a) \sum_{\substack{n\le N\\ n\equiv a \pmod p}} \Lambda(n)\\ &\quad - \sum_{0\le a<p} e_p(a) \sum_{\substack{n\le N\\ n\equiv a \pmod p}} 1\\ &\sim \frac{N}{p-1}\sum_{1\le a<p} e_p(a) - \frac{N}{p}\sum_{0\le a<p} e_p(a)\\ &= -\frac{N}{p-1},\end{aligned}$$

since $\sum_{0\le a<p} e_p(a) = 0$. □

Similarly, for kth-powers, we have

***Lemma* 6.2.** *There exists $\alpha \in \mathbb{R}$ such that*

$$\Big|\sum_{n\le N} kn^{k-1}e(\alpha n^k) - \sum_{n\le N^k} e(\alpha n)\Big| \gg N^k.$$

Note that $\sum_{n\le N} kn^{k-1} \sim N^k$.

Proof. Let p be a prime with $k|p-1$. We know that

$$\sum_{b \pmod p}\sum_{a \pmod p} e_p(ba^k)e_p(-b) = p \sum_{\substack{a \pmod p\\ a^k\equiv 1 \pmod p}} 1 = kp.$$

Hence, for some $c \in \{1,\dots,p-1\}$, we have

$$|\sum_{a \pmod p} e_p(ca^k)| \ge k-1.$$

Let $\alpha = c/p$. We see that

$$\sum_{n \le N} kn^{k-1} e(\alpha n^k) = \sum_{0 \le a < p} e_p(ca^k) \sum_{\substack{n \le N \\ n \equiv a \pmod p}} kn^{k-1} \sim \frac{N^k}{p} \sum_{0 \le a < p} e_p(ca^k).$$

Therefore

$$\begin{aligned}\sum_{n \le N} kn^{k-1} e(\alpha n^k) - \sum_{n \le N^k} e(\alpha n) &\sim \frac{N^k}{p} \sum_{0 \le a < p} e_p(ca^k) - \frac{N^k}{p} \sum_{0 \le a < p} e_p(a) \\ &= \frac{N^k}{p} \sum_{0 \le a < p} e_p(ca^k) \\ &\gg \frac{N^k(k-1)}{p}.\end{aligned}$$

□

The proofs of these lemmas indicate that if

$$\Big| \sum_{\substack{a \pmod q \\ a \in A_q}} e_q(ab) \Big| \gg 1,$$

for some $q, b \in \mathbb{N}$, then $w1_A$ is not pseudorandom. Usually, for an interesting $A \subseteq \mathbb{N}$, this is the case, which means that we need something more sophisticated to transfer 1_A into a pseudorandom function.

6.2.2 W-trick

In this subsection, we introduce the W-trick, which can be used to circumvent the problem described in the previous subsection.

Let $W \approx \prod_{p \le \log\log\log N} p$ (The exact definition depends on A) and $b \in A_W$. Define $\nu_b(n) : [N] \to \mathbb{R}_{\ge 0}$ by

$$\nu_b(n) = w(Wn + b) 1_A(Wn + b), \tag{6.6}$$

where w is a weight function chosen in such a way that $\mathbb{E}_{n \in N} \nu_b(n) = 1 + o(1)$.

When A has certain structural properties (i.e. equidistribution in arithmetic progressions), we can usually prove that ν_b is pseudorandom for all $b \in A_W$.

Assume that ν_b is pseudorandom for all $b \in A_W$ and that the dense problem (6.3) and the restriction estimate (6.5) are soluble for $f_i = \nu_{b_i}$, where $i = 1, \ldots, s$ and $b_1, \ldots, b_s \in A_W$. Then we have by (6.4) that

$$\sum_{t_1 + \cdots + t_s = n} \nu_{b_1}(t_1) \cdots \nu_{b_s}(t_s) \gg N^{s-1},$$

which conveys the solubility of

$$Wn + b_1 + \cdots + b_s = a_1 + \cdots + a_s,$$

where $a_i \in A$ and $b_i \in A_W$. Therefore, when we use the transference principle with the W-trick to prove that all sufficiently large n' can be written as $n' = a'_1 + \cdots + a'_s$, where $a'_i \in A$, we also need to show that

$$sA_W = \mathbb{Z}_W, \tag{6.7}$$

for all sufficiently large W. We call the equation (6.7) a **local problem**. The local problem is also a necessary condition for $sA \simeq \mathbb{N}$ to hold.

Typically, when we can give an asymptotic formula for (5.1) using the circle method, we can also show that ν_b is pseudorandom and thus we can use the transference principle to give a lower bound for (5.1). The lower bound has the same magnitude as the main term coming from the circle method.

6.2.3 Proving the pseudorandomness

A common strategy for proving pseudorandomness is to use the circle method machinery, while taking account of the usage of W and other possible complications. Next, we describe how one can proceed.

Let ν_b be defined as in (6.6). We use the Hardy-Littlewood decomposition to prove the pseudorandomness of ν_b. Let $Q', P' \geq 1$ be quantities to be determined. Due to the close relation between the circle method and the transference principle, we can usually show that

$$\max_{\alpha \in \mathfrak{m}_{Q,P}} \Big| \sum_{t \leq n} 1_A(t) e(\alpha t) \Big| = o(A(n)) \Rightarrow \max_{\alpha \in \mathfrak{m}_{Q',P'}} |\widehat{\nu_b}(\alpha)| = o(N).$$

This takes care of the pseudorandomness in the minor arcs, since $\widehat{1_{[N]}}(\alpha) = o(N)$ for $\alpha \in \mathfrak{m}_{Q',P'}$.

In the major arcs we use partial summation to show that, for $\alpha = a/q + \beta$, we have

$$\widehat{\nu_b}(\alpha) = e_{qW}(-ba) \frac{S_q(a,b)}{q} \widehat{1_{[N]}}(\beta) + Error, \tag{6.8}$$

where

$$S_q(a,b) := \sum_{\substack{h \ (\mathrm{mod}\ Wq) \\ h \in A_{Wq} \\ h \equiv b \ (\mathrm{mod}\ W)}} e_{Wq}(ah)$$

and the error term depends on $|\beta|$ and q. When $\alpha \in \mathfrak{M}_{Q',P'}$, the error term is usually sufficiently small. The W-trick typically guarantees that

$$S_q(a,b) = o_{N \to \infty}(q), \tag{6.9}$$

when $a \neq 0$ and $q > 1$. We also see that $\widehat{1_{[N]}}(\alpha) = o(N)$, when $a \neq 0$ and $q > 1$. Hence $\widehat{\nu_b}(\alpha) = \widehat{1_{[N]}}(\alpha) + Error$, for $\alpha \in \mathfrak{M}_{Q',P'}$.

This concludes that ν_b is a pseudorandom function. We also see that, when A can be studied using the circle method, then ν_b is usually pseudorandom.

6.3 Density version of an additive problem

The typical problem we can tackle using the transference principle is the following.

Problem. *Let $A \subseteq \mathbb{N}$ and $s \in \mathbb{N}$ with $sA \simeq \mathbb{N}$. What is the smallest $\delta_A := \delta_{A,s} > 0$ such that, for any $B \subseteq A$ with $\delta_A(B) > \delta_A$, we have*

$$sB \simeq \mathbb{N}.$$

The circle method cannot be used on this problem, due to the limited information about the set B. When we approach this problem using the transference principle, we assume that $sA \simeq N$ can be proven using the circle method.

Let

$$\delta'_A = \sup_{\substack{q,a \in \mathbb{N} \\ q \neq 1}} \delta_A(A \cap (q\mathbb{N} + a)).$$

In other words, δ'_A is the largest relative density that a non-trivial arithmetic progression can have in A. Now if $\delta_A(B) < \delta'_A$, then B can be a subset of a non-trivial arithmetic progression, in which case sB is also a subset of a non-trivial arithmetic progression. Hence $\delta_A \geq \delta'_A$. For $C \subseteq \mathbb{N}$ and $s \in \mathbb{N}$ let

$$r_C^s(n) = |\{c_1, \ldots, c_s \in C \mid n = c_1 + \cdots + c_s\}|.$$

We can prove the following lemma.

***Lemma* 6.1.** *Let $A \subseteq \mathbb{N}$, $B \subseteq A$ with $\delta_A(B) > \delta'_A$. Let $s \in N$. Assume that*

$$r_A^s(n) \ll A(n)^s n^{-1}.$$

Then there exists $s' \geq s$ such that

$$s'B \simeq \mathbb{N}.$$

Proof. The proof is similar to the proof of Theorem 1.3 in Article II. □

Because of the previous lemma we often expect that $\delta_A = \delta'_A$.

For $B \subseteq A$, define

$$f_b^B(n) := w(Wn + b)1_B(Wn + b),$$

where w and W are defined as in Section 6.2.2. We see that ν_b defined in (6.6) is a majorant function for f_b^B.

We can now confront the problem using the transference principle, provided that ν_b is pseudorandom and we can solve the **dense problem** similar to (6.3) and the **local problem**

$$sB_W = \mathbb{Z}_W.$$

The solubility of these problems is usually easy to guarantee when $\delta_A(B)$ is close to 1. The difficulties start to occur when $\delta_A(B)$ moves closer to δ'_A.

6.4 Application of sieve methods

The transference principle also seems to provide a better context for the sieve methods than the circle method. This might be due to the asymptotic nature of the circle method. For example, consider the following problem.

Problem. *What is the smallest θ such that, for all sufficiently large $n \in \mathbb{N}$, we have*

$$p_1 + p_2 + p_3 = n,$$

where p_1, p_2, p_3 are primes with $|p_i - n/3| \leq n^\theta$?

The best result with the circle method context is $\theta \leq 4/7$ [1], while the usage of the transference principle gives us $\theta \leq 11/20$ [25]. Both of these results rely on sieve methods.

6.5 Example

In this subsection, we give an example of how the transference principle can be used to prove that any positive density subset of the primes contains infinitely many 3-term arithmetic progressions.

Let $A \subseteq \mathbb{P}$ with $\delta_{\mathbb{P}}(A) > 0$. Let $W = \prod_{p \leq \log\log\log N} p$ and $b \in \mathbb{Z}_W^*$. Define functions $f_b, \nu_b : [N] \to \mathbb{R}_{\geq 0}$ by

$$f_b(n) = \frac{\phi(W)}{W} \log(Wn + b) 1_A(Wn + b)$$

and

$$\nu_b(n) = \frac{\phi(W)}{W} \log(Wn + b) 1_{\mathbb{P}}(Wn + b).$$

We see that $f_b(n) \leq \nu_b(n)$ for all $n \in \mathbb{N}$.

We demonstrate that ν_b is a pseudorandom function. Let $Q = \log^B N$ and $P = N/\log^B N$ for some $B > 1$ to be chosen later. Write $\mathfrak{M} := \mathfrak{M}_{Q,P}$ and $\mathfrak{m} := \mathfrak{m}_{Q,P}$, where $\mathfrak{M}_{Q,P}$ and $\mathfrak{m}_{Q,P}$ are defined as in Section 5.

In the minor arcs, we can show using Vaughan's identity that

$$\sup_{\alpha\in\mathfrak{m}} |\widehat{\nu_b}(\alpha)| \ll N/\log^C N,$$

for any $C \geq 1$, provided that B is large enough depending on C. This result is very similar to Theorem 4.1.

Next, we deal with the major arcs. Let $\alpha \in \mathfrak{M}(a,q)$ and $\beta = \alpha - a/q$. Using partial summation and the Siegel-Walfisz theorem we get that

$$\widehat{\nu_b}(\alpha) = e_{qW}(-ab)\frac{\phi(W)}{\phi(Wq)} \sum_{\substack{h \pmod{Wq} \\ (h,Wq)=1 \\ h\equiv b \pmod W}} e_{Wq}(ah)\widehat{1_{[N]}}(\beta) + O\Big(N/\log^C N\Big),$$

for any $C \geq 1$, provided that B is large enough depending on C. By Lemma 3.1 from Article III we have

$$\sum_{\substack{h \pmod{Wq} \\ (h,Wq)=1 \\ h\equiv b \pmod W}} e_{Wq}(ah) = 1_{(q,W)=1}\mu(q)e_{Wq}(abq^{\phi(W)}).$$

Note that this can be non-zero only when $q = 1$ or $q > \log\log\log N$. Hence

$$\widehat{\nu_b}(\alpha) = \begin{cases} o(N) & \text{when } q > 1, \\ \widehat{1_{[N]}}(\alpha) + o(N) & \text{otherwise.} \end{cases}$$

Since $\widehat{1_{[N]}}(\alpha) = o(N)$, when $\alpha \notin \mathfrak{M}(1,0)$, we obtain that ν_b is pseudorandom.

Now choose d such that A has a positive relative density in $d \pmod W$. We have

$$\sum_{a+b=2c} f_d(a)f_d(b)f_d(c) \leq \log^3(WN) \sum_{\substack{a+b=2c \\ a,b,c\leq WN+d \\ a,b,c\equiv d \pmod W}} 1_A(a)1_A(b)1_A(c). \tag{6.10}$$

Using Lemma 6.1 and the strategy explained in Section 6.1 we can obtain

$$\sum_{a+b=2c} f_d(a)f_d(b)f_d(c) \gg \sum_{a+b=2c} 1_B(a)1_B(b)1_B(c), \tag{6.11}$$

for some set $B \subseteq [N]$ with $|B| \gg N$. By Roth's theorem [27], we can deduce that

$$\sum_{a+b=2c} 1_B(a)1_B(a)1_B(a) \gg N^2. \tag{6.12}$$

We note that $a+b = 2c$ with $a, b, c \leq N$ has only N trivial solutions ($a = b = c$). Therefore by (6.10), (6.11) and (6.12), the set A has infinitely many 3-term arithmetic progressions.

7 On the Waring-Goldbach problem with almost equal summands

In Article I, we studied the Waring-Goldbach problem with summands in short intevals. The study was motivated by a recent improvement to the ternary Goldbach's problem with almost equal summands, done by Matomäki, Maynard and Shao [25]. They proved the following theorem.

Theorem 7.1. *[25, Theorem 1.1] Let $\theta > 11/20$. Every sufficiently large odd integer n can be written as a sum of three primes $n = p_1 + p_2 + p_3$ with $|p_i - n/3| \leq n^\theta$ for $i \in \{1, 2, 3\}$.*

This improved the previous result, from $4/7$ to $11/20$. The key component in this improvement was the transference principle, which we introduced in Section 6. The improvement in this variant of the Goldbach problem suggested that usage of the transference principle could yield improvement in the Waring-Goldbach problem with almost equal summands. We ended up proving the following theorem.

Theorem 7.2. (Article I). *Let $s, k \in \mathbb{N}$, $k \geq 2$, $\epsilon > 0$ and $\theta \in (0.525, 1)$. Let R_k be as in Section 1. Suppose that $s > \max(k^2+k, 560)$. Then, for every sufficiently large integer $n \equiv s \pmod{R_k}$, there exist primes $p_1, \ldots, p_s$ such that $|p_i - (n/s)^{1/k}| \leq (n/s)^{\theta/k}$ for each $i = 1, \ldots, k$ and*

$$n = p_1^k + \cdots + p_s^k.$$

This was a significant improvement on the previous results which all had $\theta > 3/4$.

7.1 Limitations

In this subsection, we will briefly explain what kind of limitations the Waring-Goldbach problem with almost equal summands has. These limitations will also demonstrate how Theorem 7.2 is close to optimal in the sense of θ. In fact, the only thing that prevents us allowing $\theta \in (1/2, 1)$, is our current knowledge about primes in short intervals.

7.1.1 Waring's problem with almost equal summands

The Waring problem with almost equal summands has been studied by Dirk Daeman. He proved the following theorem.

***Theorem* 7.1.** *[8, Theorem 1] Let $k \geq 2$ and $\theta \in (1/2, 1)$. Let $s \geq Ck^2 \log k$ for certain $C > 0$. Then, all sufficiently large natural numbers n can be written in the form*

$$n = a_1^k + \cdots + a_s^k, \tag{7.1}$$

where $|a_i - (n/s)^{1/k}| \leq (n/s)^{\theta/k}$ for $i \in \{1, \ldots, s\}$.

The number of the required summands can be improved due to a breakthrough in Vinogradov's mean value theorem by Bourgain, Demeter and Guth [5], but in the sense of θ, the result is almost the best possible. Due to the work of Wright [33] we know that if $\theta < 1/2$, then there exist natural numbers that cannot be written in the form (7.1). In fact, the set of numbers that can be written in the form (7.1) is sparse, which we see from the following lemma.

***Lemma* 7.2.** *Let $s \geq k \geq 2$ and $\theta \in (0, 1/2)$. Let*

$$E(x) := |\{n \leq x \mid n = a_1^k + \cdots + a_s^k, |a_i - (n/s)^{1/k}| \leq (n/s)^{\theta/k}\}|.$$

Then

$$E(x) = o_{k,s,\theta}(x).$$

Proof. Denote $I_U := [sU^k, s(U+1)^k)$ for $U \in \mathbb{N}$. We can see that the sets I_U are all disjoint and that if $t \in I_U$, then $\lfloor (t/s)^{1/k} \rfloor = U$. We also have

$$|I_U| = (1 + o(1))skU^{k-1}. \tag{7.2}$$

Now let

$$S_U := \{x \in I_U \mid x = a_1^k + \cdots + a_s^k, |a_i - U| \leq (U+1)^\theta + 1\}. \tag{7.3}$$

Then

$$E(x) \leq \sum_{U \in \mathbb{N}} \sum_{\substack{n \leq x \\ n \in S_U}} 1 \leq \sum_{\substack{U \in \mathbb{N} \\ sU^k \leq x}} |S_U| \leq \sum_{U \leq (x/s)^{1/k}} |S_U|.$$

Hence it suffices to show that $|S_U| = o_{k,s,\theta}(U^{k-1})$.

Let $x \in I_U$ and let a_i be as in (7.3). Write $a_i = U + b_i$. Then the equation inside (7.3) becomes

$$x = sU^k + k(b_1 + \cdots + b_s)U^{k-1} + \sum_{i=2}^{k} \binom{k}{i} (b_1^i + \cdots + b_s^i)U^{k-i},$$

where $|b_i| \leq (U+1)^\theta + 1$. Since $x \in I_U$, we have by the definition of I_U that $|b_1 + \cdots + b_s| \leq s$, provided that U is large enough in terms of k and s. We can now write

$$x = sU^k + kaU^{k-1} + b,$$

where $|a| \leq s$ and $b \ll sk^2U^{2\theta}U^{k-2}$. Therefore $|S_U| \ll s^2k^2U^{2\theta}U^{k-2}$. By $\theta < 1/2$, we get

$$|S_U| = o_{k,s,\theta}(U^{k-1}).$$

The claim now follows. □

7.1.2 Primes in short intervals

In Section 3 we already considered primes in short intervals. The best result was

$$\pi(x + x^\theta) - \pi(x) \gg \frac{x^\theta}{\log x},$$

for $\theta \geq 0.525$. For $\theta < 0.525$ we do not know whether the interval $[x, x + x^\theta]$ contains even a single prime. This gives us a hard limit when studying the Waring-Goldbach problem with almost equal summands as the representation $n = p_1^k + \cdots + p_s^k$ implies the existence of a prime in the interval $[(n/s)^{1/k} - (n/s)^{\theta/k}, (n/s)^{1/k} + (n/s)^{\theta/k}]$.

7.2 The proof

In section 6, we have already explained how the transference principle can be used to analyse an additive problem. It remains to solve the following problems for the Waring-Goldbach problem with almost equal summands.

Problem* 1.** ***(Dense problem) *Let $A_1, \ldots, A_s \subseteq [N]$ with $|A_1| + \cdots + |A_s| \geq N$. Assume also that sets $A_1, \ldots, A_s$ do not have local obstructions. Can we prove that*

$$\sum_{n = a_1 + \cdots + a_s} 1_{A_1}(a_1) \cdots 1_{A_s}(a_s) \gg N^{s-1},$$

for all $n \in [N]$?

Note that condition $|A_1| + \cdots + |A_s| \geq N$ is necessary (For example $A_1 = \cdots = A_s = [(1/s)(1-\epsilon)N]$ means that $A_1 + \cdots + A_s \subseteq [(1-\epsilon)N] \neq [N]$). Solving the dense problem is needed for the equation (6.3) to hold.

Problem* 2.** ***(Local Problem) *Let $q \in \mathbb{N}$. When*

$$n \in s\mathbb{Z}_q^{*(k)}$$

is soluble, for a given $n \in \mathbb{Z}_q$?

The necessity of solving the local problem is explained in Section 6.2.2.

Problem* 3. *(Pseudorandom majorant function) *Let $x > 1$. Can we find a suitable pseudorandom majorant function for the function that approximates*

$$f(n) = \begin{cases} 1 & \text{if } n = p^k \wedge |p - x^{1/k}| \leq x^{\theta/k}, \\ 0 & \text{otherwise}. \end{cases}$$

A suitable pseudorandom majorant function is required for Lemma 6.1.

Problem* 4. *(Restriction estimate) *For a suitable chosen pseudorandom function $f : [N] \to \mathbb{R}_{\geq 0}$, what is the smallest $s \in \mathbb{N}$ such that*

$$\int_0^1 \Big| \sum_{n \leq N} f(n) e(\alpha n) \Big|^{2s} d\alpha \ll N^{2s-1}?$$

The restriction estimate is used to guarantee that (6.5) holds. Note that if h is a majorant function of function g, then for $s \in \mathbb{N}$ we have

$$\begin{aligned} ||\widehat{g}||_{2s}^{2s} &= \sum_{a_1 + \cdots + a_s = a_{s+1} + \cdots + a_{2s}} g(a_1) \cdots g(a_{2s}) \\ &\leq \sum_{a_1 + \cdots + a_s = a_{s+1} + \cdots + a_{2s}} h(a_1) \cdots h(a_{2s}) = ||\widehat{h}||_{2s}^{2s}. \end{aligned}$$

The local problem is a straightforward application of the results of [19] and the restriction estimate can be dealt with using the standard circle method machinery. In the next two subsections, we will look into the dense problem and into the problem of finding a suitable pseudorandom function.

7.2.1 Dense problem

In this subsection, we explain how we solved the dense problem (Problem 1). Our aim was to proceed in a similar manner as Matomäki, Maynard and Shao did in their paper [25]. They used the arithmetic regularity lemma to prove that

***Lemma* 7.1.** *[25, Proposition 3.2] For any $\epsilon > 0$, there exists constants $\eta = \eta(\epsilon)$ and $c = c(\epsilon)$ such that the following statement holds. Let $N \in \mathbb{N}$ and let $f_1, f_2, f_3 : [N] \to [0,1]$ be functions, with each $f \in \{f_1, f_2, f_3\}$ satisfying the inequality*

$$\mathbb{E}_{n \in P} f(n) \geq 1/3 + \epsilon$$

for each arithmetic progression $P \subset [N]$ with $|P| \geq \eta N$. Then for each $n \in [N/2, N]$ we have

$$f_1 * f_2 * f_3(n) \geq cN^2.$$

In order to extend this result for more variables, we required the arithmetic regularity lemma regularising multiple functions simultaneously. It was mentioned in the paper by Eberhard, Green and Manners [10] (Referring to having an arithmetic regularity lemma valid for two sets simultaneously) that "While such a statement can be easily established by modifying the arguments of [13], no such result currently appears in the literature". We proved the following version of the regularity lemma.

***Lemma* 7.2.** [1] *Let $N \in \mathbb{N}$. For $k \geq 1$, let $f_1, \ldots, f_k : [N] \to [0,1]$ be functions, $\mathcal{F} : \mathbb{N} \to \mathbb{R}_+$ a growth function and $\epsilon > 0$. Then there exist a quantity $M \ll_{\epsilon,\mathcal{F}} 1$, positive integers $q, d \leq M$ and $(\mathcal{F}(M), N)$-irrational $\theta \in \mathbb{T}^d$ such that, for each $i \in \{1, \ldots, k\}$, we have a decomposition*

$$f_i = f_{str}^{(i)} + f_{sml}^{(i)} + f_{unf}^{(i)}$$

of f_i into functions $f_{str}^{(i)}, f_{sml}^{(i)}, f_{unf}^{(i)} : [N] \to [-1,1]$ such that

1. *$f_{str}^{(i)} = F_i(n/N, n \pmod q, \theta n)$ for some function $F_i : [0,1] \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{T}^d \to [0,1]$ with $||F_i||_{Lip} \leq M$,*

2. *$||f_{sml}^{(i)}||_{l^2(N)} \leq \epsilon$,*

3. *$||f_{unf}^{(i)}||_{U^2(N)} \leq 1/\mathcal{F}(M)$.*

Similar generalisation of the more general [13, Theorem 1.2] can be proven in a similar manner, but in our case, it was sufficient to study the abelian case. Using Lemma 7.2 we proved the following lemma concerning the dense problem.

***Lemma* 7.3.** *For any $\epsilon \in (0,1)$ and $s \in \mathbb{N}$, there exists a constant $\eta = \eta(\epsilon, s) > 0$ such that the following statement holds. Let N and $s > 2$ be natural numbers and, for $i \in \{1, \ldots, s\}$, let $f_i : [N] \to [0,1]$ and $\alpha_i > 0$ be such that*

$$\mathbb{E}_{n \in P} f_i(n) \geq \alpha_i + \epsilon \qquad (7.4)$$

for each arithmetic progression $P \subseteq [N]$ with $|P| \geq \eta N$. Assume that

$$\alpha_1 + \cdots + \alpha_s \geq 1.$$

Then, for each $n \in [N/2, N]$, we have

$$f_1 * \cdots * f_s(n) \gg_{\epsilon,s} N^{s-1}.$$

[1] For the notation used in this lemma, see Article I, Section 4.1.

7.2.2 Pseudorandomness

After solving the dense problem the next important question was to find a suitable pseudorandom function. Let $X, Y, W, N, m, b \in \mathbb{N}$ be such that $(W, b) = 1$,

$$\begin{aligned} W &= 2k^2 \prod_{n \le O(1)} n^2 \prod_{p \le w} p, && (7.5)\\ X &= Wm + b, && (7.6)\\ Y &= WN, && (7.7) \end{aligned}$$

where $w = \log\log\log m$ and $(X+Y)^{1/k} - X^{1/k} = X^{\theta/k}$. Let $\sigma_W(b) = \#\{z \in [W] : z^k \equiv b \pmod W\}$. The simplest candidate for a pseudorandom function is $f_b : [N] \to \mathbb{R}$ defined by

$$f_b(n) := \frac{\phi(W)}{W\sigma_W(b)} X^{1-1/k} \log X 1_{\mathbb{P}}(t) 1_{W(m+n)+b=t^k}.$$

We can prove that this function is pseudorandom when $\theta \ge 7/12$. If we assume the GRH (Generalized Riemann Hypothesis), then we can prove the pseudorandomness of this function for all $\theta > 1/2$. With some additional calculations, using f_b as the pseudorandom function, we could prove the following theorem.

Theorem. *Let $s, k \in \mathbb{N}$, $k \ge 2$, $\epsilon > 0$ and $\theta \in [7/12, 1)$. Suppose that $s > k^2 + k$. Then, for every sufficiently large integer $n \equiv s \pmod{R_k}$, there exist primes $p_1, \ldots, p_s$ such that $|p_i - (n/s)^{1/k}| \le (n/s)^{\theta/k}$ for each $i = 1, \ldots, k$ and*

$$n = p_1^k + \cdots + p_s^k.$$

Under GRH we can take $\theta \in (1/2, 1)$.

We can loosen the condition $\theta \ge 7/12$ if we use an upper bound sieve in place of $1_{\mathbb{P}}$. Let $1_{\mathbb{P}}^+$ be a majorant function for $1_{\mathbb{P}}$ defined by the linear sieve (for the definition of linear sieve see e.g [11, Chapter 12]). Then we can define a pseudorandom majorant function $\nu_b : [N] \to \mathbb{R}$ for $\frac{1}{\alpha^+} f_b$ by

$$\nu_b(n) := \frac{\phi(W)}{\alpha^+ W\sigma_W(b)} X^{1-1/k} \log X 1_{\mathbb{P}}^+(t) 1_{W(m+n)+b=t^k}, \tag{7.8}$$

where α^+ is constant chosen such that $\mathbb{E}_{n\ in[N]} \nu_b(n) = 1 + o(1)$.

We proved the pseudorandomness of $\nu_b(n)$ for $\theta > 1/2$. The strategy to prove the pseudorandomness is similar to the strategy explained in Section 6.2.3.

For the minor arcs, we used an application of [20, Lemma 1].

In the major arcs, we needed to take into account the sieve weights. We also saw that using bare partial summation for deriving (6.8)-type formula will result a requirement $s \ge Ck^2$ for some large coefficient $C > 1$. Instead we developed some ideas from [29, Section 4] to derive suitable (6.8)-type formula. For (6.9)-type vanishment of rational exponential sum we adapted ideas from [7, Section 4].

8 A density version of Waring's problem

In Article II, we studied a density version of Waring's problem. The study of the problem was motivated by similar studies on Goldbach's problem by Hongze Li and Hao Pan in [23] and Xuancheng Shao in [28]. For example Shao proved that

***Theorem* 8.1.** *Let $A \subset \mathbb{N}$ be a subset of the primes with $\delta_{\mathbb{P}}(A) > 5/8$. Then for sufficiently large odd positive integers N, there exist $a_1, a_2, a_3 \in A$ with $N = a_1 + a_2 + a_3$.*

The density results on the Goldbach problem were derived using the strategy explained in Section 6.3. The most crucial part was to understand, when the following local problem was soluble

Problem. *Let $q \in \mathbb{N}$ and $A \subseteq \mathbb{Z}_q^*$. What is the smallest $\delta > 0$ such that if $|A| > \delta|\mathbb{Z}_q^*|$, then necessarily*

$$A + A + A = \mathbb{Z}_q?$$

The strategy in Section 6.3 is also suitable for attacking a density version of Waring's problem. Using the strategy we proved the following theorem.

***Theorem* 8.2.** *Let $s, k \in \mathbb{N}$, $k \geq 2$, $s > \max(16k\omega(k) + 4k + 3, k^2 + k)$, where $\omega(k)$ is the number of distinct prime factors of k. Let $A \subseteq \mathbb{N}^{(k)}$ be such that $\delta_{\mathbb{N}^{(k)}}(A) > (1 - \mathcal{Z}_k^{-1}/2)^{1/k}$, where $\mathcal{Z}_k$ is a certain constant depending on k for which it holds that $\mathcal{Z}_k > 1$ for every k and $\lim_{k\to\infty} \mathcal{Z}_k = 1$. Let R_k be as in Section 1. Then, for all sufficiently large integers $n \equiv s \pmod{R_k}$, we have $n \in sA$.*

Note that the bound $s > k^2 + k$ coming from the restriction estimate can likely be improved using the latest progress on the restriction theory related to Waring's problem.

Using a simple density based argument we also proved the following theorem.

***Theorem* 8.3.** *Let $k \geq 2$ and $\delta > 0$. Let $A \subseteq \mathbb{N}^{(k)}$ be such that A is not a subset of any non-trivial [1] arithmetic progression and $\delta_{\mathbb{N}^{(k)}}(A) > \delta$. There exists $s = s(k, \delta) \in \mathbb{N}$ such that $sA \simeq \mathbb{N}$.*

The set $A \subseteq \mathbb{N}^{(k)}$ cannot belong to a non-trivial arithmetic progression when $\delta_{\mathbb{N}^{(k)}}(A) > \max_{p:p-1|k} \frac{p-1}{p}$. (See Article II, Introduction)

[1] By *non-trivial* we mean that the moduli of the arithmetic progression is not equal to 1.

8.1 Proof

Similarly to Section 7.2 we needed to solve four problems in order to prove Theorem 8.2.

Problem. ***(Dense problem)*** *For the relevant sets* $A_1, \ldots, A_s \subseteq [N]$ *can we prove that*

$$\sum_{n=a_1+\cdots+a_s} 1_{A_1}(a_1)\cdots 1_{A_s}(a_s) \gg N^{s-1},$$

for all $n \in \left((1-\epsilon)\frac{sN}{2}, (1+\epsilon)\frac{sN}{2}\right)$, *where* $\epsilon > 0$ *is suitable small.*

Solving the dense problem is necessary for the equation (6.3) to hold. The proof is just a simple application of a quantitative version of the Cauchy-Davenport theorem.

Lemma* 8.1.** ***(Cauchy-Davenport) *Let* p *be a prime and* $A, B \subseteq \mathbb{Z}_p$ *with* $A, B \neq \emptyset$. *Then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

Problem. ***(Local Problem)*** *Let* $W = \prod_{p\leq w} p$ *for some* $w \in \mathbb{N}$. *For* $A \subseteq \mathbb{Z}_W^{*(k)}$ *when*

$$sA = \{a \in \mathbb{Z}_W \mid a \equiv s \pmod{(R_k, q)}\}$$

for some $s \in \mathbb{N}$ *with* $s = o(k^2)$.

Note that $sA \subseteq \{a \in \mathbb{Z}_W \mid a \equiv s \pmod{(R_k, q)}\}$ for all $A \subseteq \mathbb{Z}_W^{*(k)}$. Here we want $s = o(k^2)$, since the restriction estimate to be defined below will give us the requirement $s \gg k^2$.

Solving this local problem is necessary due the use of the W-trick as explained in Section 6.2.2.

Problem. ***(Pseudorandomness)*** *Let* $A \subseteq \mathbb{N}^{(k)}$, $N \in \mathbb{N}$, $W = \prod_{p\leq \log\log\log N} p^k$ *and* $b \in [W]$ *with* $(b, W) = 1$. *Prove that the function* $f_b : [N] \to \mathbb{R}$ *is pseudorandom, where*

$$f_b(n) := \frac{k}{\sigma_W(b)}(Wn+b)^{(k-1)/k} 1_{\mathbb{N}^{(k)}}(Wn+b).$$

The pseudorandomness is required for Lemma 6.1. Although it was clear that this function is pseudorandom, there was no existing proofs of the pseudorandomness in the literature. We proved the pseudorandomness using a simpler variant of the arguments in Article I.

Problem. ***(Restriction estimate)*** *What is the smallest* $s \in \mathbb{N}$ *such that*

$$\int_0^1 \Big|\sum_{n\leq N} f_b(n)e(\alpha n)\Big|^{2s} d\alpha \ll N^{2s-1}?$$

The restriction estimate is used to guarantee that (6.5) holds. We deal with the restriction estimate using the circle method machinery.

There was also an additional complication on transferring sufficient arithmetic information from the positive density subset of k-th powers to the dense problem, but we will not address this issue here.

8.1.1 Local problem

In this subsection, we introduce the ideas used to tackle the local problem.

Let $q, s \in \mathbb{N}$. We say that (q, s) is a *Waring pair* if, for any $A \subseteq \mathbb{Z}_q^{*(k)}$ with $|A| > \frac{1}{2}|\mathbb{Z}_q^{*(k)}|$, we have $sA = \{a \in \mathbb{Z}_q \mid a \equiv s \pmod{(R_k, q)}\}$. Let $W = \prod_{p \leq w} p^k$ for some $w \in \mathbb{N}$. Our aim was to prove that

***Proposition* 8.2.** *(W, s) is a Waring pair for any $s \geq 8k\omega(k) + 2k + 2$.*

First we were able to see that Waring pairs have some multiplicative structure.

***Lemma* 8.3.** *Let $q, r, s, t \in \mathbb{N}$ and $(q, r) = 1$. If (q, s) and (r, t) are Waring pairs, then $(qr, s + t)$ is a Waring pair.*

As the usage of the previous lemma effectively doubles the number of required summands in each of its usages, it means that we can use it only a few times.

Using a generalisation of the Cauchy-Davenport theorem we were able to prove the following lemma.

***Lemma* 8.4.** *Let p be a prime. Then (p^k, s) is a Waring pair for all $s \geq 8k$.*

The next lemma contained a crucial idea for solving the local problem. It allowed us to lift the exponent at the cost of only two additional summands.

***Lemma* 8.5.** *Let $e, s \in \mathbb{N}$. Let q be a square-free natural number with $(q, k) = 1$. If (q, s) is a Waring pair, then $(q^e, s + 2)$ is also a Waring pair.*

Let A with $|A| > \frac{1}{2}|\mathbb{Z}_q^{*(k)}|$. The key idea in the proof of Lemma 8.5 was that using Hensel's lemma and the pigeonhole principle we can find a vertical arithmetic progression $a + q\mathbb{Z}_{q^{e-1}}$ and a horizontal arithmetic progression $[tq, (t + 1)q)$ such that A has a density greater than $1/2$ in those arithmetic progressions.

Applying the Cauchy-Davenport theorem and a downset idea from [24] we were able to prove the following lemma, which was the final essential item of missing information.

***Lemma* 8.6.** *Let q be a square-free natural number with $(q, k) = 1$. Then (q, s) is a Waring pair for all $s \geq 2k$.*

Combining all these results gives us Proposition 8.2.

8.2 Correction

There is an error in the proof of Theorem 8.3 in the published version of [II, Section 4.3]. The problem in the proof is that the number of required summands does not only depend on k and δ, but also the structure of the set A. We provide corrected version of the proof here.

Corrected proof of Theorem 8.3. For $B \subset \mathbb{N}$ and $s \in \mathbb{N}$ let

$$r_B^s(n) := |\{a_1, \ldots, a_s \in B \mid n = a_1 + \cdots + a_s\}|.$$

Let $N \in \mathbb{N}$ be sufficiently large and $A' = A \cap [N]$. By Cauchy-Schwarz inequality and [26, Theorem 5.7]

$$\Big(\sum_{n \in sA'} r_{A'}^s(n)\Big)^2 \le |sA'| \sum_{n \in sA'} r_{A'}^s(n)^2 \le |sA'| \sum_{n \in [sN]} r_{\mathbb{N}^{(k)} \cap [N]}^s(n)^2 \ll_{k,s} |sA'| N^{2s/k-1}$$

provided that $s > 2^k$. On the other hand

$$\sum_{n \in sA'} r_{A'}^s(n) \ge |A \cap [N]|^s \gg_{\delta,s} N^{s/k}.$$

Hence

$$|s(A \cap [N])| > c(k, s, \delta) N \tag{8.1}$$

for all large $N \in \mathbb{N}$ and for some small constant $c(k, s, \delta) > 0$ that depends on k, s and δ.

For $B \subseteq \mathbb{Z}_{\ge 0}$ we define Shnirel'man density

$$\sigma(B) := \inf_{N \in \mathbb{N}} \frac{|B \cap [N]|}{N}.$$

Next, we prove the following claim.

***Claim* 1.** *Let $B \subseteq \mathbb{N}$ and $\delta' > 0$ such that*

$$\liminf_{N \to \infty} \frac{|B \cap [N]|}{N} > \delta'. \tag{8.2}$$

Assume that B is not a subset of a non-trivial arithmetic progression. Then uB contains two consecutive natural numbers, for some $u \in \mathbb{N}$ large enough depending on δ'.

Proof of the Claim 1. By (8.2) there exists a non-zero $d \in B - B$ with $d = O_{\delta'}(1)$. Let $D = \{n \in B - B \mid n \equiv 0 \pmod d\}$. By (8.2) and the pigeonhole principle there exists an arithmetic progression $P = \{dn + a \mid n \in \mathbb{N}\}$, for some $a \in [d]$, such that

$$\liminf_{N \to \infty} \frac{|(B \cap P) \cap [N]|}{N} > \delta'/d. \tag{8.3}$$

Hence
$$\liminf_{N\to\infty} \frac{|D\cap[N]|}{N} > \delta'/d. \tag{8.4}$$
Let $H = \{n \in \mathbb{Z}_{\geq 0} \mid nd \in D\}$. We see that $0, 1 \in H$. We see by (8.4) that H has a positive Shnirel'man density. It now follows by [26, Theorem 7.7] that there exists $t = O_{\delta'}(1)$ such that
$$d\mathbb{Z} \subseteq tB - tB \tag{8.5}$$

Since B is not contained in any non-trivial arithmetic progression, there exist $u \in \mathbb{N}$ with $u = O_d(1)$ and $a_1, \ldots, a_u \in \mathbb{N}$ with $a_i + d \in B - B$ for all $i = 1, \ldots, u$ such that $(a_1, \ldots, a_u, d) = 1$. Hence $a_1, \ldots, a_u$ generates $1 \pmod d$ and so for some $v = O_d(1)$ we have
$$1 \in tB - tB + vB - vB.$$
Thus set $(t+v)B$ contains two consecutive natural numbers. $\square$

By (8.1) we can see that
$$\liminf_{N\to\infty} \frac{|sA\cap[N]|}{N} > 0.$$
Since A does not belong to a non-trivial arithmetic progression neither does sA. Thus by Claim 1 we obtain that usA contains two consecutive natural numbers for some $u \in \mathbb{N}$ with $u = O_\delta(1)$. Therefore $\sigma(usA - N) > 0$ for some $N \in usA$. Write $A'' = usA - N$. By [26, Theorem 7.7] there exists $v \in \mathbb{N}$ with $v = O_{\sigma(A'')}(1)$ such that $vA'' = \mathbb{N}$. Therefore all sufficiently large natural numbers belong to the sumset $(vus)A$ and $vus = O_{\delta,k}(1)$. $\square$

9 The Goldbach conjecture with summands in arithmetic progressions

In Article III, we studied the binary Goldbach conjecture in a case where the summands were restricted to arithmetic progressions with large moduli. Let $N > 0$ and define

$$E_{b_1,b_2,r}(N) := \#\{2n \le N \mid \ 2n \equiv b_1 + b_2 \pmod r, 2n \ne p_1 + p_2 \\ \text{for all primes } p_i \equiv b_i \pmod r\}.$$

The problem we were interested was

Problem. *Let $R, M \in \mathbb{N}$. In what circumstances, can we obtain*

$$E_{b_1,b_2,r}(N) = o(N/r),$$

where $N \le M$, $r \le R$ and $b_1, b_2 \in \mathbb{Z}_r$?

The best previous result concerning the size of R was from Claus Bauer [3].

Theorem 9.1. *[3, Theorem 1] Let $\epsilon > 0$, $A, B > 0$, $N \ge 3$ and $R \le N^{1/3-\epsilon}$. Then, for all but $O(R/\log^B N)$ primes $3 \le r \le R$, for any fixed $b_1 \pmod r$ with $(b_1, r) = 1$ and for all but $O(r/\log^B r)$ integers $b_2 \pmod r$ with $(b_2, r) = 1$, we have*

$$E_{b_1,b_2,r}(N) = o(N/r),$$

provided that A is large enough depending on B.

The proof of the previous theorem relies heavily on the Bombieri-Vinogradov theorem, but it did not reach the exponent $1/2$ (i.e. the range $R \le N^{1/2-\epsilon}$) in the Bombieri-Vinogradov theorem. The natural question was whether the gap could be filled and it was the main motivating factor for studying the problem. We were able to fill the gap and proved the following theorem.

Theorem 9.2. *Let $A, B > 0$, $N \ge 3$ and $R \le N^{1/2}/\log^A N$. Then, for all but $O(R/\log^B N)$ integers $3 \le r \le R$, for any fixed $b_1 \pmod r$ with $(b_1, r) = 1$ and for all but $O(r/\log^B r)$ integers $b_2 \pmod r$ with $(b_2, r) = 1$, we have*

$$E_{b_1,b_2,r}(N) = o(N/r),$$

provided that A is large enough depending on B.

We were also able to prove the following theorems, where the exceptional set for the moduli is very small.

Theorem 9.3. *Let $\epsilon > 0$ and $N \geq 3$. There exists $D > 0$ such that, for all but $O(\log^D N)$ primes $r \leq N^{5/24-\epsilon}$, for any fixed $b_1, b_2 \pmod r$ with $(b_1, r) = (b_2, r) = 1$, we have*

$$E_{b_1,b_2,r}(N) = o(N/r).$$

Theorem 9.4. *Let $B, \epsilon > 0$ and $N \geq 3$. There exists $D > 0$ such that, for all but $O(\log^D N)$ primes $3 \leq r \leq N^{5/12-\epsilon}$, for any fixed $b_1 \pmod r$ with $(b_1, r) = 1$ and for all but $O(r/\log^B r)$ integers $b_2 \pmod r$ with $(b_2, r) = 1$, we have*

$$E_{b_1,b_2,r}(N) = o(N/r).$$

Theorems 9.3 and 9.4 improve the previous similar results from Bauer. (See Article III, Introduction)

Assuming the GRH (Generalized Riemann Hypothesis), we can completely dispose of the exceptional sets for the moduli from Theorems 9.2 and 9.3, and replace the exponent $5/24$ in Theorem 9.3 with $1/4$.

9.1 Freiman isomorphism

The proof of Theorem 9.2 is based on the idea of using a Freiman isomorphism inside the circle method. Next, we define the Freiman isomorphism.

Let A and B be subsets of abelian groups G_A and G_B respectively. The bijective map $\phi : A \to B$ is called a *Freiman isomorphism of order s* if

$$a_1 + \cdots + a_s = a'_1 + \cdots + a'_s$$

holds if and only if

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(a'_1) + \cdots + \phi(a'_s),$$

where $a_1, \ldots, a_s, a'_1, \ldots, a'_s \in A$.

In the circle method, we can use a Freiman isomorphism in the following way. If $G_B \subseteq \mathbb{Z}$, then

$$\sum_{\substack{a_1+\cdots+a_s=n \\ a_i \in A}} 1 = \sum_{\substack{\phi(a_1)+\cdots+\phi(a_s)=n' \\ a_i \in A}} 1 = \int_0^1 \Big(\sum_{a\in A} e(\alpha\phi(a))\Big)^s e(-\alpha n'),$$

where $n' = \phi(b_1) + \cdots + \phi(b_s)$ for any choice of $b_1, \ldots, b_s \in \mathbb{N}$ with $b_1 + \cdots + b_s = n$.

9.2 The key idea

The main idea for the improvement came when we tried to use the transference principle for the problem. Due to the use of the W-trick, our pseudorandom function was twisted with a Freiman isomorphism:

$$\nu_b(n) = \frac{\phi(W)}{W}\log(Wn+b)1_{\mathbb{P}}^{+}(Wn+b).$$

When we tried to prove the pseudorandomness in the minor arcs, we saw that the size of W affected the strength of Type I sum estimates. This led us to the realisation that if we use a suitable Freiman isomorphism with the circle method, we can overcome the major problems coming from Type I and Type II sum estimates in the previous papers.

Let us illustrate this idea. Let

$$S_{b,r}(H,\alpha) := \sum_{n\le H}\Lambda(rn+b)e(\alpha n),\ S'_{b,r}(H,\alpha) := \sum_{\substack{n\le H\\ n\equiv b \pmod r}}\Lambda(n)e(\alpha n)$$

and $M = rN + b_1 + b_2$. In the previous papers, the circle method was applied in the following way.

$$\sum_{\substack{M=n_1+n_2\\ n_i\equiv b_i \pmod r}}\Lambda(n_1)\Lambda(n_2) = \int_0^1 S'_{b_1,r}(M,\alpha)S'_{b_2,r}(M,\alpha)e(-\alpha M)d\alpha.$$

We applied the circle method with Freiman isomorphism in the following way.

$$\sum_{N=n_1+n_2}\Lambda(rn_1+b_1)\Lambda(rn_2+b_2) = \int_0^1 S_{b_1,r}(N,\alpha)S_{b_2,r}(N,\alpha)e(-\alpha N)d\alpha.$$

Both sums essentially count the same solutions. The standard way to evaluate S, S'-type sums in the minor arcs is to use Vaughan's identity to split sums over $\Lambda(n)$ to Type I and Type II sums (as explained in Section 4). In the next two subsections, we will illustrate the differences between Type I and II estimates corresponding to S' and S.

Let $\alpha\in[0,1]$ and $a,q\in\mathbb{N}$ be such that $1\le a\le q$, $(a,q)=1$ and $|\alpha - a/q|\le q^{-2}$. Let $N,M\ge 1$. Let a_n be a complex sequence such that $|a_n|\le 1$. Write $X := NM$.

9.2.1 Differences between Type I estimates

For Type I sums corresponding to S', we have

$$\sum_{\substack{n\sim N, m\sim M\\ nm\equiv b \pmod r}} a_m e(\alpha nm) \ll \frac{X}{r\log^A X}, \tag{9.1}$$

provided that

$$r\log^{A'} X \le q \le X/(r\log^{A'} X) \text{ and } M \le X/(r^2\log^{A'} X)$$

for some $A' > 0$ depending on A.

For Type I sums corresponding to S, we have

$$\sum_{\substack{n\sim N, m\sim M \\ nm\equiv b \pmod r}} a_m e_r(\alpha nm) \ll \frac{X}{r\log^A X}, \tag{9.2}$$

provided that

$$\log^{A'} X \le q \le X/(r\log^{A'} X) \text{ and } M \le X/(r\log^{A'} X)$$

for some $A' > 0$ depending on A.

We can see that (9.1) leaves us a challenging major arc case $\log^{A'} X \le q < r\log^{A'} X$. Whereas the estimate (9.2) gives us the standard major arcs, which are straight-forward to evaluate.

9.2.2 Differences between Type II estimates

For Type II sums corresponding to S', we have

$$\sum_{\substack{b \pmod r \\ (b,r)=1}} \Big| \sum_{\substack{n\sim N, m\sim M \\ nm\equiv b \pmod r}} a_m b_n e(\alpha nm)\Big|^2 \ll \frac{X^2}{r\log^A X}, \tag{9.3}$$

provided that

$$r\log^{A'} X \le q \le X/(r\log^{A'} X) \text{ and } r\log^{A'} X \le M \le X/(r\log^{A'} X)$$

for some $A' > 0$ depending on A.

For Type II sums corresponding to S, we have

$$\sum_{\substack{b \pmod r \\ (b,r)=1}} \Big| \sum_{\substack{n\sim N, m\sim M \\ nm\equiv b \pmod r}} a_m b_n e_r(\alpha nm)\Big|^2 \ll \frac{X^2}{r\log^A X}, \tag{9.4}$$

provided that

$$\log^{A'} X \le q \le X/(r\log^{A'} X) \text{ and } \log^{A'} X \le M \le X/(r\log^{A'} X)$$

for some $A' > 0$ depending on A.

When we use Vaughan's identity, (9.1) and (9.3), we can estimate $S'_{b,r}(H,\alpha)$ on average over $r \le X^{1/3}/\log^{O(1)} X$, whereas when we use Vaughan's identity, (9.2) and (9.4) we can estimate $S_{b,r}(H,\alpha)$ on average over $r \le X^{1/2}/\log^{O(1)} X$. For this reason, it is beneficial to work with S instead of S'.

List of References

[1] R. C. Baker and G. Harman. The three primes theorem with almost equal summands. *R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci.*, 356(1738):763–780, 1998.

[2] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes. II. *Proc. London Math. Soc. (3)*, 83(3):532–562, 2001.

[3] C. Bauer. Goldbach's conjecture in arithmetic progressions: number and size of exceptional prime moduli. *Arch. Math. (Basel)*, 108(2):159–172, 2017.

[4] J. Bourgain. On the Vinogradov mean value. *Tr. Mat. Inst. Steklova*, 296(Analiticheskaya i Kombinatornaya Teoriya Chisel):36–46, 2017.

[5] J. Bourgain, C. Demeter, and L. Guth. Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math. (2)*, 184(2):633–682, 2016.

[6] 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*, 17:385–386, 1966.

[7] S. Chow. Roth–Waring–Goldbach. *Int. Math. Res. Not. IMRN*, (8):2341—-2374, 2018.

[8] D. Daemen. The asymptotic formula for localized solutions in Waring's problem and approximations to Weyl sums. *Bull. Lond. Math. Soc.*, 42(1):75–82, 2010.

[9] C.-J. de la Vallée Poussin. Recherches analytiques la théorie des nombres premiers. *Ann. Soc. scient. Bruxelles*, 20:183–256, 1896.

[10] S. Eberhard, B. Green, and F. Manners. Sets of integers with no large sum-free subset. *Ann. of Math. (2)*, 180(2):621–652, 2014.

[11] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[12] B. Green. Roth's theorem in the primes. *Ann. of Math. (2)*, 161(3):1609–1636, 2005.

[13] B. Green and T. Tao. An arithmetic regularity lemma, an associated counting lemma, and applications. In *An irregular mind*, volume 21 of *Bolyai Soc. Math. Stud.*, pages 261–334. János Bolyai Math. Soc., Budapest, 2010.

[14] J. Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, 24:199–220, 1896.

[15] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio Numerorum': IV. The singular series in Waring's Problem and the value of the number $G(k)$. *Math. Z.*, 12(1):161–188, 1922.

[16] D. R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, 389:22–63, 1988.

[17] H. A. Helfgott. The ternary goldbach conjecture is true, 2014.

[18] D. Hilbert. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem). *Math. Ann.*, 67(3):281–300, 1909.

[19] L. K. Hua. *Additive theory of prime numbers*. Translations of Mathematical Monographs, Vol. 13. American Mathematical Society, Providence, R.I., 1965.

[20] B. Huang. Exponential sums over primes in short intervals and an application to the Waring-Goldbach problem. *Mathematika*, 62(2):508–523, 2016.

[21] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, 15:164–170, 1972.

[22] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[23] H. Li and H. Pan. A density version of Vinogradov's three primes theorem. *Forum Math.*, 22(4):699–714, 2010.

[24] K. Matomäki. Sums of positive density subsets of the primes. *Acta Arith.*, 159(3):201–225, 2013.

[25] K. Matomäki, J. Maynard, and X. Shao. Vinogradov's theorem with almost equal summands. *Proc. Lond. Math. Soc. (3)*, 115(2):323–347, 2017.

[26] M. B. Nathanson. *Additive number theory*, volume 164 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. The classical bases.

[27] K. F. Roth. On certain sets of integers. *J. London Math. Soc.*, 28:104–109, 1953.

[28] X. Shao. A density version of the Vinogradov three primes theorem. *Duke Math. J.*, 163(3):489–512, 2014.

[29] R. C. Vaughan. *The Hardy-Littlewood method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.

[30] R. C. Vaughan and T. D. Wooley. Waring's problem: a survey. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 301–340. A K Peters, Natick, MA, 2002.

[31] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. Interscience Publishers, London and New York., 1954. Translated, revised and annotated by K. F. Roth and Anne Davenport.

[32] T. D. Wooley. New estimates for smooth Weyl sums. *J. London Math. Soc. (2)*, 51(1):1–13, 1995.

[33] E. M. Wright. The representation of a number as a sum of four 'almost equal' squares. *The Quarterly Journal of Mathematics*, os-8(1):278–279, 1937.

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

Painosalama Oy, Turku, Finland 2022

ISBN 978-951-29-8824-2 (PRINT)
ISBN 978-951-29-8825-9 (PDF)
ISSN 0082-7002 (PRINT)
ISSN 2343-3175 (ONLINE)