Niclas Technau, M.Sc.

Counting Lattice Points, Diophantine Approximation, and Metric Poissonian Pair Correlations

DOCTORAL THESIS

to achieve the university degree of

Doktor der Naturwissenschaften

submitted to

Graz University of Technology

Supervisor

O.Univ.-Prof. Dr.phil. Dr.h.c. Robert Tichy

Institute of Analysis and Number Theory

Graz, April, 2018

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral thesis.

Date

Signature

Contents

Acknowledgments

> "Gar nicht von sich reden, ist eine sehr vornehme Heuchelei."[1]
> — F. Nietzsche [86, p. 294]

The present manuscript is the outcome of several years of work, and the path before it. So, many thanks are due to the various people who helped me along that path.

Firstly, I would like to express my sincere gratitude to my supervisor, Robert Tichy, for his kind and constant support throughout my various mathematical endeavours. Additionally, he contributed to making my time in Graz not only productive but also enjoyable. With the same breath, I would like to thank my family for their kind and constant support in (almost) all my endeavours — you make my life enjoyable; there is much more to say, however I prefer to do deeds instead of using words in this matter.

Secondly, many thanks are due to my coauthors and teachers; in particularly, to Christoph (Aistleitner), Christian (Elsholtz), and Martin (Widmer) — you influenced, in multiple ways, this thesis as well as my ongoing journey to mathematical expertise: the joint work with Martin makes up Chapter 2, Christoph's influence[2] is visible in Chapters 3 to 5 while the research with Christian constitutes the Appendices A, B — sadly, some selection had to be made in order to give this thesis a unifying framework! Moreover, I am grateful to Victor (Beresnevich), and Gerhard Larcher for agreeing to be external examiners for this thesis. Furthermore, I would like to thank my teachers Mr. J. Berger, Dr. G. Metzger, and Dr. B. Leue for making those years in gymnasium more bearable by doing far more than duty required. Additionally, many cordial thanks are due to my senseis from various places — Stegen, Freiburg, Würzburg and Graz — who enhanced and fortified the way I think and work, by sharing their skills: C. Kehl, A. Kempf, S. Plos, H.-D. Rauscher, G. Riedl, T. Rönicke, and F. Scheiner.

Thirdly, I am grateful to various colleagues for the wonderful time that was allowed to spent with them in Graz, as well as in Bremen, Hanover, London, Würzburg, and York. Please pardon me for not trying to mention everyone by name — there are plainly too many! As *partes pro toto*, I cordially thank Carsten (Elsner), Dijana (Kreso), Thomas (Lachmann), Dierk (Schleicher), Sam (Chow), and Sanju (Velani). Moreover, I am very grateful to Kamil (Feucht) for being a great friend throughout the years and, besides that, for teaching me "these things you are *not* allowed to know," the basics of parkour, and riding motorcycles. Further, appreciation is due to my "arch-nemesis" for being a worthy(!) foe along the way, and getting me interested in bouldering. Furthermore, thanks are due to Irene (Pfeifer-Wilfinger) and Hermi(ne) (Panzenöck) for always helping, if needed, with bureaucratic matters.

[1] In English (translated by N. T.): "Not to talk at all about oneself is a very noble cant."

[2] Christoph also deserves thanks for being, according to my terminology, *the archduke of the Fufu Seminar* — a serious mathematical seminar that usually ends by eating fufu, an African root dish. It should be noted that the title archduke is alluding to the fact that the TU Graz is also called *Erzherzog-Johann Universität*, and that the Fufu Seminar is, similarly, a gift by a different archduke.

Last but not least, I sincerely thank the mathematical community itself — allow me to stress that without the collective efforts of previous generations to improve, put to scrutiny, and pass on their knowledge, a thesis, such as this one, would simply be inconceivable. Amongst the many names which would be worth mentioning here, I thank, as *partes pro toto*, Wolfgang Schmidt, Maxim Skriganov, and Zeév (Rudnick) for their pioneering work.

Graz, April 20, 2018; N. T.

Dedicated to Farouk, Karin, Kristin, and Mrs. Leue.

Nomenclature

The present section collects, for the convenience of the reader, notation which is frequently used in this thesis.

General notation

$\|x\|_2$ denotes the Euclidean norm of $x \in \mathbb{R}^n$.

$\|x\|_\infty$ is the maximum norm of $x \in \mathbb{R}^n$.

$R^{n\times n}$ denotes the set of $n \times n$ matrices with entries from the ring R.

$\|D\|_2$ = the spectral norm (the operator norm induced by $\|\cdot\|_2$) of $D \in \mathbb{R}^{n\times n}$.

$\lambda(S)$ abbreviates the Lebesgue measure of a measurable set $S \subseteq \mathbb{R}$.

$\mathrm{vol}(S)$ denotes the Lebesgue measure of a measurable set $S \subseteq \mathbb{R}^n$.

A_N abbreviates the set of the first N elements of a sequence $(a_n)_n$.

Geometry of numbers related notation

Γ is a lattice of full rank in $\mathbb{R}^n$, i.e. $\Gamma = A\mathbb{Z}^n$ where $A \in \mathbb{R}^{n\times n}$ is invertible.

$\Gamma^\perp$ denotes the dual lattice of Γ; i.e. if $\Gamma = A\mathbb{Z}^n$, then $\Gamma^\perp = (A^{-1})^T\mathbb{Z}^n$.

$\mathcal{L}_n$ abbreviates the set of unimodular lattices in $\mathbb{R}^n$.

$\lambda_i(\Gamma)$ is the i-th successive minima of Γ with respect to the Euclidean unit ball.

$\nu(\Gamma, \cdot)$ denotes the ν-function of the lattice Γ, cf. (2.1.1).

γ_n is the Hermite constant; i.e. the quantity $\sup_{\Gamma\in\mathcal{L}_n} \lambda_1^2(\Gamma)$.

Combinatorics related notation

$\#X$ denotes the cardinality of $X \subset \mathbb{R}$.

$X - Y = \{x - y : x \in X, y \in Y\}$ where $X, Y \subseteq \mathbb{R}$.

$\mathrm{r}_{X-Y}(d) = \#\{(x - y) \in X \times Y : d = x - y\}$ where $X, Y \subseteq \mathbb{R}$, and $d \in \mathbb{R}$.

$E(I)$ abbreviates $\#\{(a, b, c, d) \in I^4 : a + b = c + d\}$ where $I \subseteq \mathbb{R}$.

Analytic number theory related notation

$\mathcal{O}(\cdot), o(\cdot)$ is the Landau notation with their usual meaning.

$g = \Omega(f)$ means there is a $c > 0$ such that $g(x) > cf(x)$ holds for infinitely many x.

$\ll, \gg$ are the Vinogradov symbols with their usual meaning.

$g \asymp f$ denotes that both $f \ll g$, and $g \ll f$ holds.

$f \sim g$ means $f(x) = g(x)(1 + o(1))$.

(a, b) denotes the greatest common divisor of $a, b \in \mathbb{Z}$.

$\varphi(a)$ $= \#\{1 \leq b \leq a : (a, b) = 1\}$ where $a \in \mathbb{Z}$.

$\lfloor a \rfloor$ equals $\max\{b \in \mathbb{Z} : b \leq a\}$ where $a \in \mathbb{R}$.

$\langle x \rangle$ abbreviates $x - \lfloor x \rfloor$ where $x \in \mathbb{R}$.

p denotes a prime element in $\mathbb{Z}_{\geq 1}$.

$\pi(x)$ abbreviates $\#\{p : p \leq x\}$ where $x \in \mathbb{R}$.

$a \mid b$ means that $a \in \mathbb{Z}$ divides $b \in \mathbb{Z}$.

$\omega(n)$ is the cardinality of $\{p : p \mid n\}$ where $n \in \mathbb{Z}_{\geq 1}$.

$e(x)$ $= \exp(2\pi i x)$ where $x \in \mathbb{R}$.

$|x|$ is the absolute value of $x \in \mathbb{R}$ (with the exception of Appendix A where it denotes the norm of $x \in G$ for a given arithmetic semi-group G).

$\|x\|$ equals $\min\{|x - y| : y \in \mathbb{Z}\}$ where $x \in \mathbb{R}$.

$R(\cdot, \cdot, \cdot)$ denotes the Poissonian pair correlations counting function, cf. (1.3.1).

Chapter 1

Preface

> "In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat; it was a hobbit-hole, and that means comfort."
> — J. R. R. Tolkien [119, Ch.1, p.1].

In this section, we detail the content of the subsequent chapters, put the investigated problems in their general context, and mention the established methods of investigation. Doing so allows us to present the main results of the thesis at hand against that background. In the process, we draw on the papers [11, 13, 41, 42, 73, 117] which form the backbone of the present thesis. We begin by elaborating on the first chapter.

1.1 Counting Lattice Points

Counting problems in various branches of natural sciences — such as (algebraic) number theory, coding theory, Diophantine approximation, mathematical physics, Diophantine geometry, and spectral analysis — can be solved by reformulating the problem into a lattice point counting problem, cf. [26, 40, 82, 107, 128]. However, for avoiding misinterpretations, let us stress that by a lattice Γ in $\mathbb{R}^n$ we mean the $\mathbb{Z}$-span of n vectors in $\mathbb{R}^n$ which are required to be $\mathbb{R}$-linearly independent.

The general lattice point counting problem is to determine, for a given set $S \subseteq \mathbb{R}^n$, the cardinality of $\Gamma \cap S$. If S is a compact set whose boundary is not "too distorted," then one expects that $\#(\Gamma \cap S)$ roughly equals $\operatorname{vol}(S) / \det \Gamma$ where $\operatorname{vol}(S)$ denotes the Lebesgue measure of S, and $\det \Gamma \coloneqq \det A$ with $A \in \mathbb{R}^{n \times n}$ satisfying $\Gamma = A\mathbb{Z}^n$.

For applications, it is crucial to make this guess precise, and to derive good upper bounds on the error term

$$\mathcal{E}(\Gamma, S) \coloneqq \left| \#(\Gamma \cap S) - \frac{\operatorname{vol}(S)}{\det \Gamma} \right|.$$

In the literature, there are different approaches to estimate $\mathcal{E}(\Gamma, S)$ depending on the Diophantine nature of Γ, and the geometric properties of S. A general, modern approach to lattice point counting can be based on quantitative ergodic theorems; for further reading, we recommend the beautiful work of Gorodnik and Nevo [48].

Following a more classical approach, which dates back to Lipschitz and has been further studied, e.g., in [82, 105, 112], the remainder term $\mathcal{E}(\Gamma, S)$ can be bounded provided S has Lipschitz parameterizable boundary. The most refined bound along these lines of thought is, to the best of our knowledge, due to Widmer [129]. For stating it, we say that $S \subseteq \mathbb{R}^n$ is in $\mathrm{Lip}(n, M, L)$ if there exist M maps $\phi_1, \dots, \phi_M : [0,1]^{n-1} \to \mathbb{R}^n$ satisfying the Lipschitz condition

$$\|\phi_i(x) - \phi_i(y)\|_2 \leq L \|x - y\|_2 \qquad \forall_{x,y \in [0,1]^{n-1}}$$

such that S is covered by the images of the maps ϕ_i where $\|\cdot\|_2$ is the canonical Euclidean norm on $\mathbb{R}^n$; moreover, we denote by $\lambda_i(\Gamma)$, for $i = 1, ..., n$, the i-th successive minima of Γ (with respect to the Euclidean unit ball).

Theorem. *(Widmer, [129, Thm. 5.4]). Let Γ be a lattice in $\mathbb{R}^n$, and S a bounded set in $\mathbb{R}^n$ such that the boundary ∂S of S is in $\mathrm{Lip}(n, M, L)$. Then S is measurable and*

$$\mathcal{E}(\Gamma, S) \leq c(n)\, M \max_{0 \leq i < n} \frac{L^i}{\lambda_1(\Gamma) \cdot \ldots \cdot \lambda_i(\Gamma)}. \tag{1.1.1}$$

For $i = 0$, the expression in the maximum is understood as one. Furthermore, one can choose $c(n) = n^{3n^2/2}$.

Remark. *The Lipschitz assumption above is rather mild, and (1.1.1) yields that $\mathcal{E}(\Gamma, S)$ is less than $\mathrm{vol}(S)/\det(\Gamma)$ as soon as the volume of S is somewhat larger than its diameter.*

For lattice point counting theorems which do not require ∂S directly, and work rather with a tameness property called "o-minimality" we refer the reader to the work of Barroero and Widmer [17] and there references therein; in some constellations, the bound presented in [17, Thm. 1.3] is best possible (up to the involved constant).

In several problems (e.g. from algebraic number theory), it is of interest to count lattice points in homogeneously expanding sets. Therefore, we fix from now on a compact set $S \subseteq \mathbb{R}^n$, a lattice $\Gamma \subseteq \mathbb{R}^n$, and consider the homogeneously expanding family $(S_t)_{t \geq 1}$ of dilatations

$$S_t \coloneqq tS \coloneqq \{ts : s \in S\}$$

by the factor $t \geq 1$. In what follows, we are concerned with bounding $\mathcal{E}(\Gamma, S_t)$ as a function of t such that the dependence on Γ, and S is as explicit as possible.

As an illustration of the delicateness of the arising difficulties, let us make a little detour to a classical, planar example — the Gauß circle problem — in conjunction with

some of its history. On that way, we invite the reader to observe that a straightforward modification of the geometric reasoning presented down below yields, provided S is convex (and compact), that

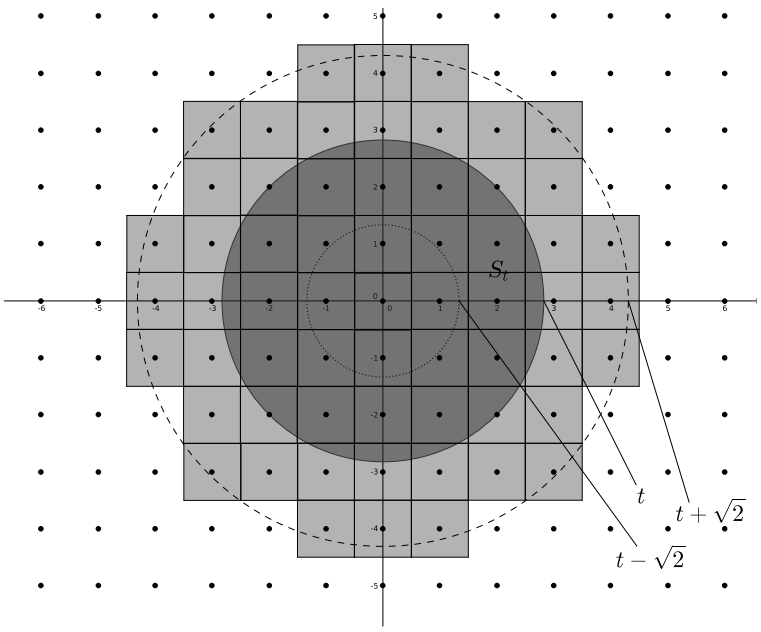
$$\mathcal{E}(\Gamma, S_t) \ll_\Gamma |\partial S_t| \ll_S t^{n-1}, \tag{1.1.2}$$

where $|\partial S_t|$ denotes the surface area of S_t.

Example (Gauß circle problem)**.** *Let $\Gamma := \mathbb{Z}^2$, and denote the planar disc*[1] *of radius t, which is centred at the origin, by*

$$D_t := \{x \in \mathbb{R}^2 : \|x\|_2 \leq t\}.$$

Trivially, $\mathbb{Z}^2 \cap D_{t-\sqrt{2}} \subseteq \mathbb{Z}^2 \cap D_t \subseteq \mathbb{Z}^2 \cap D_{t+\sqrt{2}}$. Furthermore, by attaching to each $\gamma \in \Gamma$ of norm at most $t + \sqrt{2}$ a fundamental region of Γ centred at γ (depicted as a light gray square), we get the following picture.



As illustrated above, we can conclude that $\pi t^2 + \mathcal{O}(t) \leq \#(\mathbb{Z}^2 \cap D_t) \leq \pi t^2 + \mathcal{O}(t)$. Hence, $\mathcal{E}(\mathbb{Z}^2, S_t) \ll t$. Due to Hardy and, independently, Landau we know that

$$\mathcal{E}(\mathbb{Z}^2, S_t) \neq o(t^{1/2} (\log t)^{1/4}).$$

Moreover, it is conjectured that the smallest admissible exponent $\alpha > 0$ such that

$$\mathcal{E}(\mathbb{Z}^2, D_t) \ll_\varepsilon t^{\alpha+\varepsilon} \tag{1.1.3}$$

holds for every $\varepsilon > 0$ is $\alpha = 1/2$. At the time of writing, the smallest (known) admissible value of α in (1.1.3) is $517/824 = 0.627\ldots$ which is due to Bourgain and Watt [27].

[1] As usual, discs are to be taken with respect to the Euclidean norm $\|\cdot\|_2$.

Let us come back to the task of bounding $\mathcal{E}(\Gamma, S_t)$, and consider a unimodular lattice, i.e. a lattice of determinant one, of the form $\Gamma \coloneqq \operatorname{diag}(d_1, \ldots, d_n)\,\mathbb{Z}^n$, where $d_1, \ldots, d_n \in \mathbb{R}$. By specializing $S \coloneqq [0,1]^n$, it follows that $\mathcal{E}(\Gamma, S_t) \gg_\Gamma t^{n-1}$. Hence, we cannot hope to improve upon the trivial bound (1.1.2) without excluding some lattices from our attention by making (Diophantine) assumptions on Γ. It turns out that from a metric perspective, with respect to the Haar measure on the group $\mathcal{L}_n$ of unimodular lattices in $\mathbb{R}^n$, the following function is a convenient tool for imposing such assumptions; let

$$\nu(\Gamma, \rho) \coloneqq \min\left\{|\tilde{\gamma}_1 \cdots \tilde{\gamma}_n| : \gamma \coloneqq (\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n)^T \in \Gamma, 0 < \|\gamma\|_2 \leq \rho\right\}$$

for $\rho > \gamma_n^{1/2}$ where $\gamma_n \coloneqq \sup_{\Gamma \in \mathcal{L}_n} \lambda_1^2(\Gamma)$ denotes the Hermite constant. Informally speaking, $\nu(\Gamma, \rho)$ quantifies how close, in a multiplicative sense, non-zero lattice points $\gamma \in \Gamma$ in the zero-centred ball of radius ρ come to the coordinate planes $\{(x_1, \ldots, x_n)^T \in \mathbb{R}^n : x_j = 0\}$, $j = 1, \ldots, n$. Now, if Γ is such that $\nu(\Gamma, \rho) \neq 0$ for all $\rho > \gamma_n^{1/2}$, then Γ is called weakly admissible.

In light of the Gauß circle problem, it might be even more surprising that in the scenario when S is a compact polyhedron, Skriganov was able to establish (conjecturally) best possible upper bounds for $\mathcal{E}(\Gamma, S_t)$ for a large class of lattices Γ. For stating Skriganov's result (in a special case), we introduce further notation. The lattice defined by $\Gamma^\perp \coloneqq \{x \in \mathbb{R}^n : \langle x, \gamma\rangle \in \mathbb{Z}\ \forall_{\gamma \in \Gamma}\}$, where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^n$, is called the dual lattice of Γ. This notion is of crucial importance in the following. Moreover, for $r > 0$ we introduce a special set of diagonal matrices

$$\Delta_r \coloneqq \{\delta \coloneqq \operatorname{diag}(2^{m_1}, \ldots, 2^{m_n}) : m = (m_1, \ldots, m_n)^T \in \mathbb{Z}^n,\ \|m\|_2 < r,\ \det \delta = 1\},$$

and we put

$$S(\Gamma, r) \coloneqq \sum_{\delta \in \Delta_r} (\lambda_1(\delta\Gamma))^{-n}.$$

Now, in the case that S is an aligned box, i.e. the Cartesian product of compact intervals, a special case of Skriganov's counting theorem (upon making the dependence of S explicit) can be stated as follows.

Theorem. *(Skriganov [109, Thm. 6.1]) Let $n \geq 2$ be an integer, let $\Gamma \subseteq \mathbb{R}^n$ be a unimodular lattice, and let $B \subseteq \mathbb{R}^n$ be an aligned box of volume 1. Suppose $\Gamma^\perp$ is weakly admissible, and $\rho > \gamma_n^{1/2}$. Then, for $t > 0$,*

$$\mathcal{E}(\Gamma, B) \underset{n}{\ll} (|\partial B|\, \lambda_n(\Gamma))^n \cdot (t^{n-1}\rho^{-1/2} + S(\Gamma^\perp, r))$$

where $r \coloneqq n^2 + \log \frac{\rho^n}{\nu(\Gamma^\perp, \rho)}$.

Skriganov used, amongst other things, very refined tools from Fourier analysis, and the geometry of numbers to derive his counting theorem, and invented, on the way, the notion of "dyadic minima of a lattice" — which was essential for his proof. However, we decided not detail this further, and hence refer the reader to [109].

Moreover, the above explicit version of Skriganov's result is of central importance when we deduce, in the following, a counting theorem for inhomogeneously expanding boxes. For stating it, let $\mathcal{T} \coloneqq \operatorname{diag}(t_1, \dots, t_n)$, for $t_i > 0$, and let $y \in \mathbb{R}^n$. We set

$$B \coloneqq \mathcal{T}\,[0,1]^n + y, \quad \text{and} \quad T \coloneqq (\det \mathcal{T})^{1/n} \cdot \|\mathcal{T}^{-1}\|_2 = \frac{(t_1 \cdots t_n)^{1/n}}{\min\{t_1, \dots, t_n\}} \geq 1$$

where $\|\cdot\|_2$ denotes the operator norm induced by the Euclidean norm.

Theorem ([117])**.** *Let $n \geq 2$, let $\Gamma \subseteq \mathbb{R}^n$ be a unimodular lattice, and let $B \subseteq \mathbb{R}^n$ be as above. Suppose $\Gamma^\perp$ is weakly admissible, and $\rho > \gamma_n^{1/2}$. Then,*

$$\mathcal{E}(\Gamma, B) \underset{n}{\ll} \frac{1}{\nu(\Gamma^\perp, T^\star)} \left(\frac{(\operatorname{vol}(B))^{1-1/n}}{\sqrt{\rho}} + \frac{R^{n-1}}{\nu(\Gamma^\perp, 2^R T)} \right)$$

where $x^\star \coloneqq \max\{\gamma_n, x\}$, and $R \coloneqq n^2 + \log \frac{\rho^n}{\nu(\Gamma^\perp, \rho T)}$.

Note that $\rho^n / \nu(\Gamma^\perp, \rho) \geq n^{n/2}$ by the inequality between arithmetic and geometric mean. We have $(2^R T)^\star = 2^R T$, since $T \geq 1$ and

$$\gamma_n \leq (4/3)^{(n-1)/2}, \tag{1.1.4}$$

and hence, the far right hand-side in the above theorem is well-defined.

Remark. *Let $\delta \in \mathbb{R}$ be non-zero. It follows from a zero–one-law due Kleinbock and Margulis [66, p. 456], compare also [109, Lem. 4.5], that the set of $\Gamma \in \mathcal{L}_n$ with*

$$\nu(\Gamma, \|\gamma\|_2) \leq (\log \|\gamma\|_2)^{-(n-1+\delta)}$$

for infinitely many $\gamma \in \Gamma$ has full measure if $\delta < 0$, and zero measure if $\delta > 0$. In particular, the bound on $\mathcal{E}(\Gamma, tB)$, $t \geq 1$ provided by either one of the last two theorems is, generically, far better than the trivial bound (1.1.2): for a fixed $\varepsilon > 0$, and almost every $\Gamma \in \mathcal{L}_n$ the bound $\mathcal{E}(\Gamma, tB) \underset{\Gamma}{\ll} t^{n-1}$ is sharpened to $\mathcal{E}(\Gamma, tB) = \mathcal{O}_{\Gamma,\varepsilon}((\log t)^{n-1+\varepsilon})$.

However, a draw-back of the previous two counting theorems is that they are not intrinsic in the lattice Γ, as they require Diophantine properties of $\Gamma^\perp$ to be applicable. To see if this is necessarily so, or could be circumvented in reasonable generality, we carefully analyse the relation between $\nu(\Gamma, \cdot)$, and $\nu(\Gamma^\perp, \cdot)$. As it turns out, the next result is showing that, roughly speaking, one of these functions cannot be bounded (from below) in terms of the other, as soon as the dimension of the ambient space exceeds three. More precisely, we show the following.

Theorem ([117])**.** *Let $n \geq 3$, and let $\psi : (0, \infty) \to (0, 1)$ be non-increasing. Then, there is a weakly admissible $\Gamma \in \mathcal{L}_n$, and a sequence $(\rho_l)_l \subseteq (\gamma_n^{1/2}, \infty)$ tending to ∞, as $l \to \infty$, such that*

$$\nu(\Gamma^\perp, \rho) \gg \rho^{-n^2}, \quad \text{and} \quad \nu(\Gamma, \rho_l) \leq \psi(\rho_l)$$

for all $l \in \mathbb{N} = \{1, 2, 3, \dots\}$ and for all $\rho > \gamma_n^{1/2}$.

Remark. *German [47] proved that coarse measures, the so called lattice exponents, of the decay rates of $\nu(\Gamma, \cdot)$ and $\nu(\Gamma^\perp, \cdot)$ are linked by transference inequalities. In particular, he showed, provided $n \geq 3$, that if $\nu(\Gamma, \rho) \not\gg \rho^{-\omega}$ for every $\omega > 0$, then for every $\varepsilon > 0$ the inequality $\nu(\Gamma^\perp, \rho_l) \leq \rho_l^{\varepsilon - 1/(n-2)}$ holds for a sequence of $\rho_l > \gamma_n^{1/2}$ which tends to ∞.*

1.2 The Duffin–Schaeffer Conjecture

The field of classical Diophantine approximation aims, roughly speaking, to quantify how dense the rationals are in the reals. Nowadays, Diophantine approximation is closely connected to, e.g., fractal geometry [20], ergodic theory [38], analytic number theory [32], and has practical applications [10]. A fundamental result in this area is Khintchine's theorem. For stating it, let $\psi : \mathbb{N} \to \mathbb{R}$ be a non-negative function, and denote by $W_{nr}(\psi)$ the set of all $x \in [0,1]$ for which there are infinitely many $n \in \mathbb{Z}_{\geq 1}$ satisfying $\|n\alpha\| \leq \psi(n)$ where $\|\cdot\|$ abbreviates the distance to the nearest integer.

Theorem (Khintchine)**.** *Suppose ψ is monotonically decreasing. If*

$$\sum_{n=1}^{\infty} \psi(n)$$

diverges, then $W_{nr}(\psi)$ has full Lebesgue measure and zero Lebesgue measure otherwise.

Duffin, and Schaeffer [36] showed that the above monotonicity assumption is necessary by constructing a ψ for which $W_{nr}(\psi)$ has measure zero[2] and for which the series above diverges; moreover, they conjectured that $W(\psi)$ has full measure whenever $\sum_{n=1}^{\infty} \psi(n)\varphi(n)/n$ diverges where $W(\psi)$ is the set of all $x \in [0,1]$ such that there are infinitely many coprime integers n, m with $|n\alpha - m| \leq \psi(n)$. To (dis)prove this is one of the most important open problems in metric number, and remains unsolved since 1941. However, the Duffin–Schaeffer conjecture is known to be true under some additional arithmetic conditions or regularity assumptions on the function ψ, cf. [57, 123]. In [59] Haynes, Pollington and Velani initiated a program to establish the Duffin–Schaeffer conjecture without assuming any regularity or number-theoretic properties of ψ, but instead assuming a slightly stronger divergence condition. The result of [59] was improved upon by Beresnevich, Harman, Haynes and Velani [19] by a beautiful averaging argument, which is also at the core of Chapter 3. The main result of [19] is that $W(\psi)$ has full measure provided there is some $\varepsilon > 0$ such that

$$\sum_{n=1}^{\infty} \frac{\psi(n)\varphi(n)}{n(\log n)^{\varepsilon \log\log\log n}} = \infty$$

(we understand $\log x$ as $\max(1, \log x)$, so that all appearing logarithms are positive and well-defined). In Chapter 3, we prove that the extra divergence factor can be reduced to $(\log n)^{\varepsilon}$ for a fixed $\varepsilon > 0$. In particular, this solves Problem 2 posed in [59], where it was asked whether the extra divergence factor $\log n$ is sufficient.

Theorem ([11])**.** *The Duffin–Schaeffer conjecture is true for every non-negative function $\psi : \mathbb{N} \to \mathbb{R}$ for which there is a constant $\varepsilon > 0$ such that*

$$\sum_{n=1}^{\infty} \frac{\psi(n)\varphi(n)}{n(\log n)^{\varepsilon}} = \infty.$$

[2]Loosely speaking, the underpinning reason is that $W_{nr}(\psi)$ allows approximation by **n**on-**r**educed fractions; therefore, one can construct a ψ, supported on "highly composite"' numbers (and its divisors), to make the above series diverge whilst keeping the support of ψ still small enough to enforce that $W_{nr}(\psi)$ has measure zero, by using the Borel-Cantelli lemma.

1.3 Poissonian Pair Correlations

The theory of uniform distribution mod 1 dates back, at least, to the seminal paper [127] of Weyl. It has a long and honorable history which records more than a century of intensive investigations with several practical applications, cf. [34, 72]. Nevertheless, only in recent years various authors have started to investigate a distribution property which can be considered as a uniform distribution property of second order; namely, whether the asymptotic distribution of the pair correlations has a property which is called Poissonian, and defined as follows:

Definition 1. *A sequence $(\theta_n)_n$ in $[0,1)$ is said to have the Poissonian (pair correlations) property, if for each $s \geq 0$ the pair correlation function*

$$R([-s,s],(\theta_n)_n,N) \coloneqq \frac{\#\{1 \leq i \neq j \leq N : \|\theta_i - \theta_j\| \leq s/N\}}{N} \tag{1.3.1}$$

tends to $2s$ as $N \to \infty$. Moreover, let $(a_n)_n$ denote a strictly increasing sequence of positive integers. If no confusion can arise, we write

$$R([-s,s],\alpha,N) \coloneqq R([-s,s],(\alpha a_n)_n,N)$$

and say that a sequence $(a_n)_n$ has the metric Poissonian (pair correlations) property if $(\alpha a_n)_n$ has the Poissonian property for Lebesgue almost all $\alpha \in (0,1)$.

It is known from the work of Aistleitner, Lachmann, and Pausinger [12] and, independently, from the work[3] of Larcher and Grepstad [77] that if a sequence $(\theta_n)_n$ has the Poissonian property, then it is uniformly distributed mod 1. Interest in this spacing property spread when Rudnick and Sarnak [98], motivated by a well-known conjecture from mathematical physics, proved that $(n^d)_n$ has the metric Poissonian property for $d \geq 2$. Since then, several authors have contributed to building a metric theory for this second order uniform distribution property [13, 14, 23, 73, 78, 79, 97, 99, 125].

As it turns out, recent investigations pointed towards the existence of a zero–one-law, akin to Khintchine's fundamental theorem from the previous section. We proceed to describe this putative zero–one-law: The development in this direction started with a paper of Aistleitner, Larcher, and Lewko [14], where a strong link between combinatoric properties of $(a_n)_n$, and the metric Poissonian property was uncovered; to this end, Fourier–analytic arguments, originating from [98], in combination with estimates on GCD sums, which are due to Bondarenko and Seip [25], were used. For stating the main result of [14], let $(a_n)_n$ henceforth denote a strictly increasing sequence of positive integers and abbreviate the set of the first N elements of $(a_n)_n$ by A_N. Moreover, define the additive energy $E(I)$ of a finite set integers I via

$$E(I) \coloneqq \sum_{\substack{a,b,c,d \in I \\ a+b=c+d}} 1.$$

[3] Remarkably, both papers were on the arXiv 100 years after Weyl's work [127] was published.

The main result of [14] is the implication that if there is an $\varepsilon > 0$ such that

$$E(A_N) \ll N^{3-\varepsilon},$$

then $(a_n)_n$ has the metric Poissonian property. Note that $(\#I)^2 \leq E(I) \leq (\#I)^3$ where $\#I$ denotes the cardinality of $I \subset \mathbb{Z}$ (heuristically speaking, a set I has large additive energy if and only if it contains a "large" arithmetic progression like structure). The criterion of [14] for detecting metric Poissonian sequences was further refined as follows provided that the density function $\delta(N) \coloneqq N^{-1}\#(A_N \cap \{1, \ldots, N\})$ of the sequence in question is not decaying too rapidly.

Theorem (Bloom, Chow, Gafni, Walker [23]). *Let $(a_n)_n \subseteq \mathbb{Z}_{\geq 1}$ be a strictly increasing sequence. If there exists $\varepsilon > 0$ such that*

$$E(A_N) \ll \frac{N^3}{(\log N)^{2+\varepsilon}} \quad \text{and} \quad \delta(N) \gg \frac{1}{(\log N)^{2+2\varepsilon}},$$

then $(a_n)_n$ has the metric Poissonian property.

In accordance with a probabilistic model, the authors of [23] asked, in their terminology, the following "Fundamental Question:" they conjectured the convergence side of a Khintchine law for the metric Poissonian property, i.e. a characterization of the metric Poissonian property via the convergence of a series involving $E(A_N)$.

Question (Bloom, Chow, Gafni, Walker [23]). *Is it true that if $E(A_N) \sim N^3\psi(N)$ for some weakly decreasing function $\psi : \mathbb{N} \to [0,1]$, then $(a_n)_n$ has the metric Poissonian property if and only if*

$$\sum_{N \geq 1} \frac{\psi(N)}{N} \tag{1.3.2}$$

converges?

In order to answer a related question, we construct in Chapter 4 sequences which are not metric Poissonian, in a strong sense, and whose cut-offs have additive energy located arbitrarily close to the putative convergence-divergence-threshold of (1.3.2). In fact, a slightly stronger version of the subsequent statement is proved in Chapter 4.

Theorem ([73]). *Let r be a positive integer, and let $\log_r$ denote the r-times iterated logarithm. Then, there is a strictly increasing sequence $(a_n)_n$ of positive integers with*

$$E(A_N) \asymp \frac{N^3}{\log(N)\log_2(N)\cdots\log_r(N)}$$

such that the set of $\alpha \in (0,1)$ for which $(\alpha a_n)_n$ is not Poissonian has full Lebesgue measure. Moreover, for any $\varepsilon > 0$ there is a strictly increasing sequence $(a_n)_n$ of positive integers with

$$E(A_N) \asymp \frac{(\log_r(N))^{-\varepsilon} N^3}{\log(N)\log_2(N)\cdots\log_r(N)}$$

such that the set of $\alpha \in (0,1)$ for which $(\alpha a_n)_n$ is not Poissonian has full Hausdorff dimension.

On the other hand, Chapter 3 is concerned with constructing sequences *exhibiting* the metric Poissonian property while (1.3.2) diverges. Indeed, the main result in Chapter 3 is that we can, essentially, save the sixth root of a logarithm, relative to said threshold, in the additive energy of A_N whilst preserving the Poissonian property:

Theorem ([13]). *For every $\varepsilon \in (0, 1/12)$, there is a metric Poissonian sequence $(a_n)_n$ of strictly increasing integers satisfying*

$$E(A_N) \gg \frac{N^3}{(\log N)^{5/6+\varepsilon}}.$$

The proof of this result uses, amongst other things, the insights from Chapter 4, and the Fourier–analytic methods of [14]. Furthermore, by combining the two previous theorems, it is apparent that a characterization of the metric Poissonian property cannot just depend on the additive energies of the truncations alone. Instead, the picture is more complicated — cf. the introduction of Chapter 5 for further details.

However, the high energy case is well-understood by a very recent result.

Theorem 1.3.1 (Larcher, Stockinger [79]). *If $E(A_N) = \Omega(N^3)$, then there is* **no** *$\alpha \in (0, 1)$ such that $(a_n\alpha)_n$ has the Poissonian property.*

The methods of Larcher and Stockinger are purely combinatorial, and a closer inspection of their reasoning shows that the pair correlations function, for all $\alpha \in [0, 1]$, is infinitely often "too" large. By different methods, we show a weaker statement which pre-dates the aforementioned theorem: we show that the pair correlation function of $(\alpha a_n)_n$, for sequences $(a_n)_n$ with $E(A_N) = \Omega(N^3)$, is "too" small infinitely often for almost every $\alpha \in (0, 1)$, see Theorem 4.1.3 and its proof.

1.4 Regularity of Primes in Arithmetic Progressions

Let $\omega(k)$ be the number of distinct prime factors of an integer k, and let φ denote Euler's totient function. We say that k is a P-integer if the first $\varphi(k)$ primes which do not divide k form a complete residue system modulo k. In 1978, Recaman [94] conjectured that there are only finitely many prime P-integers. In 1980, Pomerance [89] proved this, and conjectured moreover that no P-integer exceeds 30. This was proved in special cases by Hajdu, Saradha, and Tijdeman [53, 55, 101]. In fact, in [55], they proved the conjecture of Pomerance under the assumption of the Riemann Hypothesis. Eventually, in a paper of Yang and Togbé [131] the conjecture was proven unconditionally.

However, one can rephrase the definition of P-integers, see also [54], as follows: Let, without further mention, p denote a prime, $\mathbb{P}$ the set of primes, and p_n the n-th smallest prime. Then k is a P-integer if the block $p_1, p_2, \ldots, p_{\varphi(k)+\omega(k)}$ of the first $\varphi(k) + \omega(k)$ primes, lying in the closed interval $[p_1, p_{\varphi(k)+\omega(k)}]$, has precisely one element in each reduced residue class modulo k, with the exception of the $\omega(k)$ primes

which divide k (and thus lie in non-invertible residue classes). By viewing P-integers as instances of such distribution phenomena, there is an obvious and far more general notion.

Definition 2. *Let $\alpha, \beta, \gamma, \iota > 0$ denote integers, and $G = (G, \cdot)$ an arithmetical semi-group with norm $|\cdot|$, in the sense of Knopfmacher [70, p. 11], which takes only values in the positive integers. Consider for $k \in G$ the equivalence relation $a \sim b \Leftrightarrow |a| \equiv |b| \bmod |k|$ on G and let M denote the primes in G with norm in the interval $[\alpha, \beta]$. Then we say $k \in G$ is a $P(\alpha, \beta, \gamma, \iota)$-integer if M has in each equivalence class corresponding to an invertible residue class modulo $|k|$ at least γ elements, and the remaining ι primes distribute in some arbitrary equivalence classes such that $\#M = \gamma\varphi(|k|) + \iota$. (For ease of exposition, we shall simply speak of P^*-integers if no confusion can arise.)*

Let us clarify that we are mainly concerned with investigating P^*-integers in the case that G is the semi-group of the positive integers. However, a side-objective was to put P-integers into a more conceptional context. To this end, one might first look for a definition of P^*-integers in the ring of integers of a given number field. Here the role of the primes is, in general, taken by prime ideals. Moreover, to define a notion of arithmetic progressions it is natural to pull the ideals back to $\mathbb{N}$ by taking the norm, as one does to define a Dedekind zeta function.[4] Since this approach extends to even greater generality, we stated our definition of P^*-integers in the language of arithmetical semi-groups. A natural question is to estimate, for a given $k \in G$, the smallest values of α, β such that k is for the first time a P^*-integer. Let us simplify this question by considering the semi-group $G = \mathbb{N}$ of the natural numbers, endowed with its canonical norm, and by asking the following question: fix $\alpha = 2$ and estimate for a given k the smallest integer $\beta = \beta(k)$ such that k is the first time a $P(2, \beta, 1, \iota)$-integer for some ι. This problem is nothing but estimating Linnik's constant which is widely open. The following well-known probabilistic considerations in the spirit of Cramér's model suggest that β should be of magnitude $k \log^2 k$, whereas Heath-Brown [60] has conjectured that $\beta \ll k \log^2 k$ and Granville and Pomerance [51, below Thm. 1] conjectured that $\beta \gg \varphi(k) \log^2 k$.

We start by estimating the probability $P(X)$ for a random set of $f(k) \geq \varphi(k)$ many primes to *not* cover all of the $\varphi(k)$ reduced residue classes with at least one prime each. We assume that a prime p has probability $\frac{1}{\varphi(k)}$ about to be in a specific invertible residue r class modulo k, and denote by the event that none of the $f(k)$ primes is congruent r mod k. Then, writing $f(k) = C(k)\varphi(k)\log k$, we estimate that

$$P(X) = P\left(\bigcup_r X_r\right) \approx \sum_r P(X_r) \approx \frac{\varphi(k)}{k^{C(k)}} \tag{1.4.1}$$

where the union and the summation run through a complete residue system r modulo k. Hence, if $C(k) > 1 + \varepsilon$, for some fixed $\varepsilon > 0$, we expect with a positive probability that our $f(k)$ many primes cover all invertible residue classes at least once. On the other

[4] However, if the ring of integers happens to be Euclidean, as $\mathbb{Z}[i]$, there is an obvious alternative generalization of P-integers.

hand, if $C(k) < 1-\varepsilon$ holds, we expect, by using the reversed Borel-Cantelli Lemma, cf. [33], that X is likely to occur infinitely often. Since $p_n \sim n \log n$, the threshold $C = 1$ amounts to the estimate $\beta(k) \approx \varphi(k) \log k \log(\varphi(k) \log k) = O(k \log^2 k)$ for having about $\varphi(k) \log k$ primes in the interval $[2, \beta(k)]$. This approximation was suggested by a similar, but more complicated heuristic of Wagstaff [124], and is plausible in view of various results e.g. from Turán [122].[5]

Let us stress that for $k \in G$, where G is as in Definition 2, this heuristic suggests that one should need about $\varphi(|k|) \log |k|$ primes to cover the invertible residue classes modulo $|k|$ in G at least once with primes and not just $\varphi(|k|) + \omega(|k|)$ as one asks in Recaman's conjecture. Our first result shows that, under certain assumptions, this is indeed the case. Furthermore, we say G satisfies Axiom A (cf. [70, p. 75]) with $\delta > 0$, if for some $0 \leq \eta < \delta$ the counting function $N_G(x) := \#\{g \in G : |g| \leq x\}$ has the expansion $x^\delta + O(x^\eta)$ as $x \to \infty$. Thus, we can state the following result.

Theorem 1.4.1 ([42]). *Let G as in Definition 2 satisfy Axiom A with some $\delta > 0$. Let $k \in G$, and $K := |k|$. Assume that numbers $\alpha = 1$, $\beta \ll K \log^a K$ and $\iota \ll \log^b K$ are given for some fixed $a, b > 0$ in the case $0 < \delta \leq 1$ and in the case $\delta > 1$ the value of β may additionally differ from multiples of K by at most $K^{1-\epsilon}$ for some absolute constant $\epsilon > 0$. Then there are only finitely many such P^*-integers.*

For instance, the assumptions (on the semi-group) above are satisfied if G is the set of non-zero integral ideals of a number field $\mathfrak{K}$ with the usual ideal norm. Moreover, one can also interpret the property to be a P^*-integer as the resolvability (in the set of primes) of a certain set of Diophantine equations and inequalities. For determining all such solutions, it is of interest to furnish Theorem 1.4.1 with explicit bounds on k and it might be interesting in its own right to make a qualitative statement quantitative. We shall do so only in the case $G = \mathbb{N}$ since one needs explicit bounds for the prime counting function $\pi_G(x) := \#\{p \in G : g \,\text{prime}, |g| \leq x\}$, for $x > 0$, of G which are only known if one has sufficient arithmetic information about G. For instance, the error term in Landau's prime ideal theorem naturally depends on the given number field. However, once this information is given; it is a straightforward task to extend our explicit results to more general cases.

Loosely speaking, our main result states, in a quantitative manner, that blocks of primes (in the natural numbers) of approximate length $\gamma \varphi(k)$ are, in general, not evenly distributed among the reduced residue classes modulo k. More precisely, we prove the following extension of Recaman's conjecture:

Theorem 1.4.2 ([42]). *Let $\lambda \in \mathbb{N} \cup \{0\}$ and d_1, d_2, d_3 denote strictly positive real numbers. There are only finitely many $P(\alpha, \beta, \gamma, \iota)$-integers k in $\mathbb{N}$ such that the growth restrictions $\alpha = \lambda k + O(k^{1-d_1})$, $\iota = O(k^{1-d_2})$ and $\beta = O(k \log^{d_3} k)$ are satisfied.*

[5] Turán showed, assuming the Extended Riemann Hypothesis, that for any $\delta > 0$ the smallest prime $P(k, l)$ in the invertible residue class l modulo k is exceeding the quantity $\varphi(k) \log^{2+\delta}(k)$ for at most $o(\varphi(k))$ choices of l. There are other results of this kind, we refer the reader to [49] and the references therein. However, there is also reason to be cautious with respect to the above mentioned heuristic. In this direction there are, inter alia, the results of Maier [81], Rubinstein and Sarnak [96], or [67].

1.5 Iterated Multiplicative Arithmetic Functions

The study of the maximal order of arithmetic functions (for example of the divisor functions d or σ) is an integral part of introductory number theory text books. For these divisor functions d or σ satisfactory answers are well-known (see, e.g., Wigert [130] and Gronwall [52]) the methods making use of the fact that these are multiplicative functions. For the maximal order of magnitude of *iterated* arithmetic functions, much less is known. Here are some reasons which show that this is generally a very delicate subject:

1. The iterate of a multiplicative function is usually not multiplicative.

2. Understanding the iterates of the function $g(n) = \sigma(n) - n$, where σ is the sum of divisors function, would entail an understanding of odd perfect numbers.

3. Let $a(n)$ denote the number of abelian groups of order n. By results of Erdős and Ivić [44] it is known that

$$\exp\left((\log x)^{1/2+o(1)}\right) \ll \max_{n\le x} a(a(n)) \ll \exp\left((\log x)^{7/8+o(1)}\right),$$

   leaving a large gap between lower and upper bounds. Improving these bounds would seem to require an understanding of the multiplicative structure of the number $p(n)$ of unrestricted partitions, about which very little is known beyond certain congruences.

4. Let $\sigma_1(n) = \sigma(n)$ be the sum of divisors function, and $\sigma_k(n) = \sigma_1(\sigma_{k-1}(n))$ its iterates. Schinzel [102] conjectured that

$$\liminf_{n\to\infty} \frac{\sigma_k(n)}{n} < \infty.$$

   This is only established for $k = 1, 2$ and 3 by results of Mąkowski [83] and Maier [80], and conditionally on Schinzel's Hypothesis H.

In the case of multiplicative functions, the maximal order of magnitude was initially proved in a number of individual cases: The maximal order of the divisor function d has been determined by Wigert [130] and Ramanujan [91]. They proved that

$$\limsup_{n\to\infty} \frac{\log d(n) \log\log n}{\log n} = \log 2.$$

(Note that for functions of this magnitude one typically has asymptotics for $\log(f(n))$ rather than for $f(n)$ itself. From our perspective we will still say that the maximal order has been determined.) This study subsequently influenced (via results of Hardy and Ramanujan, Turán and Erdős and Kac) the development of probabilistic number theory.

Ramanujan studied the multiplicative function δ that counts the number of representations of its argument as a sum of two squares ignoring sign, i.e.,

$$\delta(n) = \tfrac{1}{4}\,\#\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 + y^2 = n\}. \tag{1.5.1}$$

If ν_p denotes the p-adic valuation, then it is well-known (see, e.g., [56, Theorem 278]) that

$$\delta(n) = \prod_{\substack{\text{prime } q|n \\ q\equiv 1 \bmod 4}} (\nu_q(n)+1) \times \prod_{\substack{\text{prime } p|n \\ p\equiv 3 \bmod 4}} \tfrac{1}{2}\Big(1+(-1)^{\nu_p(n)}\Big). \tag{1.5.2}$$

(To be precise, Ramanujan called this function $Q_2(n)$, here we use the notation used by Hardy and Wright [56, Theorem 278], and observe that $\delta(n) = \frac{r_2(n)}{4}$, where $r_2(n)$ is the sum of two squares function which also takes care of signs. The r_2 function is not quite multiplicative.) Ramanujan [93] showed that, for some positive constant a,

$$\max_{n\le x} \delta(n) = \exp\left(\frac{\log 2}{2}\ \mathrm{li}(2\log \mathrm{x}) + O((\log x)\exp(-a\sqrt{\log x}))\right),$$

which implies that

$$\max_{n\le x} \delta(n) = \exp\left((\log 2 + o(1))\frac{\log x}{\log\log x}\right).$$

This implies the very same logarithmic maximum order:

$$\limsup_{n\to\infty} \frac{\log r_2(n)\log\log n}{\log n} = \log 2.$$

Knopfmacher [69] and Nicolas [85] later also observed this. At that time they did not know about Ramanujan's work which was, as yet, unpublished: Quite remarkably, the end of Ramanujan's paper [91] of 1915 was not intended to be the end. In fact, Ramanujan's manuscript was considerably longer, and due to a shortage of resources during wartime the London Mathematical Society printed only a part of the manuscript. The second part was recovered and published many years later, first in [92], but later with detailed annotations by Nicolas and Robin [93], and also [15]. Ramanujan (see [93], Paragraphs 55 and 56) also achieved the very same result,

$$\max_{n\le x} \tilde{Q}_2(n) = \exp\left(\frac{\log 2}{2}\ \mathrm{li}(2\log \mathrm{x}) + O((\log x)\exp(-a\sqrt{\log x}))\right),$$

for the function $\tilde{Q}_2(n)$ counting non-negative pairs (x,y) with $n = x^2+xy+y^2$.

$$\tilde{Q}_2(n) = \prod_{\substack{\text{prime } q|n \\ q\equiv 1 \bmod 3}} (\nu_q(n)+1) \times \prod_{\substack{\text{prime } p|n \\ p\equiv -1 \bmod 3}} \tfrac{1}{2}\Big(1+(-1)^{\nu_p(n)}\Big). \tag{1.5.3}$$

Krätzel [71] proved for the number $a(n)$ of non-isomorphic abelian groups of order n that

$$\limsup_{n\to\infty} \frac{\log a(n)\log\log n}{\log n} = \frac{1}{4}\log 5,$$

and Knopfmacher [68] proved for the number $\beta(n)$ of squareful divisors of n that

$$\limsup_{n\to\infty} \frac{\log \beta(n)\log\log n}{\log n} = \frac{1}{3}\log 3.$$

A number of authors independently observed that these limits can be worked out more generally, for the class of prime independent multiplicative functions. Of these results we only mention the one by Shiu [106], but there are others (see [16, 35, 62, 64, 69, 84, 87, 90, 114]). Shiu [106] proved: let $f : \mathbb{N} \to \mathbb{R}$ be a multiplicative function satisfying the following conditions:

1. There exist constants A and $0 < \theta < 1$ such that $f(2^\nu) \leq \exp(A\nu^\theta)$ where $\nu \geq 1$, and
2. for all primes p and all $a \geq 1$ one has $f(p^\nu) = f(2^\nu) \geq 1$,

then the following holds:

$$\limsup_{n\to\infty} \frac{\log f(n) \log\log n}{\log n} = \log M,$$

where $M = \max_{\nu\geq 1}(f(2^\nu))^{1/\nu}$. The quest for the maximal order of the iterated divisor function was raised by Ramanujan [91] in his paper on highly composite numbers. At the very end of that paper, he gave a construction of integers $N_k = \prod_{i=1}^{k} p_i^{p_i-1}$ and observed that for these integers $d(d(N_k)) \geq \exp\left(\left(\sqrt{2}\log 4 + o(1)\right)\frac{\sqrt{\log N_k}}{\log\log N_k}\right)$. Erdős and Kátai [45], Ivić [65] and Smati [110, 111] gave results on the maximal order, but a satisfying answer about the maximal order of the iterated divisor function was only given almost 100 years after Ramanujan's paper: Buttkewitz, Elsholtz, Ford and Schlage-Puchta [29] proved, using elementary and combinatorial methods, that:

$$\limsup_{n\to\infty} \frac{\log d(d(n)) \log\log n}{\sqrt{\log n}} = C_{div} := \left(8\sum_{l=1}^{\infty}\left(\log\left(1+\frac{1}{l}\right)\right)^2\right)^{1/2}.$$

It seems to be a gap in the literature that even for the quite frequently used sums of two squares functions (δ or r_2), which often serve as a benchmark for a function not too different from the divisor function, but not being quite prime independent, there are no studies on the iterated function and Chapter B in the appendix intends to close this gap. In fact, let us recall the development for sums of multiplicative functions, where Landau investigated the number of integers representable as sums of two squares. Subsequently, this was generalised many times, for example to the number of integers consisting of primes in certain residue classes only, and eventually led to the celebrated mean value results of Wirsing and Halász.

Motivated by this development, we study a class of multiplicative functions which includes important functions - such as the divisor functions d, or $\delta = r_2(n)/4$ (the number of representations of sums of two integer squares, ignoring signs, so that it becomes a multiplicative function). For iterated arithmetic functions, it seems that the investigations are still in the beginning phase. In the spirit of Shiu's theorem, we also investigated which hypotheses on the function f, defining a certain class of function, allow one to determine the maximum order magnitude of $f(f(n))$. In some cases (including δ and $\tilde{Q}_2$), we are able to give asymptotics for the logarithmic size of this maximum. The results concerning the maximal order of functions from the said class of function are of the following kind.

Corollary ([41])**.** *If* $\alpha \in \mathbb{N}$*, then*

$$\max_{n \leq x} \log d((d(n^\alpha))^\alpha) = \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C_\alpha}{\sqrt{\tau/\alpha}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right)$$

where

$$C_\alpha = \left(8\sum_{\nu=1}^{\infty} \log\left(1 + \frac{\alpha}{1+(\nu-1)\alpha}\right)\right)^{1/2}.$$

In particular, for δ given by (1.5.1) we obtain the following.

Corollary ([41])**.** *Let* δ *be given by* (1.5.1)*. Then*

$$\max_{n \leq x} \log \delta(\delta(n)) = \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C_{div}}{\sqrt{2}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right).$$

Remark. *Since at least one of my collaborators wants to use some of the joint research presented in this thesis for his PhD thesis as well, I need to declare and detail — for bureaucratic reasons — percentages of my contribution to the research related to this matter: for the second chapter my contribution was 20%, for the third chapter it was 50%, and for the fourth chapter it was 33%.*

Chapter 2

On a Counting Theorem of Skriganov

> "Not everything that can be counted counts, and not everything that counts can be counted."
> — W. Cameron [30, p.13].

The following chapter is based on joint work with **Martin Widmer** [117].

We prove a counting theorem concerning the number of lattice points for the dual lattices of weakly admissible lattices in an inhomogeneously expanding box, which generalises a counting theorem of Skriganov. The error term is expressed in terms of a certain function $\nu(\Gamma^\perp, \cdot)$ of the dual lattice $\Gamma^\perp$, and we carefully analyse the relation of this quantity with $\nu(\Gamma, \cdot)$. In particular, we show that $\nu(\Gamma^\perp, \cdot) = \nu(\Gamma, \cdot)$ for any unimodular lattice of rank 2, but that for higher ranks it is in general not possible to bound one function in terms of the other. This result relies on Beresnevich's recent breakthrough on Davenport's problem regarding badly approximable points on submanifolds of $\mathbb{R}^n$. Finally, we apply our counting theorem to establish asymptotics for the number of Diophantine approximations with bounded denominator as the denominator bound gets large.

2.1 Introduction

In the present chapter, we are mainly concerned with four objectives. Firstly, we prove an explicit version of Skriganov's celebrated counting result [109, Thm. 6.1] for lattice points of unimodular weakly admissible lattices in homogeneously expanding aligned boxes. Secondly, we use this version to generalise Skriganov's theorem to inhomogeneously expanding, aligned boxes. Thirdly, we carefully investigate the relation between $\nu(\Gamma, \cdot)$ (see (2.1.1) for the definition) and $\nu(\Gamma^\perp, \cdot)$ of the dual lattice $\Gamma^\perp$ which captures the dependency on the lattice in these error terms. And fourthly, we apply our counting result to count Diophantine approximations.

To state our first result, we need to introduce some notation. By writing $f \ll g$ (or $f \gg g$) for functions f, g, we mean that there is a constant $c > 0$ such that $f(x) \leq cg(x)$

(or $cf(x) \geq g(x)$) holds for all admissible values of x; if the implied constant depends on certain parameters, then this dependency will be indicated by an appropriate subscript. Let $\Gamma \subseteq \mathbb{R}^n$ be a unimodular lattice, and let $\Gamma^\perp \coloneqq \{w \in \mathbb{R}^n : \langle v, w\rangle \in \mathbb{Z} \quad \forall_{v\in\Gamma}\}$ be its dual lattice with respect to the standard inner product $\langle \cdot, \cdot \rangle$. Let γ_n denote the Hermite constant, and for $\rho > \gamma_n^{1/2}$ set

$$\nu(\Gamma, \rho) \coloneqq \min\Big\{|x_1 \cdots x_n| : \ x \coloneqq (x_1, \dots, x_n)^T \in \Gamma,\, 0 < \|x\|_2 < \rho\Big\} \tag{2.1.1}$$

where $\|\cdot\|_2$ denotes the Euclidean norm. We say Γ is weakly admissible if $\nu(\Gamma, \rho) > 0$ for all $\rho > \gamma_n^{1/2}$. Note that this happens if and only if Γ has trivial intersection with every coordinate subspace. It is also worthwhile mentioning that the function $\nu(\Gamma, \rho)$ controls the rate of escape of the lattice Γ under the action of the diagonal subgroup of $\mathrm{SL}_n(\mathbb{R})$ (cf. (2.2.7)).

Furthermore, let $\mathcal{T} \coloneqq \mathrm{diag}(t_1, \dots, t_n)$ for $t_i > 0$ be the diagonal matrix with diagonal entries $t_1, \dots, t_n$, and let $y \in \mathbb{R}^n$. We set

$$B \coloneqq \mathcal{T}\,[0, 1]^n + y,$$

and we call such a set an aligned box. Moreover, we define

$$T \coloneqq (\det \mathcal{T})^{1/n} \cdot \|\mathcal{T}^{-1}\|_2 = \frac{(t_1 \cdots t_n)^{1/n}}{\min\{t_1, \dots, t_n\}} \geq 1$$

where $\|\cdot\|_2$ denotes the operator norm induced by the Euclidean norm. Then, our generalisation of Skriganov's theorem reads as follows.

Theorem 2.1.1. *Let $n \geq 2$, let $\Gamma \subseteq \mathbb{R}^n$ be a unimodular lattice, and let $B \subseteq \mathbb{R}^n$ be as above. Suppose $\Gamma^\perp$ is weakly admissible, and $\rho > \gamma_n^{1/2}$. Then,*

$$|\#(\Gamma \cap B) - \mathrm{vol}(B)| \underset{n}{\ll} \frac{1}{\nu\Big(\Gamma^\perp, T^\star\Big)}\left(\frac{(\mathrm{vol}(B))^{1-1/n}}{\sqrt{\rho}} + \frac{R^{n-1}}{\nu(\Gamma^\perp, 2^R T)}\right) \tag{2.1.2}$$

where $x^\star \coloneqq \max\{\gamma_n, x\}$, and $R \coloneqq n^2 + \log \frac{\rho^n}{\nu(\Gamma^\perp, \rho T)}$.

Note that $\rho^n/\nu(\Gamma^\perp, \rho) \geq n^{n/2}$ by the inequality between arithmetic and geometric mean.

Since $T \geq 1$ and by (1.1.4) we have $(2^R T)^\star = 2^R T$, and hence, the far right hand-side in (2.1.2) is well-defined.

The lattice Γ is called admissible if $\mathrm{Nm}\,(\Gamma) := \lim_{\rho\to\infty} \nu(\Gamma, \rho) > 0$. It is easy to show that if Γ is admissible then also $\Gamma^\perp$ is admissible (see [108, Lemma 3.1]). In this case we can choose $\rho = (\mathrm{vol}B)^{2-2/n}$, provided the latter is greater than $\gamma_n^{1/2}$, to recover the following impressive result of Skriganov ([108, Theorem 1.1 (1.11)])

$$|\#(\Gamma \cap B) - \mathrm{vol}(B)| \underset{n,\mathrm{Nm}\,(\Gamma^\perp)}{\ll} (\log(\mathrm{vol}(B))^{n-1}. \tag{2.1.3}$$

However, if Γ is only weakly admissible, then it can happen that $\Gamma^\perp$ is not weakly admissible; see Example 1. But this is a rather special situation and typically, e.g., if

the entries of A are algebraically independent, see Lemma 2.3.1, then $\Gamma = A\mathbb{Z}^n$ and its dual are both weakly admissible. This raises the question whether, or under which conditions, one can control $\nu(\Gamma^\perp, \cdot)$ by $\nu(\Gamma, \cdot)$. We have the following result where we use the convention that for an integral domain R the group of all matrices in $R^{n\times n}$ with inverse in $R^{n\times n}$ is denoted by $\mathrm{GL}_n(R)$.

Proposition 2.1.2. *Let $\Gamma = A\mathbb{Z}^n$, and suppose there exist S, R both in $\mathrm{GL}_n(\mathbb{Z})$ such that*

$$A^T S A = R,$$

and suppose S has exactly one non-zero entry in each column and in each row. Then, we have

$$\nu(\Gamma^\perp, \cdot) = \nu(\Gamma, \cdot). \tag{2.1.4}$$

A special case of Proposition 2.1.2 shows that $\nu(\Gamma^\perp, \cdot) = \nu(\Gamma, \cdot)$ whenever $\Gamma = A\mathbb{Z}^n$ with a symplectic matrix A, in particular, whenever[1] Γ is a unimodular lattice in $\mathbb{R}^2$. In these cases, one can directly compare Theorem 2.1.1 with a recent result [128, Theorem 1.1] of the second author, and we refer to [128] for more on that. On the other hand, our next result shows that in general $\nu(\Gamma, \cdot)$ can decay arbitrarily quickly even if we control $\nu(\Gamma^\perp, \cdot)$.

Theorem 2.1.3. *Let $n \geq 3$, and let $\psi : (0, \infty) \to (0, 1)$ be non-increasing. Then, there exists a unimodular, weakly admissible lattice $\Gamma \subseteq \mathbb{R}^n$, and a sequence $\{\rho_l\} \subseteq (\gamma_n^{1/2}, \infty)$ tending to ∞, as $l \to \infty$, such that*

$$\nu(\Gamma^\perp, \rho) \gg \rho^{-n^2},$$

and

$$\nu(\Gamma, \rho_l) \leq \psi(\rho_l)$$

for all $l \in \mathbb{N} = \{1, 2, 3, \ldots\}$ and for all $\rho > \gamma_n^{1/2}$.

In the case where exactly one of the functions $\nu(\Gamma, \cdot)$, and $\nu(\Gamma^\perp, \cdot)$ is controllable while the other one decays very quickly either Theorem 2.1.1 or [128, Theorem 1.1] provides a reasonable error term, but certainly not both. This highlights the complementary aspects of Theorem 2.1.1, and [128, Theorem 1.1]. Theorem 2.1.3 is deeper than Proposition 2.1.2, and relies on Beresnevich's recent breakthrough on Davenport's longstanding question about the distribution of badly approximable points on certain submanifolds of $\mathbb{R}^n$. Going even beyond Davenport's original question, Beresnevich proved that the sets of these points have full Hausdorff-dimension, and it is the full power of this result that we require to prove Theorem 2.1.3.

Very recently German [47] introduced the so-called lattice exponent $\omega(\Gamma)$ which is a coarse measure for the rate of decay of the function $\nu(\Gamma, \rho)$; it can be expressed as

$$\omega(\Gamma) = \limsup_{\rho\to\infty} \frac{-\log \nu(\Gamma, \rho)}{n \log \rho}, \tag{2.1.5}$$

[1] Let us write $Sp_{2m}(\mathbb{R})$ for the symplectic subgroup of $GL_{2m}(\mathbb{R})$ and $SL_n(\mathbb{R})$ for the special linear subgroup of $GL_n(\mathbb{R})$. The fact $Sp_2(\mathbb{R}) = SL_2(\mathbb{R})$ can be checked directly.

where for non-weakly admissible lattices this is interpreted as $\omega(\Gamma) = \infty$. German proposes the problem of studying the spectrum of the pairs $(\omega(\Gamma), \omega(\Gamma^\perp))$ as Γ runs over all unimodular lattices in $\mathbb{R}^n$. He constructs a non-weakly admissible lattice Γ with $\omega(\Gamma^\perp) = 1/(n-1)^2$ and hence, $(\omega(\Gamma), \omega(\Gamma^\perp)) = (\infty, 1/(n-1)^2)$. If we insist that Γ be also weakly admissible then we can use Theorem 2.1.3 but at the expense that we have only an estimate for $\omega(\Gamma^\perp)$. More precisely, there exists a weakly admissible lattice Γ such that $(\omega(\Gamma), \omega(\Gamma^\perp)) \in \{\infty\} \times [0, n]$.

Next, we apply Theorem 2.1.1 to deduce counting results for Diophantine approximations. We start with a bit of historical background on this, and related problems. Let $\alpha \in \mathbb{R}$, let $\iota : [1, \infty) \to (0, 1]$ be a positive decreasing function, and let $N_\alpha^{loc}(\iota, t)$ be the number of integer pairs (p, q) satisfying $|p + q\alpha| < \iota(q),\ 1 \le q \le t$. In a series of papers, starting in 1959, Erdős [43], Schmidt [103, 104], Lang [9, 74, 75], Adams [1, 2, 3, 4, 5, 6, 7, 8], Sweet [115], and others, considered the problem of finding the asymptotics for $N_\alpha^{loc}(\iota, t)$ as t gets large.

Schmidt [103] has shown that for almost every[2] $\alpha \in \mathbb{R}$ the asymptotics are given by the volume of the corresponding subset of $\mathbb{R}^2$, provided the latter tends to infinity. This is false for quadratic α; there with $\iota(q) = 1/q$ the volume is $2\log(t) + O(1)$, and by Lang's result $N_\alpha^{loc}(1/q, t) \sim c_\alpha \log(t)$ but Adams [5] has shown that $c_\alpha \neq 2$.

Opposed to the above "non-uniform" setting, where the bound on $|p + q\alpha|$ is expressed as a function of q, we consider the "uniform" situation, where the bound is expressed as a function of t. Furthermore, we shall consider the more general asymmetric inhomogeneous setting. Let $\alpha \in (0, 1)$ be irrational, $\varepsilon, t \in (0, \infty)$, and let $y \in \mathbb{R}$. We define the counting function

$$N_{\alpha,y}(\varepsilon, t) = \#\left\{(p, q) \in \mathbb{Z} \times \mathbb{N} : \begin{array}{c} 0 \le p + q\alpha - y \le \varepsilon, \\ 0 \le q \le t \end{array}\right\}. \tag{2.1.6}$$

If the underlying set is not too stretched, then $N_{\alpha,y}(\varepsilon, t)$ is roughly the volume εt of the set in which we are counting lattice points. If we let $\varepsilon = \varepsilon(t)$ be a function of t with $t = o(t\varepsilon)$ we have, by simple standard estimates,

$$N_{\alpha,y}(\varepsilon, t) \sim \varepsilon t \tag{2.1.7}$$

for any pair $(\alpha, y) \in ((0, 1) \setminus \mathbb{Q}) \times \mathbb{R}$ whatsoever. To get non-trivial estimates for our counting function, we need information on the Diophantine properties of α. Let $\phi : (0, \infty) \to (0, 1)$ be a non-increasing function such that

$$q\big|p + q\alpha\big| \ge \phi(q) \tag{2.1.8}$$

holds for all $(p, q) \in \mathbb{Z} \times \mathbb{N}$. Then [128, Theorem 1.1] implies that

$$|N_{\alpha,y}(\varepsilon, t) - \varepsilon t| \ll_\alpha \sqrt{\frac{\varepsilon t}{\phi(t)}}. \tag{2.1.9}$$

Hence, unlike in the non-uniform setting, for badly approximable α the asymptotics are given by the volume as long as the volume tends to infinity.

[2]Here "almost every" refers always to the Lebesgue measure.

Our next result significantly improves the error term in (2.1.9), provided α is "sufficiently" badly approximable, i.e., provided $\phi(t)$ decays slowly enough. We assume that

$$\varepsilon t > 4 \qquad \text{and} \qquad 0 < \varepsilon < \sqrt{\alpha}. \tag{2.1.10}$$

Corollary 2.1.4. *Put* $E := \frac{\varepsilon t}{\phi(4t\sqrt{\varepsilon t})}$, *and* $E' := 168\sqrt{\varepsilon t^3}E$. *Then, we have*

$$|N_{\alpha,y}(\varepsilon, t) - \varepsilon t| \underset{\alpha}{\ll} \frac{\log E}{\phi^2(E')}. \tag{2.1.11}$$

In particular, if α is badly approximable then

$$|N_{\alpha,y}(\varepsilon, t) - \varepsilon t| \underset{\alpha}{\ll} \log(\varepsilon t). \tag{2.1.12}$$

2.2 An Explicit Version of Skriganov's Counting Theorem

Let $\Gamma \subseteq \mathbb{R}^n$ be a lattice, and let $\lambda_i(\Gamma)$ denote the i-th successive minimum of Γ with respect to the Euclidean norm ($1 \le i \le n$). For $r > 0$ we introduce a special set of diagonal matrices

$$\Delta_r := \left\{ \delta := \operatorname{diag}(2^{m_1}, \dots, 2^{m_n}) : \, m = (m_1, \dots, m_n)^T \in \mathbb{Z}^n, \, \|m\|_2 < r, \, \det \delta = 1 \right\},$$

and we put

$$S(\Gamma, r) := \sum_{\delta \in \Delta_r} (\lambda_1(\delta\Gamma))^{-n}.$$

Now we can state Skriganov's result. In fact, his result is more general, and applies to any convex, compact polyhedron. On the other hand, the dependency on B and Γ in the error term is not explicitly stated in his counting result [109, Thm. 6.1]. By carefully following his reasoning, see Remark 1 below, we find the following explicit version of his result. Recall that γ_n denotes the Hermite constant.

Theorem 2.2.1. *[Skriganov, 1998] Let* $n \ge 2$ *be an integer, let* $\Gamma \subseteq \mathbb{R}^n$ *be a unimodular lattice, and let* $B \subseteq \mathbb{R}^n$ *be an aligned box of volume* 1. *Suppose* $\Gamma^\perp$ *is weakly admissible, and* $\rho > \gamma_n^{1/2}$. *Then, for* $t > 0$,

$$|\#(\Gamma \cap tB) - t^n| \underset{n}{\ll} (|\partial B| \, \lambda_n(\Gamma))^n \cdot (t^{n-1}\rho^{-1/2} + S(\Gamma^\perp, r)) \tag{2.2.1}$$

where $r := n^2 + \log \frac{\rho^n}{\nu(\Gamma^\perp, \rho)}$, *and* $|\partial B|$ *denotes the surface area of* B.

Remark 1. *The references and notation in this remark are the same as in [109]. Put* $\mathcal{O} := tB$, *fix a mollifier* ω *as in (11.3), and denote by* $\tilde{\chi}(\mathcal{O}, \cdot)$ *the Fourier transform of the characteristic function* $\chi(\mathcal{O}, \cdot)$ *of* $\mathcal{O}$. *Skriganov applies Lemma 11.1 to the error term*

$$R(\mathcal{O}, \Gamma) := \sup_{X \in \mathbb{R}^n} |\#((\mathcal{O} + X) \cap \Gamma) - \operatorname{vol}(\mathcal{O})|$$

to estimate it by

$$R(\mathcal{O},\Gamma) \le \operatorname{vol}(\mathcal{O}_\tau^+) - \operatorname{vol}(\mathcal{O}_\tau^-) + \sup_{X\in\mathbb{R}^n}\Big(\big|\mathcal{R}_\tau^+(\mathcal{O},X)\big| + \big|\mathcal{R}_\tau^-(\mathcal{O},X)\big|\Big)$$

where $\mathcal{O}_\tau^\pm$ *is a* τ*-coapproximation*[3] *of* $\mathcal{O}$*, and* $\mathcal{R}_\tau^\pm$ *are the Fourier series*

$$\mathcal{R}_\tau^\pm(\mathcal{O},X) \coloneqq \sum_{\gamma\in\Gamma^\perp\setminus\{0\}} \tilde\chi(\mathcal{O}_\tau^\pm,\gamma)\tilde\omega(\tau\gamma)e^{-2\pi i\langle\gamma,X\rangle}$$

defined in (11.5) where $\tilde\omega$ *denotes the Fourier transform of* ω*. Observe that* $|\partial B| \ge 1$*, and that without loss of generality* B *is centred at the origin, i.e.,* $y = -\frac12(t_1,\dots,t_n)^T$*. Hence, we can choose* $\mathcal{O}_\tau^\pm \coloneqq (t \pm |\partial B|\,\tau)B$ *with* $0<\tau<1$*, and thus*

$$\operatorname{vol}(\mathcal{O}_\tau^+) - \operatorname{vol}(\mathcal{O}_\tau^-) \underset{n}{\ll} |\partial B|^n\, t^{n-1}\tau.$$

As noted in (6.6), since B *is an aligned box, the average* $S(\Gamma_\mathfrak{f},\cdot)$ *simplifies to* $S(\Gamma^\perp,\cdot)$*, and* $\nu(\Gamma_\mathfrak{f}^\perp,\cdot) = \nu(\Gamma^\perp,\cdot)$ *for each flag of faces* $\mathfrak{f}$ *of* B*.*
Now $\mathcal{R}_\tau^\pm$ *is decomposed via (12.7) into partial sums* $\mathcal{A}_{\tau,\rho}^\pm$ *plus remainder terms* $\mathcal{B}_{\tau,\rho}^\pm$ *which are defined in (12.8) and (12.9), respectively. Let* ω_2 *denote the Fourier transform of* ω_1 *(cf. p. 57). Due to (12.12), there is a constant* $c = c(\omega_1,\omega_2)$*, independent of* Γ, t, ρ, τ*, such that*[4]

$$\max_{X\in\mathbb{R}^n} \mathcal{A}_{\tau,\rho}^\pm(\mathcal{O},X) \le cS(\Gamma^\perp,r)$$

where we may choose r *to be*

$$r \coloneqq n^2 + \log\frac{\rho^n}{\nu(\Gamma^\perp,\rho)}.$$

Hence, c *depends in fact only on the (fixed) mollifier* ω_1*. Furthermore,* $\mathcal{B}_{\tau,\rho}^\pm(\mathcal{O},X)$ *is estimated in (12.14) by*

$$\max_{X\in\mathbb{R}^n}\big|\mathcal{B}_{\tau,\rho}^\pm(\mathcal{O},X)\big| \le \frac{c_A}{2\pi}\,|\partial B|\,t^{n-1}\tau^{-A}\sum_{\substack{\gamma\in\Gamma^\perp\\ \|\gamma\|_2>\frac18\rho}} \|\gamma\|_2^{-A-1}$$

where $A > n$*. Note that for* $R>0$

$$\#\left\{\gamma\in\Gamma^\perp:\ \|\gamma\|_2 < R\right\} \underset{n}{\ll} (R/\lambda_1(\Gamma^\perp)+1)^n.$$

This in turn implies that for $k\in\mathbb{N}_0$ *we have*

$$\#\left\{\gamma\in\Gamma^\perp:\ 2^k \le \|\gamma\|_2 < 2^{k+1}\right\} \underset{n}{\ll} (2^{k+1}/\lambda_1(\Gamma^\perp))^n.$$

[3]Given a compact region $\mathcal{O}\subseteq\mathbb{R}^n$ and a real number $\tau>0$, compact regions $\mathcal{O}_\tau^\pm$ are called τ-coapproximations to $\mathcal{O}$, if $\mathcal{O}_\tau^-\subseteq\mathcal{O}\subseteq\mathcal{O}_\tau^+$ and $\operatorname{dist}(\partial\mathcal{O},\partial\mathcal{O}_\tau^\pm)\ge\tau$ are satisfied.

[4]Conceivably, we should mention a typo regarding the definition of $r_\mathfrak{f}$ in (6.5): $r_\mathfrak{f}$ is to be taken as in (12.13). In (12.13) $\varkappa_n$ denotes τ_n from Lemma 10.1, which was defined in (7.4) as two times the diameter of the Dirichlet-Voronoi region of the lattice M defined in (3.3). It is easy to see that $2\tau_n < n^2$.

Using dyadic summation, and Mahler's relations

$$1 \leq \lambda_i(\Gamma^\perp)\lambda_{n+1-i}(\Gamma) \leq n! \qquad (i = 1, \ldots, n) \tag{2.2.2}$$

yields

$$\sum_{\substack{\gamma \in \Gamma^\perp \\ \|\gamma\|_2 > \frac{1}{8}\rho}} \|\gamma\|_2^{-A-1} \underset{n}{\ll} \sum_{k > \left\lfloor \frac{\log(8^{-1}\rho)}{\log 2} \right\rfloor} 2^{(k+1)n} \lambda_1^{-n}(\Gamma^\perp) \cdot 2^{-(A+1)k} \underset{n}{\ll} \lambda_n^n(\Gamma)\rho^{n-A-1}.$$

Hence,

$$\left|\mathcal{R}_\tau^\pm(\mathcal{O}, X)\right| \underset{n}{\ll} cS(\Gamma^\perp, r) + c_A \left|\partial B\right| t^{n-1}\tau^{-A}\lambda_n^n(\Gamma)\rho^{n-A-1}.$$

Specialising $A \coloneqq 2n-1$ *implies*

$$\begin{aligned} R(\mathcal{O}, \Gamma) &\underset{n}{\ll} \left|\partial B\right|^n t^{n-1}\tau + S(\Gamma^\perp, r) + \left|\partial B\right|^n t^{n-1}\tau^{1-2n}\lambda_n^n(\Gamma)\rho^{-n} \\ &\underset{n}{\ll} (\left|\partial B\right| \lambda_n(\Gamma))^n (t^{n-1}\tau + S(\Gamma^\perp, r) + t^{n-1}\tau^{1-2n}\rho^{-n}) \end{aligned}$$

where in the last inequality we used the obvious fact $|\partial B| \geq 1$*. Finally, choosing* $\tau \coloneqq \rho^{-1/2}$ *gives the required estimate.*

For proving Theorem 2.1.1, we want to exploit Theorem 2.2.1. To this end let $\bar{t} \coloneqq (\det \mathcal{T})^{1/n}$, and let

$$U \coloneqq \bar{t}\mathcal{T}^{-1}. \tag{2.2.3}$$

Thus,

$$\#(\Gamma \cap B) = \#(U\Gamma \cap U(\mathcal{T}\,[0,1]^n + y)) = \#(\Lambda \cap \bar{t}([0,1]^n + \mathcal{T}^{-1}(y)))$$

where $\Lambda \coloneqq U\Gamma$. Moreover, we conclude by Theorem 2.2.1 that

$$\left|\#(\Gamma \cap B) - \mathrm{vol}(B)\right| \underset{n}{\ll} \lambda_n^n(\Lambda)\left(\frac{\bar{t}^{n-1}}{\sqrt{\rho}} + S(\Lambda^\perp, r)\right). \tag{2.2.4}$$

For controlling the quantities on the right hand side in terms of Γ, $\bar{t}$, ρ, and $\nu(\Gamma^\perp, \cdot)$, we need two lemmata. We will frequently use the fact that if $\Gamma = A\mathbb{Z}^n$ is unimodular then $\Gamma^\perp = (A^{-1})^T\mathbb{Z}^n$. As usual, we let $\mathrm{SL}_n(\mathbb{R})$ denote the group of all $\mathbb{R}^{n\times n}$ matrices with determinant 1.

Lemma 2.2.2. *Let* $D \coloneqq \mathrm{diag}(d_1, \ldots, d_n)$ *be in* $\mathrm{SL}_n(\mathbb{R})$*, and* $\rho > \gamma_n^{1/2}$*. Then,*

$$\nu((D\Gamma)^\perp, \rho) \geq \nu(\Gamma^\perp, \|D\|_2\,\rho), \tag{2.2.5}$$

and

$$\lambda_1^n(D\Gamma) \underset{n}{\gg} \nu(\Gamma, \left\|D^{-1}\right\|_2^\star). \tag{2.2.6}$$

Proof. For $v \coloneqq (v_1, \dots, v_n)^T \in \mathbb{R}^n$ define $\mathrm{Nm}(v) \coloneqq |v_1 \cdots v_n|$. We remark that

$$\begin{aligned}\nu((D\Gamma)^\perp, \rho) &= \nu(D^{-1}\Gamma^\perp, \rho) \\ &= \min\left\{\mathrm{Nm}(D^{-1}v) :\ v \in \Gamma^\perp,\ 0 < \left\|D^{-1}v\right\|_2 < \rho\right\} \\ &= \min\left\{\mathrm{Nm}\,(v) :\ v \in \Gamma^\perp,\ 0 < \left\|D^{-1}v\right\|_2 < \rho\right\}.\end{aligned}$$

If $\|D^{-1}v\|_2 < \rho$, then $\|v\|_2 < \|D\|_2\rho$. Thus, (2.2.5) follows. Now let $Q > 0$, and $v \in \Gamma$ with $0 < \|v\|_2 \le Q$. By the inequality of arithmetic and geometric mean, we have

$$\|Dv\|_2^n \ge n^{n/2} \cdot \mathrm{Nm}(Dv) \underset{n}{\gg} \nu(\Gamma, Q^\star).$$

Now suppose $\|v\|_2 > Q$. Since $\|v\|_2 = \|D^{-1}Dv\|_2 \le \|D^{-1}\|_2 \|Dv\|_2$, we conclude that

$$\|Dv\|_2 > \left\|D^{-1}\right\|_2^{-1} Q.$$

Hence, we have

$$\|Dv\|_2 \underset{n}{\gg} \min\left\{(\nu(\Gamma, Q^\star))^{1/n},\ \left\|D^{-1}\right\|_2^{-1} Q\right\}.$$

Specialising $Q \coloneqq \|D^{-1}\|_2$, and noticing that by the inequality of arithmetic and geometric mean, $\nu(\Gamma, \gamma_n) \underset{n}{\ll} 1$, we get (2.2.6). □

Note that $\|D^{-1}\|_2 \le \|D\|_2^{n-1}$, and hence by Lemma 2.2.2 that

$$\lambda_1^n(D\Gamma) \underset{n}{\gg} \nu(\Gamma, \|D\|_2^{n-1}), \tag{2.2.7}$$

at least if $\|D\|_2^{n-1} > \gamma_n^{1/2}$. Therefore, the function $\nu(\Gamma, \rho)$ controls the rate of escape of the lattice Γ under the action of the diagonal subgroup of $\mathrm{SL}_n(\mathbb{R})$.

Lemma 2.2.3. *Let U be as in (2.2.3), and let $s \ge 1$. Then, we have*

$$S(\Lambda^\perp, s) \underset{n}{\ll} \frac{s^{n-1}}{\nu(\Gamma^\perp, (2^s \|U\|_2)^\star)}.$$

Proof. Since $\Lambda^\perp = U^{-1}\Gamma^\perp$, we conclude by (2.2.6) that

$$S(\Lambda^\perp, s) = \sum_{\delta \in \Delta_s} \frac{1}{\lambda_1^n(\delta U^{-1}\Gamma^\perp)} \underset{n}{\ll} \sum_{\delta \in \Delta_s} \frac{1}{\nu(\Gamma^\perp, \|U\delta^{-1}\|_2^\star)}.$$

Since $\#\Delta_s \underset{n}{\ll} s^{n-1}$, and since $\nu(\Gamma^\perp, \cdot)$ is non-increasing, we get

$$S(\Lambda^\perp, s) \underset{n}{\ll} \frac{s^{n-1}}{\nu(\Gamma^\perp, (2^s \|U\|_2)^\star)}.$$ □

Now we can give the proof of Theorem 2.1.1.

Proof of Theorem 2.1.1. By (2.2.5), we conclude

$$r = n^2 + \log \frac{\rho^n}{\nu(\Lambda^\perp, \rho)} \leq n^2 + \log \frac{\rho^n}{\nu(\Gamma^\perp, \|U\|_2 \rho)} = R$$

Since $\nu(\Lambda^\perp, \cdot)$ is non-increasing, and since $(2^R \|U\|_2)^\star = 2^R \|U\|_2$ Lemma 2.2.3 yields

$$S(\Lambda^\perp, r) \underset{n}{\ll} \frac{R^{n-1}}{\nu(\Gamma^\perp, 2^R \|U\|_2)}. \tag{2.2.8}$$

By using Mahler's relation (2.2.2) and Lemma 2.2.2, we obtain

$$\lambda_n^n(\Lambda) \underset{n}{\ll} \frac{1}{\lambda_1^n(U^{-1}\Gamma^\perp)} \underset{n}{\ll} \frac{1}{\nu(\Gamma^\perp, \|U\|_2^\star)}. \tag{2.2.9}$$

Taking (2.2.8) and (2.2.9) in (2.2.4) into account, it follows that

$$|\#(\Gamma \cap B) - \mathrm{vol}(B)| \underset{n}{\ll} \frac{1}{\nu\Big(\Gamma^\perp, \|U\|_2^\star\Big)} \left(\frac{\overline{t}^{n-1}}{\sqrt{\rho}} + \frac{R^{n-1}}{\nu(\Gamma^\perp, 2^R \|U\|_2)} \right)$$

which is (2.1.2). □

2.3 Comparing $\nu(\Gamma, \cdot)$ and $\nu(\Gamma^\perp, \cdot)$

A natural question is whether one can state Theorem 2.1.1 in a way that is intrinsic in Γ, i.e. expressing $\nu(\Gamma^\perp, \cdot)$ in terms of $\nu(\Gamma, \cdot)$. However, for $n > 2$ there are weakly admissible lattices $\Gamma \subseteq \mathbb{R}^n$ such that $\Gamma^\perp$ is not weakly admissible as the following example shows.

Example 1. *Let $n \geq 3$, and let $A_0' \in \mathrm{GL}_{n-1}(\mathbb{R})$ be such that the elements of each row of A_0' are $\mathbb{Q}$-linearly independent. Choose real $x_1, \ldots, x_{n-1}, y$ outside of the $\mathbb{Q}$-span of the entries of A_0', and suppose $y \neq x_{n-1}$. Let $x = (x_1, \ldots, x_{n-1})^T$ and let r_{n-1} be the last row of A_0'. Then, the matrix*

$$A_0 \coloneqq \begin{pmatrix} A_0' & x \\ r_{n-1} & y \end{pmatrix}$$

satisfies

(i) $A_0 \in \mathrm{GL}_n(\mathbb{R})$, and
(ii) the elements in each row of A_0 are $\mathbb{Q}$-linearly independent.

The second assertion is clear and for the first suppose a linear combination of the rows vanishes. Using that the rows of A_0' are linearly independent over $\mathbb{R}$ and that $y \neq x_{n-1}$, the first claim follows at once. We now let A be the matrix we get from A_0 by swapping the first and the last row, and scaling each entry with $|\det A_0|^{-1/n}$. Clearly, (i) and (ii) remain valid for A, and the (n,n)-minor of A vanishes. We

conclude that $\Gamma \coloneqq A\mathbb{Z}^n$ *is a unimodular, and weakly admissible lattice; moreover, Cramer's rule implies that*

$$(A^{-1})^T = \begin{pmatrix} \star & \star & \dots & \star \\ \star & \ddots & \ddots & \vdots \\ \vdots & \ddots & \star & \star \\ \star & \dots & \star & 0 \end{pmatrix}$$

where an asterisk denotes some arbitrary real number, possibly a different number each time. Hence, $\Gamma^\perp$ *contains a non-zero lattice point with a zero coordinate, and thus is not weakly admissible.*

Keeping Example 1 in mind, we now concern ourselves with finding large subclasses of lattices $\Gamma \subseteq \mathbb{R}^n$ such that

1. Γ and $\Gamma^\perp$ are both weakly admissible,
2. $\nu(\Gamma^\perp, \cdot) = \nu(\Gamma, \cdot)$.

It is easy to see that the first item holds for almost all lattices in the sense of the Haar-measure on the space $\mathcal{L}_n = \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$ of unimodular lattices in $\mathbb{R}^n$. Moreover, we have the following criterion.

Lemma 2.3.1. *Suppose* $A \in \mathrm{SL}_n(\mathbb{R})$*, and suppose that the entries of* A *are algebraically independent (over* $\mathbb{Q}$*). Then,* $\Gamma \coloneqq A\mathbb{Z}^n$ *and* $\Gamma^\perp$ *are both weakly admissible.*

Proof. First note that if K is a field and $X_1, \dots, X_N$ are algebraically independent over K, then any non-empty collection of pairwise distinct monomials $X_1^{a_1} \cdots X_N^{a_N}$ is linearly independent over K. Next note that by Cramer's rule, each entry of $(A^{-1})^T$ is a sum of pairwise distinct monomials (up to sign) in the entries of A, and none of these monomials occurs in more than one entry of $(A^{-1})^T$. This shows that the entries of $(A^{-1})^T$ are linearly independent over $\mathbb{Q}$, in particular, the entries of any fixed row of $(A^{-1})^T$ are linearly independent over $\mathbb{Q}$. Thus, $\Gamma^\perp$ is weakly admissible. □

Next, we prove Proposition 2.1.2. Notice that S and S^{-1} are, up to signs of the entries, permutation matrices, and thus for every $w \in \mathbb{R}^n$

$$\mathrm{Nm}\,(w) = \mathrm{Nm}\,(Sw) = \mathrm{Nm}\,(S^{-1}w), \tag{2.3.1}$$

$$\|w\|_2 = \|Sw\|_2 = \left\|S^{-1}w\right\|_2. \tag{2.3.2}$$

Now let Aw be an arbitrary lattice point in $\Gamma = A\mathbb{Z}^n$. Then, since $R \in \mathbb{Z}^{n\times n}$, we get $(A^{-1})^T Rw \in \Gamma^\perp$. Since by hypothesis $A = S^{-1}((A^{-1})^T R)$, we conclude from (2.3.1) that $\mathrm{Nm}\,(Aw) = \mathrm{Nm}\,((A^{-1})^T Rw)$, and from (2.3.2) that $\|Aw\|_2 = \left\|(A^{-1})^T Rw\right\|_2$. This shows that $\nu(\Gamma^\perp, \cdot) \le \nu(\Gamma, \cdot)$.

Similarly, if $(A^{-1})^T w \in \Gamma^\perp$ then, since $R^{-1} \in \mathbb{Z}^{n\times n}$, we find that $AR^{-1}w \in \Gamma$, and using that $(A^{-1})^T = SAR^{-1}$ we conclude as above that $\nu(\Gamma, \cdot) \le \nu(\Gamma^\perp, \cdot)$. This proves Proposition 2.1.2.

Remark 2. *Let $I_m \coloneqq \mathrm{diag}(1,\dots,1)$ be the identity matrix, and 0_m the null matrix in $\mathbb{R}^{m\times m}$. Specialising*

$$S = R = \begin{pmatrix} 0_m & I_m \\ -I_m & 0_m \end{pmatrix}$$

in Proposition 2.1.2, we conclude that if $\Gamma = A\mathbb{Z}^n$ with a symplectic matrix A, then

$$\nu(\Gamma^\perp,\cdot) = \nu(\Gamma,\cdot). \tag{2.3.3}$$

Moreover, it is easy to see that $\mathrm{Sp}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$, and hence (2.3.3) holds for any unimodular lattice $\Gamma \subseteq \mathbb{R}^2$.

Next, we prove Theorem 2.1.3. Recall that $\alpha \coloneqq (\alpha_1,\dots,\alpha_n)^T \in \mathbb{R}^n$ is called badly approximable, if there is a constant $C = C(\alpha) > 0$ such that for any integer $q \geq 1$ the inequality

$$\max\left\{\|q\alpha_1\|,\dots,\|q\alpha_n\|\right\} \geq \frac{C}{q^{1/n}} \tag{2.3.4}$$

holds where $\|\cdot\|$ denotes the distance to the nearest integer. By a well-known transference principle, cf. [31], assertion (2.3.4) is equivalent to saying that for all non-zero vectors $q \coloneqq (q_1,\dots,q_n)^T \in \mathbb{Z}^n$ the inequality

$$\|\langle \alpha, q\rangle\| \geq \frac{\tilde{C}}{\|q\|_2^n} \tag{2.3.5}$$

holds where $\tilde{C} = \tilde{C}(\alpha) > 0$ is a constant. Let $\mathbf{Bad}(n)$ denote the set of all badly approximable vectors in $\mathbb{R}^n$. The crucial step for constructing matrices generating the lattices announced in Theorem 2.1.3 is done by the following lemma.

Lemma 2.3.2. *Let $n \geq 3$ be an integer. Fix algebraically independent real numbers $c_{i,j}$ where $i,j = 1,\dots,n$ and $i \neq j$. Then, there exist $\lambda_1,\dots,\lambda_n \in \mathbb{R}$ such that the entries of each row of*

$$A \coloneqq \begin{pmatrix} \lambda_1 & c_{1,2} & \dots & c_{1,n} \\ c_{2,1} & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & c_{n-1,n} \\ c_{n,1} & \dots & c_{n,n-1} & \lambda_n \end{pmatrix} \tag{2.3.6}$$

are algebraically independent, A is invertible, and each row-vector of $(A^{-1})^T$ is badly approximable.

For proving this lemma, we shall use the following special case of a recent Theorem of Beresnevich concerning badly approximable vectors. We say that the map $F \coloneqq (f_1,\dots,f_n)^T : \mathcal{B} \to \mathbb{R}^n$, where $\mathcal{B} \subsetneq \mathbb{R}^m$ is a non-empty ball and $m,n \in \mathbb{N}$, is non-degenerate, if 1, $f_1,\dots,f_n$ are linearly independent functions (over $\mathbb{R}$).

Theorem 2.3.3 ([18, Thm. 1])**.** *Let n, m, k be positive integers. For each $j = 1,\dots,k$ suppose that $F_j : \mathcal{B} \to \mathbb{R}^n$ is a non-degenerate, analytic map defined on a non-empty ball $\mathcal{B} \subsetneq \mathbb{R}^m$. Then,*

$$\dim_{\mathrm{Haus}} \bigcap_{j=1}^{k} F_j^{-1}\left(\mathbf{Bad}(n)\right) = m.$$

Proof of Lemma 2.3.2. We work in two steps. First, we set the scene to make use of Theorem 2.3.3.

(i) Let $M \in \mathbb{R}^{n\times n}$, and denote by $(M)_{i,j}$ the entry in the i-th row and j-th column of M. Moreover, we define a map $\tilde{F} : \mathbb{R}^n \to \mathbb{R}^{n\times n}$ by

$$\lambda \coloneqq (\lambda_1, \dots, \lambda_n)^T \mapsto \begin{pmatrix} \lambda_1 & c_{1,2} & \dots & c_{1,n} \\ c_{2,1} & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & c_{n-1,n} \\ c_{1,n} & \dots & c_{n,n-1} & \lambda_n \end{pmatrix}.$$

On a sufficiently small non-empty ball $\mathcal{B} \subsetneq \mathbb{R}^n$, centred at the origin, $\tilde{F}(\lambda)$ is invertible for every $\lambda \in \mathcal{B}$.[5] On this ball $\mathcal{B}$, we define F_j, for $j = 1, \dots, n$, by mapping λ to the j-th row of $(\left(\tilde{F}(\lambda)\right)^{-1})^T$. We claim that F_j is a non-degenerate, and analytic map. By Cramer's rule, every entry of $((\tilde{F}(\lambda))^{-1})^T$ is the quotient of polynomials in $\lambda_1, \dots, \lambda_n$ whereas the polynomial in the denominator does not vanish on $\mathcal{B}$. Hence, each F_j is an analytic function. Now we show that F_1 is non-degenerate, the argument for the other F_j being similar. The j-th component of F_1 is $(\left(\tilde{F}(\lambda)\right)^{-1})_{j,1}$ and, using Cramer's rule, is hence of the shape

$$(\det \tilde{F}(\lambda))^{-1} \left(\mathcal{R}_j + (-1)^{1+j} \prod_{k=2,\, k\neq j}^{n} \lambda_k \right)$$

where the polynomial $\mathcal{R}_j \in \mathbb{R}[\lambda_2, \dots, \lambda_n]$ is of (total) degree $< n-1$, if $j = 1$, and of (total) degree $< n-2$, if $j = 2, \dots, n$. Therefore, if a linear combination $k_0 + \sum_{j=1}^n k_j((\tilde{F}(\lambda))^{-1})_{j,1}$ with scalars $k_0, \dots, k_n \in \mathbb{R}$ equals the zero-function $\mathbf{0} : \mathcal{B} \to \mathbb{R}$, then

$$\mathbf{0} = k_0 \cdot (\det \tilde{F}(\lambda)) + \sum_{j=1}^{n} k_j (-1)^{1+j} \prod_{k=2,\, k\neq j}^{n} \lambda_k + \sum_{j=1}^{n} k_j \mathcal{R}_j.$$

Comparing coefficients, we conclude that $k_0 = 0$ and thereafter $k_1 = k_2 = \dots = k_n = 0$. Hence, F_1 is non-degenerate.

(ii) By part (i), Theorem 2.3.3 implies that the set M of all $\lambda \in \mathcal{B}$ such that $F_1(\lambda), \dots, F_n(\lambda)$ are all badly approximable, has full Hausdorff dimension. Moreover, we claim that there is a set $M^{(1)} \subseteq M$ of full Hausdorff dimension such that for every $\lambda \in M^{(1)}$ the entries of the first row of $\tilde{F}(\lambda)$ are algebraically independent. Let M_1 be the subset of M of all elements $\lambda \coloneqq (\lambda_1, \dots, \lambda_n)^T \in M$ satisfying that $\{\lambda_1, c_{1,j} : j = 2, \dots, n\}$ is algebraically *dependent*; observe that the possible values for

[5] To see this, it suffices to show $\det \tilde{F}((0, \dots, 0)^T) \neq 0$. However, by the Leibniz formula,

$$\det \tilde{F}(0, \dots, 0) = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} c_{i,\sigma(i)}$$

where the sum runs through all fixpoint-free permutations of $\{1, \dots, n\}$. Since $\{c_{i,j} : i, j = 1, \dots, n,\, i \neq j\}$ is algebraically independent, the evaluation of the polynomial on the right hand side above cannot vanish, cf. proof of Lemma 2.3.1.

λ_1 are countable, since $\mathbb{Z}[c_{1,2}, \dots, c_{1,n}, x]$ is countable and every complex, non-zero, univariate polynomial has only finitely many roots. Therefore, M_1 is contained in a countable union of hyperplanes. It is well-known that if a sequence of sets $\{E_i\} \subseteq \mathbb{R}^n$ is given, then $\dim_{\text{Haus}} \bigcup_{i\geq 1} E_i = \sup_{i\geq 1}\{\dim_{\text{Haus}} E_i\}$, cf. [21, p. 65]. Consequently,

$$n = \dim_{\text{Haus}} M = \max\{\dim_{\text{Haus}}(M \setminus M_1), \dim_{\text{Haus}} M_1\} = \dim_{\text{Haus}}(M \setminus M_1),$$

and we define $M^{(1)} \coloneqq M \setminus M_1$. Using the same argument, we conclude that there is a set $M^{(2)} \subseteq M^{(1)}$ of full Hausdorff dimension such that each of the first two rows of $\tilde{F}(\lambda)$ has algebraically independent entries for every $\lambda \in M^{(2)}$. Iterating this construction, we infer that there is a subset $M^{(n)} \subseteq M^{(n-1)} \subseteq \ldots \subseteq M$ of full Hausdorff dimension such that for every $\lambda \in M^{(n)}$ each row of the matrix $A \coloneqq \tilde{F}(\lambda)$ has algebraically independent entries, and $(A^{-1})^T$ has badly approximable row vectors. Moreover, $\lambda \in M^{(n)} \subseteq \mathcal{B}$ implies that A is invertible.

□

We also need the following easy fact whose proof is left as an exercise.

Lemma 2.3.4. *Let $m \in \mathbb{N}$, and let $\alpha \in \mathbb{R}$ be transcendental. Then, there are real numbers $\beta_1, \dots, \beta_m$ such that $\beta_1, \alpha\beta_1, \beta_2, \dots, \beta_m$ are algebraically independent.*

Proof of Theorem 2.1.3. First, we set $\tilde{\psi}(x) = \psi(x^2)$ such that for every $c > 0$ and $x \geq c$ we have $\tilde{\psi}(x) \leq \psi(cx)$. We may assume that $\tilde{\psi}(q) \ll \exp(-q)$. By writing down a suitable decimal expansion, we conclude that there exists a number $\alpha \in (0, 1)$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{\tilde{\psi}(q)}{q^{n+1}} \tag{2.3.7}$$

has infinitely many coprime integer solutions p, $q \in \mathbb{Z}$; observe that such an α is necessarily transcendental. We apply Lemma 2.3.4 with $m = n^2 - n$ and we set $c_{1,2} \coloneqq \beta_1, c_{1,3} \coloneqq \alpha\beta_1$, and we choose exactly one value β_k ($k \geq 2$) for each of the remaining $c_{i,j}$ ($i \neq j$). Thus, the real numbers $c_{i,j}$ are algebraically independent. We use Lemma 2.3.2 with these specifications to find A as in (2.3.6). For $l \in \mathbb{N}$ let p_l, q_l denote distinct solutions to (2.3.7), and put $v_l \coloneqq (0, -p_l, q_l, 0, \dots, 0)^T \in \mathbb{Z}^n$. Set $\tilde{A} \coloneqq |\det A|^{-1/n} A$, and let us consider the unimodular, weakly admissible lattice $\Gamma \coloneqq \tilde{A}\mathbb{Z}^n$. Then, the first coordinate of $\tilde{A}v_l$ equals

$$|\det A|^{-1/n}\,|-p_l c_{1,2} + q_l c_{1,3}| = |\det A|^{-1/n}\,|c_{1,2}|\,|q_l\alpha - p_l| \underset{A}{\ll} \frac{\tilde{\psi}(q_l)}{q_l^n}.$$

Since $\alpha \in (0, 1)$, we may assume, by choosing l large enough, that $p_l \leq q_l$. Hence, the j-th coordinate for $j = 2, \dots, n$ of $\tilde{A}v_l$ is $\underset{A}{\ll} q_l$. Thus, for l sufficiently large,

$$\mathrm{Nm}(\tilde{A}v_l) \underset{A}{\ll} \frac{\tilde{\psi}(q_l)}{q_l^n} \cdot q_l^{n-1} = \frac{\tilde{\psi}(q_l)}{q_l} \leq \frac{\psi(2\|\tilde{A}\|_2 q_l)}{q_l} \leq \frac{\psi(\|\tilde{A}v_l\|_2)}{q_l}.$$

Choosing $\rho_l = \|\tilde{A}v_l\|_2$, we conclude that $\nu(\Gamma, \rho_l) \leq \psi(\rho_l)$ for all l sufficiently large.

Because the rows of $(A^{-1})^T$ are badly approximable vectors by construction, $\Gamma^\perp$ is weakly admissible. Moreover, by (2.3.5), we conclude that $\mathrm{Nm}((A^{-1})^T v) \underset{A}{\gg} \|v\|_2^{-n^2}$ for every non-zero $v \in \mathbb{Z}^n$. Also note that $\left\|(A^{-1})^T v\right\|_2 < \rho$ implies $\|v\|_2 < \|A^T\|_2 \rho$. This implies that $\nu(\Gamma^\perp, \rho) \underset{A}{\gg} \rho^{-n^2}$. Hence, Γ has the desired properties. □

2.4 An Application - Proof of Corollary 2.1.4

Throughout this section we fix the unimodular lattice $\Gamma = A\mathbb{Z}^2$ where

$$A := \frac{1}{\sqrt{\alpha}} \begin{pmatrix} 1 & \alpha \\ 1 & 2\alpha \end{pmatrix},$$

and we consider the aligned box

$$B := \frac{1}{\sqrt{\alpha}} \Big(\big[y,\, y+\varepsilon\big] \times \big[y,\, y+\alpha t\big] \Big). \tag{2.4.1}$$

Then, the following relation holds

$$\#(B \cap \Gamma) = \#\left\{ (p,q) \in \mathbb{Z}^2 : \begin{array}{c} 0 \le p + \alpha q - y \le \varepsilon, \\ 0 \le p + 2\alpha q - y \le \alpha t \end{array} \right\}.$$

Because of (2.1.10), we conclude that

$$|N_{\alpha,y}(\varepsilon, t) - \#(B \cap \Gamma)| \underset{\alpha}{\ll} 1. \tag{2.4.2}$$

In order to use Theorem 2.1.1, we need to control the characteristic quantity $\nu(\Gamma, \cdot)$ of the lattice Γ. This is where the Diophantine properties of α come into play.

Lemma 2.4.1. *Let ϕ be as in (2.1.8), and suppose $\rho > \gamma_2^{1/2}$. Then, we have*

$$\nu(\Gamma^\perp, \rho) = \nu(\Gamma, \rho) \ge \frac{\phi(4\rho/\sqrt{\alpha})}{4}.$$

Proof. The claimed equality follows immediately from Proposition 2.1.2, and the remark thereafter. A vector $v \in \Gamma$ is of the shape

$$v = \frac{1}{\sqrt{\alpha}} \begin{pmatrix} z \\ z' \end{pmatrix}$$

where $z := p + q\alpha$, $z' := z + q\alpha$, and p, q denote integers. Assume that $\|v\|_2 \in (0, \rho)$. Observe that $q = 0$ implies $\mathrm{Nm}(v) \ge 1 > 4^{-1}\phi(4\rho/\sqrt{\alpha})$. Therefore, we may assume $q \neq 0$. Since $z' - z = q\alpha$, one of the numbers $|z|, |z'|$ is at least $\frac{1}{2}\alpha|q|$, and both are bounded from below by $\frac{1}{2|q|}\phi(2|q|)$. Hence,

$$\mathrm{Nm}\,(v) \ge \frac{\alpha|q|}{2\sqrt{\alpha}} \cdot \frac{\phi(2|q|)}{2|q|\sqrt{\alpha}} \ge \frac{\phi(4\rho/\sqrt{\alpha})}{4}$$

where in the last step we used that $\frac{1}{2}\sqrt{\alpha}|q| \le \frac{1}{\sqrt{\alpha}} \min\{|z|, |z'|\} \le \|v\|_2 < \rho$. □

Proof of Corollary 2.1.4. Let B be given by (2.4.1). Thus, B has sidelengths $t_1 = \alpha^{-1/2}\varepsilon$, and $t_2 = \sqrt{\alpha}t$. By (1.1.4) and (2.1.10), we are entitled to take $\rho := \varepsilon t > \gamma_2^{1/2}$ in Theorem 2.1.1. Moreover, (2.1.10) implies $t_1 < 1 < t_2$, and thus

$$T = \sqrt{\alpha \frac{t}{\varepsilon}} > \sqrt{\varepsilon t} > 2 > \gamma_2.$$

Hence, $T^\star = T$. By combining relation (2.4.2) and Theorem 2.1.1 with these specifications, it follows that

$$|N_{\alpha,y}(\varepsilon, t) - \varepsilon t| \underset{\alpha}{\ll} \frac{1}{\nu(\Gamma^\perp, T)} \left(1 + \frac{R}{\nu(\Gamma^\perp, 2^R T)}\right). \tag{2.4.3}$$

By Lemma 2.4.1, the right hand side above is $\ll R(\phi(4T/\sqrt{\alpha})\phi(2^{R+2}T/\sqrt{\alpha}))^{-1}$. The first factor in the round brackets is larger than the second one, since ϕ is non-increasing. Hence, we conclude that the right hand-side of (2.4.3) is bounded by

$$\ll R(\phi(2^{R+2}T/\sqrt{\alpha}))^{-2}. \tag{2.4.4}$$

Furthermore, Lemma 2.4.1 yields

$$R \leq 4 + \log \frac{4(\varepsilon t)^2}{\phi(4t\sqrt{\varepsilon t})} \ll \log \frac{\varepsilon t}{\phi(4t\sqrt{\varepsilon t})}. \tag{2.4.5}$$

By using the first estimate from (2.4.5), we get

$$2^R \leq 2^4 \left(\frac{4(\varepsilon t)^2}{\phi(4t\sqrt{\varepsilon t})}\right)^{\log 2} < 2^{4+2\log 2} \frac{(\varepsilon t)^2}{\phi(4t\sqrt{\varepsilon t})}.$$

Hence, (2.4.4) is bounded from above by

$$\ll \frac{\log \frac{\varepsilon t}{\phi(4t\sqrt{\varepsilon t})}}{\phi^2\left(2^{6+2\log 2} \frac{(\varepsilon t)^2}{\phi(4t\sqrt{\varepsilon t})} \sqrt{\frac{t}{\varepsilon}}\right)} \leq \frac{\log E}{\phi^2(E')}.$$

This completes the proof of Corollary 2.1.4. □

Chapter 3

The Duffin-Schaeffer Conjecture with Extra Divergence

> "Ich habe keine besondere Begabung, sondern bin nur leidenschaftlich neugierig."[1]
> — A. Einstein [39].

The present chapter is based on joint work with **Christoph Aistleitner**, **Thomas Lachmann**, **Marc Munch**, and **Agamemnon Zafeiropoulos** [11].

The Duffin–Schaeffer conjecture is a fundamental unsolved problem in metric number theory. It asserts that for every non-negative function $\psi : \mathbb{N} \to \mathbb{R}$ for almost all reals x there are infinitely many coprime solutions (a, n) to the inequality $|nx - a| < \psi(n)$, provided that the series $\sum_{n=1}^{\infty} \psi(n)\varphi(n)/n$ is divergent. In the present work we prove that the conjecture is true under the "extra divergence" assumption that divergence of the series still holds when $\psi(n)$ is replaced by $\psi(n)/(\log n)^{\varepsilon}$ for some $\varepsilon > 0$. This improves a result of Beresnevich, Harman, Haynes and Velani, and solves a problem posed by Haynes, Pollington and Velani.

3.1 Introduction and Statement of Results

Let $\psi : \mathbb{N} \to \mathbb{R}$ be a non-negative function. For every non-negative integer n define a set $\mathcal{E}_n \subset \mathbb{R}/\mathbb{Z}$ by

$$\mathcal{E}_n := \bigcup_{\substack{1 \le a \le n, \\ (a,n)=1}} \left(\frac{a - \psi(n)}{n}, \frac{a + \psi(n)}{n} \right) \pmod 1. \tag{3.1.1}$$

The Lebesgue measure of $\mathcal{E}_n$ is $\psi(n)\varphi(n)/n$, where φ denotes the Euler totient function. Writing $W(\psi)$ for the set of those $x \in [0, 1]$ which are contained in infinitely many sets $\mathcal{E}_n$, it follows directly from the first Borel–Cantelli lemma $\lambda(W(\psi)) = 0$ when

$$\sum_{n=1}^{\infty} \frac{\psi(n)\varphi(n)}{n} < \infty. \tag{3.1.2}$$

[1] In English (translated by N.T.): "I have no special gift, but I am, merely, passionately curious".

Here λ denotes the Lebesgue measure. The corresponding divergence statement, which asserts that $\lambda(W(\psi)) = 1$ whenever the series in (3.1.2) is divergent, is known as the Duffin–Schaeffer conjecture [36] and is one of the most important open problems in metric number theory. It remains unsolved since 1941.

We shall prove the following.

Theorem 3.1.1. *The Duffin–Schaeffer conjecture is true for every non-negative function $\psi : \mathbb{N} \to \mathbb{R}$ for which there is a constant $\varepsilon > 0$ such that*

$$\sum_{n=1}^{\infty} \frac{\psi(n)\varphi(n)}{n(\log n)^{\varepsilon}} = \infty. \tag{3.1.3}$$

We note that by the mass transference principle of Beresnevich and Velani [20] it is possible to deduce Hausdorff measure statements from results for Lebesgue measure, in the context of the Duffin–Schaeffer conjecture. Roughly speaking, the quantitative "extra divergence" result in Theorem 3.1.1 translates into a corresponding condition on the dimension function of a Hausdorff measure for the set where the Duffin–Schaeffer conjecture is true. For details we refer the reader to Section 4 of [59], where this connection is explained in detail.

3.2 Proof of Theorem 3.1.1

Throughout the proof, we assume that $\varepsilon > 0$ is fixed. We use Vinogradov notation "$\ll$", where the implied constant may depend on ε, but not on m, n, h or anything else.

As noted in [19], we may assume without loss of generality that for all n either $1/n \leq \psi(n) \leq 1/2$ or $\psi(n) = 0$. Furthermore, by Gallagher's zero–one law [46] the measure of $W(\psi)$ can only be either 0 or 1. Thus $\lambda(W(\psi)) > 0$ implies $\lambda(W(\psi)) = 1$.

We will use the following version of the second Borel–Cantelli lemma (see for example [58, Lemma 2.3]).

Lemma 3.2.1. *Let $\mathcal{A}_n$, $n = 1, 2, \ldots$, be events in a probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Let $\mathcal{A}$ be the set of $\omega \in \Omega$ which are contained in infinitely many $\mathcal{A}_n$. Assume that*

$$\sum_{n=1}^{\infty} \mathbb{P}(\mathcal{A}_n) = \infty.$$

Then

$$\mathbb{P}(\mathcal{A}) \geq \limsup_{N\to\infty} \frac{\left(\sum_{n=1}^{N} \mathbb{P}(\mathcal{A}_n)\right)^2}{\sum_{1\leq m,n\leq N} \mathbb{P}(\mathcal{A}_m \cap \mathcal{A}_n)}.$$

The following lemma of Pollington and Vaughan [88] allows to estimate the ratio between the measure of the overlap $\mathcal{E}_m \cap \mathcal{E}_n$ and the product of the measures of $\mathcal{E}_m$ and $\mathcal{E}_n$, and is a key ingredient in [19].

Lemma 3.2.2. *For $m \neq n$, assume that $\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n) \neq 0$. Define*

$$P(m,n) = \frac{\lambda(\mathcal{E}_m \cap \mathcal{E}_n)}{\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n)}. \tag{3.2.1}$$

Then

$$P(m,n) \ll \prod_{\substack{p \mid \frac{mn}{(m,n)^2}, \\ p > D(m,n)}} \left(1 - \frac{1}{p}\right)^{-1}, \tag{3.2.2}$$

where the product is taken over all primes p in the specified range, and where

$$D(m,n) = \frac{\max(n\psi(m), m\psi(n))}{(m,n)}. \tag{3.2.3}$$

In view of Lemma 3.2.1 it is clear that controlling $P(m,n)$ is the key to proving $\lambda(W(\psi)) > 0$. Following [19], we divide the set of positive integers into blocks

$$2^{4^h} \leq n < 2^{4^{h+1}}, \qquad h \geq 1, \tag{3.2.4}$$

and we may assume without loss of generality that the divergence condition (3.1.3) still holds when the summation is restricted to those n which are contained in a block with h being even. As noted in [19], when m and n are contained in different blocks, then automatically $P(m,n) \ll 1$. Thus the real problem is that of controlling $P(m,n)$ when m and n are contained in the same block (3.2.4) for some h.

In the sequel, let m, n be fixed, and assume that

$$2^{4^h} \leq m < n < 2^{4^{h+1}}$$

for some h. As in [19], we will average the factors $P(m,n)$ over a range of downscaled versions of the sets $\mathcal{E}_m$ and $\mathcal{E}_n$. More precisely, for $k = 1, 2, \ldots$, let $\mathcal{E}_n^{(k)}$ be defined as $\mathcal{E}_n$, but with $\psi(n)/e^k$ in place of $\psi(n)$. Correspondingly, we define

$$P_k(m,n) = \frac{\lambda\big(\mathcal{E}_m^{(k)} \cap \mathcal{E}_n^{(k)}\big)}{\lambda\big(\mathcal{E}_m^{(k)}\big)\lambda\big(\mathcal{E}_n^{(k)}\big)}$$

and

$$D_k(m,n) = \frac{\max(n\psi(m), m\psi(n))}{e^k(m,n)},$$

and note that for P_k we have the same estimate as in (3.2.2), only with D replaced by D_k. At the core of the argument in [19] is the observation that

$$\begin{aligned} \sum_{k=1}^{K} P_k(m,n) &\ll \sum_{k=1}^{K} \prod_{\substack{p \mid \frac{mn}{(m,n)^2}, \\ p > e^k}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \sum_{k=1}^{K} \frac{\log\log n}{k} \\ &\ll (\log K)(\log\log n), \end{aligned} \tag{3.2.5}$$

where the product in the first line is estimated using Mertens' second theorem. Thus when $K \gg (\log\log n)(\log\log\log n)$ we have $\sum_{k=1}^{K} P_k(m,n) \ll K$, and accordingly there is at least one value of k in this range for which $P_k(m,n) \ll 1$. This argument can be exteded over a range of pairs (m,n) instead of assuming that m,n are fixed. Together with Lemma 3.2.1 and Gallagher's zero–one law this allows to deduce the desired result, provided that we are allowed to divide $\psi(n)$ by $e^K \leq e^{\varepsilon(\log\log n)(\log\log\log n)}$ for all n and still keep the divergence of the sum of measures.

In our proof we will roughly follow the same plan. However, instead of taking (3.2.2) for granted and then averaging over different reduction factors e^k, we will take the averaging procedure into the proof of the overlap estimate which leads to Lemma 3.2.2. To see where a possible improvement could come from, we note that to obtain the estimate in Lemma 3.2.2 it is necessary to give upper bounds for sums

$$\sum_{\substack{1\leq b\leq\theta,\\(b,t)=1}} 1,$$

where we can think of $\theta \ll \log t$ as being the number D from (3.2.3), and of t as being the number $\frac{mn}{(m,n)^2}$ which appears in (3.2.2). It is necessary to relate this sum to $\theta\varphi(t)/t$. To obtain Lemma 3.2.2 one applies the classical sieve bound

$$\sum_{\substack{1\leq b\leq\theta,\\(b,t)=1}} 1 \ll \theta \prod_{\substack{p\mid t,\\p\leq\theta}} \left(1-\frac{1}{p}\right) = \theta\frac{\varphi(t)}{t} \prod_{\substack{p\mid t,\\p>\theta}} \left(1-\frac{1}{p}\right)^{-1}, \tag{3.2.6}$$

and the product on the very right is the one which also appears in (3.2.2). This sieve bound gives optimal results for some constellations of parameters, but we can use the fact that we are averaging over different values of k (which determine θ) to save some factors. We exhibit two extremal cases showing this phenomenon. The factor $P(m,n)$ can only be large when the product on the right of (3.2.6) is large. However, this product can only be large if a very large proportion of small primes divides t. Assume on the contrary that *no* small prime divides t. Then the sieve inequality in (3.2.6) is actually an equality, since on both sides we have exactly θ, but the product on the very right is extremely small and cannot cause problems. As a second extremal case, assume that *all* small primes divide t. Then the product on the very right is very large, but the sieve bound is not sharp, since in the sum on the left the only number we count is the number 1 (no other small number is coprime to t). So there is a trade-off between the way how a large proportion of primes dividing t is able to increase the value of the product on the right of (3.2.6), but at the same time reduces the quality of the sieve bound. It seems that this should be a very subtle relationship, and in general this is indeed the case (cf. [50, Proposition 2.6], where this phenomenon is addressed). However, quite surprisingly, it turns out that in our particular situation it is possible to exploit this phenomenon using only some simple calculations.

Following [88, Paragraph 3], we write m and n in their prime factorization

$$m = \prod_p p^{u_p}, \qquad n = \prod_p p^{v_p},$$

and define

$$r = \prod_{\substack{p, \\ u_p = v_p}} p^{u_p}, \qquad s = \prod_{\substack{p, \\ u_p \neq v_p}} p^{\min(u_p, v_p)}, \qquad t = \prod_{\substack{p, \\ u_p \neq v_p}} p^{\max(u_p, v_p)}.$$

Furthermore, we set

$$\delta = \min\left(\frac{\psi(m)}{m}, \frac{\psi(n)}{n}\right), \qquad \Delta = \max\left(\frac{\psi(m)}{m}, \frac{\psi(n)}{n}\right).$$

Then for every k from the first displayed formula on page 196 of [88] we have the estimate

$$\lambda(\mathcal{E}_m^{(k)} \cap \mathcal{E}_n^{(k)}) \ll \frac{\delta}{e^k}\varphi(s)\frac{\varphi(r)^2}{r}\int_1^{4\Delta rte^{-k}} S_t(\theta)\, d\theta,$$

where we write

$$S_t(\theta) = \sum_{\substack{1 \leq b \leq \theta, \\ (b,t)=1}} \frac{1}{\theta}$$

and where we used that changing $\psi(m) \mapsto \psi(m)/e^k$ and $\psi(n) \mapsto \psi(n)/e^k$ also changes $\delta \mapsto \delta/e^k$ and $\Delta \mapsto \Delta/e^k$. Since

$$\lambda(\mathcal{E}_m^{(k)})\lambda(\mathcal{E}_n^{(k)}) = \frac{\varphi(m)\varphi(n)\delta\Delta}{e^{2k}}$$

this implies

$$\begin{aligned} P_k(m,n) &\ll \frac{e^k\varphi(s)\varphi(r)^2\int_1^{4\Delta rte^{-k}} S_t(\theta)\, d\theta}{\Delta r\varphi(m)\varphi(n)} \\ &= \frac{\varphi(t)t}{\varphi(t)t}\,\frac{\varphi(s)\varphi(r)^2}{\varphi(m)\varphi(n)}\,\frac{\int_1^{4\Delta rte^{-k}} S_t(\theta)\, d\theta}{\Delta re^{-k}} \\ &= \frac{t}{\varphi(t)}\frac{\int_1^{4\Delta rte^{-k}} S_t(\theta)\, d\theta}{\Delta rte^{-k}}, \end{aligned}$$

where the last line follows from $\varphi(s)\varphi(r)^2\varphi(t) = \varphi(m)\varphi(n)$. We set $K = K(h) = \lfloor \varepsilon h \log 4 \rfloor$. Note that with this choice of K we have

$$e^K \ll (\log m)^\varepsilon, (\log n)^\varepsilon \ll e^K. \tag{3.2.7}$$

Summing over k, we deduce that

$$\sum_{k=1}^{K} P_k(m,n) \ll \sum_{k=1}^{K} \frac{t}{\varphi(t)}\frac{\int_1^{4\Delta rte^{-k}} S_t(\theta)\, d\theta}{\Delta rte^{-k}}. \tag{3.2.8}$$

As noted in [88] and [19], if $2\Delta rte^{-k} \leq 1$ then $P_k(m,n) = 0$, since in this case $\mathcal{E}_m^{(k)}$ and $\mathcal{E}_n^{(k)}$ are disjoint (see the fourth displayed formula from below on p. 195 of [88]). Furthermore, again as noted in [88] and [19], if $4\Delta rte^{-k} \geq e^K \gg (\log n)^\varepsilon$ then $P_k(m,n) \ll 1$, which follows from Lemma 3.2.2 and Mertens' second theorem.

Accordingly, for the contribution to (3.2.8) of those k for which $4\Delta rte^{-k} \notin [1, e^K)$ we have

$$\sum_{\substack{1\le k\le K,\\ 4\Delta rte^{-k}\notin[1,e^K)}} P_k(m,n) \ll K. \tag{3.2.9}$$

To estimate the contribution of the other values of k, we note that there exists a number $c \in [1, e)$ such that

$$\Big(\Big\{4\Delta rte^{-k},\ k = 1, \dots, K\Big\} \cap [1, e^K)\Big) \subset \{ce^j, j = 0, \dots, K-1\}.$$

Thus for the contribution of these k to (3.2.8) we have

$$\sum_{\substack{1\le k\le K,\\ 4\Delta rte^{-k}\in[1,e^K)}} P_k(m,n) \ \ll\ \frac{t}{\varphi(t)} \sum_{j=0}^{K-1} \frac{1}{e^j} \int_1^{ce^j} S_t(\theta)\, d\theta. \tag{3.2.10}$$

For the term on the right-hand side of (3.2.10) we have

$$\begin{aligned}
\sum_{j=0}^{K-1} \frac{1}{e^j} \int_1^{ce^j} S_t(\theta)\, d\theta &\ll \sum_{j=1}^{K} \frac{1}{e^j} \int_1^{e^j} S_t(\theta)\, d\theta \\
&= \sum_{j=1}^{K} \frac{1}{e^j} \sum_{\substack{1\le b\le e^j,\\ (b,t)=1}} \int_b^{e^j} \frac{d\theta}{\theta} \\
&= \sum_{j=1}^{K} \sum_{\substack{1\le b\le e^j,\\ (b,t)=1}} \frac{j - \log b}{e^j} \\
&= \sum_{\substack{1\le b\le e^K,\\ (b,t)=1}} \sum_{j=\lceil \log b\rceil}^{K} \frac{j - \log b}{e^j} \\
&\ll \sum_{\substack{1\le b\le e^K,\\ (b,t)=1}} \frac{1}{b} \underbrace{\sum_{i=1}^{\infty} \frac{i}{e^i}}_{\ll 1} \\
&\ll \sum_{\substack{1\le b\le e^K,\\ (b,t)=1}} \frac{1}{b}.
\end{aligned} \tag{3.2.11}$$

The sum in (3.2.11) can be estimated using a sieve with logarithmic weights. Following the lines of [50, Lemma 2.1], we have

$$\begin{aligned}
\sum_{\substack{1\le b\le e^K,\\ (b,t)=1}} \frac{1}{b} &= \sum_{\substack{1\le b\le e^K,\\ p\mid b \Longrightarrow p\nmid t}} \frac{1}{b} \le \prod_{\substack{p\le e^K,\\ p\nmid t}} \left(1 - \frac{1}{p}\right)^{-1} \\
&= \left(\prod_{p\le e^K} \left(1 - \frac{1}{p}\right)^{-1}\right) \prod_{\substack{p\le e^K,\\ p\mid t}} \left(1 - \frac{1}{p}\right).
\end{aligned} \tag{3.2.12}$$

For the first product in (3.2.12) by Mertens' theorem we have

$$\prod_{p\le e^K}\left(1-\frac{1}{p}\right)^{-1}\ll K.$$

For the second product we have

$$\prod_{\substack{p\le e^K,\\ p|t}}\left(1-\frac{1}{p}\right) \;=\; \frac{\varphi(t)}{t}\underbrace{\prod_{\substack{p>e^K,\\ p|t}}\left(1-\frac{1}{p}\right)^{-1}}_{\ll 1},$$

where Mertens' theorem and (3.2.7) were used to estimate the last product. Inserting these bounds into (3.2.11), and combining this with (3.2.9) and (3.2.10) we finally obtain

$$\sum_{k=1}^{K}P_k(m,n)\ll K. \tag{3.2.13}$$

By the definition of $P_k(m,n)$ we have

$$\begin{aligned}\sum_{k=1}^{K}P_k(m,n) &= \sum_{k=1}^{K}\frac{\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})}{\lambda(\mathcal{E}_m^{(k)})\lambda(\mathcal{E}_n^{(k)})}\\ &= \sum_{k=1}^{K}\frac{e^{2k}\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})}{\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n)},\end{aligned}$$

and consequently (3.2.13) implies that

$$\sum_{k=1}^{K}e^{2k}\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})\ll K\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n).$$

Note that the implied constant is independent of m and n. Thus, summing over m and n yields

$$\sum_{k=1}^{K}\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}e^{2k}\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})\ll K\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n).$$

Accordingly, there is at least one choice of $k=k(h)$ in the range $\{1,\dots,K\}$ such that

$$\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}e^{2k}\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})\ll\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}\lambda(\mathcal{E}_m)\lambda(\mathcal{E}_n),$$

or, equivalently, such that

$$\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}\lambda(\mathcal{E}_m^{(k)}\cap\mathcal{E}_n^{(k)})\ll\sum_{2^{4^h}\le m<n<2^{4^{h+1}}}\lambda(\mathcal{E}_m^{(k)})\lambda(\mathcal{E}_n^{(k)}), \tag{3.2.14}$$

where the implied constant does not depend on h. We replace the original function $\psi(n)$ by a function $\psi^*(n)$, where

$$\psi^*(n) = \begin{cases} 0 & \text{when } n \text{ is not in } \left[2^{4^h}, 2^{4^{h+1}}\right) \text{ for some even } h, \\ \psi(n)e^{-k(h)} & \text{when } n \text{ is in } \left[2^{4^h}, 2^{4^{h+1}}\right) \text{ for some even } h, \end{cases}$$

and write $\mathcal{E}_n^*,\ n \geq 1$, for the corresponding sets, which are defined like (3.1.1) but with ψ^* in place of ψ. By (3.2.7) we have

$$\psi^*(n) \gg \frac{\psi(n)}{(\log n)^\varepsilon}.$$

Thus the extra divergence condition in the assumptions of Theorem 3.1.1 guarantees that

$$\sum_{n=1}^{\infty} \lambda(\mathcal{E}_n^*) = \infty,$$

while (3.2.14) guarantees that

$$\sum_{1 \leq m,n \leq N} \lambda\Big(\mathcal{E}_m^* \cap \mathcal{E}_n^*\Big) \ll \sum_{1 \leq m,n \leq N} \lambda(\mathcal{E}_m^*)\lambda(\mathcal{E}_n^*)$$

(recall that $\lambda(\mathcal{E}_m^* \cap \mathcal{E}_n^*) \ll \lambda(\mathcal{E}_m^*)\lambda(\mathcal{E}_n^*)$ holds automatically when m and n are not contained in the same block for some h). Thus by Lemma 3.2.1 we have $\lambda(W(\psi^*)) > 0$, and since $\mathcal{E}_n^* \subset \mathcal{E}_n$ we also have $\lambda(W(\psi)) > 0$. By Gallagher's zero–one law, positive measure of $W(\psi)$ implies full measure. Thus $\lambda(W(\psi)) = 1$, which proves the theorem.

Chapter 4

Exceptional Sets in the Metric Pair Correlations problem

> "Homo sum, humani nihil a me alienum puto."[1]
> — Terentius [118, Act I, Sc. 1, l. 25 (77)].

The present chapter is based on joint work with **Thomas Lachmann** [73].

Let $(a_n)_n$ be a strictly increasing sequence of positive integers. Recent works uncovered a close connection between the additive energy $E(A_N)$ of the cut-offs $A_N = \{a_n : n \leq N\}$, and $(a_n)_n$ possessing metric Poissonian pair correlations which is the metric version of a uniform distribution property of "second order". Firstly, the present chapter makes progress on a conjecture[2] of Aichinger, Aistleitner, and Larcher; by sharpening a theorem of Bourgain which states that the set of $\alpha \in [0,1]$ satisfying that $(\langle \alpha a_n \rangle)_n$ with $E(A_N) = \Omega(N^3)$ does not have Poissonian pair correlations has positive Lebesgue measure. Secondly, we construct sequences with high additive energy which do not have metric Poissonian pair correlations, in a strong sense, and provide Hausdorff dimension estimates.

4.1 Introduction

In this chapter, we abbreviate that a sequence which has the Poissonian pair correlations property (cf. Definition 1), by saying it has PPC. We proceed to set the scene.

It is known that if a sequence $(\theta_n)_n$ has PPC, then it is uniformly distributed modulo 1, cf. [12, 77, 113]. Yet, the sequences $(\langle \alpha n^d \rangle)_n$ do *not* have PPC for *any* $\alpha \in \mathbb{R}$ if $d = 1$. For $d \geq 2$, Rudnick and Sarnak [98] proved that $(n^d)_n$ has metric Poissonian pair correlations (metric PPC). A result of Aistleitner, Larcher, and Lewko [14], who used a Fourier analytic approach combined with a bound on GCD sums of Bondarenko and Seip [24], uncovered the connection of the metric PPC property of $(a_n)_n$ with its combinatoric properties. For stating it, we introduce some notation.

[1] In English (translated by N.T.): "I am human, and I believe nothing human is foreign to me.

[2] Recently, said conjecture has been proven by Larcher and Stockinger [78].

Let $(a_n)_n$ denote throughout this chapter a strictly increasing sequence of positive integers, and abbreviate the set of the first N elements of $(a_n)_n$ by A_N. Moreover, define the additive energy $E(I)$ of a finite set of integers I via

$$E(I) \coloneqq \#\{(a,b,c,d) \in I^4 : a+b=c+d\},$$

and note that $(\#I)^2 \leq E(I) \leq (\#I)^3$ where $\#S$ denotes the cardinality of a set S. In the following, let $\mathcal{O}$ and o denote the Landau symbols/O-notation, and $\ll$ or $\gg$ the Vinogradov symbols. The dependence of an implied constant in one of these symbols will be indicated by mentioning this parameter in a subscript.
Now, a main finding of [14] can be stated as the implication that if the truncations A_N satisfy

$$E(A_N) = \mathcal{O}(N^{3-\varepsilon}) \tag{4.1.1}$$

for some fixed $\varepsilon > 0$, then $(a_n)_n$ has metric PPC. Roughly speaking, a set I has large additive energy if and only if it contains a "large" arithmetic progression like structure. Indeed, if $(a_n)_n$ is a geometric progression or of the form $(n^d)_n$ for $d \geq 2$, then (4.1.1) is satisfied.

Recently, Bloom, Chow, Gafni, Walker relaxed — provided that, roughly speaking, the density of the sequence does not decay faster than $1/(\log N)^2$ — the power saving bound (4.1.1) for detecting the metric PPC property of $(a_n)_n$ significantly:

Theorem 4.1.1 (Bloom, Chow, Gafni, Walker [23])**.** *If there exists an $\varepsilon > 0$ such that*

$$E(A_N) \ll \frac{N^3}{(\log N)^{2+\varepsilon}} \quad \text{and} \quad \frac{1}{N}\#(A_N \cap \{1,\dots,N\}) \gg \frac{1}{(\log N)^{2+2\varepsilon}},$$

then $(a_n)_n$ has the metric Poissonian property.

Regarding the optimal bound for $E(A_N)$ to ensure the metric PPC property of $(a_n)_n$, the two following questions were raised in [14]. For stating those, we use the convention that $f = \Omega(g)$ means for $f, g : \mathbb{N} \to \mathbb{R}$ there is a constant $c > 0$ such that $g(n) > cf(n)$ holds for infinitely many n.

Question 1. *Is it possible for $(a_n)_n$ with $E(A_N) = \Omega(N^3)$ to have the metric Poissonian property?*

Moreover, the optimality of the bound (4.1.1) was questioned in the following way.

Question 2. *Do all $(a_n)_n$ with $E(A_N) = o(N^3)$ have metric PPC?*

Both questions were answered in the negative by Bourgain whose proofs can be found in [14] as an appendix, without giving an estimate on the measure of the set that was used to answer Question 1, and without a quantitative bound on $E(A_N)$ appearing in the negation of Question 2. However, a quantitative analysis, as noted in [125], shows that the sequence Bourgain constructed for Question 2 satisfies

$$E(A_N) = \mathcal{O}_\varepsilon\left(\frac{N^3}{(\log\log N)^{\frac{1}{4}+\varepsilon}}\right) \tag{4.1.2}$$

for any fixed $\varepsilon > 0$. Moreover, Nair posed the problem[3] whether the sequence of prime numbers $(p_n)_n$, ordered by increasing value, has metric PPC. Recently, Walker [125] answered this question in the negative by showing that there is a constant $c > 0$ satisfying that for almost every $\alpha \in [0,1]$ the inequality $R([-s,s],\alpha,N) > c$ holds for infinitely many N. Thereby he gave a significantly better bound than (4.1.2) for the additive energy $E(A_n)$ for a sequence $(a_n)_n$ not having metric PPC — since the additive energy of the truncations of $(p_n)_n$ is $\asymp (\log N)^{-1} N^3$.

For a given sequence $(a_n)_n$, we denote by $\mathrm{NPPC}((a_n)_n)$ the "exceptional" set of all $\alpha \in (0,1)$ such that $(\langle \alpha a_n \rangle)_n$ does not have PPC.

Theorem 4.1.2 (Bourgain [14])**.** *If $E(A_N) = \Omega(N^3)$, then $\mathrm{NPPC}((a_n)_n)$ has positive Lebesgue measure.*

We prove the following sharpening.

Theorem 4.1.3. *If $E(A_N) = \Omega(N^3)$, then $\mathrm{NPPC}((a_n)_n)$ has full Lebesgue measure.*

For stating our second main theorem, we denote by $\mathbb{R}_{>x}$ the set of real numbers exceeding a given $x \in \mathbb{R}$.

Theorem 4.1.4. *Let $f : \mathbb{R}_{>0} \to \mathbb{R}_{>2}$ be a function increasing monotonically to ∞, and satisfying $f(x) = \mathcal{O}(x^{1/3} (\log x)^{-7/3})$. Then, there is a strictly increasing sequence $(a_n)_n$ of positive integers with $E(A_N) = \Theta(N^3/f(N))$ such that if*

$$\sum_{n \geq 1} \frac{1}{n f(n)} \tag{4.1.3}$$

diverges, then for Lebesgue almost all $\alpha \in [0,1]$

$$\limsup_{N \to \infty} R([-s,s],\alpha,N) = \infty \tag{4.1.4}$$

holds for any $s > 0$; additionally, if (4.1.3) converges and $\sup\{f(2x)/f(x) : x \geq x_0\}$ is strictly less than 2 for some $x_0 > 0$, then $\mathrm{NPPC}((a_n)_n)$ has Hausdorff dimension at least $(1+\lambda(f))^{-1}$ where

$$\lambda(f) \coloneqq \liminf_{x \to \infty} \frac{\log f(x)}{\log x}$$

denotes the lower order of infinity of f.

We record an immediate consequence of Theorem 4.1.4 by using the convention that the r-folded iterated logarithm is denoted by $\log_r(x)$, i.e.

$$\log_r(x) \coloneqq \log_{r-1}(\log(x))$$

and $\log_1(x) \coloneqq \log(x)$.

[3]This problem was posed at the problem session of the ELAZ conference in 2016.

Corollary 4.1.5. *Let r be a positive integer. Then, there is a strictly increasing sequence $(a_n)_n$ of positive integers with*

$$E(A_N) \asymp \frac{N^3}{\log(N)\log_2(N)\ldots\log_r(N)}$$

such that $\mathrm{NPPC}((a_n)_n)$ *has full Lebesgue measure. Moreover, for any $\varepsilon > 0$ there is a strictly increasing sequence $(a_n)_n$ of positive integers with*

$$E(A_N) \asymp \frac{(\log_r(N))^{-\varepsilon} N^3}{\log(N)\log_2(N)\ldots\log_r(N)}$$

such that $\mathrm{NPPC}((a_n)_n)$ *has full Hausdorff dimension.*

The proof of Theorem 4.1.4 connects the metric PPC property to the notion of optimal regular systems from Diophantine approximation. It uses, among other things, a Khintchine-type theorem due to Beresnevich. Furthermore, despite leading to better bounds, the nature of the sequences underpinning Theorem 4.1.4 is much simpler than the nature of those sequences previously constructed by Bourgain [14] (who used, inter alia, large deviations inequalities from probability theory), or the sequence of prime numbers studied by Walker [125] (who relied on estimates, derived by the circle-method, on the exceptional set in Goldbach-like problems).

4.2 First main theorem

Let us give an outline of the proof of Theorem 4.1.3. For doing so, we begin by sketching the reasoning of the proof of Theorem 4.1.2 As it turns out, except for a set of negligible measure, the counting function in (1.3.1) can be written as a function (of α) that admits a non-trivial estimate for its mean value. The mean value is infinitely often too small on sets whose measure is uniformly bounded from below. Thus, there exists a sequence of sets $(\Omega_r)_r$ of $\alpha \in [0,1]$ such that $R([-s,s],\alpha,N)$ is too small for every $\alpha \in \Omega_r$ for having PPC and Theorem 4.1.3 follows.

Our reasoning for proving Theorem 4.1.3 is building upon this argument of Bourgain while we introduce new ideas to construct a sequence of sets $(\Omega_r)_r$ that are "pairwise quasi independent" - meaning that for every fixed t the relation

$$\lambda(\Omega_r \cap \Omega_t) \leq \lambda(\Omega_r)\lambda(\Omega_t) + o(1)$$

holds as $r \to \infty$ where λ denotes the Lebesgue measure. Roughly speaking, applying a suitable version of the Borel–Cantelli lemma, combined with a sufficiently careful treatment of the $o(1)$ term, will then yield Theorem 4.1.3. However, before proceeding with the details of the proof we collect in the next paragraph some tools from additive combinatorics that are needed.

4.2.1 Preliminaries

We start with a well-know result relating, in a quantitative manner, the additive energy of a set of integers with the existence of a (relatively) dense subset with small difference set where the difference set $B - B \coloneqq \{b - b' : b, b' \in B\}$ for a set $B \subseteq \mathbb{R}$.

Lemma 4.2.1 (Balog–Szeméredi–Gowers lemma, [116, Thm 2.29])**.** *Let $A \subseteq \mathbb{Z}$ be a finite set of integers. For any $c > 0$ there exist $c_1, c_2 > 0$ depending only on c such that the following holds. If $E(A) \geq c\,(\#A)^3$, then there is a subset $B \subseteq A$ such that*

1. $\#B \geq c_1 \#A$,
2. $\#\,(B - B) \leq c_2 \#A$.

Moreover, we recall that for $\delta > 0$ and $d \in \mathbb{Z}$ the set

$$B\,(d, \delta) \coloneqq \{\alpha \in [0, 1] : \|d\alpha\| \leq \delta\}$$

is called Bohr set. The following two simple observations are useful.

Lemma 4.2.2. *Let $B \subseteq \mathbb{Z}$ be a finite set of integers. Then,*

$$\lambda\left(\left\{\alpha \in [0, 1] : \min_{d \in (B-B)\setminus\{0\}} \|d\alpha\| < \frac{\varepsilon}{\#\,(B - B)}\right\}\right) \leq 2\varepsilon$$

for every $\varepsilon \in (0, 1)$.

Proof. By observing that the set under consideration is contained in

$$\bigcup_{\substack{m,n \in B \\ m \neq n}} B\left(m - n, \frac{\varepsilon}{\#\,(B - B)}\right),$$

and

$$\lambda\left(B\left(m - n, \frac{\varepsilon}{\#\,(B - B)}\right)\right) = \frac{2\varepsilon}{\#\,(B - B)},$$

the claim follows at once. □

Lemma 4.2.3. *Suppose A is a finite intersection of Bohr sets, and B is a finite union of Bohr sets. Then, $A \setminus B$ is the union of finitely many intervals.*

Furthermore, we shall use the Borel–Cantelli lemma in a version due to Erdős, and Rényi.

Lemma 4.2.4 (Erdős–Rényi, cf. [58, Lem. 2.3])**.** *Let $(A_n)_n$ be a sequence of Lebesgue measurable sets in $[0, 1]$ satisfying*

$$\sum_{n \geq 1} \lambda\,(A_n) = \infty.$$

Then,

$$\lambda\left(\limsup_{n \to \infty} A_n\right) \geq \limsup_{N \to \infty} \frac{\left(\sum_{n \leq N} \lambda\,(A_n)\right)^2}{\sum_{m,n \leq N} \lambda\,(A_n \cap A_m)}.$$

Moreover, let us explain the main steps in the proof of Theorem 4.1.3. Let

$$\varepsilon := \varepsilon(j) := \frac{1}{10^j} c_1^2$$

where $c_1 > 0$ is a constant to be specified later-on, and j denotes a positive integer. In the first part of the argument, we show how a sequence — that is constructed in the second part of the argument — can be used to deduce Theorem 4.1.3. For every fixed j, we find a corresponding $s = s(j)$ and construct inductively a sequence $(\Omega_r)_r$ of exceptional values α with the following properties:

(i) For all $\alpha \in \Omega_r$, the pair correlation function admits the upper bound

$$R([-s, s], \alpha, N) \leq 2\tilde{c}s \tag{4.2.1}$$

for some absolute constant $\tilde{c} \in (0, 1)$, depending on (a_n) only.

(ii) For all integers $r > t \geq 1$, the relation

$$\lambda(\Omega_r \cap \Omega_t) \leq \lambda(\Omega_r)\lambda(\Omega_t) + 2\varepsilon\lambda(\Omega_t) + \mathcal{O}\left(r^{-2}\right) \tag{4.2.2}$$

holds.

(iii) Each Ω_r is the union of finitely many intervals (hence measurable).

(iv) For all $r \geq 1$, the measure $\lambda(\Omega_r)$ is uniformly bounded from below by

$$\lambda(\Omega_r) \geq \frac{c_1^2}{8}. \tag{4.2.3}$$

4.2.2 Proof of Theorem 4.1.3

1. Suppose there is $(\Omega_r)_r$ satisfying (i)–(iv). Then, by using (4.2.2), we get

$$\begin{aligned}\sum_{r,t \leq N} \lambda(\Omega_r \cap \Omega_t) &\leq 2 \sum_{2 \leq t \leq N} \sum_{1 \leq r < t} (\lambda(\Omega_r)\lambda(\Omega_t)) + 2\varepsilon N^2 + \mathcal{O}(N) \\ &\leq \left(\sum_{t \leq N} \lambda(\Omega_t)\right)^2 + 2\varepsilon N^2 + \mathcal{O}(N).\end{aligned}$$

By recalling that Ω_r depends on j, we let

$$\Omega(j) := \limsup_{r \to \infty} \Omega_r.$$

By using the inequality above in combination with Lemma 4.2.4 and (4.2.3), we obtain that the set $\Omega(j)$ has measure at least

$$\limsup_{N \to \infty} \frac{\left(\sum_{r \leq N} \lambda(\Omega_r)\right)^2}{\sum_{r,t \leq N} \lambda(\Omega_r \cap \Omega_t)} \geq \limsup_{N \to \infty} \frac{1}{1 + \frac{4\varepsilon N^2}{\left(\sum_{r \leq N} \lambda(\Omega_r)\right)^2}} \geq \limsup_{N \to \infty} \frac{1}{1 + \frac{256}{c_1^4}\varepsilon} = \frac{1}{1 + \frac{256}{c_1^4}\varepsilon}.$$

Note that due to (4.2.1), for every $\alpha \in \Omega(j)$ the sequence $(\alpha a_n)_n$ does not have PPC. Now, letting $j \to \infty$ proves the assertion.

2. For constructing $(\Omega_r)_r$ with the required properties, let $c > 0$ such that $E(A_N) > cN^3$ for infinitely many integers N. By choosing an appropriate subsequence $(N_i)_i$ and omitting the subscript i for ease of notation, we may suppose that $E(A_N) > cN^3$ holds for every N occurring in this proof. Moreover, let c_1, c_2 and B_N be as in Lemma 4.2.1, corresponding to the c just mentioned. Let

$$s = \frac{\varepsilon}{2c_2}.$$

Arguing inductively, while postponing the base step,[4] we assume that there are sets $(\Omega_r)_{1\le r<R}$ given that satisfy the properties (i)–(iv) for all distinct integers $1 \le r, t < R$. Let $N \ge R$. Since, due to Lemma 4.2.1,

$$\frac{s}{N} \le \frac{\varepsilon}{\#(B-B)},$$

Lemma 4.2.2 implies that the set $\Omega_{\varepsilon,N}$ of all $\alpha \in [0,1]$ satisfying $\|(r-t)\alpha\| < N^{-1}s$ for some distinct $r, t \in B_N$ has measure at most 2ε. Setting

$$\mathcal{D}_N := \{(r,t) \in (A_N \times A_N) \setminus (B_N \times B_N) : r \ne t\},$$

we get for $\alpha \notin \Omega_{\varepsilon,N}$ that

$$R([-s,s],\alpha,N) = \frac{1}{N}\#\{(r,t) \in \mathcal{D}_N : \|(r-t)\alpha\| < N^{-1}s\}.$$

Let ℓ_R denote the length of the smallest subinterval of Ω_r for $1 \le r < R$, and define $C(\Omega_r)$ to be the set of subintervals of Ω_r. Note that $\ell_R > 0$, and $\max_{1\le r<R} \#C(\Omega_r) < \infty$. We divide $[0,1)$ into

$$P := \left\lfloor 1 + 2\ell_R^{-1}R^2 \max_{1\le r<R} \#C(\Omega_r) \right\rfloor$$

parts $\mathcal{P}_i$ of equal lengths, i.e.

$$\mathcal{P}_i := \left[\frac{i}{P}, \frac{i+1}{P}\right)$$

where $i = 0, \dots, P-1$. Let $\mathbf{1}_X$ denote the characteristic function of a Borel set $X \subseteq [0,1]$. After writing

$$\int_{\mathcal{P}_i} \#\{(r,t) \in \mathcal{D}_N : \|(r-t)\alpha\| \le N^{-1}s\}\mathrm{d}\alpha = \sum_{(r,t)\in\mathcal{D}_N} \int_{\mathcal{P}_i} \mathbf{1}_{\left[0,\frac{s}{N}\right]}(\|(r-t)\alpha\|)\,\mathrm{d}\alpha, \quad (4.2.4)$$

[4]The base step uses simplified versions of the arguments exploited in the induction step, and will therefore be postponed.

we split the sum into two parts: one part containing differences $|r-t| > R^k P$, and a second part containing differences $|r-t| \leq R^k P$ where

$$k \coloneqq \left\lfloor \frac{1}{\log 2} \log \frac{8\,(4s+1)}{(c_1^2 - 2^{-1}c_1^4)\,s} \right\rfloor + 1.$$

The Cauchy–Schwarz inequality implies

$$\int_{\mathcal{P}_i} \mathbf{1}_{[0,\frac{s}{N}]}\left(\|(r-t)\,\alpha\|\right) \mathrm{d}\alpha \leq \sqrt{\frac{1}{P}\frac{2s}{N}}.$$

Since for any $x > 0$ there are at most $2xN$ choices of $(r,t) \in \mathcal{D}_N$ such that $|r-t| \leq x$, we obtain

$$\frac{1}{N} \sum_{\substack{(r,t)\in\mathcal{D}_N \\ |r-t|\leq PR^k}} \int_{\mathcal{P}_i} \mathbf{1}_{[0,\frac{s}{N}]}\left(\|(r-t)\,\alpha\|\right) \mathrm{d}\alpha \leq 2PR^k \sqrt{\frac{1}{P}\frac{2s}{N}}$$

which is $\leq P^{-1}R^{-k}$ if N is sufficiently large. Moreover, for any $|r-t| > PR^k$ we observe that

$$\begin{aligned}\int_{\mathcal{P}_i} \mathbf{1}_{[0,\frac{s}{N}]}(\|(r-t)\,\alpha\|)\mathrm{d}\alpha &\leq \frac{2s}{N\,|r-t|}(\#\{0 \leq j \leq |r-t| :\, j/\,|r-t| \in \mathcal{P}_i\} + 1) \\ &\leq \frac{2s}{PN} + \frac{4s}{PR^kN}.\end{aligned}$$

Also note that $\#\mathcal{D}_N \leq N^2 - (\#B_N)^2 \leq \tilde{c}N^2$ where $\tilde{c} \coloneqq 1 - c_1^2$. Therefore, the mean value (4.2.4) of the modified pair correlation counting function on the interval $\mathcal{P}_i$ admits the upper bound

$$\frac{1}{N}\left(\#\mathcal{D}_N\right)\left(\frac{2s}{PN} + \frac{4s}{PR^kN}\right) + \frac{1}{PR^k} \leq \frac{2\tilde{c}s}{P} + \frac{4s+1}{PR^k}.$$

Hence, it follows that the measure of the set $\Delta_N(i)$ of $\alpha \in \mathcal{P}_i$ with

$$\frac{1}{N}\#\left\{(r,t) \in \mathcal{D}_N :\, \|(r-t)\,\alpha\| \leq N^{-1}s\right\} \leq 2\left(1 - \frac{c_1^2}{2}\right)s \tag{4.2.5}$$

admits, by the choice of k, the lower bound

$$\lambda\left(\Delta_N(i)\right) \geq \frac{1}{P} - \frac{1}{P}\frac{2\tilde{c}s + (4s+1)\,R^{-k}}{2\left(1-\frac{c_1^2}{2}\right)s} \geq \frac{1}{P}\left(\frac{c_1^2}{2} - \frac{c_1^2}{8}\right). \tag{4.2.6}$$

Note that $\Delta_N(i)$ is the union of finitely many intervals, due to Lemma 4.2.3. So, we may take $\Delta'_N(i) \subset \Delta_N(i)$ being a finite union of intervals such that $\lambda\left(\Delta'_N(i)\right)$ equals the lower bound in (4.2.6). Let

$$\Omega_R \coloneqq \Omega_R(N) \coloneqq \Delta_N \setminus \Omega_{\varepsilon,N} \qquad \text{where} \qquad \Delta_N \coloneqq \bigcup_{i=0}^{P-1} \Delta'_N(i).$$

We are going to show now that Ω_R satisfies the properties (i) - (iv). Now, Ω_R satisfies property (iv) with $r = R$ since

$$\lambda(\Omega_R) \geq \lambda(\Delta_N) - \lambda(\Omega_{\varepsilon,N}) = \frac{c_1^2}{2} - \frac{c_1^2}{8} - 2\varepsilon \geq \frac{c_1^2}{8}.$$

Furthermore, Ω_R satisfies property (i) by construction and also property (iii) since all sets involved in the construction of Ω_R were a finite union of intervals. Let $1 \leq r < R$, and I be a subinterval of Ω_r. Then,

$$\lambda(I \cap \Delta_N) = \sum_{i:\mathcal{P}_i \cap I \neq \emptyset} \lambda(\mathcal{P}_i \cap I \cap \Delta_N) \leq \frac{2}{P} + \sum_{i:\mathcal{P}_i \subsetneq I} \lambda(\mathcal{P}_i \cap \Delta_N) \leq \frac{2}{P} + \sum_{i:\mathcal{P}_i \subsetneq I} \lambda(\Delta'_N(i)).$$

By summing over all subintervals $I \in C(\Omega_r)$, we obtain that

$$\begin{aligned}
\lambda(\Omega_r \cap \Delta_N) &\leq \sum_{I \in C(\Omega_r)} \left(\frac{2}{P} + \sum_{i:\mathcal{P}_i \subsetneq I} \lambda(\Delta'_N(i)) \right) \\
&\leq \frac{1}{R^2} + \sum_{I \in C(\Omega_r)} P\lambda(I) \frac{\lambda(\Delta_N)}{P} \\
&= \frac{1}{R^2} + \lambda(\Omega_r)\lambda(\Delta_N).
\end{aligned}$$

We deduce property (ii) from this estimate and Lemma 4.2.2 via

$$\begin{aligned}
\lambda(\Omega_r \cap \Omega_R) &\leq \lambda(\Omega_r \cap \Delta_N) \\
&\leq \lambda(\Omega_r)(\lambda(\Delta_N) - \lambda(\Omega_{\varepsilon,N})) + R^{-2} + \lambda(\Omega_r)\lambda(\Omega_{\varepsilon,N}) \\
&\leq \lambda(\Omega_r)\lambda(\Omega_R) + 2\varepsilon\lambda(\Omega_r) + R^{-2}.
\end{aligned}$$

This concludes the induction step. The only part missing now is the base step of the induction. For realizing it, let N denote the smallest integer m with $E(A_m) > cm^3$. We replace $\mathcal{P}_i$ in (4.2.4) by $[0,1]$ to directly derive

$$\int_0^1 \frac{1}{N} \# \left\{ (r,t) \in \mathcal{D}_N : \|(r-t)\alpha\| \leq N^{-1}s \right\} \mathrm{d}\alpha \leq 2\tilde{c}s,$$

and conclude that the set Ω'_1 of $\alpha \in [0,1]$ satisfying (4.2.5) has a measure at least $c_1^2/2$. Thus, $\Omega_1 \coloneqq \Omega'_1 \setminus \Omega_{N,\varepsilon}$ has measure at least as large as the right hand side of (4.2.3). For property (4.2.2), there is nothing to check and that Ω_1 is a finite union of intervals follows from Lemma 4.2.3 by observing that

$$\Omega'_1 = \bigcap_{d_1,\ldots,d_{\lfloor N2\tilde{c}s \rfloor}} \left(B\left(d_1, N^{-1}s\right)^C \cup \ldots \cup B\left(d_{\lfloor N2\tilde{c}s \rfloor}, N^{-1}s\right)^C \right)$$

where the intersection runs through any set of $\lfloor N2\tilde{c}s \rfloor$-tuples of differences $d_i = r_i - t_i \neq 0$ of components of $(r_i, t_i) \in \mathcal{D}_N$ for $i = 1, \ldots, \lfloor N2\tilde{c}s \rfloor$.

Thus, the proof is complete.

4.3 Second main theorem

The sequences $(a_n)_n$ enunciated in Theorem 4.1.4 are constructed in two steps. In the first step, we concatenate (finite) blocks, with suitable lengths, of arithmetic progressions to form a set P_A. In the second step, we concatenate (finite) blocks, with suitable lengths, of geometric progressions to form a set P_G and then define a_n to be the n-th smallest element of $P_A \cup P_G$. On the one hand, the arithmetic progression like part P_A serves to ensure, due to considerations from metric Diophantine approximation, the divergence property (4.1.4) on a set with full measure or controllable Hausdorff dimension; on the other hand, the geometric progression like part P_G lowers the additive energy, as much as it can. For doing so, a geometric block will appear exactly before and after an arithmetic block, and have much more elements.

For writing the construction precisely down, we introduce some notation. Let henceforth $\lfloor x \rfloor$ denote the greatest integer m that is at most $x \in \mathbb{R}$. Suppose throughout this section that f is as in Theorem 4.1.4. We set $P_A^{(1)}$ to be the empty set while $P_G^{(1)} \coloneqq \{1, 2\}$. Suppose $P_A^{(j-1)}, P_G^{(j-1)}$for $j \geq 2$ are already constructed. Let $C_j = 2\max\left\{P_G^{(j-1)}\right\}$. Then

$$P_A^{(j)} \coloneqq \left\{C_j + h : 1 \leq h \leq \left\lfloor \left(f(2^j)\right)^{-\beta} 2^j \right\rfloor\right\},$$

and $P_G^{(j)}$ is defined via

$$P_G^{(j)} \coloneqq \left\{2C_j + 2^i : 1 \leq i \leq \left\lfloor \left(f(2^j)\right)^{-\gamma} 2^j \left(1 - \left(f(2^j)\right)^{\gamma-\beta}\right) \right\rfloor\right\}$$

where $0 < \gamma < \beta < 3/4$ are parameters[5] to be chosen later-on. Letting

$$P_A \coloneqq \bigcup_{j\geq 1} P_A^{(j)}, \qquad P_G \coloneqq \bigcup_{j\geq 1} P_G^{(j)},$$

we denote by a_n the n-th smallest element in $P_A \cup P_G$. For $d \in \mathbb{Z}$ and finite sets of integers X, Y, we abbreviate the number of representations of d as a difference of an $x \in X$ and a $y \in Y$ by

$$\mathrm{r}_{X-Y}(d) \coloneqq \#\{(x, y) \in X \times Y : x - y = d\};$$

for later reference, we record here that the additive energy of a set X and the pair correlation counting function can be written as

$$E(X) = \sum_{d\in\mathbb{Z}} \left(\mathrm{r}_{X-X}(d)\right)^2, \tag{4.3.1}$$

and

$$R([-s, s], \alpha, N) = \frac{1}{N} \sum_{d\in\mathbb{Z}\setminus\{0\}} \mathrm{r}_{A_N-A_N}(d) \mathbf{1}_{\left[0,\frac{s}{N}\right]}(\|\alpha d\|). \tag{4.3.2}$$

[5]No particular importance should be attached to requiring $\beta < 3/4$, or using "dyadic steps lengths 2^j". Doing so is for simplifying the technical details only - eventually, it will turn out that $\beta = 2/3 = 2\gamma$ is the optimal choice of parameters in this approach. For proving this to the reader, we leave γ, β undetermined till the end of this section.

4.3.1 Preliminaries

For determining the order of magnitude of $E(A_N)$, the following considerations are useful. Since the cardinality $P_G^{(j)} \cup P_A^{(j)}$ has about exponential growth, it is reasonable to expect $E(A_N)$ to be of the same order of magnitude as the additive energy of the last block $P_G^{(J)} \cup P_A^{(J)}$ that is fully contained in A_N - note that $J = J(N)$; i.e. to expect the magnitude of $E(P_G^{(J)} \cup P_A^{(J)})$ which is roughly $E(P_A^{(J)})$. The next proposition verifies this heuristic.

Proposition 4.3.1. *Let $(a_n)_n$ be as in the beginning of Section 3, and f be as in one of the two assertions in Theorem 4.1.4. Then, $E(A_N) \asymp N^3 (f(N))^{-3(\beta-\gamma)}$.*

For the proof of Proposition 4.3.1, we need the following technical lemma.

Lemma 4.3.2. *Let $F_j := 2^j (f(2^j))^{-\delta}$, for $j \geq 1$ and fixed $\delta \in (0,1)$, where f is as in Theorem 4.1.4. Then, $\sum_{i \leq j} F_i = \mathcal{O}(F_j)$ and*

$$\sum_{d \in \mathbb{Z}} \left(\sum_{j,i \leq J} \mathrm{r}_{P_G^{(j)} - P_A^{(i)}}(d) \right)^2 = \mathcal{O}(J^6 2^{2J}).$$

Proof. Suppose that $f(x) = \mathcal{O}(x^{1/3} (\log x)^{-7/3})$ is such that (4.1.3) diverges. Because

$$\sum_{j \leq J+1} \frac{1}{f(2^j)} \geq \sum_{k \leq 2^J} \frac{1}{k f(k)}$$

diverges as $J \to \infty$ and $(f(2^j)/f(2^{j+1}))_j$ is non-decreasing, we conclude that the quotient $f(2^j)/f(2^{j+1}) \to 1$ as $j \to \infty$. Therefore, there is an i_0 such that the estimate

$$(f(2^i))^{-1} f(2^{i+h}) < (3/2)^{\frac{h}{\delta}}$$

holds for any $i \geq i_0$ and $h \in \mathbb{N}$. Hence,

$$\frac{1}{F_j} \sum_{i \leq j} F_i \leq o(1) + \sum_{i_0 \leq i \leq j} 2^{i-j} (3/2)^{j-i} = \mathcal{O}(1).$$

If f is such that (4.1.3) converges and $f(2x) \leq (2-\varepsilon) f(x)$ for x large enough, then we obtain by a similar argument that $\sum_{i \leq j} F_i$ is in $\mathcal{O}(F_j)$. Further, $\mathrm{r}_{P_G^{(j)} P_A^{(i)}}(d) = \mathcal{O}(i)$, for every $j \geq 1$, and non-vanishing for $\mathcal{O}(2^{2j})$ values of d which implies the last claim. □

We can now prove the proposition.

Proof of Proposition 4.3.1. Let $N \geq 1$ be large and denote by $J = J(N) \geq 0$ the greatest integer j such that $P_G^{(j-1)} \subseteq A_N$. By exploiting (4.3.1),

$$E(A_N) \geq E(P_A^{(J-1)}) \gg (\# P_A^{(J-1)})^3$$

which is seen to be $\gg (f(N))^{-3(\beta-\gamma)}N^3$. Hence, it remains to show that $E(A_N) = \mathcal{O}((f(N))^{-3(\beta-\gamma)}N^3)$. Note that

$$E(A_N) \leq \sum_{d\in\mathbb{Z}} (\mathrm{r}_{A_{T_J}-A_{T_J}}(d))^2 \quad \text{where} \quad T_J \coloneqq \#\bigcup_{j\leq J}(P_A^{(j)} \cup P_G^{(j)}).$$

Moreover, $\mathrm{r}_{A_{T_J}-A_{T_J}}(d) = S_1(d) + S_2(d)$ where $S_2(d)$ denotes the mixed sum

$$\sum_{i,j\leq J} (\mathrm{r}_{P_A^{(j)}-P_G^{(i)}}(d) + \mathrm{r}_{P_G^{(i)}-P_A^{(j)}}(d)),$$

and $S_1(d)$ abbreviates

$$\sum_{i,j\leq J} (\mathrm{r}_{P_G^{(i)}-P_G^{(j)}}(d) + \mathrm{r}_{P_A^{(i)}-P_A^{(j)}}(d)).$$

Using that for any $a, b \in \mathbb{R}$ the inequality $(a+b)^2 \leq 2(a^2+b^2)$ holds, we obtain

$$E(A_N) = \mathcal{O}\bigg(\sum_{d\in\mathbb{Z}}(S_1(d))^2 + \sum_{d\in\mathbb{Z}}(S_2(d))^2\bigg).$$

Lemma 4.3.2 implies that $\sum_{d\in\mathbb{Z}}(S_2(d))^2 = \mathcal{O}((\log N)^6 N^2)$ due to $J = \mathcal{O}(\log N)$. Furthermore letting $F_j = 2^j(f(2^j))^{-\beta}$, we observe that $\mathrm{r}_{P_A^{(i)}-P_A^{(j)}}(d)$ is non-vanishing for at most $4F_J$ values of d as $i, j \leq J$. Since $\mathrm{r}_{P_A^{(i)}-P_A^{(j)}}(d) \leq F_{\min(i,j)}$ holds, we deduce that

$$\sum_{i,j\leq J} \mathrm{r}_{P_A^{(i)}-P_A^{(j)}}(d) = \mathcal{O}\bigg(\sum_{j\leq J}\sum_{i\leq j} F_i\bigg) = \mathcal{O}(F_J).$$

Since $\mathrm{r}_{P_G^{(i)}-P_G^{(j)}}(d) \leq 1$, as $i, j \leq J$, is non-zero for at most $\mathcal{O}(T_J^2) = \mathcal{O}(N^2)$ values of d, we obtain that

$$\sum_{d\in\mathbb{Z}}(S_1(d))^2 = \mathcal{O}(F_J^3 + (\log N)^6 N^2) = \mathcal{O}(N^3(f(N))^{-3(\beta-\gamma)})$$

Hence, $E(A_N) = \mathcal{O}(N^3(f(N))^{-3(\beta-\gamma)})$. □

For estimating the measure or the Hausdorff dimension of $\mathrm{NPPC}((a_n)_n)$ from below, we recall the notion of an optimal regular system. This notion, roughly speaking, describes sequences of real numbers that are exceptionally well distributed in any subinterval, in a uniform sense, of a fixed interval.

Definition 3. *Let J be a bounded real interval, and $S = (\alpha_i)_i$ a sequence of distinct real numbers. S is called an optimal regular system in J if there exist constants c_1, c_2, $c_3 > 0$ - depending on S and J only - such that for any interval $I \subseteq J$ there is an index $Q_0 = Q_0(S, I)$ such that for any $Q \geq Q_0$ there are indices*

$$c_1 Q \leq i_1 < i_2 < \ldots < i_t \leq Q \tag{4.3.3}$$

satisfying $\alpha_{i_h} \in I$ for $h = 1, \ldots, t$, and

$$|\alpha_{i_h} - \alpha_{i_\ell}| \geq \frac{c_2}{Q} \tag{4.3.4}$$

for $1 \leq h \neq \ell \leq t$, and

$$c_3\lambda(I)\,Q \leq t \leq \lambda(I)\,Q. \tag{4.3.5}$$

Moreover, we need the following result(s) due to Beresnevich which may be thought of as a far reaching generalization of the classical Khintchine theorem, and the JarnĂk-Besicovitch theorem in Diophantine approximation.

Theorem 4.3.3 ([28, Thm. 6.1, Thm. 6.2])**.** *Suppose $\psi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is a continuous, non-increasing function, and $S = (\alpha_i)_i$ an optimal regular system in $(0,1)$. Let $\mathcal{K}_S(\psi)$ denote the set of ξ in $(0,1)$ such that $|\xi - \alpha_i| < \psi(i)$ holds for infinitely many i. If*

$$\sum_{n \geq 1} \psi(n) \tag{4.3.6}$$

diverges, then $\mathcal{K}_S(\psi)$ has full measure.
Conversely, if (4.3.6) converges, then $\mathcal{K}_S(\psi)$ has measure zero and the Hausdorff dimension equals the reciprocal of the lower order of $\frac{1}{\psi}$ at infinity.

For a rational $\alpha = \frac{p}{q}$, where $p, q \in \mathbb{Z}$, $q \neq 0$, we denote by $H(\alpha)$ its (naive) height, i.e. $H(\alpha) \coloneqq \max\{|p|, |q|\}$. It is well-known that the set of rational numbers in $(0,1)$ — first running through all rationals of height 1 ordered by increasing numerical value, then through all rationals with height 2 ordered by increasing numerical value, and so on — gives rise to an optimal regular system in $(0,1)$. The following lemma says, roughly speaking, that this assertion remains true for the set of rationals in $(0,1)$ whose denominators are members of a special sequence that is not too sparse in the natural numbers, and hand-tailored for our purposes. The proof can be given by modifying the proof of the classical case, compare [28, Prop. 5.3]; however, we shall give the details for making this chapter more self-contained.

Lemma 4.3.4. *Let $\vartheta : \mathbb{R}_{>0} \to \mathbb{R}_{>1}$ be monotonically increasing to infinity with $\vartheta(x) = \mathcal{O}(x^{1/4})$ and $\vartheta(2^{j+1})/\vartheta(2^j) \to 1$ as $j \to \infty$. For each $j \in \mathbb{N}$, we let*

$$B_j \coloneqq \frac{2^j}{f(2^j)\sqrt{\vartheta(2^j)}}, \qquad b_j \coloneqq \frac{2}{3} B_j.$$

Let $S = (\alpha_i)_i$ denote a sequence running through all rationals in $(0,1)$ whose denominators are in $M \coloneqq \bigcup_{j \geq 1} \{n \in \mathbb{N} : b_j \leq n \leq B_j\}$ such that $i \mapsto H(\alpha_i)$ is non-decreasing. Then, S is an optimal regular system in $(0,1)$.

Proof. Let $X \geq 2$. There are strictly less than $2X^2$ rational numbers in $(0,1)$ with height bounded by X. We take $J = J(X)$ to be the largest integer $j \geq 1$ such that $B_j \leq X$. Then, for X large enough, there are at least, due to a basic property of the Eulerian totient function,

$$\begin{aligned} \sum_{j \leq J} \sum_{b_j \leq q \leq B_j} \varphi(q) &\geq \sum_{j \leq J} \left(\frac{1}{3\pi^2} B_j^2 + \mathcal{O}(B_j \log B_j) \right) \\ &\geq \frac{1}{6\pi^2} \frac{2^{2J}}{f^2(2^J)\vartheta(2^J)} + \mathcal{O}(J 2^J) > \left(\frac{X}{5\pi} \right)^2 \end{aligned}$$

distinct such rationals in $(0,1)$ with height not exceeding X. Hence, we obtain

$$\frac{\sqrt{i}}{2} \leq H(\alpha_i) \leq \sqrt{25\pi^2(i+1)} + 1$$

for i sufficiently large. Let $Q \in \mathbb{N}$, $I \subseteq [0,1]$ be a non-empty interval, and let F denote the set of $\xi \in I$ satisfying the inequality $\|q\xi\| < Q^{-1}$ with some $1 \leq q \leq \frac{1}{1000}Q$. Note that F has measure at most

$$\sum_{q \leq \frac{1}{1000}Q} \left(\frac{2}{qQ} q\lambda(I) + \frac{2}{qQ} \right) = \frac{1}{500}\lambda(I) + \mathcal{O}\left(\frac{\log Q}{Q} \right) < \frac{1}{400}\lambda(I)$$

for $Q \geq Q_0$ where $Q_0 = Q_0(S, I)$ is sufficiently large. Let $\left\{ {}^{p_j}/_{q_j} \right\}_{1 \leq j \leq t}$ be the set of all rationals ${}^{p_j}/_{q_j} \in (0,1)$ with $q_j \in M$, $\frac{1}{1000}Q < q_j < Q$ that satisfy

$$\left| \frac{p_j}{q_j} - \frac{p_{j'}}{q_{j'}} \right| > \frac{2000}{Q^2}$$

whenever $1 \leq j \neq j' \leq t$. Observe that for J as above with $X = Q$ sufficiently large, it follows that

$$\{q \in M : b_J \leq q \leq B_J\} \subseteq \left\{ \left\lfloor \frac{Q}{1000} \right\rfloor, \left\lfloor \frac{Q}{1000} \right\rfloor + 1, \ldots, Q \right\}$$

holds and hence, there are at least

$$\frac{1}{3\pi^2} B_J^2 + \mathcal{O}(B_J \log B_J) > \frac{1}{400} Q^2$$

choices of ${}^{p_j}/_{q_j} \in (0,1)$ with $q_j \in M$ and $\frac{1}{1000}Q < q_j < Q$. Due to $\lambda(I \setminus F) > \frac{399}{400}\lambda(I)$, we conclude

$$t \geq 400 \frac{Q^2}{4000} \frac{399}{400} \lambda(I).$$

Thus, taking $c_1 := {}^1/_{1000}$, $c_2 := 2000$, and $c_3 := \frac{399}{4000}$ in (4.3.3), (4.3.4) and (4.3.5), respectively, S is shown to be an optimal regular system. □

Now we can proceed to the proof of Theorem 4.1.4.

4.3.2 Proof of Theorem 4.1.4

We argue in two steps depending on whether or not the series (4.1.3) converges. Proposition (4.3.1) implies the announced $\asymp$-bounds on $E(A_N)$ in both cases.

(i) Suppose (4.1.3) diverges, and fix $s > 0$. Let $\vartheta : \mathbb{R}_{>0} \to \mathbb{R}_{>1}$ be monotonically increasing to infinity with $\vartheta(x) = \mathcal{O}(x^{1/4})$ such that

$$\psi(n) := \frac{1}{nf(n)\vartheta(n)} \tag{4.3.7}$$

satisfies the divergence condition (4.3.6). Thus, $\vartheta(2^j)/\vartheta(2^{j-1}) \to 1$ as $j \to \infty$, and $S = (\alpha_i)_i$ from Lemma 4.3.4 is an optimal regular system. Furthermore, if $b_J \leq n \leq B_J$, for some integer J, then, by the properties of ϑ from Lemma 4.3.4 and the relation $\sum_{j \leq J} F_j = \mathcal{O}(F_J)$ from Lemma 4.3.2, we conclude that

$$\sum_{j \leq J-1} \sum_{b_j \leq m \leq B_j} \varphi(m) \asymp B_J^2$$

implies that $\alpha_i = m/n$ entails $i \geq cn^2$ where $c = c(f, \vartheta) > 0$ is a constant. Therefore, $\psi(i) \leq c^{-1} n^{-2} (f(cn^2)\vartheta(cn^2))^{-1}$. The growth assumption on f and $\vartheta(x) = \mathcal{O}(x^{1/4})$ yields that if j is large enough, then $b_j \leq n \leq B_j$ implies $cn^2 > 2^j$ and hence we obtain $\psi(i) \leq c^{-1} n^{-2} (f(2^j)\vartheta(2^j))^{-1}$. Combining these considerations, we infer that

$$n\psi(i) = \mathcal{O}(2^{-j}(\vartheta(2^j))^{-1/2}).$$

Applying Theorem 4.3.3 with ψ as in (4.3.7), implies that $\mathcal{K}_S(\psi)$ has full Lebesgue measure. Therefore, for any $\alpha \in \mathcal{K}_S(\psi)$ we get

$$\|n\alpha\| \leq n|\alpha - \alpha_i| = \mathcal{O}(2^{-j}(\vartheta(2^j))^{-1/2}) \tag{4.3.8}$$

for infinitely many i and $j = j(i)$. Now if $b_j \leq n \leq B_j$ for j sufficiently large and n, α as in (4.3.8), then it follows that by taking any integer $m \leq (f(2^j))^{\gamma}(\vartheta(2^j))^{1/3}$ that also the multiples

$$nm \leq 2^j (f(2^j))^{\gamma-1} (\vartheta(2^j))^{-1/6}$$

satisfy that $\mathbf{1}_{[0,s/T_j]}(\|\alpha(mn)\|) = 1$ where $T_j = \mathcal{O}(2^j (f(2^j))^{-\gamma})$ is as in the proof of Proposition 4.3.1. If additionally $\gamma - 1 \leq -\beta$ holds, then we obtain that

$$\mathrm{r}_{A_{T_j} - A_{T_j}}(mn) \geq 2^{j-1} (f(2^j))^{-\beta}$$

holds for j sufficiently large. By (4.3.2), we conclude that

$$R([-s, s], \alpha, T_j) \geq C(f(2^j))^{2\gamma-\beta} (\vartheta(2^j))^{1/3}$$

for infinitely many j where $C > 0$ is some constant. For the optimal choice of the parameters $\beta, \gamma > 0$, we are therefore led to maximize $\beta - \gamma$ where $2\gamma - \beta \geq 0$ and $\gamma - 1 \leq -\beta$ have to be satisfied. The solution is given if equality in the first inequality occurs, leading to $\beta = 2/3$ and $\gamma = 1/3$. Hence, (4.1.4) follows for $\alpha \in \mathcal{K}_S(\psi)$.

(ii) Suppose the series (4.1.3) converges. We keep the same sequence as in step (i) while taking $\vartheta(x) = 1 + \log(x)$, as we may. The arguments of step (i) show that any $\alpha \in \mathcal{K}_S(\psi)$ satisfies (4.1.4); now the conclusion is that $\mathcal{K}_S(\psi)$ has Hausdorff dimension at least equal to the reciprocal of

$$\liminf_{x \to \infty} \frac{-\log(\psi(x))}{\log x} = 1 + \liminf_{x \to \infty} \frac{\log f(x)}{\log x}.$$

Thus, the proof is complete.

Chapter 5

There is No Khintchine Threshold for Metric Pair Correlations

> "All the greatest things are simple, and many can be expressed in a single word: Freedom; Justice; Honour; Duty; Mercy; Hope."
> — W. Churchill [76].

The present chapter is based on joint work with **Christoph Aistleitner**, and **Thomas Lachmann** [13].

Let $\mathcal{A}(\alpha)$ denote the sequence $(\alpha a_n)_n$, where $\alpha \in [0,1]$ and where $(a_n)_n$ is a strictly increasing sequence of positive integers. If the asymptotic distribution of the pair correlations of these sequences follows the Poissonian model for almost all α in the sense of Lebesgue measure, we say that $(a_n)_n$ has the metric pair correlation property. Recent research has revealed a connection between the metric theory of pair correlations of such sequences, and the additive energy of truncations of $(a_n)_n$. Bloom, Chow, Gafni and Walker speculated that there might actually be a convergence/divergence criterion which fully characterizes the metric pair correlation property in terms of the additive energy, similar to Khintchine's criterion in the metric theory of Diophantine approximation. In the present chapter we give a negative answer to such speculations, by showing that such a criterion does not exist. To this end, we construct a sequence $(a_n)_n$ having large additive energy which, however, maintains the metric pair correlation property.

5.1 Introduction

Let us keep the notation from the previous chapter. Recall: if for an infinite sequence $(x_n)_n \subseteq [0,1)$ we have $R([-s,s],\alpha,N) \to 2s$ for all $s \geq 0$, then we say that the distribution of pair correlations is (asymptotically) *Poissonian*. Note that a sequence of independent, identically distributed (i.i.d.) random points, picked from a uniform distribution on $[0,1]$, almost surely has Poissonian pair correlations. The term "Poissonian" for this asymptotic distribution of pair correlations comes from a similarity with the distribution of spacings of points in a Poisson process, which, however, only

becomes really meaningful when also considering higher correlations (triple, quadruple etc.) or so-called neighbour spacings (which are in general much more difficult to handle than pair correlations).

The interest in such problems goes back to a paper of Berry and Tabor [22], where they gave a conjectural framework for the distribution of energy spectra of integrable quantum systems. Their model led to strong mathematical interest in distributional properties of spacing of sequences such as $(n\alpha)_n$ mod 1 (corresponding to the "harmonic oscillator") and $(n^2\alpha)_n$ mod 1 (corresponding to the "boxed oscillator"). The case of $(n\alpha)_n$ is easier to analyse; one can use considerations based on continued fractions, to show for example that the pair correlations of this sequence cannot be Poissonian for any α, since for some N the initial segment $(\alpha, 2\alpha, \ldots, N\alpha)$ mod 1 is too regularly spaced. The case of $(n^2\alpha)_n$ is much harder and is far from being well-understood. It is conjectured that the pair correlations for this sequence should be Poissonian, unless α is very well approximable by rationals; however, there exist only some partial results in this direction (see for example [61, 99, 121]). From the metric perspective, the situation is easier: it is known that the pair correlations of $(n^2\alpha)_n$ mod 1 are Poissonian for almost all α in the sense of Lebesgue measure. The same is true if $(n^2)_n$ is replaced by $(n^d)_n$ for some integer $d \geq 3$, or by an exponentially growing sequence $(a_n)_n$ of integers, see [98, 100]. We denote this property by saying that these sequences have the *metric pair correlation property*. In a recent paper [14], a connection was established between the question whether a given sequence has the metric pair correlation property, and the asymptotic order of its so-called additive energy. Let $(a_n)_n$ be a given sequence of distinct positive integers, and let A_N denote its initial segment $a_1, \ldots, a_N$. Then, the additive energy $E(A_N)$ is defined as

$$E(A_N) = \#\{n_1, n_2, n_3, n_4 \leq N : \ a_{n_1} + a_{n_2} = a_{n_3} + a_{n_4}\}.$$

Trivially, the additive energy is always between N^2 and N^3. The main results of [14] say that $(a_n)_n$ has the metric pair correlation property provided that $A_N \ll N^{3-\varepsilon}$ for some $\varepsilon > 0$, while it does not have the metric pair correlation property if $A_N \geq cN^3$ infinitely often for some positive constant c. This fits together very well with the examples from above, since sequences of the form $(n^d)_n$ for $d \geq 2$ and lacunary sequences are known to have very small additive energy, while the sequence $a_n = n, \ n \geq 1$, has an additive energy of the maximal possible order.

So, the general philosophy is that a sequence has the metric pair correlation property if its additive energy is a bit below the maximal possible order. However, the precise threshold is not known. Some results in this direction are:

- The primes do not have the metric pair correlation property [125]. The additive energy of the sequence of primes is, roughly, of order $\frac{N^3}{\log N}$.
- There exists a sequence having additive energy of order $\frac{N^3}{\log N \log\log N}$ which does not have the metric pair correlation property [73].

- For every $\varepsilon > 0$ there exists a sequence having additive energy of order $\frac{N^3}{\log N (\log\log N)^{1+\varepsilon}}$ which do have the metric pair correlation property (unpublished, but not difficult to construct using methods from [23, 73]).

These results indicate that there is a sort of transitional behaviour when the additive energy lies around the "critical" order of roughly $\frac{N^3}{\log N \log\log N}$. The methods used in [23, 73] indicate a close connection between this sort of question with problems from metric Diophantine approximation, where Khintchine's classical theorem gives a zero–one law in terms of the convergence, resp. divergence, of the infinite sum of measures of the target intervals (see for example [58] for the background). It is tempting to speculate that a similar convergence/divergence criterion might also exist for the metric theory of pair correlations, where the crucial quantity is the additive energy of $(a_n)_n$. This idea was discussed in a recent paper of Bloom, Chow, Gafni, and Walker [23], where they noted that there "appears to be reasonable evidence to speculate a sharp Khintchine-type threshold, that is, to speculate that the metric Poissonian property should be completely determined by whether or not a certain sum of additive energies is convergent or divergent". They raised the following problem, which they called the "Fundamental Question".

Question 3. *Is it true that if $E(A_N) \sim N^3\psi(N)$, for some weakly decreasing function $\psi : \mathbb{Z}_{\geq 1} \to [0,1]$, then $(a_n)_n$ is metric Poissonian if and only if*

$$\sum_{N\geq 1} \psi(N)/N \tag{5.1.1}$$

converges?

The main result of the present chapter is to show that the answer to the question above is negative, and that the metric pair correlation property cannot be fully characterized in terms of the additive energy alone. For this purpose, we construct a sequence $(a_n)_n$ whose additive energy is of order roughly $N^3/(\log N)^{5/6}$, and which *does* have the metric pair correlation property. Note that the additive energy of this sequence is significantly larger than the putative threshold, which is around $N^3/(\log N \log\log N)$. Thus, the metric theory of pair correlations cannot be reduced to a convergence/divergence criterion in terms of the additive energy. Instead, the picture is more complicated and looks as follows:

- If the additive energy is below a certain threshold, then the sequence does have the metric pair correlation property.

- If the additive energy is above a certain threshold (for infinitely many N), then the sequence cannot have the metric pair correlation property. (This threshold is different from the one in the point above.)

- Between these upper and lower thresholds there is a transition zone, where the knowledge of the additive energy alone is not sufficient to determine the metric pair correlation behaviour of the sequence. Thus, in this range the metric pair correlation property is determined by some additional number-theoretic properties of the sequence.

The following theorem is the main result of this chapter.

Theorem 5.1.1. *For every $\varepsilon \in (0, 1/12)$ there exists a strictly increasing sequence $(a_n)_n$ of positive integers which has the metric pair correlation property, and whose additive energy satisfies*

$$E(A_N) \gg \frac{N^3}{(\log N)^{5/6+\varepsilon}}. \tag{5.1.2}$$

Before turning to the proof of the theorem, we note that while our result says that the metric pair correlation property cannot be characterized in terms of the additive energy alone, the problem of finding some other way of characterizing the metric pair correlation property in terms of some arithmetic properties of $(a_n)_n$ is still open. It is likely that there is a zero–one law in the metric theory of pair correlations, but actually even this is not known. Also, our result leaves questions concerning the quantitative connection between additive energy and the metric theory of pair correlations open. For example, is it possible that a sequence has additive energy of order $N^3/(\log\log N)$ and also has the metric pair correlation property, or is it possible that the additive energy is of order $N^3/(\log N)^2$ and the sequence does not have the metric pair correlation property? Closing the gaps in our knowledge in this field would be very desirable. We consider this to be an attractive problem, as phenomena from both additive combinatorics and Diophantine approximation seem to be at work here.

5.2 Preliminaries

5.2.1 Construction of the sequence

We construct our sequence $(a_n)_n$ as the concatenation of countably many "levels" where each level consists of a collection of multiple "blocks"; those blocks are either (finite) arithmetic, or (finite) geometric progressions. Moreover, the levels are constructed in such a way that the difference set of a level interacts with the difference sets of other levels in a sufficiently "random" way such that this interaction can be handled through variance estimates. The interaction between the arithmetic blocks within a given level is the most delicate issue, and are handled using tools from metric Diophantine approximation.

The geometric blocks act in a "random" way and are only used to "fill up" our sequence. Moreover, we separate different levels by adding huge constants to elements of later levels, to gain additional "independence", which is profitable for the desired variance estimates.

The key point of the construction lies in the way how different blocks of arithmetic progressions are placed in a given level, and how they interact with each other. The arithmetic blocks are of rather small cardinality, compared to the total number of elements in a level. The additive energy of the total sequence is made large by taking many of such short blocks successively within a level. Furthermore, the arithmetic

progressions have (different) prime numbers as their moduli; these primes are confined to a certain regime[1] depending on the level on which the arithmetic progression is situated. The purpose for this rather special choice of the moduli for the arithmetic progressions is twofold. On the one hand, our choice of admissible moduli simplifies the continued fraction analysis which is used to control the contribution of the arithmetic blocks. On the other hand, the primality of the moduli, in combination with the bounds on their size, keeps the number of solution of certain linear Diophantine equations under control, which enables us to establish sufficiently good variance estimates to deal with the error terms.

These two features are responsible that we can obtain an exponent smaller than 1 for the logarithm in the estimate for the additive energy in (5.1.2). When calculating the additive energy we will see the effect of the large number of short blocks being reflected in the representation function $d \mapsto r_{A_N - A_N}(d)$, (cf. the definitions below), which looks like a saw-tooth function. This shape increases the additive energy of the truncations, being only L^2-information, while the Poissonian behaviour of the counting function, being L^1-information, is "unharmed".

Now, we proceed to write down the construction precisely. This is done by induction over the levels. Fix $\varepsilon \in (0, 1/12)$, denote by $\lfloor \cdot \rfloor$ the floor function, let $\ell(1) \coloneqq 1$, and for $j \geq 2$ let

$$\ell(j) \coloneqq \lfloor j^{1/6-\varepsilon} \rfloor. \tag{5.2.1}$$

Many mathematical objects in this chapter carry two indices, such as $m_{j,i}$. Here the first index always refers to the level, and the second index to the block within a given level. The j-th level consists of $\ell(j)$ different blocks. The first of these blocks is a geometric progression, while the others are all arithmetic progressions.

In the lemma below we construct the moduli of the arithmetic blocks.

Lemma 5.2.1. *There exists a constant $j_0 \geq 1$ such that for every $j \geq j_0$ there are prime numbers $m_{j,i}$ satisfying*

$$m_{j,i} \asymp_\varepsilon j^{1/3-\varepsilon/3} \tag{5.2.2}$$

uniformly for $1 \leq i \leq \ell(j)$, and that if $j_0 \leq j - 5\log j < h \leq j$, then $m_{j,i}$ is not equal to $m_{h,g}$ for any $g \leq \ell(h)$ and $i \leq \ell(j)$.

Proof. For an integer $j \geq 1$ in the interval $8^d \leq j < 8^{d+1}$, $d \in \mathbb{Z}_{\geq 1}$, we abbreviate by $\iota = \iota(d, \varepsilon) \geq 1$ the largest (integer) power of eight which is not exceeding $\lfloor 2^{d(1-2\varepsilon)} \rfloor$. Let us now consider the interval

$$\left(2^{d(1-\varepsilon)},\ \frac{3}{2} \cdot 2^{d(1-\varepsilon)}\right). \tag{5.2.3}$$

[1]Due to this restriction, we need to use a "recycling process", as we cannot choose completely different primes for each level, since there are not enough primes for doing so in the range of interest. This "recycling process" complicates the notation a bit, but it is necessary for our construction.

The prime number theorem implies that for sufficiently large j this interval contains

$$\frac{\frac{3}{2}2^{d(1-\varepsilon)}}{\log\left(\frac{3}{2}2^{d(1-\varepsilon)}\right)} - \frac{2^{d(1-\varepsilon)}}{\log\left(2^{d(1-\varepsilon)}\right)} + \mathcal{O}\left(\frac{2^{d(1-\varepsilon)}}{d^2}\right) > 2^{d(1-\varepsilon\cdot 3/2)}$$

many primes, and hence there are more than ι primes in the interval (5.2.3) if $j \geq j_0''$ with j_0'' sufficiently large.
Denote by $p_{d,1} < \ldots < p_{d,\iota}$ the first ι primes in the interval (5.2.3). For $j \geq j_0' \coloneqq 5j_0''$ and $i \leq \ell(j)$, we put

$$m_{j,i} \coloneqq p_{d,r(i,j)},$$

where $r\,(i,j)$ is the unique remainder $0 \leq r\,(i,j) < \iota$ satisfying $\lfloor 2^{d/2} \rfloor (j - 8^d) + i = q\iota + r(i,j)$ for some $q \in \mathbb{Z}$. Since (5.2.2) is clearly true, it remains to show the additional assertion. For doing so, suppose that $m_{j,i} = m_{h,g}$ with $h \leq j$. First note that $\frac{3}{2} \cdot 2^{d(1-\varepsilon)} < 2^{(d+1)(1-\varepsilon)}$, and hence $m_{j,i} = m_{h,g}$ implies that $8^d \leq j, h < 8^{d+1}$ for some $d \in \mathbb{Z}_{\geq 1}$. By construction $m_{j,i} = m_{h,g}$ entails

$$\lfloor 2^{d/2} \rfloor j + i \equiv \lfloor 2^{d/2} \rfloor h + g \bmod \iota,$$

and thus if $(j,i) \neq (h,g)$, then

$$\left| \lfloor 2^{d/2} \rfloor j + i - \lfloor 2^{d/2} \rfloor h - g \right| \geq \iota.$$

As $i, g \leq 2^{d/2}$, we conclude that $j - h \gg 2^{d(1/2-2\varepsilon)}$. Hence, by possibly choosing a large enough $j_0 \geq j_0'$ and $j_0 \leq j$, the additional assertion of the lemma holds true. □

Let j_0 be as in Lemma 5.2.1, and set $J_0 \coloneqq \max\{j_0, 4^{12}\}$. To define the numbers on the first J_0 levels, we put $P_G\,(j) \coloneqq P_A\,(j,i) \coloneqq j$ for every $j \leq 2^{J_0}$, and each $i \leq \ell\,(j)$. This defines only finitely many elements at the initial segment of our sequence $(a_n)_n$, which will not play any role.

For $j > J_0$ we recursively define constants $C_{j,i}$ and sets $P_G\,(j)$ and $P_A\,(j,i)$ by setting

$$C_{j,i} \coloneqq \begin{cases} \lfloor \exp(\max P_A(j-1, \ell(j-1))) \rfloor & \text{if} \quad i = 1 \\ \lfloor \exp(\max P_G(j)) \rfloor & \text{if} \quad i = 2 \\ \lfloor \exp(\max P_A(j, i-1)) \rfloor & \text{if} \quad i = 3, \ldots, \ell\,(j)\,, \end{cases} \tag{5.2.4}$$

where

$$P_G\,(j) \coloneqq \{C_{j,1} + 3^{j^h} \mid h = 0, \ldots, 2^j - 1\}$$

is a shifted geometric progression and

$$P_A(j,i) \coloneqq \{C_{j,i} + m_{j,i}h \mid h = 0, \ldots, \lfloor 2^j / j^{1/3} \rfloor\} \qquad (i = 2, \ldots, \ell\,(j))$$

are shifted arithmetic progressions whose union

$$P_A\,(j) \coloneqq \bigcup_{i=2}^{\ell(j)} P_A\,(j,i)$$

will be important in the following.
Finally, we define $a_n = a_n(\varepsilon)$ as the n-th (smallest) element of

$$\bigcup_{j\geq 1}\Big(P_G(j)\cup P_A(j)\Big).$$

Note that the sets $P_G(j)$ and $P_A(j,i)$ are arranged in such a way that (elementwise) we have

$$P_G(j)\leq P_A(j,2)\leq P_A(j,3)\leq\cdots\leq P_A(j,\ell(j))\leq P_G(j+1).$$

Furthermore, the constants $C_{j,i}$ are chosen to be huge, so as to guarantee that in the chain of inequalities above elements from one (geometric or arithmetic) block are always much larger than elements of the previous block. This rapid growth of elements when changing from one block to the next is a sort of "lacunarity" property, which creates additional independence and allows us to control the interaction between elements coming from different blocks.

5.2.2 A useful partition, and short GCD sums

Throughout this chapter, we write $X-Y$ for the difference set

$$X-Y\coloneqq\{x-y:\ x\in X,\ y\in Y\}$$

of two sets $X,Y\subseteq\mathbb{Z}$. By $\#X$ we denote the cardinality of X. Furthermore, we write r_{X-Y} for the number of ways in which $d\in\mathbb{Z}$ can be represented as a difference of elements of $X,Y\subseteq\mathbb{Z}$, that is,

$$\mathrm{r}_{X-Y}(d)\coloneqq\#\left\{(x,y)\in X\times Y:\ d=x-y\right\}.$$

If no confusion can arise, we write $\mathrm{r}(d)$ for $\mathrm{r}_{X-Y}(d)$, and if nothing else is specified we understand $\mathrm{r}((d)$ as $\mathrm{r}_{A_N-A_N}(d)$ throughout this chapter. Recall that trivially $\mathrm{r}_{X-Y}(d)\leq\min\{\#X,\#Y\}$.

Moreover, let $X^+\coloneqq X\cap\mathbb{Z}_{\geq 1}$ denote the set of positive elements of $X\subseteq\mathbb{Z}$. Since A_N-A_N is symmetric around the origin, we can confine attention to its positive part, for most of the time. Setting

$$\begin{aligned}\overline{\mathcal{D}}_N\coloneqq&(A_N-A_N)^+\setminus\{1,\dots,C_{\lfloor(\log N)/\log 7\rfloor,1}\},\\ \underline{\mathcal{D}}_N\coloneqq&(A_N-A_N)^+\cap\{1,\dots,C_{\lfloor(\log N)/\log 7\rfloor,1}\},\end{aligned}$$

where $C_{\cdot,\cdot}$ are the constants defined in (5.2.4), we can split $(A_N-A_N)^+$ into the union $\overline{\mathcal{D}}_N\uplus\underline{\mathcal{D}}_N$, where here and in the sequence the symbol $\uplus$ always indicates that the union is disjoint. To analyse the contribution of a number $d\in\overline{\mathcal{D}}_N$ to the counting function of the pair correlation distribution, we use a finer decomposition whose components are described in the next lemma.
In the following we will, tacitly, for given N denote by $J=J(N)$ the positive integer for which

$$2^{J-1}\leq N<2^J.$$

Lemma 5.2.2. *(a) If $r \geq 1$ is an integer, then*

$$C_{j,i} \gg_r \exp^{\circ r}\left(2^j\right) \tag{5.2.5}$$

holds uniformly for all $1 \leq i \leq \ell(j)$. Here $\exp^{\circ r}$ is the r-times iterated exponential function, that is, $\exp^{\circ r}(x) \coloneqq \exp^{\circ(r-1)}(\exp(x))$, and $\exp^{\circ 1}(x) \coloneqq \exp(x)$.

(b) Moreover, assume that each of "X" and "Y" represent one of the letters $\{A, G\}$, that is, $(X, Y) \subset \{(A,A),(A,G),(G,A),(G,G)\}$. Let $M(XY)$ be the union over $(P_X(j) - P_Y(i))^+ \cap \overline{\mathcal{D}}_N$ as $J/3 \leq j \leq J$ and $i \leq j$. Consider the sets

$$\overline{\mathcal{D}}_N(XY) \coloneqq M(XY) \cup \bigcup_{i<J}((P_X(J) - P_Y(i))^+ \cap (A_N - A_N)).$$

If N is sufficiently large, then $\overline{\mathcal{D}}_N(AA), \overline{\mathcal{D}}_N(AG), \overline{\mathcal{D}}_N(GA), \overline{\mathcal{D}}_N(GG)$ are pairwise disjoint.

Remark 3. *Part (b) of the lemma says, roughly speaking, that the difference sets $\overline{\mathcal{D}}_N$ are separated depending on whether the larger one of the two blocks which gives rise to a difference $d \in \overline{\mathcal{D}}_N$ is an arithmetic, or a geometric block.*

Proof. We note that

$$C_{j,i} \geq C_{j,1} \geq \exp\Big(C_{j-1,1}\Big) \geq \ldots \geq \exp^{\circ r}\Big(C_{j-r,1}\Big),$$

where $C_{j-r,1} \geq 2^j$ for sufficiently large j. This implies (5.2.5). Now assume that $X = A, Y = G$; all the other cases can be treated by a similar reasoning. As $d \in (P_X(j) - P_Y(k))^+$ can be written as $d = C_{j,i}(1 + o(1))$, which holds uniformly in $k \leq j$ and $i \leq \ell(j)$, an element $d' \in (P_{X'}(j') - P_{Y'}(k'))^+$ could be equal to d only if $X = X'$ and $Y = Y'$. □

Thus for sufficiently large N the set $\overline{\mathcal{D}}_N$ can be decomposed in the form,

$$\overline{\mathcal{D}}_N = \overline{\mathcal{D}}_N(GG) \uplus \overline{\mathcal{D}}_N(AG) \uplus \overline{\mathcal{D}}_N(GA) \uplus \overline{\mathcal{D}}_N(AA)$$

and accordingly the counting function of the pair correlation distribution

$$R([-s,s],\alpha,N) \coloneqq \frac{1}{N}\#\{1 \leq i \neq j \leq N : \|(a_j - a_i)\alpha\| \leq s/N\} \tag{5.2.6}$$

can be decomposed as

$$\overline{R}(GG) + \overline{R}(AG) + \overline{R}(GA) + \overline{R}(AA) + \underline{R},$$

where for $X, Y \in \{A, G\}$

$$\overline{R}(XY) \coloneqq \overline{R}(XY,\alpha,s,N) \coloneqq \frac{2}{N}\sum_{d \in \overline{\mathcal{D}}_N(XY)} \mathrm{r}(d)\, I_{s,N}(d\alpha),\ I_{s,N}(x) \coloneqq \begin{cases} 1 & \|x\| \leq s/N, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\underline{R} \coloneqq \underline{R}(s,\alpha,N) \coloneqq \frac{2}{N}\sum_{d\in\underline{\mathcal{D}}_N} \mathrm{r}(d)\, I_{s,N}(d\alpha).$$

By using the same methods as in [14], one can easily conclude that

$$\overline{R}(GG,\alpha,s,N) \to 2s \tag{5.2.7}$$

as $N\to\infty$, for almost all $\alpha\in[0,1]$ and each $s>0$. This follows from the fact that geometric progressions have small additive energy, and the fact that the cardinality of the geometric blocks is dominant over the total cardinality of the arithmetic blocks which implies that $1/N$ really is the correct normalization factor such that $\overline{R}(GG)$ converges as desired for $N\to\infty$.

Thus it remains to show that all the remaining terms $\overline{R}(AG), \overline{R}(GA), \overline{R}(AA)$ and $\underline{R}$ vanish in the limit $N\to\infty$, for almost all α. The contribution of $\overline{R}(AG)$, $\overline{R}(GA)$ and $\overline{R}(AA)$ is estimated using variance bounds, which we obtain from some Fourier analysis in combination with estimates on GCD sums. The contribution of $\underline{R}$ is the critical part, and is estimated with tools from the metric theory of continued fractions.

For later reference, we note that the Fourier series expansion of the indicator functions $I_{s,N}(\alpha)$ is given by

$$I_{s,N}(\alpha) \sim \sum_{n\in\mathbb{Z}} c_n e(n\alpha) \qquad \text{where} \quad c_n \coloneqq \begin{cases} \sin(2\pi ns/N)/(\pi n) & \text{if } n\neq 0,\\ 2s/N & \text{if } n=0, \end{cases} \tag{5.2.8}$$

and $e(\alpha)$ abbreviates $\exp(2\pi i\alpha)$. The next lemma is of a technical nature, and is used in a decoupling argument for the variance bounds, which are derived in Section 3.

Lemma 5.2.3. *Let $\mathcal{I},\mathcal{I}'\subseteq\mathbb{Z}_{\geq 1}$ be non-empty sets such that $\mathcal{I}>\mathcal{I}'$ holds elementwise. Define for integers $u,v>0$ the quantity*

$$C(u,v) \coloneqq \sum_{\substack{n_1,n_2\in\mathbb{Z}\setminus\{0\}\\ n_1u=n_2v}}\sum c_{n_1}c_{n_2}.$$

Then,

$$\sum_{u\in\mathcal{I}}\sum_{v\in\mathcal{I}'} C(u,v) \ll (\#\mathcal{I}'\#\mathcal{I})\frac{\max\{\mathcal{I}-\mathcal{I}'\}}{\min\mathcal{I}}. \tag{5.2.9}$$

Moreover, for $u\neq 0$ we have

$$C(u,u) \ll_s N^{-1}. \tag{5.2.10}$$

Proof. We show first that

$$C(u,v) \ll \frac{\gcd(u,v)}{\max\{u,v\}} \tag{5.2.11}$$

for distinct $u,v>0$. Note that $n_1u=n_2v$ holds if and only if there is an integer $h\neq 0$ satisfying $n_1=hu/\gcd(u,v)$ and $n_2=hv/\gcd(u,v)$. Moreover, we observe that $|c_n|\leq$

$\min\{2s/N, 1/|n|\}$ for $n \neq 0$. Combining these estimates with the Cauchy–Schwarz inequality yields

$$\begin{aligned}|C(u,v)|^2 &\leq \sum_{h\in\mathbb{Z}\setminus\{0\}} c^2_{h\frac{u}{\gcd(u,v)}} \sum_{h\in\mathbb{Z}\setminus\{0\}} c^2_{h\frac{v}{\gcd(u,v)}} \\ &\leq \sum_{h\in\mathbb{Z}\setminus\{0\}} \frac{(\gcd(u,v))^2}{(uh)^2} \sum_{h\in\mathbb{Z}\setminus\{0\}} \frac{(\gcd(u,v))^2}{(vh)^2},\end{aligned}$$

which implies (5.2.11).

Trivially $\gcd(u,v) \leq \max\{u,v\} - \min\{u,v\} \leq \max\{\mathcal{I} - \mathcal{I}'\}$, and thus (5.2.11) yields (5.2.9). Furthermore,

$$|C(u,u)| \ll \sum_{n\leq \frac{N}{2s}} \frac{4s^2}{N^2} + \sum_{n>\frac{N}{2s}} \frac{1}{n^2},$$

which yields (5.2.10). □

Letting $X \in \{AG, GA, AA\}$ and $\mathcal{D} \coloneqq \overline{\mathcal{D}}_N(X)$, then combining equation (5.2.8) with Parseval's identity yields

$$N^2 \operatorname{Var}(\overline{R}(X,s,\cdot,N)) = \sum_{u,v\in\mathcal{D}}\sum \mathrm{r}(u)\,\mathrm{r}(v)\,C(u,v). \tag{5.2.12}$$

The main term on the right hand side, as we shall see, is the sum over the diagonal terms $(\mathrm{r}(u))^2 C(u,u)$. To prove this, the next lemma shows that the contribution from the off-diagonal terms is small.

Lemma 5.2.4. *For $\mathcal{D}$ is as in (5.2.12) we have*

$$\sum_{u\in\mathcal{D}} \sum_{\substack{v\in\mathcal{D}\\ v<u}} \mathrm{r}(u)\,\mathrm{r}(v)\,C(u,v) \ll \frac{1}{N}. \tag{5.2.13}$$

Proof. We will give a detailed proof for the case $\mathcal{D} = \overline{\mathcal{D}}_N(AG)$ — the othe other cases can be dealt with analogously. Consider $i^{\pm}, j^{\pm}, k^{\pm}$ such that $J/3 \leq j^- \leq j^+ \leq J$, $k^{\pm} \leq j^{\pm}$, and $2 \leq i^{\pm} \leq \ell(j^{\pm})$. If $u \in \mathcal{D}$, then $u \in P_A(j^+, i^+) - P_G(k^+)$. If $v \in P_A(j^-, i^-) - P_G(k^-)$ with $(j^-, i^-) \neq (j^+, i^+)$, then by the large difference in size between elements from different blocks we have $v < u^{1/2}$. Hence, in this case (5.2.11) implies that

$$|C(u,v)| < u^{-1/2} \ll C_{j^+,1}^{-1/2} \ll \left(\exp^{\circ 3}(N)\right)^{-1}.$$

If $v \in P_A(j^+, i^+) - P_G(k^-)$ with $1 \leq k^- \leq j^+$ is strictly less than u, then (5.2.9) yields

$$\sum_{\substack{u,v\in P_A(j^+,i^+)-P_G(k^-)\\ v<u}}\sum \mathrm{r}(u)\,\mathrm{r}(v)\,|C(u,v)| \leq N^2 \sum_{\substack{u,v\in P_A(j^+,i^+)-P_G(k^-)\\ v<u}}\sum |C(u,v)|.$$

For each $u \in P_A(j^+, i^+) - P_G(k^-)$, we let $\mathcal{I} \coloneqq \{u\}$ and

$$\mathcal{I}' \coloneqq (P_A(j^+, i^+) - P_G(k^-)) \cap \{1, \dots, u\}.$$

Then, $\max\{\mathcal{I} - \mathcal{I}'\} \leq C_{j^+,1}$, and u exceeds $C_{j^+,2} - 3^{(j^+)^N} - C_{j^+,1}$. By applying (5.2.5) and summing over $u \in P_A(j^+, i^+) - P_G(k^-)$, we conclude that

$$\sum_{\substack{u,v \in P_A(j^+,i^+) - P_G(k^-) \\ v<u}} \sum \mathrm{r}(u)\,\mathrm{r}(v)\,|C(u,v)| \ll N^2 \frac{(\#(P_A(j^+, i^+) - P_G(k^-)))^2 C_{j^+,1}}{C_{j^+,2} - 3^{(j^+)^N} - C_{j^+,1}}.$$

Due to $J \asymp \log N$, the right-hand side is $\ll N^2/\exp^{\circ 3}(N)$. Therefore,

$$\sum_{u \in \mathcal{D}} \sum_{\substack{v \in \mathcal{D} \\ v<u}} \mathrm{r}(u)\,\mathrm{r}(v)\,|C(u,v)| \leq \sum \sum \sum_{\substack{J/3 \leq j^- \leq j^+ \leq J \\ k^\pm \leq j^\pm,\, i^\pm \leq \ell(j^\pm)}} \sum \sum \sum \sum_{\substack{u \in P_A(j^+,i^+) - P_G(k^+) \\ v \in P_A(j^-,i^-) - P_G(k^-) \\ u>v}} \mathrm{r}(u)\,\mathrm{r}(v)\,|C(u,v)|$$

$$\ll \frac{(\log N)^6 N^2}{\exp^{\circ 3}(N)},$$

which implies (5.2.13). □

5.3 Proof of Theorem 5.1.1

Our strategy is now to deal with $\overline{R}(X, s, \cdot, N)$ for $X \in \{AG, GA, AA\}$ by using variance estimates.

5.3.1 Variance bounds

Proposition 5.3.1. *For every fixed $s > 0$ we have*

$$\mathrm{Var}(\overline{R}(X, s, \cdot, N)) \ll_s \frac{1}{N} + \frac{1}{N^3} \sum_{d \in \overline{\mathcal{D}}_N(X)} (\mathrm{r}(d))^2 \ll_\varepsilon \frac{(\log N)^8}{N} \tag{5.3.1}$$

for ($X \in \{AG, GA\}$), and

$$\mathrm{Var}(\overline{R}(AA, s, \cdot, N)) \ll_s \frac{1}{N} + \frac{1}{N^3} \sum_{d \in \overline{\mathcal{D}}_N(AA)} (\mathrm{r}(d))^2 \ll_\varepsilon \frac{1}{(\log N)^{1+\varepsilon}}. \tag{5.3.2}$$

Proof. We first prove (5.3.1). Let $\mathcal{D} \coloneqq \overline{\mathcal{D}}_N(GA)$, the case $\mathcal{D} = \overline{\mathcal{D}}_N(AG)$ being analogously. Note that trivially $\#\mathcal{D} \leq N^2$. Moreover, we claim that $\mathrm{r}(u) \ll (\log N)^4$ for every $u \in \mathcal{D}$. To see this, first note that $\mathrm{r}(u)$ is at most

$$\sum_{k \leq j \leq J} \sum \mathrm{r}_{P_G(j) - P_A(k)}(u) = \sum_{k \leq j \leq (\log J)^{1/2}} \sum \mathrm{r}_{P_G(j) - P_A(k)}(u) + \sum_{(\log J)^{1/2} < j \leq J,\, k \leq j} \sum \mathrm{r}_{P_G(j) - P_A(k)}(u).$$

Since in the first sum $\mathrm{r}_{P_G(j)-P_A(k)}(u) \leq \#P_G(j) \ll \exp(O((\log\log N)^{1/2}))$ it follows that

$$\sum\sum_{k\leq j\leq (\log J)^{1/2}} \mathrm{r}_{P_G(j)-P_A(k)}(u) \ll (\log N)^3,$$

and in the second sum, due to the growth of base 3^j in the geometric progression $P_G(j)$, the bound $\mathrm{r}_{P_G(j)-P_A(k)}(u) \leq (\log\log N)\log N$, which holds for N sufficiently large, implies

$$\sum\sum_{(\log J)^{1/2}<j\leq J,\, k\leq j} \mathrm{r}_{P_G(j)-P_A(k)}(u) \ll (\log N)^4,$$

which entails $\mathrm{r}(u) \ll (\log N)^4$ for every $u \in \mathcal{D}$. Hence, (5.2.10) implies

$$\sum_{u\in\mathcal{D}} (\mathrm{r}(u))^2 |C(u,u)| \ll_s N(\log N)^8.$$

From this, in combination with (5.2.12) and (5.2.13), we infer (5.3.1).

For the rest of the proof, we let $\mathcal{D} \coloneqq \overline{\mathcal{D}}_N(AA)$. Let $j^{\pm}$ and $i^{\pm}$ be such that $j^- \leq j^+$ and $2 \leq i^{\pm} \leq \ell(j^{\pm})$. Assume $J/3 \leq j^+ \leq J$, and $u \in P_A(j^+,i^+) - P_A(j^-,i^-) \subseteq \mathcal{D}$. By the trivial estimate $\mathrm{r}(u) \ll \min\{\#P_A(j^{\pm},i^{\pm})\}$, we have

$$\frac{1}{N^2} \sum\sum\sum\sum_{\substack{j^-\leq j^+<J-5\log J\\ i^{\pm}\leq\ell(j^{\pm}),(j^-,i^-)\neq(j^+,i^+)}} \sum_{u\in P_A(j^+,i^+)-P_A(j^-,i^-)} (\mathrm{r}(u))^2 |C(u,u)| \ll \frac{1}{(\log N)^3}. \quad (5.3.3)$$

It remains to control the contribution from the range $J - 5\log J \leq j^- \leq j^+ \leq J$. We first remark that the sets $P_A(j^+,i^+) - P_A(j^-,i^-)$ are pairwise disjoint for the indices in the ranges just specified. Therefore, $\mathrm{r}(u)$ is bounded by the number of solutions $(x,y) \in \mathbb{Z}^2$ to the linear Diophantine equation

$$\tilde{u} = m_{j^+,i^+}x - m_{j^-,i^-}y \qquad \text{where} \quad \tilde{u} \coloneqq u - C_{j^+,i^+} + C_{j^-,i^-},$$

under the additional restriction that $1 \leq x,y \leq N/(\log N)^{1/3}$. Since m_{j^+,i^+} and m_{j^-,i^-} are prime numbers, the set of integer solutions to this equation admits the form

$$\{(x_0 + hm_{j^-,i^-}, y_0 - m_{j^+,i^+}h) : h \in \mathbb{Z}\},$$

where (x_0,y_0) is some solution to the above equation. Moreover, the size of $j^{\pm}$ together with (5.2.2) ensures that $m_{j^{\pm},i^{\pm}} \asymp (\log N)^{1/3-\varepsilon/3}$ holds uniformly in $i^{\pm} \leq \ell(i^{\pm})$. Hence,

$$\mathrm{r}(u) \ll \frac{N}{(\log N)^{2/3-\varepsilon/2}}. \quad (5.3.4)$$

Due to

$$\sum\sum\sum\sum_{\substack{J-5\log J\leq j^-\leq j^+\leq J\\ i^{\pm}\leq\ell(j^{\pm}),(j^-,i^-)\neq(j^+,i^+)}} \#(P_A(j^+,i^+) - P_A(j^-,i^-)) \ll \sum\sum_{J-5\log J\leq j^-\leq j^+\leq J} \frac{2^{j^+}}{(j^+)^{\varepsilon/3}} (\ell(j^+))^2$$

$$\ll_{\varepsilon} \frac{N}{(\log N)^{-1/3+2\varepsilon}},$$

we conclude from (5.3.4) that

$$\frac{1}{N^2}\sum_{\substack{J-5\log J\le j^-\le j^+\le J\\ i^\pm\le \ell(j^\pm),(j^-,i^-)\neq(j^+,i^+)}}\sum_{u\in P_A(j^+,i^+)-P_A(j^-,i^-)}(\mathrm{r}(u))^2|C(u,u)|\ll_\varepsilon \frac{1}{(\log N)^{1+\varepsilon}}.$$

Combining this with (5.3.3) yields (5.3.2). □

5.3.2 Estimates for correlations from the short progressions

Before proceeding further, we recall some results about continued fractions. For a (possibly finite) sequence $(\alpha_i)_i$ of strictly positive integers, we denote by

$$\alpha \coloneqq [\alpha_1,\alpha_2,\ldots]=\cfrac{1}{\alpha_1+\cfrac{1}{\alpha_2+\cfrac{1}{\ddots}}}$$

the associated (possibly finite) continued fraction in the unit interval $[0,1]$. Moreover, let p_n/q_n denote the n-th convergent to α. Then, the following are well-known facts, cf. for instance [28, Ch.1].

1. Legendre's theorem: If a/b is a fraction with $|\alpha - a/b| < 1/(2b^2)$, then a/b is a convergent to α.

2. We have
$$\left|\alpha-\frac{p_n}{q_n}\right|\asymp\frac{1}{\alpha_n q_n^2}, \tag{5.3.5}$$
where the implied constants are *independent* of α.

3. Borel-Bernstein theorem: Let $B\coloneqq(b_n)_n$ be a sequence of (strictly) positive real numbers, and consider the series over their reciprocals
$$\sum_{n\ge1}\frac{1}{b_n}. \tag{5.3.6}$$
If $V_B\subset[0,1]$ denotes the set of those numbers $\alpha=[\alpha_1,\alpha_2,\ldots]$ for which $\alpha_n\le b_n$ holds for all sufficiently large $n\ge1$, then
$$\lambda(V_B)=\begin{cases}1 & \text{if (5.3.6) is convergent,}\\ 0 & \text{if (5.3.6) is divergent.}\end{cases}$$

Proposition 5.3.2. *For each $\varepsilon\in(0,1/12)$, there exists a set of $\alpha\in[0,1]$ of full Lebesgue measure such that for*

$$M(j,i)\coloneqq\{q\le 2^j/j^{1/3}:\ \|m_{j,i}q\alpha\|\le s/2^j\}$$

it holds that

$$\#M(j,i)\ll_s j^{1/6+2\varepsilon/3},$$

uniformly for all $i\le\ell(j)$.

Proof. Let B denote the sequence $(n^{1+\varepsilon})_n$, and suppose that $\alpha \in V_B$ is an irrational number. By the Borel–Bernstein theorem, the set of such α has full Lebesgue measure. We argue now in two steps. Without loss of generality, we may assume that $M(j,i)$ is non-empty.

(i) We first show the following: If j is sufficiently large, then there is a unique $n = n(j) \geq 1$ such that for q_n denoting the denominator of the n-th convergent to α we have

$$M(j,i) \subseteq q_n \mathbb{Z}. \tag{5.3.7}$$

Indeed, if $q \in M(j,i)$ and $p \in \mathbb{Z}$ is such that $\|q\alpha\| = |q\alpha - p|$, then Legendre's theorem implies that there is some $n \geq 1$ with

$$\frac{p}{q} = \frac{p_n}{q_n} \qquad \text{i.e.} \quad q = p\frac{q_n}{p_n}. \tag{5.3.8}$$

Since p_n and q_n are coprime, we conclude that $p = p_n m$ and $q = m q_n$ for some $m \in \mathbb{Z}$; moreover, observe that (5.3.5) implies

$$\frac{m_{j,i} m}{\alpha_n q_n} \asymp \|m_{j,i} q \alpha\| \leq \frac{s}{2^j}. \tag{5.3.9}$$

Suppose that n is the minimal integer n' with $q_{n'}$ with $q_n \mathbb{Z} \cap M(j,i) \neq \emptyset$. The well-known recursion $q_{n+1} = \alpha_n q_n + q_{n-1}$ yields $q_{n+1} \geq \alpha_n q_n \gg_s 2^j m m_{j,i} > 2^j$ for sufficiently large j. However, $M(j,i)$ by definition is a subset of $\{1, \dots, \lfloor 2^j / j^{1/3} \rfloor\}$. This shows that n in (5.3.7) is unique.

(ii) Let $m_{\max}$ denote the largest $m \geq 1$ with $m q_n \in M(j,i)$. Then, we conclude that $m_{\max}$ must satisfy both

$$m_{\max} \leq \frac{2^j}{q_n j^{1/3}} \qquad \text{and} \qquad m_{\max} \ll s\frac{\alpha_n q_n}{m_{j,i} 2^j},$$

where we used (5.3.9). Using $\alpha \in V_B$ and $n \ll j$, we conclude from (5.3.9) that $q_n \gg 2^j/(j^{1+\varepsilon})$. Therefore,

$$m_{\max} \ll \max_{\frac{2^j}{j^{1+\varepsilon}} \leq x \leq \frac{2^j}{j^{1/3}}} \min\left\{ \frac{2^j}{x j^{1/3}},\ s\frac{\alpha_n x}{m_{j,i} 2^j} \right\}$$

where the $x \in \mathbb{R}$ maximizing in the right hand side, under the given constraints, is determined via

$$\frac{2^j}{x j^{1/3}} = s\frac{\alpha_n x}{m_{j,i} 2^j} \quad \Leftrightarrow \quad x^2 = \frac{m_{j,i} 2^{2j}}{j^{1/3} s \alpha_n}.$$

Thus,

$$m_{\max}^2 \ll \frac{s\alpha_n}{j^{1/3} m_{j,i}}$$

which implies the claim since $n \ll j$ and $\alpha \in V_B$. □

Proof of Theorem 5.1.1

The proof of Theorem 5.1.1 splits into two parts. First the bound (5.1.2) for the additive energy of the truncation A_N is demonstrated, and then the metric Poissonian property of $(a_n)_n$ is shown.

(i) It is easily seen that for two sets A, B we always have $E(A \cup B) \geq E(A) + E(B)$. Thus,

$$E(A_N) \geq \ell\,(J-1)\,E(P_A(J-1,i)) \gg (\log N)^{1/6-\varepsilon}\,\frac{N^3}{\log N},$$

where we used that the additive energy of an arithmetic progression is proportional to the third power of its number of terms, and that by construction $\#P_A\,(J-1,i) \geq 2^{J-1}/(J-1)^{1/3}$ for all i. It can be shown that the estimate $N^3(\log N)^{-5/6-\varepsilon}$ for the additive energy of $(a_n)_n$ is actually tight up to factors of double logarithmic order but — since this is not really important for the present chapter — we omit the proof.

(ii) It is a standard procedure to use the variance estimates and the results from the previous section to conclude that the contribution of $\overline{R}\,(AG)\,, \overline{R}\,(GA)\,, \overline{R}\,(AA)$ and $\underline{R}$ tends to zero in the limit; thus we only give a brief outline. Fix a rational $s > 0$. Define the sequence $N_m = \left\lfloor \exp(m^{\frac{1}{1+\varepsilon/2}}) \right\rfloor$, and note that $N_{m+1}/N_m \to 1$. Suppose for the rest of the proof that $X \in \{AG, GA, AA\}$. If $N \in \mathbb{Z}_{\geq 1}$ is such that $N_m \leq N < N_{m+1}$, then

$$N\overline{R}(X, [-s,s]\,, \alpha, N) \leq N_{m+1}\overline{R}(X, N_{m+1}/N_m\,[-s,s]\,, \alpha, N_{m+1}).$$

Denote by $E_{X,s}\,(N_m)$ the set

$$\{\alpha \in [0,1] : |\overline{R}(X, N_{m+1}/N_m[-s,s], \alpha, N) - \mu_{X,s}\,(N_m)\,| \geq 1/\log\log N_m\}$$

where $\mu_{X,s}\,(N_m)$ is the expected value of $\overline{R}(X, N_m/N_{m+1}\,[-s,s]\,, \alpha, N)$; observe that $\mu_{X,s}\,(N_m)$ tends to zero as $m \to \infty$ since the indices of those elements of $(a_n)_n$ coming from the arithmetic progressions form a set of zero density in the total index set. By combining Chebyshev's inequality with the variance estimates from Proposition 5.3.1, we obtain $\lambda\,(E_{X,s}\,(N_m)) \ll_\varepsilon (\log m)^2\, m^{-\frac{1+\varepsilon}{1+\varepsilon/2}}$. Thus, the Borel–Cantelli lemma implies that for almost all $\alpha \in [0,1]$ and each rational $s > 0$, indeed,

$$\overline{R}(X, [-s,s], \alpha, N) \underset{N\to\infty}{\longrightarrow} 0, \qquad (X \in \{AG, GA, AA\})\,. \tag{5.3.10}$$

Furthermore, from Proposition 5.3.2 we have, for almost all $\alpha \in [0,1]$, that

$$\underline{R}([-s,s]\,, \alpha, N) \ll \sum_{\substack{J-5\log J \leq j \leq J \\ i \leq \ell(j)}} \sum \sum_{d \in M(j,i)} \frac{1}{j^{1/3}} \ll_s \sum_{\substack{J-5\log J \leq j \leq J \\ i \leq l(j)}} \sum \sum \frac{1}{(\log N)^{1/3}}\,(\log N)^{1/6+2/3\varepsilon}\,.$$

Due to (5.2.1), it follows that

$$\underline{R}([-s,s]\,, \alpha, N) \ll_s \frac{\log\log N}{(\log N)^{\varepsilon/3}} \tag{5.3.11}$$

Combining (5.2.7), (5.3.10) and (5.3.11) finishes the proof.

Appendix A

On the Regularity of Primes in Arithmetic Progressions

This chapter is based on joint work with **Christian Elsholtz**, and **Robert Tichy** [42].

We prove that for $k \in \mathbb{Z}_{\geq 1}$ the primes in certain kinds of intervals cannot distribute too "uniformly" among the invertible residue classes modulo k. Hereby, we prove a generalization of a conjecture of Recaman and establish our results in a much more general setting, in particular for prime ideals in number fields, recall Definition 2.

To this end, the present chapter is organized as follows: Firstly, we deduce a necessary condition for $g \in G$, where G is always assumed to be as in Definition 2, to be a P^*-integer and prove Theorem 1.4.1. This will be done via a combinatorial argument which leads to inequalities involving sums over the prime counting function $x \mapsto \pi(x)$ evaluated at certain points. Secondly, we will remove $x \mapsto \pi(x)$ from these inequalities by approximating it and then deal with the sums in such a manner that we receive explicit formulas for seeing which large k violate the arising inequalities.

A.1 Preliminaries and Proof of Theorem 1.4.1

We first collect some results which we will need in the proofs.

Lemma A.1.1 (Cf. [120, Thm. 1]). *Let $\theta(x) := \sum_{p \leq x} \log p$ denote the Chebyshev function where the summation runs through all primes $p \leq x$. With*

$$\varepsilon(x) := \sqrt{\frac{8 \log x}{17\pi \cdot \eta}} e^{-\sqrt{\eta^{-1} \log x}} \qquad \text{for } x \geq 149, \eta := 6.455 \tag{A.1.1}$$

we have

$$|\theta(x) - x| < x\varepsilon(x), \qquad \text{for } x \geq 149. \tag{A.1.2}$$

Remark 4. *We recall that*

1. *$p_n \geq n \log n$ for any $n \geq 1$, see [95, p. 69], and*

2. *for* $k \geq 2\,953\,652\,287$ *we have, cf. [37, Thm. 6.9],*

$$E_{0,-} := 2\pi(0.5k) - \pi(k) > \frac{k}{\log(0.5k)}\left(1 + \frac{1}{\log(0.5k)} + \frac{2}{\log^2(0.5k)}\right) - \frac{k}{\log(k)}\left(1 + \frac{1}{\log(k)} + \frac{2.334}{\log^2(k)}\right). \tag{A.1.3}$$

3. *Moreover, we need the estimates*

$$\sqrt{\frac{2}{\pi}(2S+1)} \leq \prod_{s=1}^{S} \frac{2s+1}{2s} \leq \frac{2S+1}{\sqrt{S\pi}} \tag{A.1.4}$$

which are well-known (in equivalent forms) in the context of Wallis' product formula for π*, cf. [63, p. 504-505].*

4. *The following estimate holds, cf. [95, p. 72]:*

$$\varphi(k) \geq \frac{k}{1.7811 \log\log k + \frac{2.51}{\log\log k}}, \qquad k \geq 3. \tag{A.1.5}$$

5. *Let* $\operatorname{li}(x)$ *denote the integral* $\int_2^x \frac{\mathrm{d}\tau}{\log\tau}$ *for* $x > 0$*. If for an arithmetical semi-group* G *the counting functions* $g(x) := \#\{g \in G : |g| \leq x\}$ *takes the form*

$$g(x) = Ax^\delta + \mathcal{O}(x^\delta \log^{-\beta} x), \qquad \beta > 3,\ \delta > 0,\ x \to \infty, \tag{A.1.6}$$

then the prime counting function of G *can be written as*

$$\pi_G(x) = \operatorname{li}(x^\delta) + \mathcal{O}(x^\delta \log^{-c} x) \qquad \text{for any } c < \frac{\beta}{3}. \tag{A.1.7}$$

This is due to Wegmann [126]. In particular, the conclusion is true, if G *satisfies Axiom A.*

Our method to detect P^*-integers originates from [55], which we shall describe in the following. We write $\pi_G(x) = \pi(x)$ and denote for natural numbers x, K by $x \bmod K$ the unique remainder $r \in \{0, \ldots, K-1\}$ such that $x = qK + r$ holds for some $q \in \mathbb{N}$. Let us assume that k is a P^*-integer and put $K := |k|$. Then, by the symmetry of coprime residue classes modulo K about $0.5K$, the cardinalities of the sets

$$A_1 := \{p \in G :\ \alpha \leq |p| \leq \beta,\ p \,\text{prime},\ |p| \bmod K \leq 0.5K\}, \tag{A.1.8}$$
$$A_2 := \{p \in G :\ \alpha \leq |p| \leq \beta,\ p \,\text{prime},\ |p| \bmod K > 0.5K\}, \tag{A.1.9}$$

differ by at most ι elements. For checking this condition, we need to count the size of A_i. This counting is done by the following lemma:

Lemma A.1.2. *Let k denote an element of an arithmetical semi-group G, $K := |k|$, and put*

$$E_{j,1}(k) := \pi((j+0.5)K) - \pi(jK-1), \tag{A.1.10}$$

$$E_{j,2}(k) := \pi((j+1)K) - \pi((j+0.5)K) \tag{A.1.11}$$

for $j \geq 0$, $i = 1, 2$. If λ, Λ denote integers such that $\lambda K \leq \alpha < (\lambda+1)K$, and $\Lambda K \leq \beta < (\Lambda+1)K$ hold, then we have

$$\#A_i = M_i(k) + \sum_{j \in \mathcal{I}} E_{j,i}(k), \qquad \mathcal{I} := \mathcal{I}_{\lambda,\Lambda} := \{\lambda+1, \lambda+2 \ldots, \Lambda-1\}, \tag{A.1.12}$$

where $M_i(k)$ is defined in (A.1.13), (A.1.14).

Proof. We partition A_1 into subsets $A_{1,j}$ of primes having norm in $[jK, (j+0.5)K]$, and A_2 into subsets $A_{2,j}$ of primes having norm in $[(j+0.5)K, (j+1)K]$ where $\lambda \leq j \leq \Lambda$. Note that $E_{j,i}(k)$ counts how many primes are located in $A_{i,j}$ for $\lambda < j < \Lambda$ and $i = 1, 2$. This gives rise to the term $\sum_{j \in \mathcal{I}} E_{j,i}(k)$. Counting the primes near the end-points $j = \lambda$ and Λ demands more care because one needs to distinguish whether $\alpha - \lambda K \leq 0.5K$ holds or not and whether $\beta - \Lambda K \leq 0.5K$ holds or not in order to start or stop counting with the suitable $A_{i,\lambda}$ or $A_{i,\Lambda}$. Thus, we get four cases to which we shall refer to in the following manner:

Table A.1:

condition	$\alpha - \lambda K \leq 0.5K$	$\alpha - \lambda K > 0.5K$
$\beta - \Lambda K \leq 0.5K$	case (i)	case (iii)
$\beta - \Lambda K > 0.5K$	case (ii)	case (iv)

In view of equation (A.1.12), we can define the proclaimed functions M_i by using (henceforth) the short hand notation $x_j := jK$, $\overline{x}_j := \frac{x_j + x_{j+1}}{2}$ via

$$M_1(k) := \begin{cases} \pi(\overline{x}_\lambda) - \pi(\alpha - 1) + \pi(\beta) - \pi(x_\Lambda) & \text{in case (i)}, \\ \pi(\overline{x}_\lambda) - \pi(\alpha - 1) + E_{\Lambda,1}(k) & \text{in case (ii)}, \\ \pi(\beta) - \pi(x_\Lambda - 1) & \text{in case (iii)}, \\ E_{\Lambda,1}(k) & \text{in case (iv)}, \end{cases} \tag{A.1.13}$$

$$M_2(k) := \begin{cases} E_{\lambda,2}(k) & \text{in case (i)}, \\ E_{\lambda,2}(k) + \pi(\beta) - \pi(\overline{x}_\Lambda) & \text{in case (ii)}, \\ \pi(x_{\lambda+1}) - \pi(\alpha - 1) & \text{in case (iii)}, \\ \pi(x_{\lambda+1}) - \pi(\alpha - 1) + \pi(\beta) - \pi(\overline{x}_\Lambda) & \text{in case (iv)}. \end{cases} \tag{A.1.14}$$

□

It is useful to put $E_j(k) := E_{j,1}(k) - E_{j,2}(k)$, $M(k) := M_1(k) - M_2(k)$, for writing

$$\#A_1 - \#A_2 = M(k) + \sum_{j \in \mathcal{I}} E_j(k). \tag{A.1.15}$$

Moreover, we say an assertion $A(k)$ concerning natural numbers is eventually true if there exists a $k_0 \in \mathbb{N}$ such that $A(k)$ holds true for all $k \geq k_0$.

Proof of Theorem 1.4.1. Since $\alpha = 1$ we may assume $\lambda = 0$, and that either case (i) or (ii) of Table A.1 occurs. Let $0 < \delta \leq 1$ for the moment. Remark 4 gives an approximation for the prime counting function from which we infer

$$M(k) \geq 2\mathrm{li}((0.5K)^\delta) - \mathrm{li}(K^\delta) + E_\Lambda + \mathcal{O}(K^\delta \log^{-\eta}(0.5K)), \qquad \eta > 0. \tag{A.1.16}$$

Moreover, we have

$$2\mathrm{li}((0.5K)^\delta) - \mathrm{li}(K^\delta) = \int_2^{K^\delta} \frac{2^{1-\delta} - 1 + \frac{\delta \log 2}{\log(\tau)}}{\log(2^{-\delta}\tau)} \mathrm{d}\tau, \qquad \delta > 0. \tag{A.1.17}$$

Since the derivative of $x \mapsto \mathrm{li}(x^\delta)$ is eventually decreasing, it follows from the mean value theorem that $2\mathrm{li}(\overline{x}_j^\delta) - \mathrm{li}(x_j^\delta) - \mathrm{li}(x_{j+1}^\delta)$ is eventually positive for any $j \geq 1$. Hence, we conclude that

$$\sum_{j=1}^{\Lambda} E_j(k) > (\Lambda - 1)\, \mathcal{O}(K^\delta \log^{-\eta}(0.5K)), \qquad \eta > 0. \tag{A.1.18}$$

Using Equation (A.1.15) and the above estimate we find that

$$\#A_1 - \#A_2 > \frac{K^\delta \log 2}{\log(K^\delta)\log(0.5K)} + (\Lambda - 1)\, \mathcal{O}(K^\delta \log^{-\eta}(0.5K)), \tag{A.1.19}$$

which proves the claim in the case $0 < \delta \leq 1$. Now let $\delta > 1$. Then the difference $2\mathrm{li}(\overline{x}_j^\delta) - \mathrm{li}(x_j^\delta) - \mathrm{li}(x_{j+1}^\delta)$ is negative for any $j \geq 1$. We note that $M(k)$ is bounded from above by $2\mathrm{li}((0.5K)^\delta) - \mathrm{li}(K^\delta)$ up to an error term

$$\mathcal{O}(K^\delta \log^{-\eta}(0.5K)) + \begin{cases} \mathrm{li}(\beta^\delta) - \mathrm{li}((x_\Lambda - 1)^\delta) & \text{in case (i)}, \\ \mathrm{li}(x_{\Lambda+1}^\delta) - \mathrm{li}(\beta^\delta) & \text{in case (ii)}. \end{cases} \tag{A.1.20}$$

The assumption on β implies that the expressions in the brackets are in $O(K^{\delta-\epsilon})$ for some $\varepsilon > 0$ and hence $O(K^\delta \log^{-\eta}(0.5K))$. Therefore, we obtain from (A.1.17) that for some suitable constant $c > 0$ the estimate

$$M(k) < \frac{-cK^\delta}{\delta \log(K)} + \mathcal{O}(K^\delta \log^{-\eta}(0.5K)) \tag{A.1.21}$$

holds. Because the left hand side of (A.1.18) is bounded by $(\Lambda - 1)\, \mathcal{O}(K^\delta \log^{-\eta}(0.5K))$, we conclude from (A.1.15) that $-\iota < \#A_1 - \#A_2$ is eventually violated. □

A.2 Auxiliary Results

In what follows we investigate conditions for a natural number k to be a P^*-integer. It is important to notice, that M is strictly positive in case (i) and (can be) strictly

negative in case (iv) of table (A.1). Therefore, upper *and* lower bounds are needed, in order to derive the asymptotic of the difference in (A.1.15). In order to prove Theorem 1.4.2, it suffices to derive lower a bound, though upper bounds can be derived in the same way. This is done by the following two results.

Lemma A.2.1. *Let $k \geq 2\,953\,652\,287$, ε as in Lemma A.1.1, $x_j = kj$, and j be a natural number. Define the functions*

$$E_{j,-}(k) := 2\overline{x}_j \frac{1-\varepsilon(\overline{x}_j)}{\log \overline{x}_j} - x_j \frac{1+\varepsilon(x_j)}{\log x_j} - x_{j+1} \frac{1+\varepsilon(x_{j+1})}{\log x_{j+1}}, \tag{A.2.1}$$

and

$$r_j(k) := \frac{k\varepsilon(\overline{x}_j)}{\log^2 \overline{x}_j}, \qquad r_0(k) := 0. \tag{A.2.2}$$

Then the inequality

$$E_{j,-}(k) - r_j(k) < E_j(k) \tag{A.2.3}$$

holds for $j \geq 0$.

Proof. We apply the well-known formula

$$\pi(x) = \frac{\theta(x)}{\log(x)} + \int_2^x \frac{\theta(\tau)}{\tau \log^2 \tau}\,\mathrm{d}\tau \tag{A.2.4}$$

to see that $E_j(k)$ equals the sum

$$\frac{2\theta(\overline{x}_j)}{\log \overline{x}_j} - \frac{\theta(x_j)}{\log x_j} - \frac{\theta(x_{j+1})}{\log x_{j+1}} + \int_{x_j}^{\overline{x}_j} \frac{\theta(\tau)}{\tau \log^2 \tau}\,\mathrm{d}\tau - \int_{\overline{x}_j}^{x_{j+1}} \frac{\theta(\tau)}{\tau \log^2 \tau}\,\mathrm{d}\tau. \tag{A.2.5}$$

Lemma A.1.1 for $j \geq 1$ and Remark 4 for $j = 0$ yield that the first three terms above exceed $E_{j,-}(k)$ for $j \geq 0$. By using Lemma A.1.1, we infer

$$\int_{x_j}^{\overline{x}_j} \frac{\theta(\tau)}{\tau \log^2 \tau}\,\mathrm{d}\tau - \int_{\overline{x}_j}^{x_{j+1}} \frac{\theta(\tau)}{\tau \log^2 \tau}\,\mathrm{d}\tau > \frac{k}{2} \frac{1-\varepsilon(\overline{x}_j)}{\log^2 \overline{x}_j} - \frac{k}{2} \frac{1+\varepsilon(\overline{x}_j)}{\log^2 \overline{x}_j} = r_j(k) \tag{A.2.6}$$

which implies (A.2.3). □

Observing that

$$M(k) = \begin{cases} E_\lambda(k) + \pi(x_\lambda) - \pi(\alpha-1) + \pi(\beta) - \pi(x_\Lambda) & \text{in case (i)}, \\ E_\lambda(k) + \pi(x_\lambda) - \pi(\alpha-1) + 2\pi(\overline{x}_\Lambda) - \pi(x_\Lambda) - \pi(\beta) & \text{in case (ii)} \end{cases} \tag{A.2.7}$$

we derive the following technical but crucial corollary.

Corollary A.2.2. *The term $M(k)$ is bounded from below in the cases $(i)-(ii)$ by $E_{\lambda,-}(k) - r_\lambda(k) - \Delta(\lambda,k) + R(k)$ whereas we put*

$$\Delta(\lambda,k) := -\begin{cases} \pi(\alpha-1) & \text{if } \lambda = 0, \\ \frac{\alpha}{\log x_\lambda}\Big(1 + \tilde{\Delta}(x_\lambda,\alpha)\Big) & \text{if } \lambda > 0, \end{cases} \tag{A.2.8}$$

$R(k) := 0$ in case (i) and $R(k) := E_{\Lambda,-}(k) - r_\Lambda(k)$ in case (ii) and define

$$\tilde{\Delta}(x_-,x_+) := \Big(1 - \frac{x_-}{x_+}\Big)\frac{1+\varepsilon(x_-)}{\log^2 x_-} - \frac{x_-}{x_+} + 2\varepsilon(x_-), \qquad 0 < x_- \leq x_+. \tag{A.2.9}$$

Proof. The inequality

$$\pi(x_+) - \pi(x_-) < \frac{x_+}{\log x_-}\Big(1 + \tilde{\Delta}(x_-, x_+)\Big) \tag{A.2.10}$$

can be deduced from Equation (A.2.4) via

$$\begin{aligned}\pi(x_+) - \pi(x_-) &< x_+\frac{1+\varepsilon(x_+)}{\log x_+} - x_-\frac{1-\varepsilon(x_-)}{\log x_-} + \int_{x_-}^{x_+}\frac{1+\varepsilon\,(t)}{\log^2 t}\,\mathrm{d}t \\ &< \frac{x_+}{\log x_+} - \frac{x_-}{\log x_-} + 2\frac{x_+\varepsilon(x_-)}{\log x_-} + (x_+ - x_-)\frac{1+\varepsilon(x_-)}{\log^2 x_-} \end{aligned} \tag{A.2.11}$$

and bracketing out the term $\frac{x_+}{\log x_-}$ on the right hand side. Let $\lambda \geq 1$. Using the Estimate (A.2.10) with $x_+ := \alpha$ and $x_- := x_\lambda$, we get

$$\pi(\alpha - 1) - \pi(x_\lambda) < \frac{\alpha}{\log x_\lambda}\Big(1 + \Delta(x_\lambda, \alpha)\Big). \tag{A.2.12}$$

In the cases (i), (ii) the claim follows now by

$$E_{\lambda,-}\,(k) + \pi(x_\lambda) = 2\pi(\overline{x}_\lambda) - \pi(x_{\lambda+1}),\ E_{\Lambda,-}\,(k) < 2\pi(\overline{x}_\Lambda) - \pi(x_\Lambda) - \pi(\beta), \tag{A.2.13}$$

and applying Lemma A.2.1. If $\lambda = 0$, then the claim follows in the cases (i), and (ii) directly from the estimate (A.2.13) and Remark 4. □

Since we know explicit bounds for the growth of the term M, we need to derive explicit bounds for

$$\sum_{j\in\mathcal{I}} E_j. \tag{A.2.14}$$

In view of Lemma A.2.1, we can concentrate on dealing with sums

$$\sum_{j=a}^{b} E_{j,-}\,(k)\,. \tag{A.2.15}$$

To this end, we define $f\,(x) := x\,(\log x)^{-1}$, and note that $E_{j,-}\,(k)$ splits into

$$2f(\overline{x}_j) - f(x_j) - f(x_{j+1}) - 2\varepsilon(\overline{x}_j)f(\overline{x}_j) - \varepsilon(x_j)f(x_j) - \varepsilon(x_{j+1})f(x_{j+1}). \tag{A.2.16}$$

Let $E'_j\,(k)$ denote the first three terms above, and let $E''_j\,(k)$ denote the remaining three. For deriving explicit lower and upper bounds for sums over $E_{j,-}\,(k)$, it suffices to deal with the (slightly easier) sums over $E'_j\,(k)$ and $E''_j\,(k)$. This will be done in the following.

Lemma A.2.3. *For natural numbers $a \leq b$ and $k \geq e^4$ we have the following estimate*

$$\frac{8}{k}\sum_{j=a}^{b} E'_j\,(k) > \frac{\log\frac{4b+6}{9a}}{\log^2(x_{b+1})}. \tag{A.2.17}$$

Proof. Let us note that

$$E'_j(k) = \int_{x_j}^{\overline{x}_j} f'(x) - f'(x+0.5k)\,\mathrm{d}x. \tag{A.2.18}$$

Observing that $f'(x) - f'(x+0.5k)$ equals

$$\left(\frac{1}{\log x} - \frac{1}{\log(x+0.5k)}\right)\left(1 - \left(\frac{1}{\log x} + \frac{1}{\log(x+0.5k)}\right)\right) \tag{A.2.19}$$

we infer, since $k \geq e^4$, the inequality

$$\frac{1}{2}\frac{\log(1+\frac{k}{2x})}{\log(x)\log(x+0.5k)} < f'(x) - f'(x+0.5k), \qquad x \in [x_j, \overline{x}_j], \quad j \geq 1. \tag{A.2.20}$$

Integrating with respect to x from x_j to $\overline{x}_j$, in view of (A.2.18), and summing over j yields

$$\frac{k}{4}\sum_{j=a}^{b}\frac{\log(1+\frac{1}{2j+2})}{\log(\overline{x}_j)\log(x_{j+1})} < \sum_{j=a}^{b} E'_j(k). \tag{A.2.21}$$

By using partial summation, we obtain

$$\sum_{j=a}^{b}\frac{\log(1+\frac{1}{2j+2})}{\log^2(x_{j+1})} > \frac{\log\prod_{s=a}^{b}\frac{2(s+1)+1}{2(s+1)}}{\log^2(x_{b+1})}. \tag{A.2.22}$$

The estimates (A.1.4) imply that the product in the numerator above can be bounded from below by $(4b+6)^{0.5}(9a)^{-0.5}$. Therefore, we obtain (A.2.17) from (A.2.22). □

With the above estimates at hand, we can derive lower bounds on (A.2.15).

Corollary A.2.4. *Let $j \geq 1$, $a \leq b$ denote natural numbers and $\sigma_{a,b} := \sum_{j=a}^{b} j$. Then*

$$\sum_{j=a}^{b}\frac{E_{j,-}(k) - r_j(k)}{k} > \frac{\log\frac{4b+6}{9a}}{8\log^2(x_{b+1})} - 5\frac{\varepsilon(x_a)}{\log(x_a)}\sigma_{a+1,b+1} \tag{A.2.23}$$

holds.

Proof. Let us note that

$$\sum_{j=a}^{b}\frac{\varepsilon(x_j)j}{\log(x_j)} < \frac{\varepsilon(x_a)}{\log(x_a)}\sigma_{a,b} \quad \text{and} \quad \sum_{j=a}^{b}\frac{\varepsilon(\overline{x}_j)(j+0.5)}{\log(\overline{x}_j)} < \frac{\varepsilon(x_a)}{\log(x_a)}\sigma_{a+1,b+1} \tag{A.2.24}$$

hold. Observing $\sigma_{a+1,b+1} \geq \sigma_{a,b}$ implies

$$\frac{1}{k}\sum_{j=a}^{b} E''_j(k) < 4\frac{\varepsilon(x_a)}{\log(x_a)}\sigma_{a+1,b+1}. \tag{A.2.25}$$

By using (A.2.17) and (A.2.25), we deduce

$$\frac{1}{k}\sum_{j=a}^{b}(E'_j(k) - E''_j(k)) > \frac{\log\frac{4b+6}{9a}}{8\log^2(x_{b+1})} - 4\frac{\varepsilon(x_a)}{\log(x_a)}\sigma_{a+1,b+1}. \tag{A.2.26}$$

Combining this inequality with the obvious upper bounds for $\frac{1}{k}\sum_{j=a}^{b} r_j(k)$ while using $\sigma_{a+1,b+1} \geq (b-a+1)$ yields the claim. □

A.3 Proof of Theorem 1.4.2

Proof of Theorem 1.4.2. It suffices to establish that

$$S(k) := \#A_1 - \#A_2 - \iota \tag{A.3.1}$$

is eventually strictly positive. Assume for the moment that we are in the cases (i) or (ii) of Table A.1. Equation (A.1.15) and Lemma A.2.1 imply

$$S(k) > M(k) - \iota + \sum_{j\in\mathcal{I}}(E_{j,-}(k) - r_j(k)). \tag{A.3.2}$$

By using Corollary A.2.2, we deduce that $S(k)$ exceeds

$$R(k) - \Delta(\lambda, k) - \iota + \sum_{j=\lambda}^{\Lambda-1}(E_{j,-}(k) - r_j(k)). \tag{A.3.3}$$

Let $\lambda \geq 1$ and define $b = \Lambda - 1$ in case (i) and $b = \Lambda$ in case (ii). Then applying Corollary A.2.4 with $a = \lambda$, b yields that it suffices to check whether

$$-\frac{\alpha}{k}\frac{1+\tilde{\Delta}(x_\lambda,\alpha)}{\log x_\lambda} - \frac{\iota}{k} + \frac{\log\frac{4b+6}{9\lambda}}{8\log^2(x_{b+1})} - 5\frac{\varepsilon(k)}{\log(k)}\sigma_{1,b+1} > 0. \tag{A.3.4}$$

As $x_\lambda\alpha^{-1} - 1 < Ck^{-d_1}$ holds for some $C > 0$, there is an explicitly computable $C_1 > 0$ such that $1 + \tilde{\Delta}(x_\lambda, \alpha) < C_1\varepsilon(k)$. Hence, we can estimate the left hand side of (A.3.4) from below by

$$-C\varepsilon(k) - \frac{\iota}{k} + \frac{\log\frac{4b+6}{9\lambda}}{8\log^2(x_{b+1})} - \frac{5\varepsilon(k)}{\log(k)}\sigma_{1,b+1}. \tag{A.3.5}$$

Using the bounds $b + 2 \leq C_3\log^{d_3} k$, $\iota < C_2k^{1-d_2}$ with some $C_2, C_3 > 0$ yields that it suffices to prove that

$$\frac{\log\frac{4b+6}{9\lambda}}{8\log^2(x_{b+1})} - \frac{5}{4}\varepsilon(k)C_3^2\log^{2d_3-1}(k) - C_1\varepsilon(k) - \frac{C_2}{k^{d_2}} > 0 \tag{A.3.6}$$

is positive. This is certainly true for sufficiently large k if we can establish that $\frac{4b+6}{9\lambda}$ exceeds 1 eventually. Since for a P^*-integer $\gamma \geq 1$ implies $\beta \geq p_{\varphi(k)}$, we conclude from Remark 4 that

$$\beta > \varphi(k)\log\varphi(k) \gg k\frac{\log k}{\log\log k}. \tag{A.3.7}$$

Hence, b can be assumed to be arbitrarily large, as desired. Now let $\lambda = 0$. Applying Corollary A.2.4 with $a = 1$, and b as before, we deduce from (A.3.3) that it suffices to check whether

$$E_{0,-}(k) - \frac{\pi(\alpha)+\iota}{k} + \frac{\log\frac{4b+6}{9}}{8\log^2(x_{b+1})} - 5\frac{\varepsilon(k)}{\log(k)}\sigma_{1,b+1} > 0. \tag{A.3.8}$$

Since $\pi(\alpha) < C_1 k^{1-d_1}$, $\iota < C_2 k^{1-d_2}$ and $\sigma_{1,b+1} \leq C_3^2 \log^{2d_3-1} k$ we see that we need to check

$$E_{0,-}(k) + \frac{\log \frac{4b+6}{9}}{8 \log^2(x_{b+1})} - 5\varepsilon(k) C_3^2 \log^{2d_3-1} k - C_1 k^{-d_1} - C_2 k^{-d_2} > 0, \qquad \text{(A.3.9)}$$

which is satisfied for sufficiently large k. This proves the claim in the cases (i) or (ii). In the case (iii) or (iv), we write $\alpha = x_\lambda - \Delta$ for some $0 < \Delta = O(k^{1-d_1})$. In comparison to $S(k)$ in the cases (i) and (ii), we have to add the additional expression $E = \pi(x_\lambda + \Delta) - \pi(x_\lambda) - (\pi(x_\lambda) - \pi(x_\lambda - \Delta))$ to the former $S(k)$. One checks easily that $E = O(x_\lambda \varepsilon(x_\lambda))$. Hence, E can not effect the sign of $S(k)$ for large k in the cases (i) and (ii) since its order is lower than the order of $S(k)$, as we see by considering the terms in (A.3.6) and (A.3.9). This completes the proof. □

Using the above proof we can state explicit bounds on certain kinds of P^*-integers.

Corollary A.3.1. *Let $b + 2 \leq C_3 \log^{d_3} k$, $\iota < C_2 k^{1-d_2}$ with some $C_2, C_3 > 0$. Under the assumptions of Theorem 1.4.2 there is an effectively computable number $C_0 > 0$ such that every natural number $k \geq C_0$ satisfying (A.3.6) if $\lambda \geq 1$, or (A.3.9) if $\lambda = 0$ is not such a $P(\alpha, \beta, \gamma, \iota)$-integer.*

Remark 5. *Let us add some further comments:*

- It poses no general problem to modify our arguments to study the distribution of other sequences in residue classes, since we essentially employed the euclidean structure, properties of the norm function, and the growth properties of the prime counting function. E.g. one can derive similar results about the distribution of numbers or elements with s prime factors where s is a fixed natural number, while considering semi-groups with the just mentioned properties.

- Moreover, one could slightly relax the growth restriction in Theorem 1.4.2 and still conclude finiteness of such P^*-integers. However, this would only complicate the technical aspects of the proof and bring no deeper insight.

Appendix B

The Maximal Order of Iterated Multiplicative Functions

The present chapter is based on joint work with **Christian Elsholtz**, and **Marc Technau** [41].

Following Wigert, a great number of authors including Ramanujan, Gronwall, Erdős, Ivić, Heppner, J. Knopfmacher, Nicolas, Schwarz, Wirsing, Freiman, Shiu et al. determined the maximal order of several multiplicative functions, generalizing Wigert's result

$$\max_{n\leq x} \log d(n) = (\log 2 + o(1))\frac{\log x}{\log\log x}.$$

On the contrary, for many multiplicative functions, the maximal order of iterations of the functions remains wide open. The case of the iterated divisor function was only recently solved, answering a question of Ramanujan (1915). Here, we determine the maximal order of $\log f(f(n))$ for a class of multiplicative functions f which are related to the divisor function. As a corollary, we apply this to the function counting representations as sums of two squares of non-negative integers, also known as $r_2(n)/4$, and obtain an asymptotic formula:

$$\max_{n\leq x} \log f(f(n)) = (c + o(1))\frac{\sqrt{\log x}}{\log\log x},$$

with some explicitly given positive constant c.

B.1 Hypotheses and results

In what follows, we give a description of a class of arithmetic functions for which we can determine the maximal order of its first iterate. The imposed restrictions could be relaxed somewhat, but our main objective here is to deal with the function δ. The important features here are the following: δ is a multiplicative function which acts affinely on the exponents of primes q from a certain subset of primes $Q \subseteq \mathbb{P}$ (in this case, primes $\equiv 1 \bmod 4$), and takes only the values $0, 1$ on powers of primes

$p \in \mathbb{P} \setminus Q$ (subject to a rule which, as it turns out, is not important for the problem under consideration, provided that Q is not too sparse, see Assumption (A.1) in Section B.1).

In [29], the case $Q = \mathbb{P}$ with the multiplicative arithmetic function d acting as $d(p^\nu) = \nu + 1$ was studied. By elaborating on their method, we obtain upper and lower bounds on the maximal order of first iterates of arithmetic functions which enjoy similar properties as those observed from d and δ, see Theorem B.1.1 and Theorem B.1.2. In particular, we determine the maximal order of $\delta \circ \delta$ in Corollary B.1.4. This also works for other functions, see Corollary B.1.3.

In detail, we start with a strictly increasing sequence of primes $(q_j)_{j\geq 1}$. As for the sequence of all primes we know $q_j = j(\log j + \log(\log j) + \mathcal{O}(1))$, due to the prime number theorem; a somewhat regular subsequence of the primes, with some positive density of the primes, will obtain $q_j = \tau j(\log j + \log(\log j) + \mathcal{O}(1))$, where τ is the inverse density of Q in $\mathbb{P}$, compare (A.1)) below.

Set $Q = \{q_j : j \in \mathbb{N}\}$ and let $\langle Q \rangle$ be the monoid (multiplicatively) generated by Q. Furthermore, fix a map $g : \mathbb{N}_0 \to \mathbb{N}$ with $g(0) = 1$ and let[1]

$$g^\dagger(y) = \inf\{x \in \mathbb{N} : g(x) = y\}. \tag{B.1.1}$$

Finally, assume that

1. $(q_j)_{j\geq 1}$ satisfies the asymptotic expansion

   $$q_j = \tau j\Big(\log j + \log(\log j) + \mathcal{O}(1)\Big),$$

   where $\tau > 0$ is some constant,

2. g is monotonically increasing,

3. $g(\mathbb{N}) \supseteq \langle Q \rangle$,

4. $g^\dagger(b) + c_* b g^\dagger(a) \leq g^\dagger(ab)$ for all $a, b \in \langle Q \rangle$ such that $q_1 \leq a \leq b$, where $c_* > 1/q_1$ is some constant,

5. $g(i)/g(i-1) = 1 + \mathcal{O}(i^{-1/2-\epsilon})$ for some $\epsilon > 0$,

6. $g(x) \leq c_f x$ for all $x \in \mathbb{N}$, where $c_f > 0$ is some constant,

7. $g^\dagger(q) = c_\dagger q + \mathcal{O}(q/\log q)$ as $Q \ni q \to \infty$, where $c_\dagger > 0$ is some constant. (Note that $g^\dagger(q)$ is finite due to (A.3).)

Now let f be a multiplicative arithmetic function satisfying

$$f(p^\nu) \begin{cases} = g(\nu) & \text{if } p \in Q, \\ \in \{0, 1\} & \text{if } p \notin Q \end{cases} \tag{B.1.2}$$

[1]The symbol $g^\dagger$ was chosen to allude to a pseudo inverse.

for a prime power $p^\nu \geq 1$. Furthermore, let $f(0) = 1$. We write

$$M(x) = \max_{n \leq x} \log f(f(n)). \tag{B.1.3}$$

On writing $\log_k$ for the k-fold iterate of the natural logarithm, our main results may now be stated as follows:

Theorem B.1.1. *Let M be as in (B.1.3). Then,*

$$M(x) \leq \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C}{\sqrt{\tau c_\dagger}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right), \tag{B.1.4}$$

where the implied constant depends on Q, f and

$$C = \left(8\sum_{j\geq 1}\left(\log\frac{g(j)}{g(j-1)}\right)^2\right)^{1/2}. \tag{B.1.5}$$

Throughout the rest of the chapter, C will always denote the constant defined in (B.1.5). We also note in passing that throughout all implied constants may depend on the function f and the set Q and an ϵ, where obvious.

Theorem B.1.2. *Letting $g(\nu) = \alpha\nu + 1$ on the above hypotheses, the following holds*

$$M(x) \geq \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C}{\sqrt{\tau/\alpha}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right). \tag{B.1.6}$$

Upon combining Theorem B.1.1 and Theorem B.1.2, we immediately deduce the following corollary:

Corollary B.1.3. *Letting $g(\nu) = \alpha\nu+1$ for some $\alpha \in \mathbb{N}$, and on the above hypotheses, it holds that*

$$M(x) = \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C}{\sqrt{\tau/\alpha}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right).$$

Observe that, in the case $Q = \mathbb{P}$, the function f in the setting of Corollary B.1.3 arise naturally as number of divisors of monic monomials, i.e.,

$$f(n) = d(n^\alpha).$$

Turning back to the function δ given by (1.5.1), and recalling (1.5.3), we obtain the following result:

Corollary B.1.4. *Let δ be given by* (1.5.1)*. Then*

$$\max_{n\leq x} \log \delta(\delta(n)) = \frac{\sqrt{\log x}}{\log_2 x}\left(\frac{C}{\sqrt{2}} + \mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right).$$

B.2 Preliminaries

B.2.1 Notation

At this point it is convenient to introduce some additional notation used throughout the rest of the chapter. We usually use the letter ν to denote an exponent in the prime factorisation of some integer. We write ν_i if the primes in this factorisation are indexed by i and we write $\nu_p(\,\cdot\,)$ for the p-adic valuation. Additionally, let

- $\Omega(n) = \sum_{p|n} \nu_p(n)$, $\omega(n) = \sum_{p|n} 1$,
- $\Pi_Q(n) = \max\{m \in \langle Q \rangle : m \mid n\}$,
- $\Omega_Q = \Omega \circ \Pi_Q$
- $\omega_Q = \omega \circ \Pi_Q$,
- $\pi_Q(x) = \#\{q \in Q : q \leq x\}$.

B.2.2 Auxilliary results

We would like to give the reader our perspective on the problem at hand. In order to keep the notation simple, let $Q = \mathbb{P}$ for the moment. Then, for any positive integer n,

$$\log f(f(n)) = \sum_{\substack{q \in Q \\ q | f(n)}} \log g\Big(q^{\nu_q(f(n))}\Big).$$

Vaguely speaking, in order to give estimates on $M(x)$, one needs to exhibit some control over the prime factors of integers N, which appear as values $N = f(n)$ for $n \leq x$. This sort of control is provided by Lemma B.2.1.

Additionally, one might like to remove g from the above sum and perhaps also take advantage of the fact that (weighted) sums of $\nu_q(f(N))$ over q are more readily controlled than values of $\nu_q(f(N))$ for some individual q. Lemma B.2.2 makes this happen and is the source of the main term in Theorem B.1.1 and Theorem B.1.2.

Finally, Lemma B.2.3 is a technical tool used to handle the case when $N = f(n)$ does not have sufficiently many prime factors q with small exponent $\nu_q(N)$.

Lemma B.2.1. *For an $N \in \langle Q \rangle$, let m_N be the least positive integer m such that $f(m) = N > 1$. Then*

1. *$m_N = q_1^{\nu_1} \cdots q_r^{\nu_r}$ for some ν_j where $\nu_1 \geq \ldots \geq \nu_r$,*
2. *if N' divides N, then $m_{N'} \leq m_N$,*
3. *if $q_j > q_{r+1}^{1/s_k}$ for some $j \leq r$, then $\Omega(g(\nu_j)) \leq k$, where $s_k = c_* q_1^k$.*

Proof. Pick some $p \notin Q$ and let $\nu = \nu_p(m_N)$. Then $1 < N = f(m_N) = f(p^\nu) f(m_N/p^\nu)$, so that $m_N = m_N/p^\nu$. Hence, $\nu = 0$ and $p \nmid m_N$. Now, writing $m_N = q_1^{\nu_1} \cdots q_r^{\nu_r}$, note that one can permute the exponents without changing the value under f. Therefore, by minimality of m_N, we must have $\nu_1 \geq \ldots \geq \nu_r$. This proves (1).

Turning to (2), if we write $m_N = q_1^{\nu_1} \cdots q_r^{\nu_r}$, then $N = \prod_{j \leq r} g(\nu_j)$, and since $N' \mid N$ there is a partition $\nu_k = \nu_{k,1} + \ldots + \nu_{k,r}$ such that $N'_j = \prod_{k \leq s} q_k^{\nu_{k,j}} \mid g(\nu_j)$. By Assumption (A.3) on g, the value N'_j is attained by g. Hence, we may look at $m_* = q_1^{\nu'_1} \cdots q_r^{\nu'_r}$, where $\nu'_j = g^\dagger(N'_j)$. Clearly, $f(m_*) = N'$, and, by monotonicity of g, $\nu'_j \leq \nu_j$, so that $m_{N'} \leq m_* \leq m_N$.

To prove (3), let us assume for the sake of contradiction that $q_j > q_{r+1}^{1/s_k}, \Omega_Q(g(\nu_j)) > k$. Then there is a decomposition $\Pi_Q(g(\nu_j)) = ab$, where $a \geq q_1$, $b \geq q_1^k$. Now consider

$$m^* = q_j^{g^\dagger(b)} q_{r+1}^{g^\dagger(a)} \prod_{i \neq j} q_i^{\nu_i}.$$

Evidently, $f(m^*) = f(m_N) = N$ and

$$\frac{m^*}{m_N} = q_j^{g^\dagger(b) - \nu_j} q_{r+1}^{g^\dagger(a)} \leq q_j^{-c_* g^\dagger(a) b} q_{r+1}^{g^\dagger(a)}.$$

since (A.4) implies

$$g^\dagger(b) - \nu_j \leq g^\dagger(b) - g^\dagger(ab) = g^\dagger(b)\left(1 - \frac{g^\dagger(ab)}{g^\dagger(b)}\right) \leq -c_* g^\dagger(a) b,$$

which, by assumption, is $\leq -c_* q_1^k$. But this shows that $m^* < m_N$, which contradicts the definition of m_N. Hence, $\Omega_Q(g(\nu_j)) \leq k$. □

Lemma B.2.2. *Let $\nu_1, \ldots, \nu_t$ be positive integers. Then*

$$\sum_{j \leq t} \log g(\nu_j) \leq \frac{C}{2} \left(\sum_{j \leq t} j \nu_j \right)^{1/2}, \tag{B.2.1}$$

where C is given by (B.1.5).

If additionally $\nu_t \geq \nu$, then

$$\sum_{j \leq t} \log g(\nu_j) \ll \sqrt{\frac{1}{\nu^{2\epsilon}} + \frac{(\log g(\nu))^2}{\nu}} \left(\sum_{j \leq t} j \nu_j \right)^{1/2},$$

with ϵ from (A.5).

Proof. (Compare [29, Lemma 3.3].) First note that the right hand side of (B.2.1) is minimal if the ν_js are decreasing. Hence, we may subsequently assume that $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_t$. Let $y_i = \#\{j : \nu_j \geq i\}$ and observe that

$$\sum_{j \leq t} j \nu_j = \sum_{j \leq t} \sum_{i \leq \nu_j} j = \sum_{i \geq 1} \sum_{j \leq y_i} j = \frac{1}{2} \sum_{i \geq 1} y_i (y_i + 1) \geq \frac{1}{2} \sum_{i \geq 1} y_i^2. \tag{B.2.2}$$

By partial summation,

$$\sum_{j\le t}\log g(\nu_j)=\sum_{i\ge 1}(y_i-y_{i+1})\log g(i)=\sum_{i\ge 1}y_i\log\frac{g(i)}{g(i-1)}. \tag{B.2.3}$$

The first claim now follows by applying the Cauchy–Schwarz inequality to the right hand side, and taking (B.2.2) into account.

Moreover, if $\nu_t\ge\nu$, then $y_1=y_2=\ldots=y_\nu$ and

$$\sum_{i\le A}y_i\log\frac{g(i)}{g(i-1)}=y_1\log g(\nu).$$

By splitting up the sum in (B.2.3) in sums over the ranges $i\le\nu$ and $i>\nu$, and applying the Cauchy–Schwarz inequality, we obtain

$$\sum_{j\le t}\log g(\nu_j)\le\left(\sum_{i\ge 1}y_i^2\right)^{1/2}\left(\frac{(\log g(\nu))^2}{\nu}+\sum_{i>\nu}\left(\log\frac{g(i)}{g(i-1)}\right)^2\right)^{1/2}.$$

By (A.5) and $\log(1+1/i)<1/i$, the second sum is $\ll\nu^{-2\epsilon}$. In view of (B.2.2), we have established the second claim. □

Lemma B.2.3. *For every $\varepsilon>0$, and $s:=\omega_Q(n)\ge 2$,*

$$f(n)\ll\left(\frac{(c_f+\varepsilon)\log n}{s\log s}\right)^s.$$

Proof. See [29, Lemma 3.2] and, recalling that there g is $x\mapsto x+1$, use (A.6) instead of $x+1\le 2x$. □

B.3 Proof of Theorem B.1.1

Let n be a positive integer such that $f(f(n))>1$ and $N=\Pi_Q(f(n))$. As before, $f(f(n))=f(N)$.

We now write N as a product of powers of elements in Q and split these into two groups according to the size of their exponents. More precisely, we write $N=N'N''$, where

$$N'=u_1^{b_1}\cdots u_w^{b_w},\quad N''=v_1^{a_1}\cdots v_s^{a_s}$$

and $u_1<\ldots<u_w$, $v_1<\ldots<v_s$ all belong to Q, are all distinct, and $a_i\le(\log_2 n)^K$ and $b_i>(\log_2 n)^K$, for $K=\max\{6,2/\epsilon\}$, with ϵ is from (A.5).

Clearly, $\log f(N)=\log f(N')+\log f(N'')$, so that it suffices to deal with $f(N')$ and $f(N'')$ separately, as we shall do in the subsequent subsections. The main term in (B.1.4) comes from $\log f(N'')$, see (B.3.3), and the term $\log f(N')$ is seen to be somewhat smaller, see (B.3.1).

B.3.1 Bounding $f(N')$

Write $m_{N'} = q_1^{\beta_1} \cdots q_h^{\beta_h}$. Due to Lemma B.2.1 (2) we have $m_{N'} \le m_N \le n$ and, hence, $h \ll \log n$. Lemma B.2.1 (3) yields $\Omega(g(\beta_i)) \ll \log_2 h \ll \log_3 n$ for every i. Therefore, there are $\gg b_j / \log_3 n$ values of i such that $u_j \mid g(\beta_i)$. Furthermore, assuming, as we may, that n is sufficiently large, Lemma B.2.2 with $\nu = \lfloor (\log_2 n)^K \rfloor$ shows that, for $\epsilon' = K/2 - 2$,

$$\log f(N') = \sum_{j \le w} \log g(b_j) \ll (\log_2 n)^{-\min\{\epsilon K, 2\}} \left(\sum_{j \le w} j b_j \right)^{1/2}.$$

Moreover,

$$\begin{aligned} \frac{1}{\log_3 n} \sum_{j \le w} j b_j &\le \sum_{j \le w} \frac{u_j b_j}{\log_3 n} \\ &\ll \sum_{i \le h} \sum_{p \mid g(\beta_i)} p \le \sum_{i \le h} g(\beta_i) \\ &\ll \sum_{i \le h} \beta_i \ll \log m_{N'} \le \log n. \end{aligned}$$

Hence,

$$\log f(N') \ll \frac{\sqrt{(\log n) \log_3 n}}{(\log_2 n)^2}. \tag{B.3.1}$$

B.3.2 Bounding $f(N'')$

To estimate $f(N'')$ we may assume that

$$s > \frac{\sqrt{\log n}}{(\log_2 n)^{K/2}}, \tag{B.3.2}$$

for otherwise Lemma B.2.3 implies that

$$\log f(N'') \ll \frac{\sqrt{\log n}}{(\log_2 n)^{K/2-1}}.$$

We shall prove the following proposition that is crucial for estimating $f(N')$; it is, relating the upper bound appearing after exploiting Lemma B.2.2 with $m_{N''}$. However, the argument is more involved than above.

Proposition B.3.1. *Let $K = \max\{6, 2/\epsilon\}$, with ϵ is from* (A.5). *Suppose $N'' = v_1^{a_1} \cdots v_s^{a_s}$ where $u_1 < \ldots < u_w$, $v_1 < \ldots < v_s$ all belong to Q, are all distinct, and $a_i \le (\log_2 n)^K$, and s satisfies (B.3.2). Then,*

$$\log m_{N''} \ge \left(1 + \mathcal{O}\left(\frac{\log_3 n}{\log_2 n}\right)\right) c_\dagger \tau \frac{(\log_2 n)^2}{4} \sum_{j \le s} j a_j.$$

Let us suppose for the moment that Proposition B.3.1 is proved, we can conclude by Lemma B.2.1 (2) that

$$\log n \geq \log m_{N''} \geq \left(1 + \mathcal{O}\left(\frac{\log_3 n}{\log_2 n}\right)\right) c_\dagger \tau \frac{(\log_2 n)^2}{4} \sum_{j \leq s} j a_j.$$

Inequality (B.2.1) implies that

$$\log f(N'') \leq \frac{\sqrt{\log n}}{\log_2 n}\left(\frac{C}{\sqrt{c_\dagger \tau}} + \mathcal{O}\left(\frac{\log_3 n}{\log_2 n}\right)\right), \tag{B.3.3}$$

which concludes the proof of Theorem B.1.1.

Proof of Proposition B.3.1. Denote by $m_{N''} = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ the minimal element of $f^{-1}(N'')$, as in Lemma B.2.1. Our first goal is to establish that r cannot be too small. By Lemma B.2.1, and letting $s_0 = 1$ for the moment, the last sum in

$$\Omega(N'') = \sum_{j \leq s} a_j = \sum_{i \leq r} \Omega(g(\alpha_i)) \tag{B.3.4}$$

is seen to be

$$= \sum_{k \geq 1} k\Big(\pi_Q\Big(q_{r+1}^{1/s_{k-1}}\Big) - \pi_Q\Big(q_{r+1}^{1/s_k}\Big)\Big) = r + 1 + \sum_{k \geq 1} \pi_Q\Big(q_{r+1}^{1/s_k}\Big) =: r + E.$$

To handle E, we split the term for $k = 1$ from the sum and estimate the rest trivially, thereby obtaining $E \ll \pi\Big(q_{r+1}^{1/s_1}\Big)$. Also, by (B.3.4), $\Omega(N'') \geq r$, so that

$$\Omega(N'') = r + \mathcal{O}\Big(\pi\Big(q_{r+1}^{1/c_* q_1}\Big)\Big). \tag{B.3.5}$$

Hence,

$$r \leq \Omega(N'') \leq r + r^\theta, \tag{B.3.6}$$

where $\theta \in (1/c_* q_1, 1)$ is some constant (recall that by (A.4) this interval is non-empty). In particular, $r \gg s$ so that by (B.3.2), r must be large if n is sufficiently large. The next goal is to determine $g(\alpha_i)$ for all i in a suitable range. To this end, first note that by Lemma B.2.1 (3) we find that $g(\alpha_i)$ is prime for all $i > r^\theta$. Let $\varepsilon = (3K+1)(\log_3 n)/\log_2 n$, and assume that n is sufficiently large as to ensure that $\varepsilon < 1 - \theta$. By (B.3.2),

$$2r^\theta \leq 2(\Omega(N''))^\theta \leq 2\Big(s(\log_2 n)^K\Big)^\theta \leq s^{1-\varepsilon} \leq \sum_{s - s^{1-\varepsilon} < j < s} a_j, \tag{B.3.7}$$

for n sufficiently large. Hence,

$$\sum_{j \leq s - s^{1-\varepsilon}} a_j \leq \Omega(N'') - 2r^\theta \leq r - r^\theta. \tag{B.3.8}$$

As explained above, $g(\alpha_i)$ is prime for all $i > r^\theta$ and from (B.3.8) we know that this surely is the case for all $i \geq r - \sum_{k \leq j} a_k$, where $j \leq s - s^{1-\varepsilon}$. Since, by

Lemma B.2.1 (1) the values $g(\alpha_i)$ are decreasing as i increases this yields that $g(\alpha_i) = v_j$ for $r - \sum_{k\le j} a_k < i \le r - \sum_{k<j} a_k$. By (B.3.6) and (B.3.7),

$$r - \sum_{k\le j} a_k = r - \Omega(N'') + \sum_{k\le s-j} a_{j+k} \ge s - j - r^\theta \ge \frac{1}{2}s^{1-\varepsilon}. \tag{B.3.9}$$

From (A.7) and (A.1) we deduce that

$$g^\dagger(q_j) \ge c_\dagger q_j + \mathcal{O}(q_j/\log q_j) \ge c_\dagger \tau j \log j \tag{B.3.10}$$

for all sufficiently large j. Hence, by (B.3.10) and (B.3.9),

$$\log m_{N''} \ge c_\dagger \tau \sum_{s^{1-\varepsilon}\le j\le s-s^{1-\varepsilon}} j(\log j)a_j(\log s + \mathcal{O}(\log_3 n)).$$

By (B.3.2), we find that the right hand side above exceeds

$$\begin{aligned}&\sum_{s^{1-\varepsilon}\le j\le s-s^{1-\varepsilon}} (1-\varepsilon)(\log s)^2 j a_j\left(1+\mathcal{O}\left(\frac{\log_3 n}{\log s}\right)\right)\\ &\ge \sum_{s^{1-\varepsilon}\le j\le s-s^{1-\varepsilon}} (1+\mathcal{O}(\varepsilon))(\log_2 n)^2 j a_j.\end{aligned}$$

By the choice of ε, we get $s^\varepsilon \gg (\log_2 n)^{-K-1}$. Also, $\sum_{j\le s} ja_j \ge \frac{1}{2}s^2$. Now recalling that $a_j \le (\log_2 n)^K$ for every j, we infer that

$$\begin{aligned}\sum_{s^{1-\varepsilon}\le j\le s-s^{1-\varepsilon}} ja_j &= \sum_{j\le s} ja_j + \mathcal{O}\Big(s^{2-\varepsilon}(\log_2 n)^K\Big)\\ &= \left(1+\mathcal{O}\left(\frac{1}{\log_2 n}\right)\right)\sum_{j\le s} ja_j,\end{aligned}$$

thus completing the proof. □

B.4 Proof of Theorem B.1.2

Recall that the main term in the upper bound in Theorem B.1.1 stems from an application of Lemma B.2.2. Given some large $x > 1$, we wish to find an integer n smaller than x, such that

$$\log f(f(n)) = \sum_{\substack{q\in Q\\ q\mid f(n)}} \log g(\nu_q(f(n)))$$

is large, the idea is to realise equality in Lemma B.2.2. Therefore, recalling that the inequality was obtained by applying the Cauchy–Schwarz inequality to (B.2.3), we would like to have

$$\#\{q\in Q : \nu_q(f(n)) \ge i\} \approx \text{const} \times \log\frac{g(i)}{g(i-1)} \quad (i \ge 1)$$

with some constant, independent of i. Furthermore, to have suitable control over $f(n)$ it seems reasonable to choose n such that the factorisation of $f(n)$ is known. With this in mind, let $\varepsilon = c_{\mathrm{e}}\frac{\log_3 x}{\log_2 x}$ for c_{e} sufficiently large, where

$$t = \left\lfloor \left(\frac{8 \log g(1)}{C} - \varepsilon \right) \frac{\sqrt{\log x}}{\log_2 x} \right\rfloor,$$

and consider

$$\nu_j \coloneqq \left\lfloor 1 - \frac{1}{\alpha} + \frac{1}{(\alpha+1)^{j/t} - 1} \right\rfloor \quad (1 \le j \le t).$$

Evidently,

$$\nu_j = \frac{1}{\log(\alpha+1)} \frac{t}{j} + \mathcal{O}(1) \tag{B.4.1}$$

Letting

$$n = \prod_{j \le t} \prod_{i \le \nu_j} q_{\nu_1 + \ldots + \nu_{j-1} + i}^{g^\dagger(q_j)},$$

we find that

$$f(n) = \prod_{j \le t} g(g^\dagger(q_j))^{\nu_j} = \prod_{j \le t} q_j^{\nu_j}.$$

Now it remains to give a good lower bound on $\log f(f(n))$ and an upper bound on n. To obtain the upper bound, let

$$y_i = \#\{j : \nu_j \ge i\} = \left\lfloor \frac{t}{\log(\alpha+1)} \log\Big(1 + \frac{1}{i - 1 + \alpha^{-1}}\Big) \right\rfloor. \tag{B.4.2}$$

Observe that $\nu_1 + \ldots + \nu_t \ll t \log t$. Using (A.1) we find that

$$\log q_{\nu_1 + \ldots + \nu_t} \le \log t + 2 \log_2 t + \mathcal{O}(1).$$

Hence,

$$\begin{aligned} \log n &\le \sum_{j \le t} \nu_j g^\dagger(q_j) \log q_{\nu_1 + \ldots + \nu_j} \\ &\le \frac{\tau}{\alpha} \Big((\log t)^2 + 3(\log_2 t) \log t + \mathcal{O}(\log t) \Big) \sum_{j \le t} j \nu_j. \end{aligned}$$

Since $y_i = \mathcal{O}(t/i)$ and by (B.4.1) and (B.1.5),

$$\begin{aligned} \sum_{j \le t} j \nu_j &= \frac{1}{2} \sum_{i \le \nu_1} y_i (y_i + 1) \\ &= \frac{t^2}{2(\log(\alpha+1))^2} \sum_{i=1}^{\infty} \Big(\log\Big(1 + \frac{1}{i - 1 + \alpha^{-1}}\Big) \Big)^2 + \mathcal{O}(t \log t) \\ &= \frac{t^2 C^2}{16(\log(\alpha+1))^2} + \mathcal{O}(t \log t). \end{aligned}$$

By the definition of t, $\log t = \frac{1}{2}\log_2 x - \log_3 x + \mathcal{O}(1)$ and $\log_2 t = \log_3 x + \mathcal{O}(1)$. By choosing c_{e} sufficiently large, we get

$$\left(1+\mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right)\left(1-\frac{Cc_{\mathrm{e}}}{8\log(\alpha+1)}\frac{\log_3 x}{\log_2 x}\right)^2 \le 1.$$

Thus, we infer

$$\log n \le \frac{\tau}{\alpha}\left(1+\mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right)\left(1-\frac{\varepsilon C}{8\log(\alpha+1)}\right)^2 \log x$$

so that $n \le x^{\tau/\alpha}$ if x is sufficiently large. Next, we estimate $\log f(f(n))$: Using partial summation and (B.4.2),

$$\begin{aligned}\log f(f(n)) &= \sum_{j\le t}\log g(\nu_j) = \sum_{i\ge 1}(y_i - y_{i+1})\log g(i)\\ &= \sum_{i\ge 1} y_i \log\frac{g(i)}{g(i-1)}.\end{aligned}$$

Due to the construction of n the last sum simplifies to:

$$\begin{aligned}&\sum_{i\le\nu_1} y_i \log\frac{g(i)}{g(i-1)}\\ &= \sum_{i\le\nu_1}\left(\frac{t}{\log(\alpha+1)}\left(\log\frac{g(i)}{g(i-1)}\right)^2 + \mathcal{O}(1/i)\right)\\ &= \frac{C^2}{8\log(\alpha+1)}t + \mathcal{O}(\log t)\\ &= \frac{\sqrt{\log x}}{\log_2 x}\left(C+\mathcal{O}\left(\frac{\log_3 x}{\log_2 x}\right)\right).\end{aligned}$$

Since $M(x^{\tau/\alpha}) \ge \log f(f(n))$, we infer (B.1.6). This concludes the proof.

Bibliography

[1] W. W. Adams. Asymptotic diophantine approximations to e. *Proc. Nat. Acad. Sci. U.S.A.*, 55:28–31, 1966.

[2] W. W. Adams. Asymptotic diophantine approximations and Hurwitz numbers. *Amer. J. Math.*, 89:1083–1108, 1967.

[3] W. W. Adams. Simultaneous asymptotic diophantine approximations. *Mathematika*, 14:173–180, 1967.

[4] W. W. Adams. Asymptotic diophantine approximations and equivalent numbers. *Proc. Amer. Math. Soc.*, 19:231–235, 1968.

[5] W. W. Adams. A lower bound in asymptotic diophantine approximations. *Duke Math. J.*, 35:21–35, 1968.

[6] W. W. Adams. Simultaneous asymptotic diophantine approximations to a basis of a real cubic number field. *J. Number Theory*, 1:179–194, 1969.

[7] W. W. Adams. Simultaneous diophantine approximations and cubic irrationals. *Pacific J. Math.*, 30:1–14, 1969.

[8] W. W. Adams. Simultaneous Asymptotic Diophantine Approximations to a Basis of a Real Number Field. *Nagoya Math. J.*, 42:79–87, 1971.

[9] W. W. Adams and S. Lang. Some computations in diophantine approximations. *J. Reine Angew. Math.*, 220:163–173, 1965.

[10] F. Adiceam, V. Beresnevich, J. Levesley, S. Velani, and E. Zorin. Diophantine approximation and applications in interference alignment. *Adv. Math.*, 302:231–279, 2016.

[11] C. Aistleitner, T. Lachmann, M. Munsch, N. Technau, and A. Zafeiropoulos. The Duffin-Schaeffer conjecture with extra divergence. Preprint, available at `https://arxiv.org/abs/1803.05703`, 2018.

[12] C. Aistleitner, T. Lachmann, and F. Pausinger. Pair correlations and equidistribution. *J. Num. Theory*, 182:206–220, 2018.

[13] C. Aistleitner, T. Lachmann, and N. Technau. There is no Khintchine threshold for metric pair correlations. Preprint, available at `https://arxiv.org/abs/1802.02659`, 2018.

[14] C. Aistleitner, G. Larcher, and M. Lewko. Additive energy and the Hausdorff dimension of the exceptional set in metric pair correlation problems. With an appendix by Jean Bourgain. *Israel J. Math.*, 222(1):463–485, 2017.

[15] G. E. Andrews and B. Berndt. Highly Composite Numbers. *Chapter in: Ramanujan's lost notebook, Part III*, pages 359–402, 2012.

[16] B. Babanazarov and Y. I. Podzharskii. On the maximal order of arithmetic functions. *Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk*, (1):18–23, 1987.

[17] F. Barroero and M. Widmer. Counting lattice points and o-minimal structures. *Int. Math. Res. Not.*, 2014(18):4932–4957, 2013.

[18] V. Beresnevich. Badly approximable points on manifolds. *Invent. Math.*, 202:1199–1240, 2015.

[19] V. Beresnevich, G. Harman, A. Haynes, and S. Velani. The Duffin-Schaeffer conjecture with extra divergence II. *Math. Z.*, 275(1-2):127–133, 2013.

[20] V. Beresnevich and S. Velani. A mass transference principle and the Duffin-Schaeffer conjecture for Hausdorff measures. *Ann. Math. (2)*, 164(3):971–992, 2006.

[21] V. Bernik and M. Dodson. *Metric Diophantine approximation on manifolds*. Cambridge University Press, 1999.

[22] M. Berry and M. Tabor. Level clustering in the regular spectrum. *Proc. R. Soc. London A: Math., Phys. and Engin. Sci.*, 356(1686):375–394, 1977.

[23] T. F. Bloom, S. Chow, A. Gafni, and A. Walker. Additive energy and the metric Poissonian property. *Mathematika, to appear*. Preprint available at `https://arxiv.org/abs/1709.02634`.

[24] A. Bondarenko and K. Seip. GCD sums and complete sets of square-free numbers. *Bull. London Math. Soc.*, 47(1):29–41, 2015.

[25] A. Bondarenko and K. Seip. Large greatest common divisor sums and extreme values of the Riemann zeta function. *Duke Math. J.*, 166(9):1685–1701, 2017.

[26] J.-B. Bost. Theta invariants of euclidean lattices and infinite-dimensional hermitian vector bundles over arithmetic curves. Preprint, available at `https://arxiv.org/abs/1512.08946`, 2017.

[27] J. Bourgain and N. Watt. Mean square of zeta function, circle problem and divisor problem revisited. Preprint, available at `https://arxiv.org/abs/1709.04340`, 2017.

[28] Y. Bugeaud. *Approximation by algebraic numbers.* Cambridge University Press, 2004.

[29] Y. Buttkewitz, C. Elsholtz, K. Ford, and J.-C. Schlage-Puchta. A problem of Ramanujan, Erdős, and Kátai on the iterated divisor function. *Int. Math. Res. Not.*, 2012(17):4051–4061, 2011.

[30] W. B. Cameron. *A Casual Introduction to Sociological Thinking.* Random House, 1963.

[31] J. Cassels. *An Introduction to Diophantine Approximation.* Cambridge University Press, 1957.

[32] S. Chow. Bohr sets and multiplicative diophantine approximation. *Duke Math. J., to appear.* Preprint, available at `https://arxiv.org/abs/1703.07016`, 2018.

[33] K. L. Chung and P. Erdős. On the application of the Borel-Cantelli lemma. *Trans. Amer. Math. Soc.*, 72(1):179–186, 1952.

[34] M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications.* Springer, 1997.

[35] A. A. Drozdova and G. A. Freiman. The estimation of certain arithmetic functions. *Elabuz. Gos. Ped. Inst. Ucen. Zap.*, 3:160–165, 1958. (In Russian).

[36] R. J. Duffin and A. C. Schaeffer. Khintchine's problem in metric Diophantine approximation. *Duke Math. J.*, 8:243–255, 1941.

[37] P. Dusart. Estimates of some functions over primes without R.H. 2010. Preprint. avaliable at `http://arxiv.org/pdf/1002.0442v1.pdf`.

[38] M. Einsiedler, A. Katok, and E. Lindenstrauss. Invariant measures and the set of exceptions to Littlewood's conjecture. *Ann. Math. (2)*, 164(2):513–560, 2006.

[39] A. Einstein. letter from 11th of March 1952 to C. Seeling, available at `http://www.library.ethz.ch/de/Ressourcen/Digitale-Bibliothek/Einstein-Online/Princeton-1933-1955`.

[40] H. El Gamal, G. Caire, and M. O. Damen. Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of mimo channels. *IEEE Transactions on Information Theory*, 50(6):968–985, 2004.

[41] C. Elsholtz, M. Technau, and N. Technau. The maximal order of iterated multiplicative functions. Preprint, available at `https://arxiv.org/abs/1709.04799`, 2017.

[42] C. Elsholtz, N. Technau, and R. Tichy. On the regularity of primes in arithmetic progressions. *Int. J. Number Theory*, 13(05):1349–1361, 2017.

[43] P. Erdős. Some results on diophantine approximation. *Acta Arith.*, 5:359–369, 1959.

[44] P. Erdős and A. Ivić. On the iterates of the enumerating function of finite abelian groups. *Bull. Acad. Serbe Sci. Arts Cl. Sci. Math. Natur.*, 17:13–22, 1989.

[45] P. Erdős and I. Kátai. On the growth of $d_k(n)$. *Fibonacci Quart.*, 7:267–274, 1969.

[46] P. Gallagher. Approximation by reduced fractions. *J. Math. Soc. Japan*, 13:342–345, 1961.

[47] O. German. Diophantine exponents of lattices. *Proc. Steklov Inst. Math.*, 296(2):29–35, 2017.

[48] A. Gorodnik and A. Nevo. Counting lattice points. *J. Reine Angew. Math.*, 2012(663):127–176, 2012.

[49] A. Granville. Least prime in arithmetic progressions. *Théorie des nombres/ Number Theory*, pages 306–321, 1989. ed. J.-M. De Koninck and C. Lévesque.

[50] A. Granville, D. Koukoulopoulos, and K. Matomäki. When the sieve works. *Duke Math. J.*, 164(10):1935–1969, 2015.

[51] A. Granville and C. Pomerance. On the least prime in certain arithmetic progressions. *J. London Math. Soc.*, 2(2):193–200, 1990.

[52] T. Gronwall. Some asymptotic expressions in the theory of numbers. *Trans. Amer. Math. Soc.*, 14(1):113–122, 1913.

[53] L. Hajdu and N. Saradha. On a problem of Recaman and its generalization. *J. Number Theory*, 131:18–24, 2011.

[54] L. Hajdu and N. Saradha. On generalizations of problems of Recaman and Pomerance. *J. Number Theory*, 162:552–563, 2016.

[55] L. Hajdu, N. Saradha, and R. Tijdeman. On a conjecture of Pomerance. *Acta Arith.*, 155(2):175–184, 2012.

[56] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[57] G. Harman. Some cases of the Duffin and Schaeffer conjecture. *Quart. J. Math. Oxford Ser. (2)*, 41(164):395–404, 1990.

[58] G. Harman. *Metric number theory*. Oxford: Clarendon Press, 1998.

[59] A. K. Haynes, A. D. Pollington, and S. L. Velani. The Duffin-Schaeffer conjecture with extra divergence. *Math. Ann.*, 353(2):259–273, 2012.

[60] D. R. Heath-Brown. Almost-primes in arithmetic progressions and short intervals. *Proc. Cambridge Phil. Soc.*, 83(3):357–375, 1978.

[61] D. R. Heath-Brown. Pair correlation for fractional parts of αn^2. *Math. Proc. Cambridge Phil. Soc.*, 148(3):385–407, 2010.

[62] E. Heppner. Die maximale Ordnung primzahl-unabhängiger multiplikativer Funktionen. *Arch. Math.*, 24:63–66, 1973.

[63] H. Heuser. *Lehrbuch der Analysis. Teil 1.* Vieweg+Teubner, 17th edition, 2009. (In German).

[64] T. Hilberdink. Maximal order of a class of multiplicative functions. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 43:217–237, 2014.

[65] A. Ivić. On the maximal order of certain arithmetic functions. *Filomat*, 9(3):483–492, 1995.

[66] D. Kleinbock and G. A. Margulis. Logarithm laws for flows on homogeneous spaces. *Invent. Math.*, 138(3):451–494, 1999.

[67] S. Knapowski and P. Turán. Comparative prime-number theory. I: Introduction. *Acta Math. Hung.*, 13(3-4):299–314, 1962.

[68] J. Knopfmacher. A prime-divisor function. *Proc. Amer. Math. Soc.*, 40:373–377, 1973.

[69] J. Knopfmacher. Arithmetical properties of finite rings and algebras, and analytic number theory. VI. Maximum orders of magnitude. *J. Reine Angew. Math.*, 277:45–62, 1975.

[70] J. Knopfmacher. *Abstract analytic number theory. 2nd ed.* Dover Publications, 1990.

[71] E. Krätzel. Die maximale Ordnung der Anzahl der wesentlich verschiedenen abelschen Gruppen n-ter Ordnung. *Q. J. Math., Oxford II. Ser.*, 21:273–275, 1970.

[72] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences.* Courier Corporation, 2012.

[73] T. Lachmann and N. Technau. On Exceptional Sets in the Metric Poissonian Pair Correlations problem. Preprint, available at `https://arxiv.org/abs/1708.08599`, 2017.

[74] S. Lang. Asymptotic approximations to quadratic irrationalities. I. *Amer. J. Math.*, 87:488–496, 1965.

[75] S. Lang. Asymptotic Diophantine approximations. *Proc. Nat. Acad. Sci. U.S.A.*, 55:31–34, 1966.

[76] R. M. Langworth. Churchill by himself. *Public Affairs*, 2008.

[77] G. Larcher and S. Grepstad. On pair correlation and discrepancy. *Arch. Math.*, 109(2):143–149, 2017.

[78] G. Larcher and W. Stockinger. Pair correlation of sequences $(\{a_n\alpha\})_{n\in\mathbb{N}}$ with maximal order of additive energy. Preprint, available at `https://arxiv.org/abs/1802.02901`, 2018.

[79] G. Larcher and W. Stockinger. Some negative results related to Poissonian pair correlation problems. Preprint, available at `https://arxiv.org/abs/1803.05236`, 2018.

[80] H. Maier. On the third iterates of the φ- and σ-functions. *Colloq. Math.*, 49(1):123–130, 1984.

[81] H. Maier. Primes in short intervals. *Mich. Math. J.*, 32:221–225, 1985.

[82] D. W. Masser and J. D. Vaaler. Counting algebraic numbers with large height II. *Trans. Amer. Math. Soc.*, 359:427–445, 2007.

[83] A. Mąkowski. On two conjectures of Schinzel. *Elemente der Math.*, 31:140–141, 1976.

[84] J.-L. Nicolas. Grandes valeurs d'une certaine classe de fonctions arithmétiques. *Studia Sci. Math. Hungar.*, 15(1-3):71–77, 1980.

[85] J.-L. Nicolas. On highly composite numbers. *Ramanujan revisited, Proc. Conf., Urbana-Champaign/Illinois.*, pages 215–244, 1988.

[86] F. Nietzsche. *Menschliches, Allzumenschliches*. Jazzybee Verlag, 2012.

[87] K. Norton. Upper bounds for sums of powers of divisor functions. *J. Number Theory*, 40(1):60–85, 1992.

[88] A. D. Pollington and R. C. Vaughan. The k-dimensional Duffin and Schaeffer conjecture. *Mathematika*, 37(2):190–200, 1990.

[89] C. Pomerance. A note on the least prime in an arithmetic progression. *J. Number Theory*, 12:218–223, 1980.

[90] A. G. Postnikov. *Introduction to analytic number theory*, volume 68. American Mathematical Society, 1988.

[91] S. Ramanujan. Highly composite numbers. *Proc. London Math. Soc.*, 14:347–409, 1915. Republished (2000) in Collected papers of Srinivasa Ramanujan.

[92] S. Ramanujan. *The Lost Notebook and Other Unpublished Papers*. Narosa, 1988.

[93] S. Ramanujan. Highly composite numbers. Annotated and with a foreword by Jean-Louis Nicolas and Guy Robin. *Ramanujan J.*, 1(2):119–153, 1997.

[94] B. Recaman. Problem 672. *J. Recreational Math.*, 10:283, 1978.

[95] J. B. Rosser, L. Schoenfeld, et al. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 1962.

[96] M. Rubinstein and P. Sarnak. Chebyshev's bias. *Experimental Math.*, 3(3):173–197, 1994.

[97] Z. Rudnick. A metric theory of minimal gaps. Preprint, available at `https://arxiv.org/abs/1710.01911`, 2017.

[98] Z. Rudnick and P. Sarnak. The pair correlation function of fractional parts of polynomials. *Comm. Math. Phys.*, 194(1):61–70, 1998.

[99] Z. Rudnick, P. Sarnak, and A. Zaharescu. The distribution of spacings between the fractional parts of $n^2\alpha$. *Invent. Math.*, 145(1):37–57, 2001.

[100] Z. Rudnick and A. Zaharescu. The distribution of spacings between fractional parts of lacunary sequences. *Forum Math.*, 14(5):691–712, 2002.

[101] N. Saradha. Conjecture of pomerance for some even integers and odd primorials. *Publ. Math. Debrecen*, 79(3):699–706, 2011.

[102] A. Schinzel. Ungelöste Probleme. *Elemente der Math.*, 14:60–61, 1959.

[103] W. M. Schmidt. A metrical theorem in Diophantine approximation. *Canad. J. Math*, 12:619–631, 1960.

[104] W. M. Schmidt. Simultaneous approximation to a basis of a real numberfield. *Amer. J. Math.*, 88:517–527, 1966.

[105] W. M. Schmidt. The distribution of sublattices of $\mathbb{Z}^m$. *Monatshefte Math.*, 125(1):37–81, 1998.

[106] P. Shiu. The maximum orders of multiplicative functions. *Quart. J. Math. Oxford Ser. (2)*, 31(122):247–252, 1980.

[107] M. M. Skriganov. The spectrum band structure of the three-dimensional Schrödinger operator with periodic potential. *Invent. Math.*, 80(1):107–121, 1985.

[108] M. M. Skriganov. Constructions of uniform distributions in terms of geometry of numbers. *Algebra Analiz.*, 6(3):200–230, 1994.

[109] M. M. Skriganov. Ergodic theory on SL(n), Diophantine approximations and anomalies in the lattice point problem. *Invent. Math.*, 132:1–72, 1998.

[110] A. Smati. Sur un problème de S. Ramanujan. *C. R., Math., Acad. Sci. Paris*, 340(1):1–4, 2005.

[111] A. Smati. Sur un problème d'Erdős et Kátai. *Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Comput.*, 29:213–238, 2008.

[112] P. G. Spain. Lipschitz: a new version of an old principle. *Bull. London Math. Soc.*, 27:565–566, 1995.

[113] S. Steinerberger. Localized quantitative criteria for equidistribution. *Acta Arith.*, 180(2):183–199, 2017.

[114] D. Suryanarayana and R. S. Rao. On the true maximum order of a class of arithmetical functions. *Math. J. Okayama Univ.*, 17(2):95–101, 1975.

[115] M. M. Sweet. A theorem in Diophantine approximations. *J. Number Theory*, 5:245–251, 1973.

[116] T. Tao and V. H. Vu. *Additive Combinatorics*. Cambridge University Press, 2006.

[117] N. Technau and M. Widmer. On a counting theorem of Skriganov. Preprint, available at `https://arxiv.org/abs/1611.02649`, 2016.

[118] P. A. Terentius. *Heautontimorumenos*. available at `https://la.wikisource.org/wiki/Heautontimorumenos`.

[119] J. R. R. Tolkien. The hobbit, or there and back again., 1997. first published 1937.

[120] T. Trudgian. Updating the error term in the prime number theorem. *The Ramanujan J.*, 39(2):225–234, 2016.

[121] J. L. Truelsen. Divisor problems and the pair correlation for the fractional parts of $n^2\alpha$. *Int. Math. Res. Not.*, 2010(16):3144–3183, 2010.

[122] P. Turán. Über die Primzahlen der arithmetischen Progression. *Acta Sci. Math.(Szeged)*, 8:226–235, 1936.

[123] J. D. Vaaler. On the metric theory of Diophantine approximation. *Pacific J. Math.*, 76(2):527–539, 1978.

[124] S. S. Wagstaff. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.*, 33:1073–1080, 1979.

[125] A. Walker. The primes are not metric Poissonian. *Mathematika*, 64(1):230–236, 2018.

[126] H. Wegmann. Beiträge zur Zahlentheorie auf freien Halbgruppen. II. Zum elementaren Beweis des Primzahlsatzes. *J. Reine Angew. Math.*, 221:150–159, 1966.

[127] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

[128] M. Widmer. Weakly admissible lattices, Diophantine approximation, and o-minimality. *Mathematika, to appear*. Preprint available at `https://arxiv.org/abs/1612.09467`.

[129] M. Widmer. Counting primitive points of bounded height. *Trans. Amer. Math. Soc.*, 362(9):4793–4829, 2010.

[130] S. Wigert. Sur l'ordre de grandeur du nombre des diviseurs d'un entier. *Ark. Mat.*, 3(18):1–9, 1907.

[131] S. Yang and A. Togbé. Proof of the P-integer conjecture of Pomerance. *J. Number Theory*, 140:226–234, 2014.