

Lena Wurzinger, BSc

# **Sumsets in multiplicatively defined sets**

## **MASTER'S THESIS**

to achieve the university degree of

Diplom-Ingenieurin

Master's degree programme: Mathematics

submitted to

**Graz University of Technology**

Supervisor

Assoc.Prof. Dipl.-Math. Dr.rer.nat.habil. Christian Elsholtz

Institute of Analysis and Number Theory

Graz, July 2023

# Contents

<b>Introduction</b>	<b>3</b>
<b>Acknowledgements</b>	<b>5</b>
<b>1 Sieve methods</b>	<b>6</b>
1.1 The large sieve . . . . .	6
1.2 Gallagher's larger sieve . . . . .	15
<b>2 Primes</b>	<b>17</b>
2.1 Distribution . . . . .	18
2.2 The ternary inverse Goldbach problem . . . . .	19
<b>3 Squares</b>	<b>27</b>
3.1 Previous results . . . . .	27
3.2 Bounds in $\mathbb{Z}/p\mathbb{Z}$ . . . . .	28
3.2.1 Weil's inequality . . . . .	28
3.2.2 Quadratic residue patterns . . . . .	29
3.2.3 Further bounds on $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p \cup \{0\}$ . . . . .	33
3.3 Application of sieve methods . . . . .	39
<b>4 Squarefree Numbers</b>	<b>46</b>
4.1 Basic properties . . . . .	47
4.2 Discussing sumsets . . . . .	49
<b>5 Hilbert cubes</b>	<b>60</b>
5.1 Squares . . . . .	61
5.2 Pure powers . . . . .	64
5.2.1 General outline . . . . .	64
5.2.2 Estimates concerning arithmetic progressions . . . . .	66
<b>Bibliography</b>	<b>73</b>
<b>Index of Notation</b>	<b>76</b>

# Introduction

Our main goal is to investigate sumsets, i.e., sets of the form

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\},$$

that lie in multiplicatively defined sets. More concretely, we assume that  $\mathcal{A}$  and  $\mathcal{B}$  are contained in some interval  $[1, N]$ , with  $N$  a positive integer, and derive bounds for the cardinality of  $\mathcal{B}$ , given that  $\mathcal{A}$  is of a certain size.

In Chapter 1, we give an introduction to sieve methods. Sieves can be employed to bound the cardinality of a set  $\mathcal{C} \subseteq [1, N]$  using information about the distribution of  $\mathcal{C}$  modulo a set of primes. In subsequent chapters, we are able to leverage the multiplicative structure of our sets of interest in order to apply these sieves. The main sources for this chapter were the book by Friedlander and Iwaniec [18, Chapter 9] (for the large sieve), and Gallagher's paper on his larger sieve [19]; the discussion of the large sieve in the book by Brüdern [3] proved to be enlightening as another source for comparison, and we found some additional motivation on how a certain function was chosen in Selberg's notes [36].

We start the second chapter with a brief discussion of some well-known facts pertaining to the distribution of the prime numbers. In Section 2.2, we discuss the work done by Elsholtz [13] concerning sumsets in the set of primes and present his solution to the *Inverse Ternary Goldbach Problem*.

In the third chapter, we study sumsets  $\mathcal{A} + \mathcal{B}$  contained in the set of squares. We give an overview of the work done by various authors regarding sets of this type (as well as their reduction modulo primes, i.e., sumsets lying in the quadratic residues  $\mathcal{Q} \cup \{0\}$ ). Particularly, Gyarmati [20, Theorem 9] showed that if  $|\mathcal{A}| \geq 9 \log N$ , then  $|\mathcal{B}| \leq 8 \log N$ . My advisor and I were able to generalize this result; after proving an auxilliary lemma<sup>1</sup> concerning sumsets in  $\mathcal{Q} \cup \{0\}$ , we were able to show<sup>2</sup>:

**Theorem.** *Let  $m$  be a positive integer, or a function  $m = m(N)$  taking values in the positive integers. Then there are constants  $C_1, C_2$  (independent of  $m$ ) such that, if*

$$|\mathcal{A}| \geq C_1 m^2 \log N,$$

*then*

$$|\mathcal{B}| \leq C_2 m (\log N)^{1/m}.$$

---

<sup>1</sup>See Lemma 3.10 in the main text of this thesis.

<sup>2</sup>This is Theorem 3.13 in Chapter 3.

A result of this type shows an asymmetry: When  $|\mathcal{A}|$  is slightly larger than  $\log N$ , then our bound on  $|\mathcal{B}|$  is much smaller. For instance, when  $|\mathcal{A}| \gg (\log \log N)^2 \log N$ , then  $|\mathcal{B}| \ll \log \log N$ . The auxilliary lemma, Lemma 3.10, is vital for our proof; directly copying the method<sup>3</sup> in [20] would not work. Furthermore, while the estimate discussed in Corollary 3.4 does not offer much flexibility for  $|\mathcal{B}|$  in the range above, the special case  $m(N) = \log \log N$  can be derived from it, as can be seen in the proof of Theorem 3.12.

In Chapter 4, we study sumsets in the squarefree numbers. After proving some facts regarding the distribution of the squarefree numbers, we discuss Konyagin's paper [26], where he investigates sets  $\mathcal{A}$  with  $\mathcal{A} + \mathcal{A}$  in the squarefree numbers.

The final chapter 5 deals with Hilbert cubes, i.e., sets of the form

$$\begin{aligned} H(a_0; a_1, \dots, a_d) &:= a_0 + \{0, a_1\} + \dots + \{0, a_d\} \\ &= \{a_0 + \varepsilon_1 a_1 + \dots + \varepsilon_d a_d : \varepsilon_1, \dots, \varepsilon_d \in \{0, 1\}\}. \end{aligned}$$

We provide exposition on the work done by Dietmann and Elsholtz [10, 11] regarding the dimension  $d$  of such cubes lying in the set of squares or in the set of pure powers.

---

<sup>3</sup>That is, if one were to use the bound provided by Lemma 3.5.

# Acknowledgements

I would like to thank my advisor Christian Elsholtz. I am beyond grateful that he always took the time to discuss things with me, for his kind encouragement, and for his invaluable advice.

I would also like to thank Igor Shparlinski for drawing our attention to a result of Davenport and Erdős [8], who proved a result closely related to Lemma 3.10, and also work of Karatsuba. We intend to take the opportunity to incorporate their ideas in subsequent work.

# 1 Sieve methods

Sieves are tools for examining sifted sets, that is, sets of the form

$$(\mathcal{M}; \mathcal{P}', \Omega) = \{m \in \mathcal{M} : m \bmod p \notin \Omega_p \text{ for any } p \in \mathcal{P}'\},$$

where  $\mathcal{M} \subseteq \mathbb{N}$  is a set of positive integers,  $\mathcal{P}'$  is usually a subset of the primes  $\mathcal{P}$  (or a subset of the prime-powers) and the set  $\Omega = \{\Omega_p : p \in \mathcal{P}'\}$  contains sets of residue classes  $\Omega_p$  modulo  $p$ . The idea behind the name is that in order to obtain  $(\mathcal{M}; \mathcal{P}', \Omega)$  from  $\mathcal{M}$ , we exclude certain residue classes: these excluded residue classes were “sifted”, so to speak. We will always denote the number of sifted residue classes modulo  $p$  by  $\omega(p) = |\Omega_p|$ .

The best-known sifting process is certainly the *sieve of Eratosthenes*, which relies on the fact that any composite integer  $m$  has a prime factor  $p$  such that  $p \leq \sqrt{m}$ . Therefore, if one sifts from the interval  $\mathcal{M} = [2, N]$  all integers that are divisible by a prime  $p$  in  $\mathcal{P}' = \{p \in \mathcal{P} : p \leq \sqrt{N}\}$  – that is, we exclude all  $m \in \mathcal{M}$  with

$$m \bmod p \in \Omega_p \text{ for some } p \in \mathcal{P}' \text{ where } \Omega_p = \{0\}$$

– the sifted set  $(\mathcal{M}; \mathcal{P}', \Omega)$  contains exactly all primes in the interval  $[\lfloor \sqrt{N} \rfloor + 1, N]$ .

In this chapter, we will study two different sieves: “The large sieve” and “The larger sieve”. In general, large sieve methods are quite powerful when  $\mathcal{M}$  is an interval and the number of residue classes to be sifted is relatively large. In the first section of this chapter, we present a proof of the large sieve (along with a discussion on a useful variant) as outlined in [18]; in the second section, we focus on the larger sieve. While writing this chapter, we found valuable insights not only in [18] but also in [3].

## 1.1 The large sieve

The large sieve was invented in 1941 by Linnik; since then, it has been thoroughly studied, and many variants of it have been developed. A common way to present the large sieve is as an inequality concerning trigonometric polynomials of the form

$$S(\alpha) = \sum_{M < n \leq M+N} a_n e(\alpha n),$$

where we denote  $e(\alpha n) = \exp(2\pi i \alpha n)$ , and  $\mathcal{A} = (a_n)_{M < n \leq M+N}$  with  $a_n \in \mathbb{C}$ .

Of course, in general the best upper bound for the expression  $|S(\alpha)|$  is given by Cauchy's inequality

$$|S(\alpha)|^2 \leq N \sum_{M < n < M+N} |a_n|^2.$$

However, one can achieve nontrivial estimates by taking the average of  $|S(\alpha_r)|^2$  over multiple “well-spaced”  $\alpha_r$ . By “well-spaced”, we mean that for some  $\delta > 0$ , the nearest integer to the difference of distinct  $\alpha_r \neq \alpha_s$  is at a distance  $\|\alpha_r - \alpha_s\|_{\mathbb{R}/\mathbb{Z}} \geq \delta$ ; if this is the case, we call the points  $(\alpha_r)_{r=1}^K$   **$\delta$ -spaced**.

More precisely, we have the following analytic version of the large sieve:

**Theorem 1.1** (The large sieve). *For any set of  $\delta$ -spaced points  $\alpha_r$ , and any complex numbers  $(a_m)_{m < n < M+N}$ , where  $0 < \delta \leq \frac{1}{2}$  and  $M \in \mathbb{Z}, N \in \mathbb{N}$ , we have*

$$\sum_r |S(\alpha_r)|^2 \leq (\delta^{-1} + N - 1) \sum_{m < n < M+N} |a_n|^2.$$

At first glance, it might not be obvious how to employ the large sieve for studying sifted sets  $(\mathcal{M}; \mathcal{P}', \Omega)$  as described in this chapter's introduction. We will later (in Theorem 1.3) see that the large sieve can be used to bound the modulus of the sum

$$\sum_{m \in (\mathcal{M}; \mathcal{P}', \Omega)} a_m$$

from above. By considering special  $(a_n)_{M < n < M+N}$ , namely the indicator function of the set  $(\mathcal{M}; \mathcal{P}', \Omega)$ ,

$$a_n = \begin{cases} 1 & \text{if } n \in (\mathcal{M}; \mathcal{P}', \Omega), \\ 0 & \text{otherwise,} \end{cases}$$

we can therefore find an upper bound for the cardinality of the set  $(\mathcal{M}; \mathcal{P}', \Omega)$ .

Before stating the next lemma, it is worth recalling the notation used relating functions in terms of growth. For two functions  $f : \mathbb{C} \rightarrow \mathbb{R}^+$  and  $g : \mathbb{C} \rightarrow \mathbb{R}^+$ , we say  $f(z) \ll g(z)$ , or equivalently  $f(z) = O(g(z))$ , as  $|z| \rightarrow \infty$  if the ratio  $f(z)/g(z)$  is bounded by some absolute constant as  $|z| \rightarrow \infty$ . Similarly, we say  $g(z) \gg f(z)$  if  $f(z) \ll g(z)$ . (These definitions can be extended to limit points other than  $\infty$ , but in this thesis, we will primarily focus on the case  $|z| \rightarrow \infty$ .)

For the proof of the large sieve, we need the following

**Lemma 1.2** (Beurling-Selberg, see [18, p. 153, Lemma 9.2]). *Let  $F : \mathbb{C} \rightarrow \mathbb{C}$  be the function defined via*

$$F(z) = \frac{\sin^2 \pi z}{\pi^2} \left( \sum_{n=0}^{\infty} \frac{1}{(z-n)^2} - \sum_{n=1}^{\infty} \frac{1}{(z+n)^2} + \frac{2}{z} \right).$$

*Then  $F$  is entire and  $|F(z)| \ll e^{2\pi|\operatorname{Im}(z)|}$ . Moreover,*

1.  $F(x) \geq \operatorname{sgn} x$  if  $x$  is real.
2.  $\int_{-\infty}^{\infty} (F(x) - \operatorname{sgn} x) dx = 1$ .

*Proof.* The second factor  $\sum_{n=0}^{\infty} (z-n)^{-2} - \sum_{n=1}^{\infty} (z+n)^{-2} + 2z^{-1}$  has double poles in the integers, while it is holomorphic on  $\mathbb{C} \setminus \mathbb{Z}$  where converge both series converge locally uniformly. The poles get cancelled out by the corresponding double zeros of the entire function  $(\sin^2 \pi z)/\pi^2$ . Hence  $F$  is entire.

Using the partial fraction expansion

$$\frac{\pi^2}{\sin^2 \pi z} = \sum_{n=0}^{\infty} \frac{1}{(z-n)^2} + \sum_{n=1}^{\infty} \frac{1}{(z+n)^2},$$

we can write  $F$  in the following two ways:

$$F(z) = 1 + \frac{2 \sin^2 \pi z}{\pi^2} \left( \frac{1}{z} - \sum_{n=0}^{\infty} \frac{1}{(z+n)^2} \right) \quad (1.1)$$

and

$$-F(-z) = 1 + \frac{2 \sin^2 \pi z}{\pi^2} \left( \frac{1}{z} - \sum_{n=1}^{\infty} \frac{1}{(z+n)^2} \right). \quad (1.2)$$

We will rely heavily on these two expressions for proof of the remaining assertions.

To begin with, the rightmost factors  $z^{-1} + \sum_{n=0}^{\infty} (z-n)^{-2}$  and  $z^{-2} + \sum_{n=1}^{\infty} (z-n)^{-2}$  are bounded outside a neighbourhood of zero in the right half plane, while  $|\sin \pi z|^2 \leq c e^{2\pi |\operatorname{Im}(z)|}$  for some positive constant  $c$ , i.e.  $|\sin \pi z|^2 \ll e^{2\pi |\operatorname{Im}(z)|}$ . This implies the claimed asymptotics.

Moreover, for real  $x > 0$ ,

$$\frac{1}{x} = \int_0^{\infty} \frac{1}{(x+w)^2} dw.$$

Approximating this integral by Riemann sums yields the bounds

$$\sum_{n=1}^{\infty} \frac{1}{(x+n)^2} < \frac{1}{x} < \sum_{n=0}^{\infty} \frac{1}{(x+n)^2},$$

so the assertion that  $F(x) \geq \operatorname{sgn} x$  follows under consideration of Eq. (1.1) and Eq. (1.2).

Finally,

$$\int_{-\infty}^{\infty} (F(x) - \operatorname{sgn} x) dx = \int_0^{\infty} (F(x) + F(-x)) dx = 2 \int_0^{\infty} \frac{\sin^2 \pi x}{\pi^2 x^2} dx = 1. \quad \square$$



*Proof of the large sieve.* As described on page 157 (Lemma 5.2.1) of [3], the norm of a continuous linear map equals the norm of its dual. For our specific case, let us consider the map  $T : \mathbb{C}^N \rightarrow \mathbb{C}^R, \underline{a} \mapsto E\underline{a}$  with  $E = (e(n\alpha_r))_{n,r}$ . Then the inequality claimed in Theorem 1.1,

$$\sum_r |S(\alpha_r)|^2 = \sum_r \left| \sum_{m < n < M+N} a_n e(\alpha_r n) \right|^2 \leq (\delta^{-1} + N - 1) \sum_{m < n < M+N} |a_n|^2,$$

says that the norm of the operator  $T$  is at most  $\delta^{-1} + N - 1$ .

Here, taking the dual of the operator  $T$  just corresponds to transposing and conjugating the matrix  $E$ . In order to prove our theorem, it therefore suffices to show that

$$\sum_{M < n \leq M+N} \left| \sum_r c_r e(\alpha_r n) \right|^2 \leq (\delta^{-1} + N - 1) \sum_{m < n < M+N} |c_n|^2.$$

holds for any complex numbers  $(c_r)_r$ .

Without loss of generality, we assume that  $M = -1$ . (Otherwise, replace  $c_r$  with  $c_r e(\alpha_r(M+1))$ .) Now,

$$\sum_{0 \leq n \leq N-1} \left| \sum_r c_r e(\alpha_r n) \right|^2 \leq \sum_{n \in \mathbb{Z}} b(n) \left| \sum_r c_r e(\alpha_r n) \right|^2,$$

where  $b(x)$  is any function that majorizes the indicator function of the interval  $[0, N-1]$ . Under the assumption that  $b(x)$  is continuous and rapidly decreasing as  $x \rightarrow \pm\infty$ , we can use Poisson's formula to write the latter sum as

$$\sum_r \sum_s c_r \bar{c}_s \sum_{n \in \mathbb{Z}} b(n) e((\alpha_r - \alpha_s)n) = \sum_r \sum_s c_r \bar{c}_s \sum_{n \in \mathbb{Z}} \hat{b}(n - \alpha_r + \alpha_s).$$

Here

$$\hat{b}(t) = \int_{-\infty}^{\infty} b(x) e(-xt) dx$$

denotes the Fourier transform of  $b$ .

If we choose  $b$  in such a way that  $\hat{b}(t) = 0$  for  $|t| \geq \delta$ , then

$$\sum_r \sum_s c_r \bar{c}_s \sum_{n \in \mathbb{Z}} \hat{b}(n - \alpha_r + \alpha_s) = \hat{b}(0) \sum_r |c_r|^2$$

due to the fact that the  $\alpha_r$  are  $\delta$ -spaced.

Therefore, our goal is to find a function  $b$  that satisfies the above conditions and such that  $\hat{b}(0)$  is small. To this end, we consider the function

$$\begin{aligned} G(x) &= \frac{1}{2}F(x) + \frac{1}{2}F(d-x) \\ &= \mathbf{1}_{[0,d]} + \frac{1}{2}(F(x) - \operatorname{sgn} x) + \frac{1}{2}(F(d-x) - \operatorname{sgn}(d-x)) \\ &\geq \mathbf{1}_{[0,d]}, \end{aligned}$$

where  $F$  is the function from Lemma 1.2,  $\mathbf{1}_{[0,d]}$  is the indicator function of the interval  $[0, d]$ , and  $d = \delta(N - 1)$ .

We see that  $G$  majorizes the indicator function of the interval  $[0, d]$ . Moreover, by the Paley-Wiener theorem<sup>1</sup>,  $\hat{G}(t) = 0$  if  $|t| \geq 1$ . Finally, by Lemma 1.2,  $\hat{G}(0) = d + 1$ .

Now we set  $b(x) = G(\delta x)$ . Then  $b$  majorizes the indicator function of  $[0, N - 1]$ . Furthermore,  $\hat{b}(t) = 0$  if  $t \geq \delta$ , and

$$\hat{b}(0) = \frac{1}{\delta} \hat{G}(0) = N - 1 + \frac{1}{\delta}.$$

We conclude that

$$\sum_{0 \leq n \leq N-1} \left| \sum_r c_r e(\alpha_r n) \right|^2 \leq \left( N - 1 + \frac{1}{\delta} \right) \sum_r |c_r|^2. \quad \square$$

It is clear that an essential part of the above proof was choosing the “right” function  $b$ . Some motivation on how to actually find this function can be found in Selberg’s notes on sieves [36] (pp. 214-217). We sketch how to do this in the special case where  $d$  (as in the proof above) is an integer.

The goal is to find some integrable entire function  $G$  that majorizes the indicator function of the interval  $[0, d]$ , so clearly, we need  $G(m) \geq 1$  for  $m \in [0, d]$  and  $G(m) \geq 0$  for  $|m| > d$ . By the Poisson summation formula,

$$\hat{G}(0) = \sum_{m=-\infty}^{\infty} G(m) \geq d + 1.$$

Considering that we want  $\hat{G}(0)$  to be as small as possible, we require that  $G(m) = 1$  for  $m \leq d$  and  $G(m) = 0$  for  $|m| > d$ . Thus  $G$  has local minima for  $1 \leq m \leq d - 1$  and  $|m| > d$ , which implies that  $G'(m) = 0$  in these points. In addition, we may assume  $G'(0) = -G'(d)$ . (Given some other  $G$ , we could always achieve this by replacing  $G(z)$  with  $(G(z) + G(d - z))/2$ .)

Moreover, we want  $\tilde{G}$  to be an integrable function supported on  $(-1, 1)$ . Then, by Fourier inversion,

$$G(z) = \int_{-1}^1 e(zy) \hat{G}(y) dy,$$

so  $|G(z)| \ll \exp(2\pi|\operatorname{Im}(z)|)$ .

---

<sup>1</sup>More specifically, we can use the following special case of the Paley-Wiener theorem (that is given on p. 135 in [27]): Let  $f$  be an entire, integrable function with  $|f(z)| \ll \exp(2\pi c|z|)$  (for some constant  $c > 0$ ), and let  $a = \limsup_{y \rightarrow -\infty} \log |f(iy)|/|y|$ ,  $b = \limsup_{y \rightarrow +\infty} \log |f(iy)|/|y|$ . Then  $\hat{f}$  is a continuous function and (as described in the proof of the more general case on p. 133, [27]),  $\hat{f}(x) = 0$  if  $x \notin [-a, b]$  (on p. 133, this is only true almost everywhere, but due to the continuity of  $\hat{f}$  in this special case, it holds for all  $x$ ). Here, we get that  $\hat{G}$  is supported on  $[-1, 1]$ , so, by continuity,  $\hat{G}(t) = 0$  if  $|t| \geq 1$ .

From these considerations, we can conclude that there is some constant  $\lambda$  such that

$$h(z) = \frac{G(w)}{\sin^2 \pi w} - \frac{1}{\pi^2} \left( \sum_{n=0}^d \frac{1}{(w-n)^2} + \frac{\lambda}{w} + \frac{\lambda}{d-w} \right)$$

is a bounded entire function, i.e. constant. To be more precise, boundedness can be shown in the following way: Let  $\epsilon \in (0, 1/4\pi)$ . We distinguish four cases:

1. Case  $z \in \{z : \operatorname{Im}(z) > \epsilon\}$ : From the asymptotics for  $G$ , it clear that  $|G(z)/\sin^2 \pi z|$  is bounded by some constant, and the modulus of any of the finitely many rational functions is also bounded.
2. Case  $z \in \{z : \operatorname{Im}(z) \leq \epsilon, \operatorname{Re}(z) \leq d+1\}$ :  $h$  is holomorphic, hence it is continuous and bounded on this compact rectangle.
3. Case  $z \in \{z : \operatorname{Im}(z) \leq \epsilon, \operatorname{Re}(z) > d+1, |z-n| > \epsilon \text{ for all } n \in \mathbb{Z}\}$ :  $|\sin^2 \pi z| \geq \epsilon'$  is bounded away from zero and  $G(z)$  as well as the rational functions are bounded.
4. Case  $z \in \{z : \operatorname{Im}(z) \leq \epsilon, \operatorname{Re}(z) > d+1, |z-n_z| \leq \epsilon \text{ for some } n_z \in \mathbb{Z}\}$ : Fix such a  $z$  and let  $n_z = m$ . By differentiating  $n$  times under the integral, we can show that  $a_{m,n} = G^{(n)}(z) \leq c(2\pi)^n$  for some constant  $c$  independent of  $z$  (within this set); we recall that  $G(m) = G'(m) = 0$ . Hence  $G(z) = \sum_{n \geq 2} a_{m,n} \frac{(z-m)^n}{n!}$ .

Moreover, the Taylor coefficients of  $\sin^2 \pi z$  around  $m$  only depend on  $m \bmod 1$ , so they are the same for any integer  $m$ :  $\sin^2 \pi z = \sum_{n \geq 2} b_n (z-m)^n$ . Now  $|\sum_{n \geq 2} \frac{a_{m,n}}{n!} (z-m)^{n-2}| \leq \sum_{n \geq 2} c(2\pi)^n \epsilon^{n-2} \leq c/\epsilon^2$  and  $|\sum_{n \geq 2} b_n (z-m)^{n-2}| \geq \epsilon''$  is bounded away from zero for  $z$  with  $|z-m| \leq \epsilon$ .

Therefore,  $|G(z)/\sin^2 \pi z|$  is bounded by some constant independent of  $m$ , while the rational functions are also clearly bounded on this set.

Moreover, considering that the limit of  $h(z)$  along points  $w_n = n + 1/2$  is certainly 0 (note that  $G$  is integrable, so  $G(w_n) \rightarrow 0$  as  $n \rightarrow \infty$ ),  $h$  is the constant zero function, so we actually get

$$G(w) = \frac{\sin^2 \pi w}{\pi^2} \left( \sum_{n=0}^d \frac{1}{(w-n)^2} + \frac{\lambda}{w} + \frac{\lambda}{d-w} \right).$$

Using the partial fraction expansion of  $\pi^2/\sin^2 \pi w$ , this can be written as

$$G(w) = 1 + \frac{\sin^2 \pi w}{\pi^2} \left( \frac{\lambda}{w} + \frac{\lambda}{d-w} - \sum_{m=1}^{\infty} \left( \frac{1}{(m+w)^2} + \frac{1}{(m+d-w)^2} \right) \right).$$

Now some care has to be put into choosing the appropriate constant  $\lambda$  such that  $G$  indeed majorizes the indicator function of  $[0, d]$ . We refer to [36] (pp. 214-218) for an explanation on how to do this, and on how to proceed for general  $d > 0$ .

As announced in the beginning of this section, we can use the large sieve to bound the modulus of the sifting function

$$Z = \sum_{n \in (\mathcal{M}; \mathcal{P}, \Omega)} a_n.$$

More specifically, we have the following theorem:

**Theorem 1.3** (Arithmetic version of the large sieve.). *Let  $\mathcal{M} \subseteq [M, M + N]$ ,  $Q \in \mathbb{N}$  and let  $\Omega$  contain sets of sifted residue classes. For any complex numbers  $a_m$  supported on  $m \in (\mathcal{M}; \mathcal{P}, \Omega)$ , we have*

$$\left| \sum_m a_m \right|^2 \leq \frac{N - 1 + Q^2}{L} \sum_m |a_m|^2,$$

where

$$L = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}.$$

*Proof.* For ease of notation, let

$$h(p) = \frac{\omega(p)}{p - \omega(p)},$$

and extend  $h$  as a multiplicative function supported on the squarefree numbers. Let

$$S(\alpha) = \sum_m a_m e(n\alpha).$$

We note that it suffices to show that for any  $q$ ,

$$h(q)|S(0)|^2 \leq \sum_{a \bmod q}^* \left| S\left(\frac{a}{q}\right) \right|^2, \quad (1.3)$$

where  $\sum^*$  represents the sum over coprime residue classes. The points  $a/q$  with  $a, q \leq Q$  and  $(a, q) = 1$  are  $1/Q^2$ -spaced. Indeed, let  $a/q \neq a'/q'$  be two such numbers. Then

$$\left\| \frac{a}{q} - \frac{a'}{q'} \right\|_{\mathbb{R}/\mathbb{Z}} = \left\| \frac{aq' - a'q}{qq'} \right\|_{\mathbb{R}/\mathbb{Z}} \geq \frac{1}{qq'} \geq \frac{1}{Q^2}.$$

Therefore, after summing over all  $q \leq Q$ , the large sieve can be applied:

$$\sum_{q \leq Q} h(q)|S(0)|^2 \leq \sum_{q \leq Q} \sum_{a \bmod q}^* |S(a/q)|^2 \leq (Q^2 + x) \sum_m |a_m|^2.$$

Now we prove the remaining assertion Eq. (1.3). We proceed by induction on the number of prime factors of  $q$ .

Suppose  $q = p \in \mathcal{P}$ . We define

$$Z_p(v) = \sum_{m \equiv v \pmod{p}} a_m.$$

Note that  $Z_p(v) = 0$  for all  $v \in \Omega_p$ . Thus, by Cauchy's inequality

$$\begin{aligned} |S(0)|^2 &= \left| \sum_{v=1}^p Z_p(v) \right|^2 \leq (p - \omega(p)) \sum_{v=1}^p |Z_p(v)|^2 \\ &= \left(1 - \frac{\omega(p)}{p}\right) \sum_{v=1}^p |S(v/q)|^2 \\ &= \left(1 - \frac{\omega(p)}{p}\right) \sum_{v \not\equiv 0 \pmod{p}}^* |S(v/q)|^2 + \left(1 - \frac{\omega(p)}{p}\right) |S(0)|^2. \end{aligned}$$

Rearranging yields

$$h(p)|S(0)|^2 \leq \sum_{v \not\equiv 0 \pmod{p}}^* |S(a/q)|^2,$$

i.e. the induction base.

For the induction step, we note that if  $(q_1, q_2) = 1$ , then, by the Chinese remainder theorem,

$$\sum_{v \not\equiv 0 \pmod{q_1 q_2}}^* |S(v/q_1 q_2)|^2 \leq \sum_{v_1 \not\equiv 0 \pmod{q_1}}^* \sum_{v_2 \not\equiv 0 \pmod{q_2}}^* |S(v_1/q_1 + v_2/q_2)|^2.$$

We apply the induction hypothesis twice (the first time with  $a_n e(nv_1/q_1)$ ) to get the lower bound

$$h(q_2) \sum_{v_1 \not\equiv 0 \pmod{q_1}}^* |S(v_1/q_1)|^2 \geq h(q_2)h(q_1)|S(0)|^2,$$

and we are done.  $\square$

By letting  $(a_m)_m$  be the indicator function of  $(\mathcal{M}; \mathcal{P}, \Omega)$ , Theorem 1.3 implies the following:

**Corollary 1.4** (Montgomery's sieve). *Let  $\mathcal{M} \subseteq [1, N]$ ,  $Q \in \mathbb{N}$  and let  $\Omega$  contain sets of sifted residue classes. Then*

$$|(\mathcal{M}; \mathcal{P}, \Omega)| \leq \frac{N + Q^2}{L}$$

where

$$L = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}.$$

In particular, if  $Q = \sqrt{N}$ , then

$$|(\mathcal{M}; \mathcal{P}, \Omega)| \leq \frac{2N}{L}.$$

It can be come useful to bound  $L$  by easier expressions. Following [38], we will now establish some bounds.

**Lemma 1.5.** *If we adopt the convention that  $\exp(\log 0) := 0$ , then the following lower bounds hold:*

$$L \geq \sum_{m \geq 1} \frac{1}{m!} \left( \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m \quad (1.4)$$

and

$$L \geq \sum_{m \geq 1} \exp \left( m \log \left( \frac{1}{m} \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right) \right). \quad (1.5)$$

*Remark 1.1.* It should be noted that the sum over  $p \leq Q^{1/m}$  is nonempty only if  $Q^{1/m} \geq 2$ , that is, only if  $m \leq \log Q / \log 2$ . Therefore, we are in fact only summing over  $1 \leq m \leq \log Q / \log 2$ .

Moreover, since all summands are non-negative, we can give a lower bound by fixing  $m$  and using the corresponding term, i.e.

$$L \geq \exp \left( m \log \left( \frac{1}{m} \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right) \right).$$

*Proof.* First of all, we note that

$$\begin{aligned} \exp \left( m \log \left( \frac{1}{m} \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right) \right) &= \left( \frac{1}{m} \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m \\ &= \frac{1}{m^m} \left( \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m \leq \frac{1}{m!} \left( \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m, \end{aligned}$$

so Eq. (1.4) implies Eq. (1.5).

Now, in order to prove Eq. (1.4), we rewrite

$$\frac{\omega(p)}{p - \omega(p)} = \frac{\omega(p)/p}{1 - \omega(p)/p} = \sum_{h \geq 1} \left( \frac{\omega(p)}{p} \right)^h.$$

Therefore

$$\begin{aligned} L &= \sum_{q \leq Q} \mu(q)^2 \prod_{p|q} \frac{\omega(p)}{p - \omega(p)} = \sum_{q \leq Q} \mu(q)^2 \prod_{p|q} \sum_{h \geq 1} \left( \frac{\omega(p)}{p} \right)^h \\ &= \sum_{q \leq Q} \mu(q)^2 \sum_{r \in R_q} \prod_{p^n || r} \left( \frac{\omega(p)}{p} \right)^n, \end{aligned}$$

where  $R_q = \{r \in \mathbb{N} : \prod_{p|r} p = q\}$ . We notice that any  $q_0$  of the form  $q_0 = \prod_{p|r} p$  is squarefree, hence  $\mu(q_0)^2 = 1$ . Thus, with  $\hat{R}_Q = \{r \in \mathbb{N} : \prod_{p|r} p \leq Q\}$  and  $\Omega(r)$  denoting the total number of prime factors of  $r$ ,

$$L = \sum_{r \in \hat{R}_Q} \prod_{p^n \| r} \left( \frac{\omega(p)}{p} \right)^n = \sum_{m \geq 1} \sum_{\substack{r \in \hat{R}_Q, \\ \Omega(r)=m}} \prod_{p^n \| r} \left( \frac{\omega(p)}{p} \right)^n.$$

Certainly, all numbers of the form  $r_0 = p_1 \cdots p_m$ , where the  $p_i$  are (not necessarily distinct) primes and  $p_i \leq Q^{1/m}$  for each  $p_i$ , satisfy  $\Omega(r_0) = m$  and  $r_0 \in \hat{R}_Q$ . Furthermore, the product

$$\prod_{p^n \| r} \left( \frac{\omega(p)}{p} \right)^n$$

shows up as a summand in the binomial expansion of  $\left( \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m$  with a factor of at most  $m!$ . From this, we can conclude that

$$L = \sum_{m \geq 1} \sum_{\substack{r \in \hat{R}_Q, \\ \Omega(r)=m}} \prod_{p^n \| r} \left( \frac{\omega(p)}{p} \right)^n \geq \sum_{m \geq 1} \frac{1}{m!} \left( \sum_{p \leq Q^{1/m}} \frac{\omega(p)}{p} \right)^m. \quad \square$$

## 1.2 Gallagher's larger sieve

In this section, we discuss Gallagher's larger sieve.

**Theorem 1.6** (Gallagher's larger sieve, [19]). *Let  $\mathcal{A}$  be a set of integers with counting function  $A(x) = \sum_{a \in \mathcal{A}, a \leq x} 1$  and let  $\mathcal{S}$  be a set of prime powers. Suppose that for  $q \in \mathcal{S}$ ,  $\mathcal{A}$  lies in at most  $\nu(q)$  residue classes modulo  $q$ . Then, provided the denominator is positive, the following bound holds:*

$$A(x) \leq \frac{-\log x + \sum_{q \in \mathcal{S}} \Lambda(q)}{-\log x + \sum_{q \in \mathcal{S}} \Lambda(q)/\nu(q)}.$$

where  $\Lambda(p^k) = \log p$  is the von Mangoldt function.

In particular, if  $\mathcal{S}$  is a set of primes, we get

$$A(x) \leq \frac{-\log x + \sum_{p \in \mathcal{S}} \log p}{-\log x + \sum_{p \in \mathcal{S}} \log p / \nu(p)}.$$

*Proof.* Let  $q \in \mathcal{S}$  and define  $A_q(h, x) = \sum_{a \in \mathcal{A}, a \leq x, a \equiv h \pmod{q}} 1$  as the counting function of the elements of  $\mathcal{A}$  that are congruent to  $h \pmod{q}$ . Certainly,  $A(x) = \sum_{h=1}^q A_q(h, x)$ ,

and therefore (by Cauchy's theorem)

$$\begin{aligned}
A(x)^2 &= \left( \sum_{h=1}^q A_q(h, x) \right)^2 \leq \nu(q) \sum_{h=1}^q A_q(h, x)^2 \\
&= \nu(q) \sum_{h=1}^q \sum_{\substack{a, a' \in \mathcal{A} \\ a, a' \leq x \\ a, a' \equiv h \pmod{q}}} 1 \\
&= \nu(q) A(x) + \nu(q) \sum_{\substack{a \neq a' \in \mathcal{A} \\ a, a' \leq x \\ a - a' \equiv 0 \pmod{q}}} 1.
\end{aligned}$$

Next, we multiply by  $\Lambda(q)/\nu(q)$  and sum over all  $q \in \mathcal{S}$ . This results in

$$\begin{aligned}
A(x)^2 \sum_{q \in \mathcal{S}} \Lambda(q)/\nu(q) &\leq A(x) \sum_{q \in \mathcal{S}} \Lambda(q) + \sum_{q \in \mathcal{S}} \sum_{\substack{a \neq a' \in \mathcal{A} \\ a, a' \leq x \\ a - a' \equiv 0 \pmod{q}}} \Lambda(q) \\
&= A(x) \sum_{q \in \mathcal{S}} \Lambda(q) + \sum_{0 \neq |d| \leq x} \sum_{\substack{a, a' \in \mathcal{A} \\ a - a' = d}} \sum_{q \in \mathcal{S}, q|d} \Lambda(q) \\
&\leq A(x) \sum_{q \in \mathcal{S}} \Lambda(q) + (A(x)^2 - A(x)) \log x,
\end{aligned}$$

where the last line follows from the fact that  $\sum_{t|m} \Lambda(t) = \log(|m|)$ .

Dividing both sides of the inequality by  $A(x)$  and rearranging, we get

$$A(x) \left( \sum_{q \in \mathcal{S}} \Lambda(q)/\nu(q) - \log x \right) \leq \sum_{q \in \mathcal{S}} \Lambda(q) - \log x,$$

and, provided the denominator is positive,

$$A(x) \leq \frac{-\log x + \sum_{q \in \mathcal{S}} \Lambda(q)}{-\log x + \sum_{q \in \mathcal{S}} \Lambda(q)/\nu(q)}.$$

□



## 2 Primes

Let  $\mathcal{A}$  and  $\mathcal{B}$  be two subsets of the positive integers. We define

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}$$

as the sum of the two sets. It might be natural to try to write certain interesting sets, for instance the set of primes  $\mathcal{P}$ , as a sumset  $\mathcal{A} + \mathcal{B}$  in a nontrivial way (i.e. with  $|\mathcal{A}|, |\mathcal{B}| \geq 2$ ). It is not hard to argue that for the set of primes, this is impossible (using the fact that  $\mathcal{P}$  contains small primes such as 2 and 3). Indeed, the only way to write 2 as a sum of two positive integers is  $2 = 1 + 1$ , and 3 can only be represented as  $2 + 1$  or  $1 + 2$ . Thus, one of  $\mathcal{A}, \mathcal{B}$ , say  $\mathcal{B}$ , would have to contain  $\{1, 2\}$  (i.e. a whole system of representatives of the residue classes modulo 2); however, for  $a \in \mathcal{A} \setminus \{1\}$ ,  $a + 1$  and  $a + 2$  cannot both be prime.

Now one might wonder whether that would change if finitely many errors were allowed: that is, are there sets  $|\mathcal{A}|, |\mathcal{B}| \geq 2$  such that

$$\mathcal{A} + \mathcal{B} = \mathcal{P}'$$

and  $\mathcal{P}' \cap [x, \infty) = \mathcal{P} \cap [x, \infty)$  for sufficiently large  $x$ , that is, is the symmetric difference  $(\mathcal{A} + \mathcal{B}) \triangle \mathcal{P} = ((\mathcal{A} + \mathcal{B}) \cup \mathcal{P}) \setminus ((\mathcal{A} + \mathcal{B}) \cap \mathcal{P})$  finite? In this case, we would write

$$\mathcal{A} + \mathcal{B} \sim \mathcal{P}.$$

If this were true, we would say that the set of primes is *asymptotically additively reducible*.

The question whether or not the set of prime numbers is asymptotically additively reducible was posed by Ostmann (see [29], p. 13). Therefore, it is sometimes called “Ostmann’s problem”; it is also known as “The inverse Goldbach problem”. It is still open, but it is generally believed that such a decomposition does not exist.

Elsholtz[13] answered the analogous question (i.e. “The ternary inverse Goldbach problem”) whether

$$\mathcal{A} + \mathcal{B} + \mathcal{C} \sim \mathcal{P}$$

with three sets  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  of cardinality at least two is possible negatively. In his proof, which we discuss in the second section of this chapter, the sieves from the previous chapter play a vital role.

## 2.1 Distribution

In this subsection, we collect several theorems related to the distribution of the prime numbers (without providing proofs) that will be utilised in certain proofs throughout this thesis. One of the most well-known theorems concerning the prime numbers is certainly the following version of the prime number theorem:

**Theorem 2.1** (The Prime Number Theorem; see, for instance, [3], p.41 ). *Let*

$$\pi(x) = \sum_{p \leq x} 1$$

*denote the number of primes contained inside the interval  $[1, x]$ . Then*

$$\pi(x) \sim \frac{x}{\log x}$$

*and*

$$\vartheta(x) := \sum_{p \leq x} \log p \sim x,$$

*i.e.,  $\frac{\pi(x)}{x/\log x} \rightarrow 1$  and  $\vartheta(x)/x \rightarrow 1$  as  $x \rightarrow \infty$ .*

Moreover, for coprime positive integers  $q, a$ , let

$$\pi(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1,$$

denote the number of primes  $\leq x$  that are congruent to  $a$  modulo  $q$ , and let  $\varphi$  denote Euler's totient function, i.e.,  $\varphi(q) = |\{a \in [0, q-1] : q \text{ and } a \text{ are coprime}\}|$ . Then the primes are distributed uniformly in these coprime residue classes (see p. 419 in [24]), i.e.,

$$\pi(x; q, a) \sim \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

There are also estimates for sums related to  $\pi(x; q, a)$  when  $q$  is not necessarily a fixed constant:

**Theorem 2.2** (A version of Linnik's theorem [24, Corollary 18.8, p. 442]). *There is a positive constant  $L > 0$  such that, if  $N \geq Q^L$ ,*

$$\sum_{\substack{p \leq N \\ p \equiv 1 \pmod{Q}}} \log p \gg \frac{N}{\varphi(Q)\sqrt{Q}},$$

*where the implied constant is absolute (and  $\varphi$  denotes Euler's totient function).*

**Theorem 2.3** (Brun-Titchmarsh Inequality, [3], p. 172). *Let  $q, a$  be coprime positive integers, and let  $x, y > 0$ . Then there is an absolute constant  $c > 0$  such that for all  $y > cq$ ,*

$$\pi(x + y; q, a) - \pi(x; q, a) < \frac{2y}{\varphi(q)(5/6 + \log(y/q))}.$$

In fact, Theorem can be proved using a variant of Montgomery's larger sieve. We briefly indicate how to set up the sifting procedure:

For any prime not dividing  $q$ , let  $a'(p)$  be the inverse of  $q$  modulo  $p$ , that is,

$$qq'(p) \equiv 1 \pmod{p},$$

and let  $Q > 0$  be a parameter which we will fix momentarily. We choose

$$\begin{aligned} \mathcal{N} &= \left( \frac{x-a}{q}, \frac{x+y-a}{q} \right] \cap \mathbb{Z}, \\ \mathcal{P}' &= \{p : p \nmid q, p \leq Q\}, \\ \Omega_p &= \{-aq'(p)\}. \end{aligned}$$

Let  $\mathcal{N}^* = \{n \in \mathcal{N} : n \not\equiv -aq'(p) \pmod{p} \text{ for any } p \in \mathcal{P}'\}$  denote the sifted set. Furthermore, let  $\hat{p}$  be a prime number in  $(x, x+y]$  with  $\hat{p} \equiv a \pmod{q}$ . Then there is exactly one  $n \in \mathcal{N}$  such that

$$\hat{p} = qn + a.$$

If  $\hat{p} > Q$ , then certainly  $\hat{p} = qn + a \not\equiv 0 \pmod{p}$  for all  $p \in \mathcal{P}'$ , thus  $n \in \mathcal{N}^*$ . Hence,

$$\pi(x + y; q, a) - \pi(x; q, a) \leq \pi(Q) + |\mathcal{N}^*| \leq Q + |\mathcal{N}^*|.$$

Now, as described [3, pp. 172-178],  $|\mathcal{N}^*|$  can be bounded using a variant of Theorem 1.4; then, further analysis of the provided bound is required in order to complete the proof of Theorem 2.1.

## 2.2 The ternary inverse Goldbach problem

As announced in the introduction, we now outline the proof in [13], demonstrating that the set of primes cannot be asymptotically decomposed as

$$\mathcal{P} \sim \mathcal{A} + \mathcal{B} + \mathcal{C}$$

with  $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2$ . We start by assuming that there exist sets  $\mathcal{A}, \mathcal{B}$  with  $|\mathcal{A}|, |\mathcal{B}| \geq 2$  and

$$\mathcal{A} + \mathcal{B} \sim \mathcal{P}.$$

Then we can derive the following asymptotics for the counting functions  $A(x) = \sum_{a \in \mathcal{A}, a \leq x} 1$  and  $B(x) = \sum_{b \in \mathcal{B}, b \leq x} 1$ :

**Theorem 2.4.** *As  $x$  tends to infinity,*

$$\frac{x^{1/2}}{(\log x)^5} \ll A(x) \ll x^{1/2}(\log x)^4.$$

*The same holds for  $B(x)$ .*

It should be noted that Elsholtz and Harper [14, Theorem 2.6] improved the bounds given in Theorem 2.4 to

$$\frac{x^{1/2}}{\log x \log \log x} \ll A(x) \ll x^{1/2} \log \log x.$$

However, for our discussion, the estimates given in Theorem 2.4 suffice.

Let us discuss how sieves can be applied to this problem: Consider  $a \in \mathcal{A}$ ,  $b \in \mathcal{B}$  sufficiently large such that

$$a + b = p_1 \in \mathcal{P}.$$

Then for all primes  $p < p_1$ , we have that

$$a \not\equiv -b \pmod{p},$$

meaning that a residue class that occurs in  $\mathcal{B}$  induces a forbidden residue class in  $\mathcal{A}$ . We will sift these forbidden residue classes to obtain bounds for  $A(x)$ . On the other hand, all classes that *do not* occur in  $\mathcal{B}$  can also be used for sifting to obtain bounds for  $B(x)$ . In this way, this combined sieve method uses information about *all* residue classes.

Moreover, we know that there exists an integer  $x_0$  such that

$$(\mathcal{A} + \mathcal{B}) \cap [x_0, \infty) = \mathcal{P} \cap [x_0, \infty).$$

Thus, by the Prime Number Theorem (Theorem 2.1), an upper bound on  $A(x)$  implies a lower bound on  $B(x)$  (and vice versa). More specifically, we have  $A(x)B(x) \gg x/\log x$ .

We will see that if many residue classes could be excluded from  $\mathcal{B}$ , then we could derive an upper for  $B(x)$  that would contradict already known lower bounds. Hence the number of residue classes covered by  $\mathcal{B}$  cannot be too small, which, by the method described above, leads to a new upper bound for  $A(x)$ , which then in turn leads to a new lower bound for  $B(x)$ . We will iterate this procedure twice.

As announced in the beginning of this chapter, we will present a solution to the inverse ternary Goldbach problem. In fact, it follows directly from Theorem 2.4.

**Corollary 2.5.** *There do not exist sets  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  with  $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}| \geq 2$  and*

$$\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{P}',$$

*where  $\mathcal{P}' \cap [x_0, \infty) = \mathcal{P} \cap [x_0, \infty)$  for some  $x_0 > 0$ .*

In order to prove the corollary, we need the following lemma, which is a special case of a theorem (Theorem 3 of [30]) of Pomerance, Sárközy, and Stewart.

**Lemma 2.6.** *Let  $\epsilon > 0$ . Furthermore, let  $x \in \mathbb{N}$  and  $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \{1, \dots, x\}$  be nonempty sets of integers. If  $x$  is sufficiently large and  $\min(|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|) \geq x^{1/3+2\epsilon}$ , then there exists a prime  $p < x^{1/3+\epsilon}$  and some integer  $m \in \mathcal{A} + \mathcal{B} + \mathcal{C}$  such that  $p \mid m$ .*

*Proof of the corollary.* Let  $\epsilon > 0$ . Since  $(\mathcal{A} + \mathcal{B}) + \mathcal{C} = (\mathcal{A} + \mathcal{C}) + \mathcal{B} = \mathcal{A} + (\mathcal{B} + \mathcal{C})$ , we can apply the theorem to each of the three sets. This yields

$$A(x), B(x), C(x) \gg \frac{x^{1/2}}{(\log x)^5} \gg x^{1/2-\epsilon}.$$

Moreover, if we set  $\mathcal{A}_1 = \mathcal{A} \cap [x^{2/5}, \infty)$ , then we still have  $A_1(x) \gg x^{1/2-\epsilon}$ .

Now we choose  $x$  large enough that  $P \cap [x, \infty) = P' \cap [x, \infty)$  and that the lemma can be applied. Then there exist some  $m \in \mathcal{A}_1 + \mathcal{B} + \mathcal{C}$  and some prime  $p < x^{1/3+\epsilon}$  such that  $p \mid m = a_1 + b + c \geq a_1 \geq x^{2/5} > x^{1/3+\epsilon} > p$ . Therefore  $m \in \mathcal{A} + \mathcal{B} + \mathcal{C}$  is composite.  $\square$

The first iteration of our sifting process leads to the following proposition.

**Proposition 2.7.** *Let  $\epsilon > 0$ . Then, as  $x \rightarrow \infty$ ,*

$$x^{1/2-\epsilon} \ll A(x) \ll x^{1/2+\epsilon}.$$

*The same bounds hold for  $B(x)$ .*

*Proof.* Let  $x \geq x_0^2$ . Then we know that  $\mathcal{P}' \cap [x^2, \infty) = \mathcal{P} \cap [x^2, \infty)$ . We set  $\mathcal{A}_1 = \mathcal{A} \cap (x^{1/2}, x)$  and  $\mathcal{B}_1 = \mathcal{B} \cap (0, x)$ .

For primes  $p \in (x_0, x^{1/2})$ , let  $\nu_{\mathcal{A}_1}(p)$  and  $\nu_{\mathcal{B}_1}(p)$  denote the number of residue classes modulo  $p$  that contain elements of  $\mathcal{A}_1$  and  $\mathcal{B}_1$ , respectively.

For any integers  $a_1 \in \mathcal{A}_1, b_1 \in \mathcal{B}_1$ , we have that  $a_1 + b_1$  is a prime strictly greater than  $x^{1/2}$ , so it follows that

$$a_1 + b_1 \not\equiv 0 \pmod{p}$$

for all primes  $p \leq x^{1/2}$ .

To get our sifting routine started, we need already known lower bounds for  $B(x)$ ; we sketch Hornfeck's bounds. Since  $|\mathcal{B}| \geq 2$ , we can apply Montgomery's sieve (Corollary 1.4) with  $\omega(p) = 2$ . This leads to

$$\begin{aligned} A(x) &\leq \frac{2x}{\sum_{q \leq x^{1/2}} \mu^2(q) \prod_{p|q} \frac{2}{p-2}} \\ &\leq \frac{2x}{\sum_{q \leq x^{1/2}} \mu^2(q) \prod_{p|q} \frac{2}{p}} \\ &\leq \frac{2x}{\sum_{q \leq x^{1/2}} \frac{d(q)}{q}} \\ &\ll \frac{x}{(\log x)^2}, \end{aligned}$$

where  $d$  is the divisor function, i.e.  $d(n) = |\{m \in \mathbb{N} : n = mk \text{ for some } k \in \mathbb{N}\}|$ ; the last inequality is due to the fact that (see for instance [3], p. 12)

$$\sum_{n \leq N} d(n) = N \log N + O(N),$$

so by partial summation (as in [3], Lemma 1.1.3, p. 9)

$$\begin{aligned} \sum_{n \leq N} \frac{d(n)}{n} &= \log N + O(1) + \int_1^N \left( \frac{\log x}{x} + \frac{O(1)}{x} \right) dx \\ &= \log N + O(1) + \frac{1}{2}(\log N)^2 + O(\log N) \\ &\gg (\log N)^2. \end{aligned}$$

From  $A(x)B(x) \gg x/\log x$ , we now get  $B(x) \gg \log x$ . In particular,  $\mathcal{B}$  is infinite, so a similar argument to above shows for any  $k \in \mathbb{N}$  that  $A(x) \ll x/(\log x)^{k+1}$  and  $B(x) \gg (\log x)^k$ .

*Iteration A.* We will use the bound for  $L$  in Montgomery's sieve that we described in Remark 1.1 with the following choice of  $m$ :

$$m = m_A = \left\lfloor \frac{\epsilon}{4} \frac{\log x}{\log \log x} \right\rfloor.$$

Let  $y = x^{1/(2m)}$ . Then

$$y \sim x^{\frac{2}{\epsilon} \frac{\log \log x}{\log x}} = \exp \left( \log x \frac{2}{\epsilon} \frac{\log \log x}{\log x} \right) = (\log x)^{\frac{2}{\epsilon}}.$$

We split the primes that we will use for the sieve process, i.e. the primes in the interval  $(x_0, y]$ , into two sets, namely

$$\begin{aligned}\mathcal{P}_{A1} &= \{p \in \mathcal{P} \cap (x_0, y] : \nu_{\mathcal{B}_1}(p) < p^{1-\epsilon}\}, \\ \mathcal{P}_{A2} &= \{p \in \mathcal{P} \cap (x_0, y] : \nu_{\mathcal{B}_1}(p) \geq p^{1-\epsilon}\}.\end{aligned}$$

We say that condition A1 is satisfied if  $\mathcal{P}_{A1}$  contains at least half of the primes in the interval  $(x_0, y]$ , and analogously, condition A2 is satisfied if  $\mathcal{P}_{A2}$  contains at least half of the primes in the interval  $(x_0, y]$ . Clearly, one of these two conditions must be fulfilled.

We note that in the case of condition A1, many residue classes are sifted from  $\mathcal{B}_1$ . The plan is therefore to derive a lower bound for  $B(x)$  that contradicts Hornfeck's bounds using Gallagher's sieve. Knowing that hence condition A2 must be fulfilled, we use Montgomery's sieve to derive a new lower bound for  $A(x)$  (and thus a new upper bound for  $B(x)$ ).

Before we start sifting, we list a few general remarks regarding the asymptotics of certain sums over primes.

*Remark 2.1.* We recall that by Prime Number Theorem (Theorem 2.1) (see, for instance, [3] on p. 41), for  $N \rightarrow \infty$ ,

$$\sum_{p \leq N} \log p \sim N,$$

which implies that

$$\sum_{p \leq N} \frac{\log p}{p^{1-\epsilon}} \gg \sum_{p \leq N} \frac{\log p}{N^{1-\epsilon}} \sim \frac{N}{N^{1-\epsilon}} = N^\epsilon.$$

Another consequence of the Prime Number Theorem is that, as  $y \rightarrow \infty$ , the interval  $(2y/3, y]$  contains approximately a third of the primes in the interval  $(x_0, y]$ .

As a direct consequence of Remark 2.1, we get the following lemma:

**Lemma 2.8.** *We have that*

$$-\log x + \sum_{p \in \mathcal{P}_{A1}} \log p \ll y.$$

**Lemma 2.9.** *Suppose that condition A1 is satisfied. Then*

$$\sum_{p \in \mathcal{P}_{A1}} \frac{\log p}{p^{1-\epsilon}} \gg y^\epsilon.$$

*Proof of the lemma.* Since condition A1 holds, we know that in the sum

$$\sum_{p \in \mathcal{P}_{A1}} \frac{\log p}{p^{1-\epsilon}},$$

we are summing over at least half of the primes in the interval  $(x_0, y]$ . Since  $\log p/p^{1-\epsilon}$  is monotonically decreasing, the sum is smallest if the  $p$  are as large as possible. This, in conjunction with our earlier remarks on the Prime Number Theorem (Theorem 2.1) in Remark 2.1, justifies the following approximation:

$$\sum_{p \in \mathcal{P}_{A1}} \frac{\log p}{p^{1-\epsilon}} \gg \sum_{p \in \mathcal{P} \cap (2y/3, y]} \frac{\log p}{p^{1-\epsilon}} \gg y^\epsilon - \left(\frac{2y}{3}\right)^\epsilon \gg y^\epsilon \quad \square$$

Due to the fact that  $y^\epsilon \sim (\log x)^2 \gg \log x$  and  $\frac{1}{\nu_{B_1}(p)} \gg \frac{1}{p^{1-\epsilon}}$  for  $p \in \mathcal{P}_{A1}$ , the previous Lemma 2.9 implies:

**Lemma 2.10.** *Suppose that condition A1 is satisfied. Then*

$$-\log x + \sum_{p \in \mathcal{P}_{A1}} \frac{\log p}{\nu_{B_1}(p)} \gg y^\epsilon.$$

**Lemma 2.11.** *Suppose that condition A2 holds. With  $\omega(p) = \nu_{B_1}(p) \geq p^{1-\epsilon}$  for  $p \in \mathcal{P}_{A2}$ , we have that*

$$\sum_{p \in \mathcal{P}_{A2}} \frac{\omega(p)}{p} \gg \frac{y^{1-\epsilon}}{\log y}$$

as  $y \rightarrow \infty$ .

*Proof of the lemma.* We can argue similarly to the proof of Lemma 2.9. Indeed, an application of an almost identical monotonicity argument yields

$$\sum_{p \in \mathcal{P}_{A2}} \frac{\omega(p)}{p} \gg \sum_{p \in \mathcal{P}_{A2}} \frac{p^{1-\epsilon}}{p} \gg \left( \pi(y) - \pi\left(\frac{2}{3}y\right) \right) y^{-\epsilon} \gg \frac{y^{1-\epsilon}}{\log y}. \quad \square$$

**1. Case: Condition A1 holds.** We apply Gallagher's sieve from Theorem 1.6 with  $\mathcal{S} = \mathcal{P}_{A1}$  and  $\nu(p) = \nu_{B_1}(p)$ , so

$$B(x) \leq \frac{-\log x + \sum_{p \in \mathcal{P}_{A1}} \log p}{-\log x + \sum_{p \in \mathcal{P}_{A1}} \log p / \nu_{B_1}(p)},$$

where the denominator is positive for sufficiently large  $x$  by Lemma 2.10. Moreover, since  $\nu_{B_1}(p) \leq p^{1-\epsilon}$ , and by Lemma 2.8 and Lemma 2.10,

$$B(x) \leq \frac{-\log x + \sum_{p \in \mathcal{P}_{A1}} \log p}{-\log x + \sum_{p \in \mathcal{P}_{A1}} \log p / p^{1-\epsilon}} \ll \frac{y}{y^\epsilon} = y^{1-\epsilon} \ll (\log x)^{2(1-\epsilon)/\epsilon}.$$

This contradicts previous lower bounds on  $B(x)$  (i.e. Hornfeck's bound), so the second case must be true.



**2. Case: Condition A2 holds.** We use Montgomery's sieve from Corollary 1.4 with  $\omega(p) = \nu_{B_1}(p) \geq p^{1-\epsilon}$  for  $p \in \mathcal{P}_{A_2}$  to bound  $A_1(x) \leq 2x/L$ .

By Remark 1.1, we get the following bound (where the second line, with an appropriate constant  $c > 0$ , follows from Lemma 2.11):

$$\begin{aligned}
L &\geq \exp \left( m \log \left( \frac{1}{m} \sum_{p \in \mathcal{P}_{A_2}} \frac{\omega(p)}{p} \right) \right) \\
&\geq \exp \left( m \log \left( \frac{c}{m} \frac{(x^{1/(2m)})^{1-\epsilon}}{\log(x^{1/(2m)})} \right) \right) \\
&= \exp \left( m \log \left( \frac{2cx^{(1-\epsilon)/(2m)}}{\log(x)} \right) \right) \\
&= \exp \left( m \left( \log 2 + \log c - \log \log x + \frac{1-\epsilon}{2m} \log x \right) \right) \\
&\gg \exp \left( m (\log 2 + \log c) + \left( \frac{1}{2} - \frac{\epsilon}{2} - \frac{\epsilon}{4} \right) \log x \right) \\
&\gg x^{1/2-\epsilon},
\end{aligned}$$

where, as stated previously,  $m = m_A = \left\lfloor \frac{\epsilon}{4} \frac{\log x}{\log \log x} \right\rfloor$ . Therefore,

$$A(x) = A_1(x) + O(x^{1/2}) \ll x^{1/2+\epsilon},$$

for any  $\epsilon > 0$ . Since  $A(x)B(x) \gg \pi(x) \sim x/\log x \gg x^{1-\delta}$  for any  $\delta > 0$ , this also implies that  $B(x) \gg x^{1/2-\hat{\epsilon}}$  for any  $\hat{\epsilon} > 0$ . The remaining statements of Proposition 2.7 follow by symmetry.  $\square$

*Iteration B.* We start our sifting procedure from anew, so we can utilize the bounds gained from the first iteration. We apply the same argument with different parameters: we let  $m = 2$ , so  $y = x^{1/4}$ ,  $c = 20$ . Again, we split the primes in the interval  $(x_0, y]$  into two sets, this time

$$\begin{aligned}
\mathcal{P}_{B_1} &= \{p \in \mathcal{P} \cap (x_0, y] : \nu_{B_1}(p) < p/(c \log p)\}, \\
\mathcal{P}_{B_2} &= \{p \in \mathcal{P} \cap (x_0, y] : \nu_{B_1}(p) \geq p/(c \log p)\}.
\end{aligned}$$

We say that condition  $B_i$ , where  $i = 1, 2$ , is satisfied if the set  $\mathcal{P}_{B_i}$  contains at least half of the primes.

Condition B1 is true in the case where  $\mathcal{B}$  covers too few different residue classes. Again, we will apply Gallagher's sieve to show that this case is impossible; then we will use Montgomery's sieve to get a new bound on  $A(x)$ .

**1. Case: Condition B1 holds.** In this case, we see that for sufficiently large  $y$ ,

$$\begin{aligned}
 \sum_{p \in \mathcal{P}_{B1}} \frac{\log p}{\nu_{B1}(p)} &\geq \sum_{p \in \mathcal{P}_{B1}} \frac{c(\log p)^2}{p} \\
 &\geq \frac{c}{2} \left( (\log y)^2 - \left( \log \frac{2y}{3} \right)^2 \right) \\
 &= \frac{c}{2} \left( (\log y)^2 - \left( \log \frac{2}{3} + \log y \right)^2 \right) \\
 &= c \left( \log \frac{3}{2} \right) (\log y) - \frac{c}{2} \left( \log \frac{2}{3} \right)^2 \\
 &\geq 2 \log x,
 \end{aligned}$$

and an application of Gallagher's sieve shows

$$B(x) \leq \frac{-\log x + \sum_{p \in \mathcal{P}_{B1}} \log p}{-\log x + \sum_{p \in \mathcal{P}_{B1}} \log p / \nu_{B1}(p)} \leq \frac{y}{\log x} = \frac{x^{1/4}}{\log x}.$$

This contradicts the bounds from Proposition 2.7, so Condition B1 holds.

**2. Case: Condition B2 holds.** We apply Montgomery's sieve with  $\omega(p) = \nu_{B1}(p) \geq p/(c \log p)$  for  $p \in \mathcal{P}_{B2}$ . Then (with appropriate constants  $c'$  and  $c''$ ):

$$\begin{aligned}
 L &\geq \exp \left( m \log \left( \frac{1}{m} \sum_{p \in \mathcal{P}_{B2}} \frac{\nu_{B1}(p)}{p} \right) \right) \\
 &\geq \exp \left( m \log \left( \frac{1}{m} \sum_{p \in \mathcal{P}_{B2}} \frac{1}{c \log p} \right) \right) \\
 &\geq \exp \left( m \log \left( \frac{c'}{m} \frac{y}{(\log y)^2} \right) \right) \\
 &= \exp \left( 2 \log \left( \frac{c'}{2} \frac{x^{1/4}}{(\log x^{1/4})^2} \right) \right) \\
 &= \exp \left( \frac{1}{2} \log x - 4 \log \log x + c'' \right) \\
 &\gg x^{1/2} (\log x)^{-4}.
 \end{aligned}$$

Therefore,  $A_1(x) \leq 2x/L \ll x^{1/2} (\log x)^4$ . Consequently

$$A(x) \ll A_1(x) + O(x^{1/2}) \ll x^{1/2} (\log x)^4$$

and

$$B(x) \gg x^{1/2} (\log x)^{-5}.$$

By symmetry, the same bounds hold for  $B(x)$  and  $A(x)$ , respectively.  $\square$

# 3 Squares

## 3.1 Previous results

Let  $\mathcal{S} = \{1, 4, 9, \dots\}$  denote the set of all squares of positive integers. In this chapter, we want to investigate sets  $\mathcal{A}, \mathcal{B} \subset \mathbb{N}$  with

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\} \subseteq \mathcal{S}.$$

First of all, we note that  $\mathcal{S}$  is *asymptotically additively reducible* (as defined in chapter 2). Indeed, suppose there were sets  $\mathcal{A}, \mathcal{B} \subset \mathbb{N}$ ,  $|\mathcal{A}|, |\mathcal{B}| \geq 2$ ,

$$\mathcal{A} + \mathcal{B} = \mathcal{S}',$$

such that the symmetric difference  $\mathcal{S}' \triangle \mathcal{S}$  is finite. Since there are infinitely many squares, at least one of  $\mathcal{A}$  and  $\mathcal{B}$ , say  $\mathcal{A}$ , would need to be infinite. Furthermore,  $\mathcal{B}$  would necessarily contain at least two elements,  $b_1$  and  $b_2$ . Consequently, for any element  $a \in \mathcal{A}$ , both  $a + b_1$  and  $a + b_2$  would belong to  $\mathcal{S}'$ . This implies that  $\mathcal{S}'$  would have infinitely many pairs of elements with difference  $|b_1 - b_2|$ , whereas the gap between consecutive squares in  $\mathcal{S}$ ,  $(n+1)^2 - n^2 = 2n+1$ , approaches infinity (so only finitely many squares can differ by  $|b_1 - b_2|$ ). This contradicts the finiteness of  $\mathcal{S} \triangle \mathcal{S}'$ .

Nevertheless, this still leaves open the question of how large one of the summands can be, given that the other one is of a certain size. For  $|\mathcal{A}| = 2, 3$ , it is known that there exist arbitrarily large sets  $\mathcal{B}$  such that  $\mathcal{A} + \mathcal{B} \subset \mathcal{S}$ . In fact, according to [32] (Theorem 4), for the case  $|\mathcal{A}| = 2$ , a set  $\mathcal{B} \subset [1, N]$  can be as large as  $\exp((\log 2 - o(1)) \log N / \log \log N)$ , but at most  $\exp((\log 2 + o(1)) \log N / \log \log N)$ . For the case  $|\mathcal{A}| = 3$ , it has been shown in [12] that it is possible to have  $\mathcal{B} \subset [1, N]$  with  $|\mathcal{B}| \gg (\log N)^{15/17}$ . By contrast, it is conjectured that for  $|\mathcal{A}| \geq 4$ , the set  $\mathcal{B}$  is bounded by an absolute constant: in [1] (p. 19), the authors explain that this would be follow from the *Bombieri-Lang conjecture*.

Moreover, by employing Gallagher's larger sieve 1.6 (as demonstrated in [20], Theorem 9), it is possible to establish that

$$\min(|\mathcal{A}|, |\mathcal{B}|) \ll \log N,$$

where  $\mathcal{A}, \mathcal{B} \subset [1, N]$ ,  $\mathcal{A} + \mathcal{B} \subset \mathcal{S}$ . In section 3.2, we explain how to derive this bound (Theorem 3.11). Moreover, we discuss what can be said about the cardinality of  $\mathcal{B}$

when  $|\mathcal{A}|$  exceeds the mentioned bound, specifically when  $|\mathcal{A}|$  is slightly above that bound, say  $|\mathcal{A}| \geq m \log N$  for some constant  $m$ . To accomplish this, we will use sieve methods and a character sum estimate. Therefore, in Section 3.2 of this chapter we will analyse  $\mathcal{A} + \mathcal{B}$  reduced modulo  $p$ , and encounter some results that are interesting in their own right.

## 3.2 Bounds in $\mathbb{Z}/p\mathbb{Z}$

As discussed above, we want to bound the cardinality of sets  $\mathcal{A}, \mathcal{B} \subseteq [1, N]$  such that  $\mathcal{A} + \mathcal{B} \subset \mathcal{S}$ . To utilize sieve methods effectively, we must first examine the quantities

$$\begin{aligned}\nu_{\mathcal{A}}(p) &= |\{x \in \mathbb{Z}/p\mathbb{Z} : \text{there is } a \in \mathcal{A} \text{ such that } a \equiv x \pmod{p}\}|, \\ \nu_{\mathcal{B}}(p) &= |\{y \in \mathbb{Z}/p\mathbb{Z} : \text{there is } b \in \mathcal{B} \text{ such that } b \equiv y \pmod{p}\}|,\end{aligned}$$

for prime numbers  $p$ . It is clear that this corresponds to studying the cardinality of sets  $\mathcal{A}_p, \mathcal{B}_p \subseteq \mathbb{Z}/p\mathbb{Z}$  with

$$\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_{p,0} := \{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}.$$

In this section, we thus explore the relationship between  $\mathcal{A}_p$  and  $\mathcal{B}_p$  and establish certain upper bounds.

### 3.2.1 Weil's inequality

In several proofs, we will rely on a lemma due to Weil (Theorem 2C, p.43, in [35]) that provides a useful estimate for sums involving multiplicative characters (such as the Legendre symbol).

**Lemma 3.1** (Weil). *Let  $\chi$  be a multiplicative character of order  $d > 1$  of  $\mathbb{Z}/p\mathbb{Z}$ . Assume that  $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$  has  $k$  distinct zeros in the algebraic closure of  $\mathbb{Z}/p\mathbb{Z}$  and that it is not a constant multiple of the  $d$ th power of a polynomial over  $\mathbb{Z}/p\mathbb{Z}$ . Then the following bound holds:*

$$\left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi(f(x)) \right| \leq (k-1)\sqrt{p}.$$

The proof of Lemma 3.1 is beyond the scope of this thesis. However, it is worth mentioning that it can be derived from the *Riemann hypothesis in function fields*, which has been established by Weil in the 1940s, following Hasse's proof for the special case of elliptic curves in the 1930s. (For additional information, we refer to Appendix A in [33], where a more modern proof due to Bombieri is presented. Further details on deriving related bounds can also be found in [39] as well as Section 4.4 in [28].)

### 3.2.2 Quadratic residue patterns

In this subsection, we analyse the frequency of recurring fixed patterns in  $\mathbb{Z}/p\mathbb{Z}$  (for instance, three consecutive quadratic residues followed by a nonresidue) and establish a bound for their occurrence. Our exposition is based on the enlightening discussion provided in [7].

Firstly, we recall that the set

$$\mathcal{Q}_p = \{x^2 : x \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

is called the set of **quadratic residues** (modulo  $p$ ). Furthermore, we recall that the **Legendre symbol** is a quadratic character modulo  $p$  (if  $p$  is an odd prime), defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x \in \mathcal{Q}_p, \\ 0 & \text{if } x = 0, \\ -1 & \text{if } x \in (\mathbb{Z}/p\mathbb{Z})^* \setminus \mathcal{Q}_p. \end{cases}$$

Now, let us assume that

$$\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p,$$

and that  $\mathcal{B}_p = \{b_1, \dots, b_k\}$  is some fixed set with  $k$  elements. Then every element  $a \in \mathcal{A}_p$  gives us a certain pattern: namely elements  $a + b_1, \dots, a + b_k$  with certain gaps, all lying in  $\mathcal{Q}_p$ . In a similar vein, given a set with  $\ell$  elements  $\{c_1, \dots, c_\ell\}$ , one might ask how many  $a \in \mathbb{F}_p$  satisfy the pattern

$$\left(\frac{a + c_i}{p}\right) = \epsilon_i \quad \text{for } i = 1, \dots, \ell,$$

where  $(\epsilon_1, \dots, \epsilon_\ell) \in \{-1, 1\}^\ell$ . Let us briefly examine some heuristics: Approximately half of the elements of  $\mathbb{F}_p$  are nonresidues and residues, respectively. Thus, if we were considering independent random variables  $X_{i,a}$  that could take values in  $\{-1, 1\}$  with equal probabilities, the probability that

$$(X_{1,a}, \dots, X_{\ell,a}) = (\epsilon_1, \dots, \epsilon_\ell)$$

would be  $(1/2)^\ell$ . Hence, the expected number of  $a \in \mathbb{F}_p$  fitting the pattern, i.e., the expected value of the random variable

$$Y = \sum_{a \in \mathbb{F}_p} \mathbf{1}_{[(X_{1,a}, \dots, X_{\ell,a}) = (\epsilon_1, \dots, \epsilon_\ell)]},$$

where  $\mathbf{1}_A$  denotes the indicator random variable of the event  $A$ , would be

$$\mathbb{E}(Y) = \frac{p}{2^\ell}.$$

In fact, defining, for  $\vec{c} = (c_1, \dots, c_\ell)$ ,  $\vec{\epsilon} = (\epsilon_1, \dots, \epsilon_\ell)$ , the number

$$N_p(\vec{c}, \vec{\epsilon}) := \left| \left\{ a \in \mathbb{F}_p : \left( \frac{a + c_i}{p} \right) = \epsilon_i \text{ for } i = 1, \dots, \ell \right\} \right|$$

of  $a \in \mathbb{F}_p$  satisfying a certain pattern, we can prove the following:

**Theorem 3.2.** *With  $N_p(\vec{c}, \vec{\epsilon})$  defined as above, we have*

$$\left| N_p(\vec{c}, \vec{\epsilon}) - \frac{p}{2^\ell} \right| \leq \frac{\ell}{2} \sqrt{p} + \frac{\ell}{2}.$$

We observe that the error bound is in  $O_\ell(\sqrt{p})$ , as is the standard deviation of the random variable  $Y$  discussed above.

*Proof.* We remark that

$$h_{c_i, \epsilon_i}(a) := \frac{1}{2} \left( 1 + \epsilon_i \left( \frac{a + c_i}{p} \right) \right) = \begin{cases} 1 & \text{if } \left( \frac{a + c_i}{p} \right) = \epsilon_i, \\ 0 & \text{if } \left( \frac{a + c_i}{p} \right) = -\epsilon_i, \\ 1/2 & \text{if } \left( \frac{a + c_i}{p} \right) = 0, \end{cases}$$

and let

$$h(a) = \prod_{i=1}^{\ell} h_{c_i, \epsilon_i}(a).$$

We note that  $h(a) = 1$  if and only if  $a$  matches the pattern. Otherwise, either  $h(a) = 1/2$  (which happens only if the  $a + c_i = 0$  and all other  $a + c_j$  fit the pattern, so at most  $\ell$  times), or  $h(a) = 0$ . Hence,

$$N_p(\vec{c}, \vec{\epsilon}) = \sum_{a \in \mathbb{F}_p} h(a) + \frac{e_\ell}{2},$$

where  $|e_\ell| \leq \ell$ . Plugging in the definition of  $h$  and expanding the product (and using

the multiplicativity of the Legendre symbol), we get

$$\begin{aligned}
N_p(\vec{c}, \vec{\epsilon}) &= \sum_{a \in \mathbb{F}_p} \prod_{i=1}^{\ell} \frac{1}{2} \left( 1 + \epsilon_i \left( \frac{a + c_i}{p} \right) \right) + \frac{e_\ell}{2} \\
&= \frac{1}{2^\ell} \sum_{a \in \mathbb{F}_p} \prod_{i=1}^{\ell} \left( 1 + \epsilon_i \left( \frac{a + c_i}{p} \right) \right) + \frac{e_\ell}{2} \\
&= \frac{1}{2^\ell} \sum_{a \in \mathbb{F}_p} \left( 1 + \sum_{\substack{I \subseteq [1, \ell] \\ I \neq \emptyset}} \prod_{i \in I} \epsilon_i \left( \frac{a + c_i}{p} \right) \right) + \frac{e_\ell}{2} \\
&= \frac{p}{2^\ell} + \frac{1}{2^\ell} \sum_{\substack{I \subseteq [1, \ell] \\ I \neq \emptyset}} \left( \prod_{i \in I} \epsilon_i \right) \sum_{a \in \mathbb{F}_p} \left( \frac{f_I(a)}{p} \right) + \frac{e_\ell}{2},
\end{aligned}$$

where

$$f_I(a) = \prod_{i \in I} (a + c_i)$$

We can apply Weil's lemma 3.1 to bound each summand  $|\sum_{a \in \mathbb{F}_p} \left( \frac{f_I(a)}{p} \right)| \leq (|I| - 1)\sqrt{p}$ , so that (by the triangle inequality),

$$\begin{aligned}
\left| N_p(\vec{c}, \vec{\epsilon}) - \frac{p}{2^\ell} \right| &\leq \frac{1}{2^\ell} \sum_{\substack{I \subseteq [1, \ell] \\ I \neq \emptyset}} (|I| - 1)\sqrt{p} + \frac{e_\ell}{2} \\
&= \frac{1}{2^\ell} \sqrt{p} \sum_{j=1}^{\ell} \binom{\ell}{j} (j - 1) + \frac{e_\ell}{2} \\
&< \frac{1}{2^\ell} \sqrt{p} \sum_{j=1}^{\ell} \binom{\ell}{j} j + \frac{e_\ell}{2} \\
&= \ell \frac{2^{\ell-1}}{2^\ell} \sqrt{p} + \frac{e_\ell}{2} \\
&= \ell \frac{\sqrt{p}}{2} + \frac{e_\ell}{2}. \quad \square
\end{aligned}$$

We want to estimate the cardinality of the sets  $\mathcal{A}$  and  $\mathcal{B}$  such that  $\mathcal{A} + \mathcal{B} \subset \mathcal{S} \cap [1, N]$ , where  $\mathcal{S}$  denotes the set squares. Let  $p$  be a prime,  $\mathcal{A}_p = \mathcal{A} \bmod p$ ,  $\mathcal{B}_p = \mathcal{B} \bmod p$ . Then

$$\mathcal{A}_p + \mathcal{B}_p \subset \mathcal{Q}_{p,0},$$

where  $\mathcal{Q}_{0,p} = \mathcal{Q}_p \cup \{0\}$ , with  $\mathcal{Q}_p$  the set of quadratic residues modulo  $p$ . We can adapt the proof of Theorem 3.2 in order to get a relation between  $\nu_{\mathcal{A}}(p) = |\mathcal{A}_p|$  and  $\nu_{\mathcal{B}}(p) = |\mathcal{B}_p|$ :

**Lemma 3.3.** *Let  $\ell \in \mathbb{N}$ ,  $\ell < p$ ,  $\mathcal{B}_1 = \{b_1, \dots, b_\ell\} \subset \mathbb{F}_p$ , where  $p$  is a prime. Let  $\mathcal{Q}$  denote the set of quadratic residues, and let  $\mathcal{Q}_{0,p} = \mathcal{Q} \cup \{0\}$ . If  $\mathcal{A}_p \subset \mathbb{F}_p$  and*

$$\mathcal{A}_p + \mathcal{B}_p \subset \mathcal{Q}_{0,p},$$

*then*

$$|\mathcal{A}_p| \leq \frac{p}{2^{\ell-1}} + \ell p^{1/2}.$$

*Proof.* Let

$$h(x) = \frac{1}{2^\ell} \prod_{i=1}^{\ell} \left( \frac{x + b_i}{p} \right).$$

We note that, for every  $a \in \mathcal{A}_p$ , the elements  $a + b_1, \dots, a + b_\ell$  are distinct (since the  $b_i$  are distinct) elements of  $\mathcal{Q}_{0,p}$ , so in particular at most one them is zero, all others are residues. Thus

$$h(a) \geq 1/2,$$

and, since  $h(x) \geq 0$  for all  $x \in \mathbb{F}_p$ ,

$$\sum_{x \in \mathbb{F}_p} h(x) \geq \sum_{a \in \mathcal{A}_p} h(a) \geq \frac{1}{2} |\mathcal{A}_p|.$$

Now, the proof of theorem 3.2 shows that on the other hand,

$$\sum_{x \in \mathbb{F}_p} h(x) < \frac{p}{2^\ell} + \frac{\ell}{2} p^{1/2}.$$

Combining these two inequalities gives the desired result

$$|\mathcal{A}_p| \leq \frac{p}{2^{\ell-1}} + \ell p^{1/2}. \quad \square$$

Lemma 3.3 implies the following:

**Corollary 3.4.** *Let  $\mathcal{A}, \mathcal{B} \subset \mathbb{N}$  be sets of positive integers such that their sumset  $\mathcal{A} + \mathcal{B} \subset \mathcal{S}$  lies in the squares. Let  $p$  be a prime number and define (as before)*

$$\begin{aligned} \nu_{\mathcal{A}}(p) &= |\{x \in \mathbb{Z}/p\mathbb{Z} : \text{there is } a \in \mathcal{A} \text{ such that } a \equiv x \pmod{p}\}|, \\ \nu_{\mathcal{B}}(p) &= |\{y \in \mathbb{Z}/p\mathbb{Z} : \text{there is } b \in \mathcal{B} \text{ such that } b \equiv y \pmod{p}\}|. \end{aligned}$$

*Then we have*

$$\nu_{\mathcal{A}}(p) \leq \frac{p}{2^{\nu_{\mathcal{B}}(p)-1}} + \nu_{\mathcal{B}}(p) p^{1/2}.$$

It is worth noting that the bound in Corollary 3.4 is particularly relevant when considering  $\nu_{\mathcal{B}}(p) \leq \log p$ , as its effectiveness does not increase beyond that threshold.



### 3.2.3 Further bounds on $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p \cup \{0\}$

We proceed with our examination of the cardinality of sets  $\mathcal{A}_p, \mathcal{B}_p$ , where their sumset lies in the quadratic residues  $\mathcal{Q}_p$  (and possibly  $\{0\}$ ) modulo a prime  $p$ . We begin by presenting a more general lemma by Erdős and Shapiro [16] that can be applied to our specific situation.

**Lemma 3.5.** *For any nonprincipal character  $\chi$ , and any two sets  $\mathcal{A}_p, \mathcal{B}_p \subseteq \mathbb{Z}/p\mathbb{Z}$ ,*

$$\left| \sum_{\substack{a \in \mathcal{A}_p, \\ b \in \mathcal{B}_p}} \chi(a+b) \right| \leq \sqrt{p} \sqrt{|\mathcal{A}_p| |\mathcal{B}_p|}$$

*Proof.* Let

$$\tau(\chi) = \sum_{h=1}^p \chi(h) e(h/p).$$

Then (see, for instance, [24], p. 48, Lemma 3.1)

$$|\tau(\chi)| = \sqrt{p}.$$

Moreover,

$$\tau(\bar{\chi})\chi(t) = \sum_{h=1}^p \bar{\chi}(h) e(ht/p),$$

so

$$\tau(\bar{\chi}) \sum_{\substack{a \in \mathcal{A}_p, \\ b \in \mathcal{B}_p}} \chi(a+b) = \sum_{h=1}^p \sum_{\substack{a \in \mathcal{A}_p, \\ b \in \mathcal{B}_p}} \bar{\chi}(h) e(h(a+b)/p)$$

Taking absolute values, applying the triangle inequality and then the Cauchy-Schwarz inequality, we get

$$\begin{aligned} \sqrt{p} \left| \sum_{\substack{a \in \mathcal{A}_p, \\ b \in \mathcal{B}_p}} \chi(a+b) \right| &\leq \sum_{h=1}^p \left| \sum_{a \in \mathcal{A}_p} e(ha/p) \right| \left| \sum_{b \in \mathcal{B}_p} e(hb/p) \right| \\ &\leq \left( \sum_{h=1}^p \left| \sum_{a \in \mathcal{A}_p} e(ha/p) \right|^2 \sum_{h=1}^p \left| \sum_{b \in \mathcal{B}_p} e(hb/p) \right|^2 \right)^{1/2}. \end{aligned}$$

Now,

$$\sum_{h=1}^p \left| \sum_{a \in \mathcal{A}_p} e(ha/p) \right|^2 = \sum_{h=1}^p \sum_{a, a' \in \mathcal{A}_p} e(ha/p) e(ha'/p) = \sum_{a, a' \in \mathcal{A}_p} \sum_{h=1}^p e(ha/p) e(ha'/p) = p |\mathcal{A}_p|,$$

and (analogously)

$$\sum_{h=1}^p \left| \sum_{b \in \mathcal{B}} e(hb/p) \right|^2 = p |\mathcal{B}_p|. \quad \square$$

In our case, i.e.,  $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p \cup \{0\}$ , we have

$$(|\mathcal{A}_p| - 1) |\mathcal{B}_p| \leq \sqrt{p} \sqrt{|\mathcal{A}_p| |\mathcal{B}_p|}.$$

If  $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p$ , this can be improved to

$$|\mathcal{A}_p| |\mathcal{B}_p| = \left| \sum_{\substack{a \in \mathcal{A}_p, \\ b \in \mathcal{B}_p}} \chi(a+b) \right| \leq \sqrt{p} \sqrt{|\mathcal{A}_p| |\mathcal{B}_p|} \leq \sqrt{p} \sqrt{|\mathcal{A}_p| |\mathcal{B}_p|},$$

so

$$|\mathcal{A}_p| |\mathcal{B}_p| \leq p.$$

In [22], Hanson and Petridis proved the following theorem.

**Theorem 3.6.** *Let  $p$  be a prime and let  $Z_d = \{z \in \mathbb{Z}/p\mathbb{Z} : z^d = 1\}$ . Assume that we have  $\mathcal{A}_p, \mathcal{B}_p \subseteq \mathbb{Z}/p\mathbb{Z}$  such that  $\mathcal{A}_p + \mathcal{B}_p \subseteq Z_d \cup \{0\}$ . Then*

$$|\mathcal{A}_p| \cdot |\mathcal{B}_p| \leq d + |\mathcal{A}_p \cap (-\mathcal{B}_p)|,$$

where  $-\mathcal{B}_p = \{-b : b \in \mathcal{B}_p\}$ .

Before discussing the proof of Theorem 3.6, it is worth pointing out that  $\mathcal{Q}_p = Z_{(p-1)/2}$ . Assuming that

$$\mathcal{A}_p + \mathcal{B}_p = \mathcal{Q}_p,$$

we have  $a + b \neq 0$  for all  $a \in \mathcal{A}, b \in \mathcal{B}$ . Therefore,  $|\mathcal{A}_p \cap (-\mathcal{B}_p)| = 0$  and

$$\frac{p-1}{2} = |\mathcal{A}_p + \mathcal{B}_p| \leq |\mathcal{A}_p| |\mathcal{B}_p| \leq \frac{p-1}{2},$$

where the last inequality is a consequence of Theorem 3.6. Hence every element  $q \in \mathcal{Q}_p$  has a unique representation  $q = a + b$ . In summary:

**Corollary 3.7.** *Let  $\mathcal{Q}_p$  denote the set of quadratic residues modulo some prime  $p$ , and assume that*

$$\mathcal{A}_p + \mathcal{B}_p = \mathcal{Q}_p.$$

*Then every  $q \in \mathcal{Q}_p$  has a unique representation  $q = a + b$ , i.e.,*

$$|\mathcal{A}_p| |\mathcal{B}_p| = \frac{p-1}{2}.$$

Specifically, this demonstrates that when  $(p-1)/2$  is a prime, no nontrivial (i.e.,  $|\mathcal{A}_p|, |\mathcal{B}_p| \geq 2$ ) additive decomposition of  $\mathcal{Q}_p$  is possible. Several authors have examined the cardinality of  $\mathcal{A}_p, \mathcal{B}_p$  in such decompositions (refer to [34, 37, 6, 5]), and the following can be shown.

**Theorem 3.8** ([5]). *Assume that  $\mathcal{A}_p + \mathcal{B}_p = \mathcal{Q}_p$ . Then  $\frac{1}{4}\sqrt{p} \leq |\mathcal{A}_p|, |\mathcal{B}_p| \leq 2\sqrt{p} + 1$ .*

Using bounds such as those described in Theorem 3.8 and information about the typical size of divisors of  $p-1$  (obtained from [17]), the authors in [22] were able to utilise Corollary 3.7 to prove:

**Corollary 3.9.** *For almost all primes  $p \leq x$ , as  $x \rightarrow \infty$ , the set of quadratic residues  $\mathcal{Q}_p$  cannot be written as  $\mathcal{A}_p + \mathcal{B}_p = \mathcal{Q}_p$ , where  $|\mathcal{A}_p|, |\mathcal{B}_p| \geq 2$ .*

*Proof of Theorem 3.6.* We assume that  $M := |\mathcal{A}| \leq |\mathcal{B}|$ , and let  $\mathcal{A} = \{a_1, \dots, a_M\}$  and  $r = |\mathcal{B} \cap (-\mathcal{A})|$ . If  $M = 1$ , then  $\mathcal{A} = \{a_1\}$  and it is clear that  $r \in \{0, 1\}$ . In the case  $r = 0$ ,

$$|\mathcal{A}||\mathcal{B}| = |\mathcal{B}| = |\mathcal{B} + \mathcal{A}| \leq |Z_d| = d = d + r,$$

and, similarly, if  $r = 1$ , then

$$|\mathcal{A}||\mathcal{B}| = |\mathcal{B}| = |\mathcal{B} + \mathcal{A}| \leq |Z_d \cup \{0\}| = d + 1 = d + r$$

In both cases, we see that

$$|\mathcal{A}||\mathcal{B}| \leq d + r.$$

Now, suppose that  $M \geq 2$ . We choose  $c_1, \dots, c_M$ , not all zero, such that the polynomial

$$G(x) = \sum_{k=1}^M c_k (x + a_k)^{M-1} = \sum_{j=0}^{M-1} x^j \binom{M-1}{j} \sum_{k=1}^M c_k a_k^{M-1-j}$$

is a constant and

$$\sum_{k=1}^M c_k a_k^{M-1} = 1.$$

In other words, we choose  $c_1, \dots, c_M$  as a solution to the equation

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ a_1 & a_2 & \dots & a_{M-1} & a_M \\ a_1^2 & a_2^2 & \dots & a_{M-1}^2 & a_M^2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_1^{M-1} & a_2^{M-1} & \dots & a_{M-1}^{M-1} & a_M^{M-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{M-1} \\ c_M \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Since the matrix on the right hand side is a Vandermonde matrix, and thus (as the  $a_i$  are pairwise distinct) regular, we see that it is indeed possible to find such  $c_i$ . Taking  $j$ th derivatives, we note that

$$G^{(j)}(x_0) = 0$$

for any  $x_0$  and any  $j \geq 1$ .

Next, we let  $D = d + M - 1$ ; since

$$M = |\mathcal{A}| \leq |\mathcal{A} + \mathcal{B}| \leq d + 1 \leq \frac{p-1}{2} + 1,$$

we have

$$D \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1.$$

Moreover, we define

$$F(x) = -1 + \sum_{k=1}^M c_k (x + a_k)^D.$$

By the binomial theorem and our choice of  $c_i$ 's, we get

$$\begin{aligned} F(x) &= -1 + \sum_{k=1}^M c_k \sum_{j=0}^D \binom{D}{j} x^{D-j} a_k^j \\ &= -1 + \sum_{j=0}^D \binom{D}{j} x^{D-j} \sum_{k=1}^M c_k a_k^j \\ &= -1 + \binom{D}{M-1} x^{D-M+1} \sum_{k=1}^M c_k a_k^j + \sum_{j=M}^D \binom{D}{j} x^{D-j} \sum_{k=1}^M c_k a_k^j \\ &= -1 + \binom{D}{M-1} x^d + \sum_{j=M}^D \binom{D}{j} x^{D-j} \sum_{k=1}^M c_k a_k^j, \end{aligned}$$

so  $F$  is a polynomial of degree  $d$ .

For any  $b \in \mathcal{B}$ ,  $k = 1, \dots, M$ , we have  $(b + a_k)^{d+1} = (b + a_k)$ , thus

$$F(b) = -1 + \sum_{k=1}^M c_k (b + a_k)^D = -1 + \sum_{k=1}^M c_k (b + a_k)^{d+1} (b + a_k)^{M-2} = -1 + G(b) = 0.$$

Differentiating  $1 \leq \ell \leq M - 2$  times yields

$$\begin{aligned}
F^{(\ell)}(b) &= D \cdots (D - \ell + 1) \sum_{k=1}^M c_k (x + a_k)^{D-\ell} \\
&= D \cdots (D - \ell + 1) \sum_{k=1}^M c_k (x + a_k)^{d+1} (x + a_k)^{M-2-\ell} \\
&= D \cdots (D - \ell + 1) \sum_{k=1}^M c_k (x + a_k)^{M-1-\ell} \\
&= \frac{D \cdots (M - \ell + 1)}{D \cdots (M - \ell + 1)} G^{(\ell)}(b) = 0;
\end{aligned}$$

therefore,  $F$  has a zero of order at least  $M - 1$  at  $b$ . If additionally  $b \in \mathcal{B} \setminus (-\mathcal{A})$ , then  $(b + a_k)^d = 1$  for all  $k = 1, \dots, M$ , then

$$\begin{aligned}
F^{(M-1)}(b) &= D \cdots (D - M + 2) \sum_{k=1}^M c_k (x + a_k)^{D-M+1} \\
&= D \cdots (D - M + 2) \sum_{k=1}^M c_k (x + a_k)^d \\
&= D \cdots (D - M + 2) \sum_{k=1}^M c_k = 0.
\end{aligned}$$

This shows that at these  $|\mathcal{B}| - r$  points  $b$ ,  $F$  has a zero of order at least  $M$ . This allows us to conclude that

$$r(M - 1) + (|\mathcal{B}| - r)M \leq \deg F = d,$$

that is (since  $r(M - 1) + (|\mathcal{B}| - r)M = -r + M|\mathcal{B}|$ , and we defined  $r = |\mathcal{B} \cap (-\mathcal{A})|$  and  $M = |\mathcal{A}|$ ),

$$-|\mathcal{B} \cap (-\mathcal{A})| + |\mathcal{A}||\mathcal{B}| \leq d. \quad \square$$

As mentioned in the Acknowledgements, the following result is closely related to work of Davenport and Erdős [8], and also results of Karatsuba.<sup>1</sup>

---

<sup>1</sup>We would like to point out that Lemma 3.10 and its proof are very similar to [4, Lemma 2]. While our multiplicative constants (depending on  $m$ ) are slightly better, replacing Lemma 3.10 by [4, Lemma 2] in the proof of Theorem 3.13 would yield a similar result. However, we found our inequality independently and were only made aware of the connection to the aforementioned result recently.

**Lemma 3.10.** *Let  $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p \cup \{0\}$ , and let  $m \in \mathbb{N}$  be a positive integer. Then*

$$|\mathcal{B}_p|(|\mathcal{A}_p| - 1)^{2m} \leq \frac{(2m)!}{m!} |\mathcal{A}_p|^m p + (2m - 1) |\mathcal{A}_p|^{2m} \sqrt{p}.$$

*Proof.* Let  $\chi$  denote the Legendre symbol. For fixed  $b \in \mathcal{B}_p$ ,  $\chi(a + b) \geq 0$ , and  $\chi(a + b) = 1$  for all but at most one  $a \in \mathcal{A}_p$ , thus

$$\sum_{a \in \mathcal{A}_p} \chi(a + b) \geq |\mathcal{A}_p| - 1,$$

so

$$\sum_{b \in \mathcal{B}_p} \left( \sum_{a \in \mathcal{A}_p} \chi(a + b) \right)^{2m} \geq |\mathcal{B}_p|(|\mathcal{A}_p| - 1)^{2m}.$$

On the other hand, we can give an upper bound using Weil's lemma 3.1 (and the multiplicativity of the Legendre symbol) as follows:

$$\begin{aligned} \sum_{b \in \mathcal{B}_p} \left( \sum_{a \in \mathcal{A}_p} \chi(a + b) \right)^{2m} &\leq \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left( \sum_{a \in \mathcal{A}_p} \chi(a + x) \right)^{2m} \\ &= \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \sum_{a_1, \dots, a_{2m} \in \mathcal{A}} \chi((x + a_1) \cdots (x + a_{2m})) \\ &= \sum_{a_1, \dots, a_{2m}} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi((x + a_1) \cdots (x + a_{2m})) \\ &\leq m! \binom{2m}{m} \sum_{\substack{a_1, \dots, a_m, \\ a_i = a_{m+i}}} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi((x + a_1)^2 \cdots (x + a_m)^2) \\ &\quad + \sum_{\substack{a_1, \dots, a_{2m} \\ (\text{remaining } a_i)}} \left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi((x + a_1) \cdots (x + a_{2m})) \right| \\ &\leq \frac{(2m)!}{m!} |\mathcal{A}_p|^m p + (2m - 1) |\mathcal{A}_p|^{2m} \sqrt{p}. \end{aligned}$$

Regarding the penultimate inequality: the purpose of the first sum is to take care of all possible combinations of  $a_i$  that result in the product over  $(x - a_i)$  being the square of another polynomial; while there may be some overcounting, this is not an issue as each term in the sum is nonnegative.

The constant  $m! \binom{2m}{m}$  arises as follows: there are  $\binom{2m}{m}$  ways to choose indices  $i_1 < i_2 < \dots < i_m \in [1, 2m]$ ; we take the sum over all  $(a_1, \dots, a_m) \in \mathcal{A}$ , and say that  $(x - a_k)$  is in the  $i_k$ th factor of the polynomial. This determines the placement of  $m$  of the factors. For the remaining ones, there are at most  $m!$  different placements.

As a representative for all of these different combinations, we choose the index set  $1 < \dots < m$ , and say that the  $m + i$ th factor is the same as the  $i$ th one.

So the claimed inequality follows.  $\square$

We would like to compare the bound in Lemma 3.10 with other estimates. For simplicity, we consider the similar case where  $\mathcal{A}_p + \mathcal{B}_p \subseteq \mathcal{Q}_p$ . The same proof as in Lemma 3.10 shows

$$|\mathcal{B}_p| |\mathcal{A}_p|^{2m} \leq \frac{(2m)!}{m!} |\mathcal{A}_p|^m p + (2m-1) |\mathcal{A}_p|^{2m} \sqrt{p},$$

that is,

$$|\mathcal{B}_p| \leq \frac{(2m)!}{m!} \frac{p}{|\mathcal{A}_p|^m} + (2m-1) \sqrt{p}.$$

If  $|\mathcal{A}_p| \geq \sqrt[m]{p}$ , then this gives the upper bound

$$|\mathcal{B}_p| \leq \left( \frac{(2m)!}{m!} + (2m-1) \right) \sqrt{p}.$$

For constant  $m$ , this is asymptotically better than the bounds that we could derive using Lemma 3.5,

$$|\mathcal{B}_p| \leq p^{1 - \frac{1}{2m}},$$

and Theorem 3.2,

$$|\mathcal{B}_p| \ll \sqrt{p} \log p.$$

### 3.3 Application of sieve methods

Throughout this section, let  $N \in \mathbb{N}$ ,  $\mathcal{A}, \mathcal{B} \subset [1, N]$ , such that

$$\mathcal{A} + \mathcal{B} \subset \mathcal{S},$$

where  $\mathcal{S}$  denotes the set of squares. Moreover, for any prime number  $p$ , we define (as before)

$$\begin{aligned} \nu_{\mathcal{A}}(p) &= |\{x \in \mathbb{Z}/p\mathbb{Z} : \text{there is } a \in \mathcal{A} \text{ such that } a \equiv x \pmod{p}\}|, \\ \nu_{\mathcal{B}}(p) &= |\{y \in \mathbb{Z}/p\mathbb{Z} : \text{there is } b \in \mathcal{B} \text{ such that } b \equiv y \pmod{p}\}|. \end{aligned}$$

**Theorem 3.11** (Part of Thm. 9 in [20]). *We have  $\min(|\mathcal{A}|, |\mathcal{B}|) \ll \log N$ .*

*Proof.*<sup>2</sup> We recall that, from the discussion immediately after Lemma 3.5, we get

$$(\nu_{\mathcal{A}}(p) - 1)\nu_{\mathcal{B}}(p) \leq \sqrt{p}\sqrt{\nu_{\mathcal{A}}(p)\nu_{\mathcal{B}}(p)}.$$

For  $p \geq 5$ , this shows that

$$\min(\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p)) \leq 2\sqrt{p}.$$

Let  $y = (8 \log N)^2$ ,  $\mathcal{M}_1 = \{p \leq y : \nu_{\mathcal{A}}(p) \leq 2\sqrt{p}\}$ ,  $\mathcal{M}_2 = \{p \leq y : \nu_{\mathcal{B}}(p) \leq 2\sqrt{p}\}$ . Since

$$\sum_{p \leq y} \log p = (1 + o(1))y,$$

there is  $j \in \{1, 2\}$  such that

$$\sum_{p \in \mathcal{M}_j} \log p \geq (1 + o(1))y/2$$

without loss of generality  $j = 1$ .

Then (by partial summation)

$$\sum_{p \in \mathcal{M}_j} \frac{\log p}{2\sqrt{p}} \geq \frac{1}{4}(1 + o(1))\sqrt{y} = 2(1 + o(1)) \log N.$$

Thus, by Gallagher's larger sieve,

$$|\mathcal{A}| \leq \frac{y}{(1 + o(1))\sqrt{y}/2} = 2(1 + o(1))\sqrt{y} = 16(1 + o(1)) \log N \ll \log N. \quad \square$$

**Theorem 3.12.** *Suppose that*

$$|\mathcal{A}| > c_1 \log \log N,$$

*where  $c_1 = 8/\log 2$ . Then (for sufficiently large  $N$ )*

$$|\mathcal{B}| \leq c_2 \log N (\log \log N)^2,$$

*where  $c_2 = (16/\log 2)^2$ .*

*Proof.* Let

$$\mathcal{M} = \{p \in \mathcal{P} : \nu_{\mathcal{A}}(p) \geq c_0 \log p\},$$

where  $\mathcal{P}$  denotes the set of primes and  $c_0 = 1/\log 2$ , and let

$$y = (8c_0 \log N \log \log N)^2.$$

---

<sup>2</sup>We slightly changed the proof for simplicity, the implicit constant in [20] is 4, not 16.



We note that by the Prime Number Theorem (Theorem 2.1), for sufficiently large  $y$ , we have

$$\sum_{p \leq y} \log p \geq \frac{3}{4}y.$$

Thus, one of the following two cases has to hold (for sufficiently large  $N$ ).

**Case 1:** Suppose that

$$\sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \log p \geq y/4.$$

For all  $p \notin \mathcal{M}$ , we have  $\nu_{\mathcal{A}}(p) \leq c_0 \log p$ . Thus, by partial summation,

$$\begin{aligned} \sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{A}}(p)} &\geq \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{c_0 \log p} \\ &\geq \frac{1}{4c_0} \frac{y}{\log y} + \int_2^y \left( \sum_{\substack{p \notin \mathcal{M} \\ p \leq x}} \log x \right) \frac{1}{x \log^2 x} dx \\ &\geq \frac{1}{4c_0} \frac{y}{\log y} \\ &\geq \log N + \frac{1}{8c_0} \frac{y}{\log y}. \end{aligned}$$

Now, by Gallagher's larger sieve,

$$\begin{aligned} |\mathcal{A}| &\leq \frac{y}{-\log N + \sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{A}}(p)}} \\ &\leq \frac{y}{y/(8c_0 \log y)} \\ &= 8c_0 \log y \\ &\leq 8c_0 \log \log N, \end{aligned}$$

a contradiction to our assumption that  $|\mathcal{A}| > 8c_0 \log \log N$ .

**Case 2:** Suppose that

$$\sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \log p \geq y/2.$$

Let  $p \in \mathcal{M}$ ; then there is a subset  $\mathcal{A}' \subseteq \mathcal{A}$  such that the cardinality of  $\mathcal{A}'_p = \mathcal{A}' \pmod p$  is  $|\mathcal{A}'_p| \in [c_0 \log p, c_0 \log p + 1]$ . Clearly,

$$\mathcal{A}' + \mathcal{B} \subset \mathcal{S},$$

thus, by Lemma 3.3,

$$\nu_B(p) \leq 2 + (c_0 \log p + 1)p^{1/2} \leq 2c_0(\log p)p^{1/2}.$$

Now, by partial summation,

$$\begin{aligned} \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_B(p)} &\geq \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{c_0(\log p)p^{1/2}} \\ &\geq \frac{y}{2} \frac{1}{c_0(\log y)y^{1/2}} + \int_2^y \left( \sum_{\substack{p \in \mathcal{M} \\ p \leq x}} \log p \right) \frac{\log x + 2}{2x^{3/2} \log^2 x} dx \\ &\geq \frac{y^{1/2}}{2c_0 \log y} \\ &\geq 2 \log N. \end{aligned}$$

Thus, by Gallagher's larger sieve,

$$\begin{aligned} |\mathcal{B}| &\leq \frac{y}{-\log N + \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_B(p)}} \\ &\leq \frac{y}{\log N} \\ &= (16c_0)^2 \log N (\log \log N)^2, \end{aligned}$$

which shows the claim.  $\square$

**Theorem 3.13.** *Let  $m$  be a positive integer, or a function  $m = m(N)$  taking values in the positive integers. Then there are constants  $C_1, C_2$  (independent of  $m$ ) such that, if*

$$|\mathcal{B}| \geq C_1 m^2 \log N,$$

then

$$|\mathcal{A}| \leq C_2 m (\log N)^{1/m}.$$

*Proof of Theorem 3.13.* Let

$$\mathcal{M} = \left\{ p \in \mathcal{P} : \nu_{\mathcal{A}}(p) \geq \left( \frac{(2m)!}{m!(2m-1)} \sqrt{p} \right)^{1/m} \right\},$$

where  $\mathcal{P}$  denotes the set of primes. Note that, by Stirling's formula (as  $m \rightarrow \infty$ ),

$$\frac{(2m)!}{m!} = \frac{\sqrt{4\pi m} \left(\frac{2m}{e}\right)^{2m}}{\sqrt{2\pi m} \left(\frac{m}{e}\right)^m} (1 + o(1)),$$

so

$$\begin{aligned} ((2m)!/(2m-1)m!)^{1/m} &= (\sqrt{2}/(2m-1))^{1/m} \frac{4m}{e} (1+o(1)) \\ &= \frac{4}{e} m (1+o(1)). \end{aligned}$$

We choose  $c_0, c_1$  such that

$$c_0 m \geq ((2m)!/(2m-1))^{1/m} \geq c_1 m.$$

Moreover, we set

$$y = c''(m \log N)^2,$$

where  $\exp(8/c_1) = c'$ .

Assume that  $|\mathcal{B}| > 8(c')^2 m^2 \log N$ . We note that by the Prime Number Theorem (Theorem 2.1), for sufficiently large  $y$ , we have

$$\sum_{p \leq y} \log p \geq \frac{3}{4} y.$$

Thus, one of the following two cases has to hold (for sufficiently large  $N$ ).

**Case 1:** Suppose that

$$\sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \log p \geq y/2.$$

For  $p \in \mathcal{M}$ , we have

$$\begin{aligned} \nu_{\mathcal{B}}(p) &\leq \frac{(2m)! \nu_{\mathcal{A}}(p)^m}{m! (\nu_{\mathcal{A}}(p) - 1)^{2m}} p + (2m-1) \frac{\nu_{\mathcal{A}}(p)^{2m}}{(\nu_{\mathcal{A}}(p) - 1)^{2m}} \sqrt{p} \\ &\leq 4m \left( \frac{\nu_{\mathcal{A}}(p)}{(\nu_{\mathcal{A}}(p) - 1)} \right)^{2m} \sqrt{p} \\ &= 4m \left( 1 + \frac{1}{(\nu_{\mathcal{A}}(p) - 1)} \right)^{2m} \sqrt{p} \\ &\leq 4m \left( 1 + 2/(c_1 m p^{1/(2m)}) \right)^{2m} \sqrt{p}. \end{aligned}$$

by Lemma 3.10. Now, by partial summation,

$$\begin{aligned} \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{B}}(p)} &\geq \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{4m (1 + 2/(c_1 m^2 p^{1/(2m)}))^{2m} \sqrt{p}} \\ &\geq \frac{1}{4m (1 + 2/(c_1 m))^{2m}} \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{\sqrt{p}} \\ &\geq \frac{1}{4m (1 + 2/(c_1 m))^{2m}} y^{1/2}. \end{aligned}$$

We estimate

$$\begin{aligned}
(1 + 2/(c_1 m))^{2m} &= \exp(2m \log(1 + 2/(c_1 m))) \\
&\leq \exp(2m \cdot 4/(c_1 m)) \\
&\leq \exp(8/c_1) \\
&= c'.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\frac{1}{4m(1 + 2/(c_1 m))^{2m}} y^{1/2} &\geq \frac{1}{4mc'} y^{1/2} \\
&\geq \log N + \frac{1}{8mc'} y^{1/2}.
\end{aligned}$$

Thus, by Gallagher's larger sieve,

$$\begin{aligned}
|\mathcal{B}| &\leq \frac{y}{-\log N + \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{B}}(p)}} \\
&\leq \frac{y}{\frac{1}{8mc''} y^{1/2}} \\
&= 8mc' \sqrt{y} \\
&= 8(c')^2 m^2 \log N.
\end{aligned}$$

where  $c'' = (2/c')^2$ . This contradicts our assumption on the cardinality of  $\mathcal{B}$ .

**Case 2:** Suppose that

$$\sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \log p \geq y/4.$$

For all  $p \notin \mathcal{M}$ , we have  $\nu_{\mathcal{A}}(p) \leq \left( \frac{(2m)!}{2m-1} \sqrt{p} \right)^{1/m} \leq c_0 m p^{1/(2m)}$ . Thus, by partial summation,

$$\begin{aligned}
\sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{A}}(p)} &\geq \sum_{\substack{p \in \mathcal{M} \\ p \leq y}} \frac{\log p}{c_0 m p^{1/(2m)}} \\
&\geq \frac{1}{4 c_0 m y^{1/(2m)}} + \frac{1}{c_0 m^2} \int_2^y \left( \sum_{\substack{p \notin \mathcal{M} \\ p \leq x}} \log x \right) \frac{1}{x^{1/(2m)+1}} dx \\
&\geq \frac{1}{4 c_0 m} y^{1-1/(2m)} \\
&= \frac{1}{8 c_0 m} y^{1-1/(2m)} + \frac{1}{8 c_0 m^2} y^{1-1/(2m)} \\
&\geq \log N + \frac{1}{8 c_0 m} y^{1-1/(2m)}.
\end{aligned}$$

(For the last inequality, recall that  $y = c''(m \log N)^2$ , so it certainly holds true for sufficiently large  $N$ .) Now, by Gallagher's larger sieve,

$$\begin{aligned}
 |\mathcal{A}| &\leq \frac{y}{-\log N + \sum_{\substack{p \notin \mathcal{M} \\ p \leq y}} \frac{\log p}{\nu_{\mathcal{A}}(p)}} \\
 &\leq \frac{y}{\frac{1}{8c_0 m} y^{1-1/(2m)}} \\
 &= c' m y^{1/(2m)} \\
 &= c' m (c''(m \log N)^2)^{1/2m} \\
 &= \tilde{c} m^{1+1/m} (\log N)^{1/m}.
 \end{aligned}$$

(Note that  $m^{1/m} \rightarrow 1$  as  $m \rightarrow \infty$ , so it is bounded by some constant.)  $\square$

**Corollary 3.14.** *Let  $h(N) = o(\log \log N)$ . Then there are constants  $C_1, C_2$  such that, if*

$$|\mathcal{B}| \geq C_1 \frac{\log N (\log \log N)^2}{h(N)^2},$$

*then*

$$|\mathcal{A}| \leq C_2 \frac{\log \log N}{h(N)} \exp(h(N)).$$

*Proof.* Choose  $m(N) = \lfloor \log \log N / h(N) \rfloor$  in Theorem 3.13.  $\square$

Moreover, we note that choosing  $m(N) = \lfloor \log \log N \rfloor$  gives a different proof of Theorem 3.12.

## 4 Squarefree Numbers

Let  $\mathcal{S}_{\text{free}}$  denote the set of *squarefree numbers*, i.e., the set of all positive integers that are not divisible by the square of any prime number. In this chapter, we study sets  $\mathcal{A}$  such that

$$\mathcal{A} + \mathcal{A} = \{a + a' : a, a' \in \mathcal{A}\} \subseteq \mathcal{S}_{\text{free}}.$$

Note that we do not exclude the case  $a = a'$ .

It seems reasonable to first examine the size of  $\mathcal{S}_{\text{free}} \cap [1, N]$ . A proof that  $|\mathcal{S}_{\text{free}} \cap [1, N]|$  is of order  $6/\pi^2 N$  will be given in section 4.1, along with a discussion of associated concepts.

In section 4.2, following the insights presented in Konyagin's paper [26], we give bounds for

$$\text{ES}_N := \max\{|\mathcal{A}| : \mathcal{A} \subseteq [1, N], \mathcal{A} + \mathcal{A} \subseteq \mathcal{S}_{\text{free}}\}$$

and

$$\text{BR}_N := \sup \left\{ \frac{\max_x |M(x)|}{\int_0^1 |M(x)| dx} : M(x) = \sum_{\substack{n \in \mathcal{S}_{\text{free}}, \\ n \leq N}} a_n e(nx), a_n \in \mathbb{C} \right\},$$

for  $N \in \mathbb{N}$ , where  $e(nx) = \exp(2\pi i x)$  and we consider all possible coefficients  $a_n \in \mathbb{C}$  for the trigonometric polynomial  $M$ . To see a connection between the two quantities  $\text{ES}_N$  and  $\text{BR}_N$ , we choose  $\mathcal{A} \subseteq [1, N]$  such that  $\mathcal{A} + \mathcal{A} \subseteq \mathcal{S}_{\text{free}}$  and  $|\mathcal{A}| = \text{ES}_N$ . Then

$$\hat{M}(x) = \left( \sum_{a \in \mathcal{A}} e(ax) \right)^2 = \sum_{(a, a') \in \mathcal{A} \times \mathcal{A}} e((a + a')x)$$

is a trigonometric polynomial of the form  $\sum_{n \in \mathcal{S}_{\text{free}}, n \leq 2N} a_n e(nx)$ ; moreover,

$$\max_x |\hat{M}(x)| = |\mathcal{A}|^2 \quad \text{and} \quad \int_0^1 |\hat{M}(x)| dx = |\mathcal{A}|.$$

Hence

$$\text{BR}_{2N} \geq |\mathcal{A}|^2 / |\mathcal{A}| = \text{ES}_N. \tag{4.1}$$

## 4.1 Basic properties

In the preceding chapters, the two sets we considered (namely the set of primes  $\mathcal{P}$  and the set of squares  $\mathcal{S}$ ) were sets with density zero in the positive integers. To clarify, by the **density** of a set (as per [3], p. 14), we refer to the limit as  $N \rightarrow \infty$  of the probability that a number that is chosen uniformly at random in  $[1, N]$  lies in the respective set, i.e.,

$$\lim_{N \rightarrow \infty} \frac{1}{N} |[1, N] \cap \mathcal{S}| = \lim_{N \rightarrow \infty} \frac{\sqrt{N}}{N} = \lim_{N \rightarrow \infty} \frac{1}{\sqrt{N}}$$

for the set of squares, and, by the Prime Number Theorem (Theorem 2.1), the quantity

$$\lim_{N \rightarrow \infty} \frac{1}{N} |[1, N] \cap \mathcal{P}| = \lim_{N \rightarrow \infty} \frac{N/\log N}{N} = \lim_{N \rightarrow \infty} \frac{1}{\log N}$$

for the set of primes; both limits exist and evaluate to zero. By contrast, the set of squarefree numbers has positive density in the positive integers, i.e., the limit

$$\lim_{N \rightarrow \infty} \frac{1}{N} |[1, N] \cap \mathcal{S}_{\text{free}}|$$

exists and is positive. In fact, in [23] (p. 355, Theorem 333), one can find the following asymptotics:

**Theorem 4.1.** *The density of the squarefree numbers in the positive integers is  $6/\pi^2$ . To be more precise,*

$$|\mathcal{S}_{\text{free}} \cap [1, N]| = \frac{6}{\pi^2} N + O(\sqrt{N}).$$

Prior to outlining the proof of Theorem 4.1, we give a concise overview of a few pertinent notions.

The **Möbius function** (as defined in [23] on p. 304) can be expressed as

$$\mu(n) = \begin{cases} 0 & \text{if } n \notin \mathcal{S}_{\text{free}} \\ (-1)^r & \text{if } n = p_1 \cdots p_r, \text{ where } p_1, \dots, p_r \text{ are the different prime factors of } n. \end{cases}$$

In particular, the square of the Möbius function  $\mu^2$  is just the indicator function of the set of squarefree numbers. Hence, we can reformulate the statement of Theorem 4.1 as

$$\sum_{n \leq N} \mu(n)^2 = \frac{6}{\pi^2} N + O(\sqrt{N}).$$

Moreover,  $\mu$  is a multiplicative function, that is, if  $n$  and  $m$  are coprime, then  $\mu(nm) = \mu(n)\mu(m)$ . Consider the function

$$g(n) = \sum_{d|n} \mu(d)$$

(where the expression  $d|n$  denotes that  $d$  is a divisor of  $n$ ). By the multiplicativity of  $\mu$ ,  $g$  is automatically also multiplicative. Since  $g(1) = 1$  and  $g(p^k) = 1 - 1 + 0 + \dots + 0 = 0$  for any prime  $p$ , we conclude  $g$  is the indicator function of the set  $\{1\}$ , that is:

**Lemma 4.2.**

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \geq 2. \end{cases}$$

Lemma 4.2 can be used to derive the following formula ([23], p. 307).

**Theorem 4.3.** *Suppose that  $F, f : \mathbb{R} \rightarrow \mathbb{C}$  are two functions. Then*

$$F(x) = \sum_{n=1}^{\lfloor x \rfloor} f(n)$$

for all  $x > 0$  if and only if

$$f(x) = \sum_{n=1}^{\lfloor x \rfloor} \mu(n) F(x/n)$$

for all  $x > 0$ .

Lastly (as discussed in [3], p. 22), we note that another implication of Lemma 4.2 is that

$$\sum_{n \geq 1} \frac{1}{n^s} \sum_{n \geq 1} \frac{\mu(n)}{n^s} = 1 \quad (4.2)$$

for all  $s \in \mathbb{C}$  with  $\text{Re}(s) > 1$  (where both series converge absolutely).

*Proof sketch of Theorem 4.1.* Let

$$q(N) := |\mathcal{S}_{\text{free}} \cap [1, N]|.$$

We note that we can partition the set of integers into sets  $\mathcal{S}_1, \mathcal{S}_2, \dots$  such that

$$\mathcal{S}_d = \{n \in \mathbb{N} : \text{the largest square factor of } n \text{ is } d^2\}.$$

We observe that  $\mathcal{S}_1 = \mathcal{S}_{\text{free}}$ , and that  $\mathcal{S}_d = \{n \in \mathbb{N} : n = d^2 m, m \in \mathcal{S}_f\}$ , thus

$$|\mathcal{S}_d \cap [1, N]| = q(N/d^2).$$

Therefore,

$$N = \sum_{d=1}^{\lfloor \sqrt{N} \rfloor} q(N/d^2),$$



and by the inversion formula (Theorem 4.3, with  $x = \sqrt{N}$ ,  $F(x) = \lfloor x^2 \rfloor$ ,  $f(x) = q(x^2)$ ), we get

$$\begin{aligned} q(N) &= \sum_{d=1}^{\lfloor \sqrt{N} \rfloor} \mu(d) \left\lfloor \frac{N}{d^2} \right\rfloor \\ &= \sum_{d=1}^{\lfloor \sqrt{N} \rfloor} \mu(d) \left( \frac{N}{d^2} + O(1) \right) \\ &= N \sum_{d=1}^{\lfloor \sqrt{N} \rfloor} \frac{\mu(d)}{d^2} + O(\sqrt{N}). \end{aligned}$$

Now, using (4.2) with  $s = 2$ , we know that  $\sum_{n=1}^{\infty} \mu(n)/n^2 = 1/(\sum_{n=1}^{\infty} 1/n^2)$ . Using the fact that  $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$ , and bounding the sum's tail by an integral, we can further calculate

$$\begin{aligned} N \sum_{d=1}^{\lfloor \sqrt{N} \rfloor} \frac{\mu(d)}{d^2} + O(\sqrt{N}) &= N \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - N \sum_{d=\lfloor \sqrt{N} \rfloor+1}^{\infty} \frac{\mu(d)}{d^2} + O(\sqrt{N}) \\ &= N \frac{6}{\pi^2} + O \left( N \sum_{d=\lfloor \sqrt{N} \rfloor+1}^{\infty} \frac{1}{d^2} \right) + O(\sqrt{N}) \\ &= N \frac{6}{\pi^2} + O \left( N \int_{\sqrt{N}}^{\infty} \frac{1}{x^2} dx \right) + O(\sqrt{N}) \\ &= N \frac{6}{\pi^2} + O(\sqrt{N}). \end{aligned} \quad \square$$

## 4.2 Discussing sumsets

In this section, we establish bounds for

$$\text{ES}_N := \max\{|\mathcal{A}| : \mathcal{A} \subseteq [1, N], \mathcal{A} + \mathcal{A} \subseteq \mathcal{S}_{\text{free}}\}$$

and

$$\text{BR}_N := \sup \left\{ \frac{\max_x |M(x)|}{\int_0^1 |M(x)| dx} : M(x) = \sum_{\substack{n \in \mathcal{S}_{\text{free}}, \\ n \leq N}} a_n e(nx), a_n \in \mathbb{C} \right\},$$

following (as mentioned in the introduction of this chapter) [26].

**Theorem 4.4.** *There are effective positive constants  $C_1, C_2$  such that*

$$\begin{aligned} \text{BR}_N &\leq N^{11/15} \exp\left(\frac{C_1 \log N}{\sqrt{\log \log N}}\right) \\ \text{ES}_N &\leq N^{11/15} \exp\left(\frac{C_2 \log N}{\sqrt{\log \log N}}\right) \end{aligned}$$

for all  $N \geq 3$ .

In "On the number of rational points on certain elliptic curves"[2], the authors Bombieri and Zannier describe that the following lemma, crucial for the proof of Theorem 4.4, can be derived as a direct consequence of the bounds provided in their paper.

**Lemma 4.5.** *Let  $X \geq 3$  and  $\Delta_{ij}$ ,  $1 \leq i < j \leq 4$  be positive integers. Then the cardinality*

$$\begin{aligned} &|\{(p_1, p_2, p_3, p_4) : p_i \leq X \text{ distinct primes,} \\ &\quad p_i^2 \Delta_{jk} - p_j^2 \Delta_{ik} + p_k^2 \Delta_{ij} = 0 \ \forall \ 1 \leq i < j < k \leq 4\}| \end{aligned}$$

is at most  $\exp(C \log X / \sqrt{\log \log X})$  for some constant  $C > 0$ .

More specifically, in the proof of Theorem 4.7, Konyagin appeals to Lemma 4.5 in order to bound the number of octuples in

$$\begin{aligned} \mathcal{Q}_Y(X) = \{ &(p_{k-3}, p_{k-2}, p_{k-1}, p_k, a_{k-3}, a_{k-2}, a_{k-1}, a_k) : p_i \leq X \text{ distinct, } a_i < p_i^2, \\ &0 \leq a_j p_i^2 - a_i p_j^2 \leq Y \text{ for } i < j\}, \end{aligned}$$

where  $X, Y > 0$ , in the following way:

**Lemma 4.6.**  $|\mathcal{Q}_Y(X)| \ll Y^4 \exp(C \log X / \log \log X)$ , where  $C$  is some positive constant.

*Proof.* We define

$$a_{k-i} p_{k-j}^2 - a_{k-j} p_{k-i}^2 := \Delta_{k-i, k-j}$$

for  $k-j < k-i$ . By Laplace expansion

$$0 = \begin{vmatrix} p_o^2 & p_r^2 & p_s^2 \\ p_o^2 & p_r^2 & p_s^2 \\ a_o & a_r & a_s \end{vmatrix} = p_o^2 \Delta_{rs} - p_r^2 \Delta_{os} + p_s^2 \Delta_{ro}.$$

Also, it can be checked that

$$\Delta_{k-3, k-2} \Delta_{k-1, k} - \Delta_{k-3, k-1} \Delta_{k-2, k} + \Delta_{k-3, k} \Delta_{k-2, k-1} = 0.$$

Given  $p_i$  and  $\Delta_{i,j}$  for all  $k-3 \leq i < j \leq k$ , we can recover the value of the  $a_i$ 's. Therefore, we can give an upper bound on the number of octuples

$$(p_{k-3}, p_{k-2}, p_{k-1}, p_k, a_{k-3}, a_{k-2}, a_{k-1}, a_k)$$

by giving an upper bound on the number of  $p_i, \Delta_{i,j}$  satisfying:

- $p_{k-3}, p_{k-2}, p_{k-1}, p_k \leq X$ , distinct,
- $0 < \Delta_{k-i, k-j} \leq Y$ ,
- $\Delta_{k-3, k-2} \Delta_{k-1, k} + \Delta_{k-3, k} \Delta_{k-2, k-1} = \Delta_{k-3, k-1} \Delta_{k-2, k} \leq Y^2$ ,
- $p_o^2 \Delta_{rs} - p_r^2 \Delta_{os} + p_s^2 \Delta_{ro} = 0$  for all  $k-3 \leq o, r, s \leq k$ .

Fixing positive integers  $S_1, S_2$  such that  $S_1 + S_2 \leq Y^2$ , we aim to bound

$$|\{(\Delta_{i,j})_{i,j} : k-3 \leq i < j \leq k, \\ \Delta_{k-3, k-2} \Delta_{k-1, k} = S_1, \Delta_{k-3, k} \Delta_{k-2, k-1} = S_2, \\ \Delta_{k-3, k-2} \Delta_{k-1, k} + \Delta_{k-3, k} \Delta_{k-2, k-1} = \Delta_{k-3, k-1} \Delta_{k-2, k}\}|.$$

Denoting by  $d(n)$  the number of divisors of a positive integer  $n$ , we see that there are at most  $d(S_1)$  choices for  $\Delta_{k-3, k-2}$ , and that this already determines  $\Delta_{k-1, k}$ ; considering the other two conditions analogously, we conclude that the cardinality of the set above can be at most

$$d(S_1)d(S_2)d(S_1 + S_2).$$

Hence, by Lemma 4.5, there can be at most

$$d(S_1)d(S_2)d(S_1 + S_2) \exp\left(C \log X / \sqrt{\log \log X}\right)$$

octuples  $(p_{k-3}, p_{k-2}, p_{k-1}, p_k, a_{k-3}, a_{k-2}, a_{k-1}, a_k)$  corresponding to  $S_1, S_2$ . Therefore, the total number of all possible octuples is bounded from above by

$$\exp\left(C \log X / \sqrt{\log \log X}\right) \sum_{S_1 + S_2 \leq Y^2} d(S_1)d(S_2)d(S_1 + S_2).$$

Moreover,  $d(n) \ll \exp(\log n / \log \log n)$  (this can be found in [31], p. 24, Satz 5.2), so

$$\begin{aligned} & \sum_{S_1 + S_2 \leq Y^2} d(S_1)d(S_2)d(S_1 + S_2) \\ & \ll \sum_{S_1 + S_2 \leq Y^2} \exp\left(\frac{\log S_1}{\log \log S_1}\right) \exp\left(\frac{\log S_2}{\log \log S_2}\right) \exp\left(\frac{\log(S_1 + S_2)}{\log \log(S_1 + S_2)}\right) \\ & \ll \sum_{\substack{S_1 \leq S_2 \\ S_1 + S_2 \leq Y^2}} \exp\left(\frac{\log S_1}{\log \log S_1}\right) \exp\left(\frac{\log S_2}{\log \log S_2}\right) \exp\left(\frac{\log(2S_2)}{\log \log(2S_2)}\right) \\ & \ll \sum_{\substack{S_1 \leq S_2 \\ S_1 + S_2 \leq Y^2}} \exp\left(\frac{\log S_1}{\log \log S_1}\right) \exp\left(\frac{2 \log S_2}{\log \log S_2}\right) \\ & \ll Y^4 \exp\left(\frac{3 \log Y^2}{\log \log Y}\right) \\ & \ll Y^4 \exp\left(\frac{12 \log X}{\log \log X}\right). \end{aligned}$$

□

**Theorem 4.7.** *Let  $n_1, \dots, n_z$  be distinct positive integers in  $[1, N]$ . Then there is an effective constant  $C_3 > 0$  such that*

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right) \leq C_3 N Z + X^{16/5} Z^{6/5} \exp \left( \frac{C_3 \log N}{\sqrt{\log \log N}} \right)$$

for all positive integers  $X \geq 3$ , where  $Z(p, h) = |\{k : n_k \equiv h \pmod{p}\}|$ .

We note that, for  $Z^{1/5} \exp \left( \frac{C_3 \log N}{\sqrt{\log \log N}} \right) \ll X^{4/5}$ , Theorem 4.7 gives a better estimate than the inequality

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right) \leq (X^4 + \pi N) Z,$$

which can be found in [15] (and proved with the help of the analytic version of the large sieve, Theorem 1.1).

*Proof.* Let

$$S(x) = \sum_{j=1}^Z e(n_j x).$$

Then, recalling that

$$\sum_{a=0}^{q-1} e(ma/q) = \begin{cases} 0 & \text{if } m \notin \mathbb{Z}, \\ q & \text{if } m \in \mathbb{Z}, \end{cases}$$

we get

$$\begin{aligned} \sum_{a=0}^{q-1} \left| S \left( \frac{a}{q} \right) \right|^2 &= \sum_{a=0}^{q-1} \sum_{j=1}^Z \sum_{k=1}^Z e((n_j - n_k)a/q) \\ &= \sum_{j,k} \sum_{a=0}^{q-1} e((n_j - n_k)a/q) \\ &= q |\{(j, k) : n_j \equiv n_k \pmod{q}\}| \\ &= q \sum_{h=0}^{q-1} Z(q, h)^2. \end{aligned}$$

Since

$$\sum_{a=1}^{q-1} \left| S \left( \frac{a}{q} \right) \right|^2 = \sum_{a=0}^{q-1} \left| S \left( \frac{a}{q} \right) \right|^2 - Z^2,$$

and

$$-Z^2 = -2Z \sum_{h=0}^{q-1} Z(q, h) + Z^2,$$

the preceding calculation yields

$$\sum_{a=1}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2 = q \sum_{h=0}^{q-1} \left( Z(q, h) - \frac{Z}{q} \right)^2.$$

We take to sum over all  $q = p^2$ ,  $p \leq X$  in order to obtain

$$\sum_{p \leq X} \sum_{a=1}^{p^2-1} \left| S\left(\frac{a}{p^2}\right) \right|^2 = \sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2.$$

Now we consider  $q = a/p^2$ ,  $q' = a'/p'^2$ , and realise that  $q = q'$  is only possible if  $p = p'$  and  $a = a'$ : indeed,  $q = q'$  implies  $ap'^2 = a'p^2$ ; since  $a$  is not divisible by  $p^2$ ,  $p'$  has to be divisible by  $p$ , and then it is clear that  $a = a'$ . Thus we can order all elements  $q_k = a_k/p_k^2$  of this form in a strictly increasing manner, i.e.,  $q_1 < \dots < q_K$  for some  $K > 1$ . This allows us to rewrite our sum again:

$$\sum_{k=1}^K \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2 = \sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2.$$

Let  $0 < Y < X^2$  be arbitrary, and let<sup>1</sup>

$$\begin{aligned} \mathcal{K}' &= \{k : 4 \leq k \leq K, q_k - q_{k-3} \leq Y/X^4\}, \\ \mathcal{K}_j &= \{k : 1 \leq k \leq K, k \notin \mathcal{K}', k \equiv j \pmod{3}\} \text{ for } j = 0, 1, 2. \end{aligned}$$

Then

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2 = S' + S_0 + S_1 + S_2,$$

where

$$\begin{aligned} S' &= \sum_{k \in \mathcal{K}'} \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2, \\ S_j &= \sum_{k \in \mathcal{K}_j} \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2 \text{ for } j = 0, 1, 2. \end{aligned}$$

<sup>1</sup>In [26], there appears to be a typo in the definition of  $\mathcal{K}'$  on p. 497, where it states ' $q_k - q_{k-3} \leq Y/X^2$ ' instead of ' $q_k - q_{k-3} \leq Y/X^4$ '. This error is repeated again in the first line on p. 498 of [26]. It is evident that it was intended to say  $Y/X^4$ , as  $a_k/p_k^2 - a_{k-2}/p_{k-3}^2 > 1/X^2$  only implies  $a_k/p_k^2 - a_{k-2}/p_{k-3}^2 > Y/X^4$ , not  $a_k/p_k^2 - a_{k-2}/p_{k-3}^2 > Y/X^2$ . Moreover, in other parts of the paper, such as the fourth line on page 498,  $Y/X^4$  is stated correctly.

If  $k \in \mathcal{K}'$ , the denominators of  $q_{k-i} = a_{k-i}/p_{k-i}$ ,  $i = 0, 1, 2, 3$ , are distinct. Otherwise, there would be  $0 \leq i < j \leq 3$  such that  $p_{k-i} = p_{k-j}$ , but then

$$\frac{a_k}{p_k^2} - \frac{a_{k-3}}{p_{k-3}^2} \geq \frac{a_{k-i}}{p_{k-i}^2} - \frac{a_{k-j}}{p_{k-j}^2} \geq \frac{1}{p_{k-i}^2} \geq \frac{1}{X^2} \geq \frac{Y}{X^4},$$

so  $k \notin \mathcal{K}'$ .

For  $k \in \mathcal{K}'$ , we see that since

$$p_{k-j}^2 p_{k-i}^2 \leq X^4$$

and

$$0 < \frac{a_{k-i}}{p_{k-i}^2} - \frac{a_{k-j}}{p_{k-j}^2} \leq \frac{a_k}{p_k^2} - \frac{a_{k-3}}{p_{k-3}^2} \leq \frac{Y}{X^4},$$

we obtain

$$0 < a_{k-i} p_{k-j}^2 - a_{k-j} p_{k-i}^2 := \Delta_{k-i, k-j} \leq Y.$$

Thus, by Lemma 4.6,

$$|\mathcal{K}'| \leq Y^4 \exp(C' \log X / \sqrt{\log \log X})$$

for some constant  $C' > 0$ .

Now, clearly  $|S(a_k/p_k^2)|^2 \leq Z^2$ , so we have

$$S' \leq Z^2 Y^4 \exp(C' \log x / \sqrt{\log \log X}).$$

Furthermore, we see that  $|a_\ell/p_\ell^2 - a_k/p_k^2| > Y/X^4$  if  $k, \ell \in \mathcal{K}_j$  for some  $j$ , and  $a_k/p_k^2 \geq 1/X^2 \geq Y/X^4$ . Due to (a weaker version of) Theorem 1.1, we have

$$S_j \leq \left( \frac{X^4}{Y} + \pi N \right) Z$$

for  $j = 0, 1, 2$ .

In conclusion,

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2 = S' + S_0 + S_1 + S_2 \quad (4.3)$$

$$\leq Y^4 Z^2 \exp(C' \log X / \sqrt{\log \log X}) + 3 \frac{X^4}{Y} Z + 3\pi N Z \quad (4.4)$$

In fact, the inequality 4.3 above still holds true for  $Y \geq X^2$  since, in this case,

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2 \leq \sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} Z^2 \leq \sum_{p \leq X} p^4 Z^2 \leq X^5 Z^2 \leq Y^4 Z^2.$$

Choosing  $Y = (X^4/Z)^{1/5}$  in inequality 4.3 yields

$$\begin{aligned} \sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left( Z(p^2, h) - \frac{Z}{p^2} \right)^2 &\leq X^{16/5} Z^{6/5} \exp \left( C' \frac{\log X}{\sqrt{\log \log X}} \right) + 3X^{16/5} Z^{6/5} + 3\pi NZ \\ &\leq X^{16/5} Z^{6/5} \exp \left( C'' \frac{\log X}{\sqrt{\log \log X}} \right) + 3\pi NZ \end{aligned}$$

for some  $C'' > 0$ , which concludes the proof.  $\square$

In order to derive Theorem 4.4 from Theorem 4.7, we need the following lemma:

**Lemma 4.8.** *Let  $X \geq 3$  be a positive integer and let*

$$Y = X^{1/4} \exp \left( -\frac{\tilde{C} \log X}{\sqrt{\log \log X}} \right),$$

where  $\tilde{C}$  is an appropriate constant specified in the proof below. Then there is a set of prime numbers  $\mathcal{P}' \subseteq [1, X]$  such that  $|\mathcal{P}'|$  contains at least half of the primes in  $[1, X]$  and such that for any quadruple  $p_1, p_2, p_3, p_4 \in \mathcal{P}'$ , and any  $a_1, a_2, a_3, a_4 \in \mathbb{N}$  such that  $a_i < p_i^2$  for  $i = 1, 2, 3, 4$ , and

$$a_1/p_1^2 < a_2/p_2^2 < a_3/p_3^2 < a_4/p_4^2,$$

the following inequality holds:

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{Y}{X^2}.$$

*Proof.* Let

$$\begin{aligned} \mathcal{Q}_Y(X) = \{ (p_1, p_2, p_3, p_4, a_1, a_2, a_3, a_4) : p_i \leq X \text{ distinct, } a_i < p_i^2, \\ 0 \leq a_j p_i^2 - a_i p_j^2 \leq Y \text{ for } i < j \}. \end{aligned}$$

By Lemma 4.6, we get

$$|\mathcal{Q}_Y(X)| \leq X \exp \left( (C' - \tilde{C}) \frac{\log X}{\sqrt{\log \log X}} \right)$$

We can choose  $\tilde{C}$  in such a way that

$$|\mathcal{Q}_Y(X)| \leq \frac{\pi(X)}{8},$$

where  $\pi(X) = \sum_{p \leq X} 1$  denotes the number of primes in  $[1, X]$ . Let

$$\begin{aligned} \mathcal{P}' = \{ p \leq X : p \text{ prime,} \\ p \neq p_1 \text{ for any octuple in } \mathcal{Q}_Y(X) \text{ with any of the first four coordinates } p_i. \}, \end{aligned}$$

then

$$|\mathcal{P}'| \geq \pi(x) - 4|\mathcal{Q}_Y(X)| \geq \frac{\pi(X)}{2}.$$

Consider  $p_1, p_2, p_3, p_4 \in \mathcal{P}'$  and arbitrary  $a_1, a_2, a_3, a_4$  satisfying the assumptions of the lemma. If there are  $i < j$  such that  $p_i = p_j$ , then

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{a_j}{p_j^2} - \frac{a_i}{p_i^2} \geq \frac{1}{p_i^2} \geq \frac{1}{X^2},$$

which proves the assertion in this case.

Otherwise, all  $p_i$  are pairwise distinct. Since  $p_i \notin \mathcal{P}'$ , we know that there are  $i < j$  such that

$$\Delta_{i,j} = a_j p_i^2 - a_i p_j^2 > Y.$$

Then

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{a_j}{p_j^2} - \frac{a_i}{p_i^2} = \frac{\Delta_{i,j}}{p_i^2 p_j^2} > \frac{Y}{X^4}. \quad \square$$

We define

$$F(x) = \sum_{n=1}^N e(nx),$$

and note that, for any  $q \in \mathbb{N}$ ,

$$F_q(x) := \sum_{a=1}^q F\left(x - \frac{a}{q}\right) = \sum_{n=1}^N e(nx) \sum_{e(-an/q)} = q \sum_{\substack{1 \leq n \leq N, \\ q|n}} e(nx).$$

Letting  $X = \max(3, \lfloor N^{4/15} \rfloor)$ , and choosing  $Y$  and  $\mathcal{P}'$  as specified in Lemma 4.8, we define

$$G(x) = \frac{1}{|\mathcal{P}'|} \sum_{p \in \mathcal{P}'} F_{p^2}(x) = \sum_{n=1}^N d_n e(nx).$$

For any squarefree  $n$ , we have  $d_n = 0$ .

**Lemma 4.9.** *The following inequality holds uniformly with respect to  $x$ :*

$$G(x) - F(x) \leq N^{11/15} \exp\left(\frac{C_1 \log N}{\sqrt{\log \log N}}\right),$$

where  $C_1 > 0$  is some constant.

*Proof.* As explained on p. 199 in [24], the triangle inequality implies that

$$|F(x)| = \left| \sum_{n=1}^N e(nx) \right| \leq \sum_{n=1}^N |e(nx)| = \sum_{n=1}^N 1 = N,$$



and by the formula for geometric series

$$|F(x)| = \left| \sum_{n=1}^N e(nx) \right| = \left| \frac{1 - e((n+1)x)}{1 - e(x)} \right| \leq \frac{2}{|1 - e(x)|} \leq \frac{1}{2\|x\|_{\mathbb{R}/\mathbb{Z}}},$$

where for the last inequality we used that  $|1 - e(x)| = 2|\sin \pi x| \geq 4\|x\|_{\mathbb{R}/\mathbb{Z}}$  and that  $|\sin \pi t| \geq 2|t|$  for  $|t| \leq 1/2$ . Hence

$$|F(x)| \leq \min \left( N, \frac{1}{2\|x\|_{\mathbb{R}/\mathbb{Z}}} \right).$$

Therefore,

$$\begin{aligned} G(x) - F(x) &= \frac{1}{|\mathcal{P}'|} \sum_{p \in \mathcal{P}'} \sum_{a=1}^{p^2-1} F\left(x - \frac{a}{p}\right) \\ &= \frac{1}{|\mathcal{P}'|} \sum_{p \in \mathcal{P}'} \sum_{a=1}^{p^2-1} \min \left( N, \|x - a/p^2\|_{\mathbb{R}/\mathbb{Z}}^{-1} \right). \end{aligned}$$

Moreover, since  $|\mathcal{P}'| \gg \pi(X) \gg N^{4/15}/\log N$ ,

$$G(x) - F(x) \ll N^{-4/15} \log N \sum_{p \in \mathcal{P}'} \sum_{a=1}^{p^2-1} \min \left( N, \|x - a/p^2\|_{\mathbb{R}/\mathbb{Z}}^{-1} \right). \quad (4.5)$$

Now, we fix  $x$ . For the three fractions that are closest to  $x$ , we bound the minimum by  $N$ . For the remaining fractions, we notice that by Lemma 4.8, for any positive integer  $m$ , the number of fractions  $a/p^2$  such that  $\|x - \frac{a}{p^2}\|_{\mathbb{R}/\mathbb{Z}} < mY/(2X^4)$  does not exceed  $6m$ ; this can be shown as follows<sup>2</sup>:

We start by labelling the fractions as  $a_j/p_j^2$  such that  $a_j/p_j^2 < a_{j+1}/p_{j+1}^2$ , hence (by our choice of  $\mathcal{P}'$  in accordance with Lemma 4.8)

$$\frac{a_{k+3}}{p_{k+3}^2} - \frac{a_k}{p_k^2} > \frac{Y}{X^4}.$$

Then, for  $M \geq 3\ell$ ,

$$\frac{a_{k+M}}{p_{k+M}^2} - \frac{a_k}{p_k^2} \geq \frac{a_{k+3\ell}}{p_{k+3\ell}^2} - \frac{a_k}{p_k^2} = \sum_{j=1}^{\ell} \left( \frac{a_{k+3j}}{p_{k+3j}^2} - \frac{a_{k+3(j-1)}}{p_{k+3(j-1)}^2} \right) \geq \sum_{j=1}^{\ell} \frac{Y}{X^4} = \ell \frac{Y}{X^4}. \quad (4.6)$$

<sup>2</sup>In the paper [26], this is stated with  $3m$  instead of  $6m$ . It is conceivable that this can be achieved by carefully considering the maximum distance of  $a/p^2$  and  $a'/p'^2$  when both are close to  $x$ ; however, the multiplicative constant gets lost in the subsequent step anyway, so any additional effort would be in vain.

Note that for all  $j$ ,  $a_j/p_j^2 \in (0, 1)$ , and partition  $(0, 1)$  into two intervals,

$$(0, 1) = (0, 1/2) \cup [1/2, 1).$$

Suppose that there is some fraction  $a_k/p_k^2$  such that  $\|x - \frac{a_k}{p_k^2}\|_{\mathbb{R}/\mathbb{Z}} < mY/(2X^4)$ . We may then assume that  $k$  is the minimum index satisfying  $\|x - \frac{a_j}{p_j^2}\|_{\mathbb{R}/\mathbb{Z}}$  for the interval that  $a_k/p_k^2$  lies in. If  $a_j/p_j^2$  is another number in the same interval such that  $\|x - \frac{a}{p^2}\|_{\mathbb{R}/\mathbb{Z}} < mY/(2X^4)$ , then  $a_k/p_k^2 < a_j/p_j^2$ , and (since their distance is at most  $1/2$ )

$$\begin{aligned} \frac{a_j}{p_j^2} - \frac{a_k}{p_k^2} &= \left\| \frac{a_j}{p_j^2} - \frac{a_k}{p_k^2} \right\|_{\mathbb{R}/\mathbb{Z}} \\ &\leq \left\| x - \frac{a_j}{p_j^2} \right\|_{\mathbb{R}/\mathbb{Z}} + \left\| x - \frac{a_k}{p_k^2} \right\|_{\mathbb{R}/\mathbb{Z}} \\ &< m \frac{Y}{X^4}. \end{aligned}$$

By inequality 4.6, this shows that  $j - k \leq 3m - 1$ .

Therefore, we can reorder our remaining fractions (i.e., all fractions but the three we excluded in the beginning) in such a way that the  $k$ th fraction  $a/p^2$  satisfies

$$\|x - a/p^2\|_{\mathbb{R}/\mathbb{Z}} \geq \frac{kY}{12X^4}.$$

Therefore, by inequality 4.5,

$$\begin{aligned} G(x) - F(x) &\ll N^{-4/15} \log N \left( N + \sum_{k \leq X^3} \frac{X^4}{kY} \right) \\ &\ll N^{11/15} \log N + N^{-4/15} \log N \frac{X^4}{Y} \sum_{k \leq X^3} \frac{1}{k} \\ &\ll N^{11/15} \log N + N^{-4/15} \log N \frac{X^4}{X^{1/4}} \exp \left( \frac{\tilde{C} \log X}{\sqrt{\log \log X}} \right) \log(X^3) \\ &\ll N^{11/15} \log N + N^{11/15} \log N \exp \left( \frac{\tilde{C}' \log N}{\sqrt{\log \log N}} \right) \log N \\ &\ll N^{11/15} \exp \left( \frac{\tilde{C}'' \log N}{\sqrt{\log \log N}} \right). \end{aligned} \quad \square$$

Finally, we arrive at the proof of Theorem 4.4.

*Proof of Theorem 4.4.* Let

$$M(x) = \sum_{\substack{1 \leq n \leq N, \\ n \in \mathcal{S}_{\text{free}}}} a_n e(nx)$$

be some trigonometric polynomial with  $\{n : a_n \neq 0\} \subset \mathcal{S}_{\text{free}}$ . Then, for any  $x$ ,

$$\begin{aligned} \int_0^1 G(x-y)M(y) \, dy &= \sum_{n=1}^N \sum_{m=1}^N d_n a_m e(nx) \int_0^1 e((m-n)y) \, dy \\ &= \sum_{n=1}^N a_n d_n e(nx) = 0, \end{aligned}$$

recalling that  $d_n = 0$  for squarefree  $n$ .

Similarly,

$$\begin{aligned} \int_0^1 F(x-y)M(y) \, dy &= \sum_{n=1}^N \sum_{m=1}^N a_m e(nx) \int_0^1 e((m-n)y) \, dy \\ &= \sum_{n=1}^N a_n e(nx) = M(x). \end{aligned}$$

Hence

$$\int_0^1 (F(x-y) - G(x-y)) M(y) \, dy = M(x),$$

so, by Lemma 4.9,

$$\begin{aligned} |M(x)| &\leq \int_0^1 |F(x-y) - G(x-y)| |M(y)| \, dy \\ &\leq N^{11/15} \exp\left(\frac{C \log N}{\sqrt{\log \log N}}\right) \int_0^1 |M(y)| \, dy, \end{aligned}$$

so

$$\text{BR}_N := \sup \left\{ \frac{\max_x |M(x)|}{\int_0^1 |M(x)| \, dx} : M(x) = \sum_{n \in \mathcal{S}_{\text{free}}, n \leq N} a_n e(nx) \right\} \leq N^{11/15} \exp\left(\frac{C_1 \log N}{\sqrt{\log \log N}}\right),$$

and by inequality 4.1,

$$\text{ES}_N \leq N^{11/15} \exp\left(\frac{C_2 \log N}{\sqrt{\log \log N}}\right).$$

□

## 5 Hilbert cubes

Let  $d \geq 1$  be a positive integer, and let  $a_0, a_1, \dots, a_d \in \mathbb{Z} \setminus \{0\}$ . Then we call

$$\begin{aligned} H(a_0; a_1, \dots, a_d) &:= a_0 + \{0, a_1\} + \dots + \{0, a_d\} \\ &= \{a_0 + \varepsilon_1 a_1 + \dots + \varepsilon_d a_d : \varepsilon_1, \dots, \varepsilon_d \in \{0, 1\}\} \end{aligned}$$

a  $d$ -dimensional **Hilbert cube**. For  $a_0 = 0$  and  $a_1, \dots, a_d$  as above, we adapt our definition to say that

$$H(0; a_1, \dots, a_d) := \{\varepsilon_1 a_1 + \dots + \varepsilon_d a_d : \varepsilon_i \in \{0, 1\}, \text{ not all } \varepsilon_i = 0\},$$

is a **homogeneous Hilbert cube** of dimension  $d$ . Notably, in the case where all  $a_i$  are distinct,  $H(0; a_1, \dots, a_d)$  is the set containing all nonempty subset sums of  $\{a_1, \dots, a_d\}$ .

In this chapter, we discuss results obtained by Dietmann and Elsholtz[10, 11] concerning the maximal dimension of Hilbert cubes contained in certain sets. In the first section, we examine Hilbert cubes in the set of squares  $\mathcal{S}$ , and show that the maximal dimension of a Hilbert cubes  $H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S} \cap [1, N]$ , for  $N \in \mathbb{N}$ , is of order  $d \ll \log \log N$ . In the second section, we focus on the set of **pure integer powers**

$$\mathcal{V} := \{n^k : n \in \mathbb{N}, k \in \mathbb{N}, k \geq 2\} = \{n^p : n \in \mathbb{N}, p \in \mathcal{P}\},$$

and derive certain estimates for the dimension of homogeneous Hilbert cubes contained in  $\mathcal{V} \cap [1, N]$ .

We will observe that information about the maximum length of arithmetic progressions within the set under consideration plays a crucial role in our proofs. For completeness, we recall that an **arithmetic progression of length  $k$**  is a set of the form

$$\{n, n + m, \dots, n + (k - 1)m\},$$

where  $n \in \mathbb{Z}$  is an integer and  $m \in \mathbb{N}$  is a positive integer; it is called **homogeneous** if  $n = m$ , i.e., if it is of the form

$$\{n, 2n, \dots, kn\}$$

for some  $n, k \in \mathbb{N}$ .

## 5.1 Squares

In this section, we prove results that enable us to analyse the dimension Hilbert cubes in the set of squares. Our discussion is based on the findings presented in [11].

We give a lower bound for the cardinality of Hilbert cubes contained in sets without arithmetic progressions of length  $k$ . More concretely, we show

$$|H(a_0; a_1, \dots, a_d)| \geq 2 \left( \frac{k}{k-1} \right)^{d-1} - 1 \quad (5.1)$$

for any Hilbert cube  $|H(a_0; a_1, \dots, a_d)|$ . Since the set of squares  $\mathcal{S}$  does not contain any arithmetic progressions of length four (see Volume II, p. 440 of [9], for the history of this problem), Eq. (5.1) implies

$$|H(a_0; a_1, \dots, a_d)| \geq 2 \left( \frac{4}{3} \right)^{d-1} - 1 \quad (5.2)$$

for any Hilbert cube  $H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S}$ .

By contrast, we can write  $H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S} \cap [1, N]$  as a sumset using two summands, namely  $H(a_0; a_1, \dots, a_d) = H(a_0; a_1, \dots, a_{\lfloor d/2 \rfloor}) + H(0; a_{\lfloor d/2 \rfloor + 1}, \dots, a_d)$ , so, by Theorem 3.11 from Chapter 3,

$$\min(|H(a_0; a_1, \dots, a_{\lfloor d/2 \rfloor})|, |H(0; a_{\lfloor d/2 \rfloor + 1}, \dots, a_d)|) \ll \log N. \quad (5.3)$$

Combining the estimates from Eq. (5.2) and Eq. (5.3), we obtain  $(4/3)^d \ll \log N$ , i.e.,

$$d \ll \log \log N.$$

Summarising our considerations, we can state the following theorem (Theorem 1 in [11]).

**Theorem 5.1.** *Let  $a_0 \in \mathbb{N}_0$  be a nonnegative integer and let  $a_1, \dots, a_d \in \mathbb{N}$  be positive integers. Assume that*

$$H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S} \cap [1, N].$$

*where  $N \in \mathbb{N}$ . Then the following holds:*

$$d \ll \log \log N.$$

For the remainder of this section, we will concern ourselves with establishing the bound in Eq. (5.1) and applying our theorem in order to give a bound on the dimension of Hilbert cubes in  $\mathcal{S}'(f) = \{f(x) : x \in \mathbb{Z}\}$ , where  $f$  is a quadratic polynomial subject to certain conditions. For the former, we need the following lemma.

**Lemma 5.2.** *Let  $\alpha \in (0, 1)$ ,  $\mathcal{B} \subset \mathbb{Z}$  a finite nonempty set of integers, and let  $h \in \mathbb{Z} \setminus \{0\}$ . If*

$$|\mathcal{B} \cap (\mathcal{B} + h)| > (1 - \alpha)|\mathcal{B}|,$$

*then  $\mathcal{B}$  contains an arithmetic progression of the form  $b, b+h, \dots, b + \lfloor 1/\alpha \rfloor h$  for some  $b \in \mathcal{B}$ .*

*Proof.* For  $b \in \mathcal{B}$ , we define

$$r(b) = \min_{r \geq 1} \{r : b + rh \notin \mathcal{B}\}.$$

Let  $r \geq 1$  be a nonnegative integer. We note that

$$\begin{aligned} |\{b \in \mathcal{B} : b + (r-1)h \in \mathcal{B}, b + rh \notin \mathcal{B}\}| &= |\{b + (r-1)h \in \mathcal{B} : b \in \mathcal{B}, b + rh \notin \mathcal{B}\}| \\ &\leq |\{b' \in \mathcal{B} : b' + h \notin \mathcal{B}\}| \\ &= |\mathcal{B}| - |\mathcal{B} \cap (\mathcal{B} + h)| \\ &< \alpha|\mathcal{B}|, \end{aligned}$$

and thus, the number of  $b \in \mathcal{B}$  such that  $r(b) = r$  is strictly less than  $\alpha|\mathcal{B}|$ . Therefore, the number of  $b \in \mathcal{B}$  with  $r(b) \leq k$  is strictly less than  $k\alpha|\mathcal{B}|$ .

With  $k = \lfloor 1/\alpha \rfloor$ , we see that the number of  $b \in \mathcal{B}$  such that  $r(b) \leq k$  is strictly less than

$$k\alpha|\mathcal{B}| \leq \frac{1}{\alpha}\alpha|\mathcal{B}| = |\mathcal{B}|,$$

thus there exists  $b_0 \in \mathcal{B}$  with

$$r(b_0) = \min_{r \geq 1} \{r : b_0 + rh \notin \mathcal{B}\} \geq k + 1,$$

so  $b, b+h, \dots, b+kh \in \mathcal{B}$ . □

**Lemma 5.3.** *Let  $k \geq 3$ , and let  $\mathcal{S}' \subseteq \mathbb{N}$  be a set of integers that does not contain any arithmetic progressions of length  $k$ . Let  $a_0 \in \mathbb{Z}$  be an integer, and let  $\mathcal{A} = \{a_1, \dots, a_d\} \subset \mathbb{Z} \setminus \{0\}$  be a set of  $d$  nonzero integers. If  $H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S}'$ , then*

$$|H(a_0; a_1, \dots, a_d)| \geq 2 \left( \frac{k}{k-1} \right)^{d-1} - 1.$$

*Proof.* Let

$$c = \frac{k}{k-1} = 1 + \frac{1}{k-1},$$

and for  $i = 1, \dots, d$ , let

$$H_i = a_0 + \{0, a_1\} + \dots + \{0, a_i\}.$$

First, we assume that  $a_0 \neq 0$ . Suppose that there is some  $i < d$  such that

$$\frac{|H_{i+1}|}{|H_i|} < c.$$

Then

$$c|H_i| > |H_{i+1}| = |H_i + \{0, a_{i+1}\}| = 2|H_i| - |(H_i + \{0, a_{i+1}\}) \cap H_i|,$$

i.e.,

$$|(H_i + \{0, a_{i+1}\}) \cap H_i| > (2 - c)|H_i| = (1 - (c - 1))|H_i|.$$

By Lemma 5.2, this implies that  $H_i$  contains an arithmetic progression of length

$$\left\lfloor \frac{1}{c-1} \right\rfloor + 1 = \left\lfloor \frac{1}{1/(k-1)} \right\rfloor + 1 = k,$$

a contradiction to the fact that  $H_i \subseteq \mathcal{S}$ , a set without arithmetic progressions of length  $k$ . Hence, for all  $i = 1, \dots, d$ ,

$$\frac{|H_i|}{|H_{i+1}|} \geq \frac{k}{k-1},$$

so

$$|H_d| = 2 \frac{|H_d|}{|H_1|} = 2 \frac{|H_2|}{|H_1|} \frac{|H_3|}{|H_2|} \dots \frac{|H_d|}{|H_{d-1}|} \geq 2 \left( \frac{k}{k-1} \right)^{d-1}.$$

If  $a_0 = 0$ , we do the same calculation as above, and then subtract 1 to account for the fact that the empty sum is not included.  $\square$

We note the lower bound given in Lemma 5.3 is not necessarily optimal. In fact, in the case  $k = 3$  and  $a_0 \neq 0$ , one can show that all sums  $a_0 + \varepsilon_1 a_1 + \dots + \varepsilon_d a_d$  have to be distinct. Otherwise, as is discussed in [10] (Proof of Lemma 3), there would be disjoint index sets  $I, I' \subseteq [1, d]$  such that  $\sum_{i \in I} a_i = \sum_{j \in I'} a_j$ . But then

$$a_0, \quad a_0 + \sum_{i \in I} a_i, \quad a_0 + \sum_{i \in I \cup I'} a_i$$

would form a 3 term arithmetic progression, a contradiction.

Finally, let us discuss an application of Theorem 5.1. For  $a, b, c \in \mathbb{Z}$ ,  $a \neq 0$ , define by  $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$  a quadratic polynomial with integer coefficients, and consider

$$\mathcal{S}'(f) = \{f(x) : x \in \mathbb{Z}\}.$$

We notice that

$$\begin{aligned} 4af(x) + b^2 - 4ac &= 4a^2x^2 + 4abx + 4ac + b^2 - 4ac \\ &= 4a^2x^2 + 4abx + b^2 \\ &= (2ax + b)^2. \end{aligned}$$

Hence, for  $a_0, \dots, a_d \in \mathbb{N}$ , if  $H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S}'(f)$ , then

$$H(4aa_0 + b^2 - 4ac; 4aa_1, \dots, 4aa_d) \subseteq \mathcal{S} \cup \{0\}.$$

This observation is the key ingredient in the proof of the following corollary.

**Corollary 5.4.** *Let  $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$  be a quadratic polynomial with  $a > 0$  and  $4a + b^2 - 4ac \geq 1$ . Assume that  $a_1, \dots, a_d \in \mathbb{N}$  and*

$$H(a_0; a_1, \dots, a_d) \subseteq \mathcal{S}'(f) \cap [1, N],$$

where  $N \in \mathbb{N}$  is a positive integer. Then

$$d \ll \log \log N.$$

*Proof.* Assume that  $f(x) \in H(a_0; a_1, \dots, a_d)$ . Now, as above, we write

$$4af(x) + b^2 - 4ac = (2ax + b)^2.$$

Since by assumption  $f(x) \in [1, N]$ , we have

$$4aN + b^2 - 4ac \geq (2aN + b)^2 = 4af(x) + b^2 - 4ac \geq 4a + b^2 - 4ac \geq 1.$$

Thus,

$$H(4aa_0 + b^2 - 4ac; 4aa_1, \dots, 4aa_d) \subseteq \mathcal{S} \cap [1, 4aN + b^2 - 4ac],$$

where  $\mathcal{S}$  denotes the set of squares. By Theorem 5.1, this implies that

$$d \ll \log \log(4aN + b^2 - 4ac) \ll \log \log N. \quad \square$$

## 5.2 Pure powers

### 5.2.1 General outline

In this section, we present results from [11] concerning homogeneous Hilbert cubes in the set of pure integer powers  $\mathcal{V}$ . More concretely, our goal is to prove the following theorem.

**Theorem 5.5.** *Let  $\mathcal{V}$  denote the set of pure integer powers, and let  $a_1, \dots, a_d$  be positive integers such that*

$$H(0; a_1, \dots, a_d) \subseteq \mathcal{V} \cap [1, N].$$

*If the  $a_i$  are pairwise distinct, then*

$$d \ll \frac{(\log \log N)^3}{\log \log \log N}.$$

*Otherwise, if not all  $a_i$  are necessarily distinct, one can still show that*

$$d \ll \frac{(\log \log N)^4}{(\log \log \log N)^2}.$$



In contrast to the set of squares in Section 5.1, the set of pure powers  $\mathcal{V}$  contains arbitrarily long arithmetic progressions. In fact, we will see (in Lemma 5.9) that the longest homogeneous arithmetic progression contained in  $\mathcal{V} \cap [1, N]$  is of order  $\log \log N / \log \log \log N$ .

However, analogous to our proof of Theorem 5.1 in Section 5.1, we will need to analyse quantities pertaining to arithmetic progressions. To this end, let us fix some set of integers  $\mathcal{W}$ . (In our application later, we will let  $\mathcal{W} = \mathcal{V}$ .) We define

$$f_{\mathcal{W}}(N) = \max_{\mathcal{B}_1, \dots, \mathcal{B}_5} \min_{1 \leq i \leq 5} |\mathcal{B}_i|,$$

where the maximum goes over all sets of positive integers  $\mathcal{B}_1, \dots, \mathcal{B}_5$  such that for all  $i \neq j$ ,  $\mathcal{B}_i + \mathcal{B}_j \subset \mathcal{W} \cap [1, N]$ . In other words,  $f_{\mathcal{W}}(N)$  is the minimal upper bound such that

$$\min_{1 \leq i \leq 5} |\mathcal{B}_i| \leq f_{\mathcal{W}}(N)$$

for any choice of  $\mathcal{B}_1, \dots, \mathcal{B}_5$  as above.

Moreover, denoting by  $r_{\mathcal{W},h}(n)$  the number of ways that a positive integer  $n$  can be written as a sum of  $h$  elements in  $\mathcal{W}$  (up to permutation of the summands), let

$$g_{\mathcal{W}}(h, N) := \max_{n \leq N} r_{\mathcal{W},h}(n).$$

Our strategy for proving Theorem 5.5 is as follows: We give upper bounds for  $f_{\mathcal{V}}(N)$  and  $g_{\mathcal{V}}(h, N)$ , which we then utilise to bound to the dimension of a Hilbert cube contained in  $\mathcal{V}$  by virtue of the following lemma.

**Lemma 5.6.** *Let  $\{a_1, \dots, a_d\} \subseteq \mathbb{N}$  be a set containing  $d$  distinct positive integers, and assume that  $H(0; a_1, \dots, a_d) \subset \mathcal{W} \cap [1, N]$ . Then*

$$d \leq 5(h! f_{\mathcal{W}}(N) g_{\mathcal{W}}(h, N))^{1/h} + 5h + 4$$

for any  $h \in \mathbb{N}$ .

In fact, in the situation of Lemma 5.6 above, we will be able to show (Corollary 5.10) that  $g_{\mathcal{V}}(h, N) \ll h! (\log \log N / \log \log \log N)^h$ . Moreover (in Lemma 5.8) we will see that  $f_{\mathcal{V}}(N) \ll (\log N)^M$ , where  $M > 0$  is some constant. Now, by the above Lemma 5.6, and since  $h! \leq h^h$ ,

$$d \ll \left( h^{2h} (\log N)^M \left( c_1 \frac{\log \log N}{\log \log \log N} \right)^{h-1} \right)^{1/h} + 5h + 4.$$

Choosing  $h = \log \log N$  yields

$$\begin{aligned} d &\ll \left( (\log \log N)^{2 \log \log N} (\log N)^M \left( \frac{\log \log N}{\log \log \log N} \right)^{\log \log N} \right)^{1/\log \log N} + \log \log N \\ &= (\log \log N)^2 \exp(M \log \log N / \log \log N) \frac{\log \log N}{\log \log \log N} + \log \log N \\ &\ll \frac{(\log \log N)^3}{\log \log \log N}. \end{aligned}$$

Now, for the case of repeated  $a_i$ : If there are  $\ell$  distinct  $i$  such that  $a_i = a$ , then  $H(0; a_1, \dots, a_d) \subset \mathcal{V} \cap [1, N]$  contains the homogeneous arithmetic progression

$$a, a + a, \dots, \underbrace{a + \dots + a}_{\ell \text{ times}}.$$

We will see that  $\ell \ll \log \log N / \log \log \log N$  (Lemma 5.9), which, using the special case above to bound the number of distinct  $a_i$ , implies the bound for the general case given in Theorem 5.5.

### 5.2.2 Estimates concerning arithmetic progressions

In this subsection, we will prove the various lemmas mentioned in the preceeding subsection, starting with the proof of Lemma 5.6.

*Proof of Lemma 5.6.* Let us write

$$h \wedge \mathcal{W} := \{v_1 + \dots + v_m : m \in \mathbb{N}, v_i \in \mathcal{V}, v_i \neq v_j \text{ if } i \neq j\}$$

for the  $h$ -fold disjoint sumset of  $\mathcal{W}$ . Taking into account that there are at most  $h!g_{\mathcal{W}}(h, N)$  ways to write any number  $\leq N$  as a sum of distinct elements in  $\mathcal{W}$ , we see that

$$|h \wedge \mathcal{W}| \geq \frac{|\mathcal{W}|(|\mathcal{W}| - 1) \dots (|\mathcal{W}| - h + 1)}{h!g_{\mathcal{W}}(h, N)} \geq \frac{(|\mathcal{W}| - h)^h}{h!g_{\mathcal{W}}(h, N)}, \quad (5.4)$$

as long as  $g_{\mathcal{W}}(h, N) > 0$ .

Now, let us decompose

$$\{a_1, \dots, a_d\} = \mathcal{A}_1 \cup \mathcal{A}_5 \cup R$$

into disjoint subsets with  $|\mathcal{A}_1|, \dots, |\mathcal{A}_5| = \lfloor d/5 \rfloor$  and  $|R| \leq 4$ .

For  $h \geq d$ , the inequality holds trivially. For  $h \leq d$ , we see that  $g_{\mathcal{W}}(h, N) > 0$ , and by Eq. (5.4)

$$|h \wedge \mathcal{A}_i| \geq \frac{(|\mathcal{A}_i| - h)^h}{h!g_{\mathcal{W}}(h, N)} = \frac{(\lfloor d/5 \rfloor - h)^h}{h!g_{\mathcal{W}}(h, N)}.$$

Furthermore, for  $i \neq j$ ,

$$h\widehat{\mathcal{A}}_i + h\widehat{\mathcal{A}}_j \subseteq H(a_0; a_1, \dots, a_d) \subseteq \mathcal{V} \cap [1, N].$$

Thus, by definition of  $f_{\mathcal{W}}$ , there is some  $i$  such that  $|h\widehat{\mathcal{A}}_i| \leq f_{\mathcal{W}}(N)$ .

Therefore, and since  $\lfloor d/5 \rfloor \geq d/5 - 4/5$  for integers  $d$ ,

$$\frac{(d/5 - 4/5 - h)^h}{h!g_{\mathcal{W}}(h, N)} \leq f_{\mathcal{W}}(N).$$

Rearranging yields

$$d \leq 5(f_{\mathcal{W}}(N)h!g_{\mathcal{W}}(h, N))^{1/h} + 4 + 5h. \quad \square$$

**Lemma 5.7.** *Let  $\mathcal{A} = \{a_1, \dots, a_d\}$  be a set of  $d$  distinct positive integers, and assume that*

$$H(a_0; a_1, \dots, a_d) \subseteq \mathcal{W} \cap [1, N],$$

*where  $\mathcal{W}$  is a set without homogeneous arithmetic progressions of length  $v \geq 3$ , and  $N$  is a positive integer. Then*

$$g_{\mathcal{W}}(h, N) \leq h!(v-1)^{h-1}.$$

*Proof.* (Following the proof of Lemma 9 in [10]). We proceed by induction on  $h$ .

The base case  $h = 1$  is clear. Before performing the induction step, we discuss the case  $h = 2$ , as it illustrates the general strategy.

Let  $n \in \mathbb{N}$ , and suppose that

$$n = a_{i_1} + a_{j_1} = \dots = a_{i_v} + a_{j_v},$$

where  $i_k, j_\ell$  for  $k, \ell = 1, \dots, v$  are  $2v$  elements of  $[1, d]$ . Then

$$\begin{aligned} n &= a_{i_1} + a_{j_1}, \\ 2n &= a_{i_1} + a_{j_1} + a_{i_2} + a_{j_2}, \\ &\dots \\ vn &= a_{i_1} + a_{j_1} + \dots + a_{i_v} + a_{j_v}, \end{aligned}$$

contradicting the fact that  $\mathcal{W}$  does not contain any homogeneous arithmetic progressions of length  $v$ . Thus

$$g_{\mathcal{W}}(2, N) \leq v - 1.$$

Now let  $h > 2$ , and assume that the claim has been proved for all  $h' \leq h$ . Let  $n \leq N$  be a positive integer, and let  $M$  be maximal such that there are  $M$  disjoint index sets  $I_j \subseteq [1, d]$  with

$$n = \sum_{i \in I_j} a_i$$

for  $j = 1, \dots, M$ . The same argument as before shows  $m \leq v - 1$ . Assume there is another  $I' \subseteq [1, d]$ , different from all  $I_j$ , such that

$$n = \sum_{i \in I'} a_i.$$

By the maximality of  $M$ , there is some  $j$  such that  $I' \cap I_j \neq \emptyset$ ; let  $i \in I' \cap I_j$ . Then  $I' \setminus \{i\}$  provides a way to write  $n - a_i \leq N$  as a sum of  $h - 1$  summands from  $\mathcal{A}$ , and clearly  $I'$  is uniquely defined by  $i$  and  $I' \setminus \{i\}$ , for which there are at most  $(v - 1)h$  and  $g_{\mathcal{W}}(h - 1, N)$  choices, respectively. Therefore (applying the induction hypothesis)

$$g_{\mathcal{W}}(h, N) \leq (v - 1)h g_{\mathcal{W}}(h - 1, N) \leq (v - 1)h(h - 1)!(v - 1)^{h-2} = h!(v - 1)^{h-1}. \quad \square$$

**Lemma 5.8.** *There is a constant  $M > 0$  with the following property: if  $\mathcal{A}_1, \dots, \mathcal{A}_5 \subseteq [1, N]$  are sets of positive integers with*

$$\mathcal{A}_i + \mathcal{A}_j \subseteq \mathcal{V}$$

for all  $i \neq j$ , then

$$\min_{1 \leq i \leq 5} |\mathcal{A}_i| \ll (\log N)^M.$$

In other words,

$$f_{\mathcal{V}}(N) \ll (\log N)^M,$$

where  $f_{\mathcal{V}}(N)$  is defined as in subsection 5.2.1

For purposes, the exact value of  $M$  is not important, but via a more detailed analysis, one can obtain  $M = 48$ .

*Proof.* For  $i = 1, \dots, 5$ , we write  $|\mathcal{A}_i| = t_i$ ,

$$\mathcal{A}_i = \{a_{i1}, \dots, a_{it_i}\},$$

and represent uniquely

$$a_{i,j} = 2^{u_{ij}}(4s_{ij} + e_{ij})$$

with  $e_{ij} \in \{-1, 1\}$ ,  $j = 1, \dots, t_i$ ; notice that for all  $i, j$ ,  $u_{ij} \leq \lfloor \log N / \log 2 \rfloor$ .

We define

$$\mathcal{A}_{i,u,e} := \{a_{ij} \in \mathcal{A}_i : u_{ij} = u, e_{ij} = e\}$$

for  $i \in \{1, \dots, 5\}$ ,  $u \in \{0, \dots, \lfloor \log N / \log 2 \rfloor\}$ , and  $e \in \{-1, 1\}$ . Clearly

$$\mathcal{A}_i = \bigcup_{u,e} \mathcal{A}_{i,u,e}.$$

Choosing among all  $\mathcal{A}_{i,u,e}$  the one with the maximal cardinality and denoting it by  $\mathcal{A}_{i,u_i,e_i}$ , we get

$$|\mathcal{A}_i| \ll \log N |\mathcal{A}_{i,u_i,e_i}|. \quad (5.5)$$

Without loss of generality, we may assume that  $e_1 = e_2$  and that either  $u_1 = u_2 = 0$  or both  $u_1, u_2$  are positive. Either way, for  $a_1 \in \mathcal{A}_{1,u_1,e_1}, a_2 \in \mathcal{A}_{2,u_2,e_2}$ , we get

$$\begin{aligned} a_1 + a_2 &= 2^{u_1}(4s_1 + e_1) + 2^{u_2}(4s_2 + e_2) \\ &= 2^{g_{\mathcal{W}}(u_1, u_2)}(2z + 1) \\ &= y^q, \end{aligned}$$

where  $s_1, s_2, y, z$  are integers,

$$0 < g_{\mathcal{W}}(u_1, u_2) = \begin{cases} u_1 + 1 & \text{if } u_1 = u_2, \\ \min\{u_1, u_2\} & \text{otherwise,} \end{cases}$$

and  $q$  is a prime that divides  $g_{\mathcal{W}}(u_1, u_2)$ . Letting

$$Q(u_1, u_2) = \prod_{q|g_{\mathcal{W}}(u_1, u_2)} q,$$

we see that

$$2^{Q(u_1, u_2)} \leq a_1 + a_2 \leq 2N,$$

so

$$Q(u_1, u_2) \ll \log N.$$

Let  $p$  be a prime such that  $p \equiv 1 \pmod{Q(u_1, u_2)}$ , and write  $\overline{\mathcal{A}}_p$  and  $\overline{\mathcal{B}}_p$  for the reductions of  $\mathcal{A}_{1,u_1,e_1}$  and  $\mathcal{A}_{2,u_2,e_2}$  modulo  $p$ ; furthermore, denote  $\nu_{\mathcal{A}}(p) = |\overline{\mathcal{A}}_p|$  and  $\nu_{\mathcal{B}}(p) = |\overline{\mathcal{B}}_p|$ . Then, for any  $\varepsilon > 0$ ,

$$\nu_{\mathcal{A}}(p)\nu_{\mathcal{B}}(p) \ll_{\varepsilon} p^{1+\varepsilon}. \quad (5.6)$$

The proof of Eq. (5.6) can be found in this chapter's main source [11]; we decided to skip it.

By Theorem 2.2, we have

$$\begin{aligned} \sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} \frac{\log p}{p^{1/2+\varepsilon}} &\gg N_1^{-1/2-\varepsilon} \sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} \log p \\ &\gg \frac{N_1^{-1/2-\varepsilon}}{\varphi(Q(u_1, u_2))\sqrt{Q(u_1, u_2)}} \end{aligned}$$

for  $N_1 \geq Q(u_1, u_2)^L$ . Moreover, by the Brun-Titchmarsh inequality (Theorem 2.1)

$$\begin{aligned} \sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} \log p &\ll \log N_1 \sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} 1 \\ &\ll \log N_1 \frac{N_1}{\varphi(Q(u_1, u_2))(\log N_1 - \log Q)} \\ &\ll \frac{N_1}{\varphi(Q(u_1, u_2))}. \end{aligned}$$

Now, by Eq. (5.6),  $\min(\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p)) \ll_{\varepsilon} p^{1/2+\varepsilon}$ , so

$$\sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} \frac{\log p}{\min(\nu_{\mathcal{A}}(p), \nu_{\mathcal{B}}(p))} \gg \frac{N_1^{-1/2-\varepsilon}}{\varphi(Q(u_1, u_2)) \sqrt{Q(u_1, u_2)}},$$

and we may assume w.l.o.g. that

$$\sum_{\substack{p \leq N_1, \\ p \equiv 1 \pmod{Q(u_1, u_2)}}} \frac{\log p}{\nu_{\mathcal{A}}(p)} \gg \frac{N_1^{-1/2-\varepsilon}}{\varphi(Q(u_1, u_2)) \sqrt{Q(u_1, u_2)}}.$$

We choose  $N_1 = (\log N)$ , noting that  $Q(u_1, u_2) \ll \log N$ , so the conditions of Theorem 2.2 are satisfied. Next, we apply Gallagher's larger sieve (Theorem 1.6).

$$\begin{aligned} |\mathcal{A}_{1, u_1, e_1}| &\leq \frac{-\log N + \frac{N_1}{\varphi(Q(u_1, u_2))}}{-\log N + \frac{N_1^{-1/2-\varepsilon}}{\varphi(Q(u_1, u_2)) \sqrt{Q(u_1, u_2)}}} \\ &\ll N_1^{1/2+\varepsilon} \sqrt{Q(u_1, u_2)} \\ &\ll (\log N)^{L/2+3}. \end{aligned}$$

Thus, by Eq. (5.5),

$$|\mathcal{A}_1| \ll \log N |\mathcal{A}_{i, u_i, e_i}| \ll (\log N)^{L'}.$$

□

**Lemma 5.9.** *Let  $\mathcal{V}$  denote the set of all pure integer powers, and let  $\ell(N)$  denote the maximum positive integer such that there is  $x \in \mathcal{V}$  with*

$$x, 2x, \dots, \ell(N)x \in \mathcal{V} \cap [1, N].$$

*Then*

$$\frac{\log \log N}{\log \log \log N} \ll \ell(N) \ll \frac{\log \log N}{\log \log \log N}.$$

*Proof.* **Lower bound** (following [21]): Let

$$n = \left\lfloor \frac{\log \log N}{4 \log \log \log N} \right\rfloor,$$

and let  $p_1, \dots, p_m$  denote all prime numbers  $\leq n$ . We describe how to find a number  $x$  such that  $jx$  is a  $p_j$ th power for all  $1 \leq j \leq m$ .

To this end, we write  $1 \leq j \leq m$  as

$$j = p_1^{w_{p_1}(j)} \dots p_m^{w_{p_m}(j)}.$$

Then

$$jx = p_1^{w_{p_1}(j)+w_{p_1}(x)} \cdots p_m^{w_{p_m}(j)+w_{p_m}(x)}$$

is a  $p_j$ th power if and only if each exponent is divisible by  $p_j$ . Hence we need to solve the following system of equations for  $w_1, \dots, w_m$ :

$$w_t \equiv -w_{p_t}(j) \pmod{p_j} \text{ for } 1 \leq j \leq n, 1 \leq t \leq m.$$

By the Chinese remainder theorem, a solution  $w_t$  exists, and can be chosen to lie inside  $[0, p_1 \cdots p_m]$ , for  $1 \leq t \leq m$ . Noting that

$$\log p_1 \cdots p_m = \sum_{p \leq n} \log p \ll n,$$

we see that

$$w_t \ll \exp(\log p_1 \cdots p_m) \ll \exp(n),$$

so  $w_t \leq \exp(2n)$  (for  $N$  sufficiently large). Hence

$$nx = np_1^{w_1} \cdots p_m^{w_m} \leq (p_1 \cdots p_m)^{p_1 \cdots p_m} \leq \exp(2n)^{\exp(2n)} = \exp(\exp(2n \log 2n)) < N,$$

for sufficiently large  $N$ .

**Upper bound:** For the proof of the upper bound, we note that if  $2x \in \mathcal{V}$ , then  $x$  has to be even (as otherwise  $2x \equiv 2 \pmod{4}$  would not be a square). Hence there is  $k \geq 1$  such that

$$2^k \parallel x,$$

that is,  $2^k$  divides  $x$  and  $k$  is maximal with that property. Then also

$$2^k \parallel nx$$

for all odd  $n \leq \ell(N)$ . Moreover, since  $nx$  is a  $q$ th power, necessarily

$$q \mid k.$$

Furthermore, since  $2^k \leq x \leq N$ , we have

$$k \ll \log N.$$

Hence, denoting by  $\omega(k)$  the number of distinct prime factors of  $k$ , there are at most

$$\omega(k) \ll \frac{\log k}{\log \log k} \ll \frac{\log \log N}{\log \log \log N}$$

possible values for  $q$ . Now, we remark that if  $n_1, n_2$  are squarefree such that  $n_1x = a^q$  and  $n_2x = b^q$  are both a  $q$ th power, then  $n_1 = n_2$ . Indeed, since

$$\frac{n_1}{n_2} = \left(\frac{a}{b}\right)^q,$$

$\sqrt[q]{n_1/n_2}$  is rational, so  $n_1/n_2 = 1$ . It can be shown that the odd squarefree numbers have positive density,<sup>1</sup> and thus, since each odd squarefree  $n$  needs “its own” prime exponent, this already implies

$$\ell(N) \ll \frac{\log \log N}{\log \log \log N}. \quad \square$$

Combining Lemma 5.7 and Lemma 5.9, we get:

**Corollary 5.10.** *Let  $\mathcal{A} = \{a_1, \dots, a_d\}$  be a set of  $d$  distinct positive integers, and assume that*

$$H(a_0; a_1, \dots, a_d) \subseteq \mathcal{W} \cap [1, N].$$

*Then*

$$g_{\mathcal{V}}(h, N) \ll h! (\log \log N / \log \log \log N)^h.$$

---

<sup>1</sup>According to Theorem 4.1, we know that the squarefree numbers have density  $6/\pi^2$ . It is evident that if the odd squarefree numbers do have a particular density, it would necessarily be  $4/\pi^2$ . This is due to the fact that multiplication by 2 establishes a one-to-one correspondence between the odd squarefree numbers in  $[1, N]$  and the even squarefree numbers in  $[1, 2N]$ . A proof that they do indeed have this density can be found in [25].



# Bibliography

- [1] N. Alon, O. Angel, I. Benjamini, and E. Lubetzky, *Sums and products along sparse graphs*, Israel Journal of Mathematics **188** (2012), no. 1, 353–384.
- [2] E. Bombieri and U. Zannier, *On the number of rational points on certain elliptic curves*, Izvestiya: Mathematics **68** (2004), no. 3, 437.
- [3] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer, Berlin-Heidelberg, 1995.
- [4] D.A. Burgess, *On character sums and primitive roots*, Matematika **7** (1963), no. 4, 3–16.
- [5] Y.-G. Chen and P. Xi, *A conjecture of Sárközy on quadratic residues, ii*, arXiv preprint arXiv:2202.02780 (2022).
- [6] Y.-G. Chen and X.-H. Yan, *A conjecture of Sárközy on quadratic residues*, Journal of Number Theory **229** (2021), 100–124.
- [7] K. Conrad, *Quadratic residue patterns modulo a prime*, <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QuadraticResiduePatterns.pdf>, 2014.
- [8] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), no. 3-4, 252–265.
- [9] L. E. Dickson, *History of the theory of numbers, vol. ii*, chelsea publ, Co., New York (1971).
- [10] R. Dietmann and C. Elsholtz, *Hilbert cubes in progression-free sets and in the set of squares*, Israel Journal of Mathematics **192** (2012), 59–66.
- [11] ———, *Hilbert cubes in arithmetic sets*, Revista Matemática Iberoamericana **31** (2015), no. 4, 1477–1498.
- [12] A. Dujella and C. Elsholtz, *Sumsets being squares*, Acta Math. Hungar **141** (2013), no. 4, 353–357.
- [13] C. Elsholtz, *The inverse Goldbach problem*, Matematika **48** (2001), 151–158.
- [14] C. Elsholtz and A. Harper, *Additive decompositions of sets with restricted prime factors*, Transactions of the American Mathematical Society **367** (2015), no. 10, 7403–7427.
- [15] P. Erdős and A. Sárközy, *On divisibility properties of integers of the form  $a + a'$* , Acta Math. Hungar **50** (1987), 117–122.

- [16] P. Erdős and H. N. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. **7** (1957), 861–865.
- [17] K. Ford, *The distribution of integers with a divisor in a given interval*, Annals of mathematics (2008), 367–433.
- [18] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society, Providence, 2010.
- [19] P. X. Gallagher, *A larger sieve*, Acta Arithmetica **18** (1971), 77–81.
- [20] K. Gyarmati, *On a problem of diophantus*, Acta Arithmetica **97** (2001), 53–65.
- [21] K. Gyarmati, A. Sárközy, and C. Stewart, *On sums which are powers*, Acta Mathematica Hungarica **99** (2003), no. 1-2, 1–24.
- [22] B. Hanson and G. Petridis, *Refined estimates concerning sumsets contained in the roots of unity*, Proceedings of the London Mathematical Society **122** (2021), no. 3, 353–358.
- [23] G. H. Hardy, E. M. Wright, et al., *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.
- [24] H. Iwaniec and E. Kowalski, *Analytic number theory*, vol. 53, American Mathematical Soc., Providence, 2021.
- [25] G.J.O. Jameson, *Even and odd square-free numbers*, The Mathematical Gazette **94** (2010), no. 529, 123–127.
- [26] S. V. Konyagin, *Problems on the set of squarefree numbers*, Izvestiya: Mathematics **68** (2004), no. 3, 493–520.
- [27] P. Koosis, *Introduction to  $H_p$  spaces*, Cambridge University Press, Cambridge, 1998.
- [28] C. Moreno, *Algebraic curves over finite fields*, no. 97, Cambridge University Press, 1993.
- [29] H.-H. Ostmann, *Additive Zahlentheorie, 1. Teil: Allgemeine Untersuchungen*, Springer Verlag, Berlin-Heidelberg-New York, 1968.
- [30] C. Pomerance, A. Sárközy, and C. Stewart, *On divisors of sums of integers. iii*, Pacific Journal of Mathematics **133** (1988), 363–379.
- [31] K. Prachar, *Primzahlverteilung*, vol. 91, Springer Berlin, 1957.
- [32] J. Rivat, A. Sárközy, and C.L. Stewart, *Congruence properties of the  $\Omega$ -function on sumsets*, Illinois Journal of Mathematics **43** (1999), no. 1, 1–18.
- [33] M. Rosen, *Number theory in function fields*, vol. 210, Springer Science & Business Media, 2002.
- [34] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo  $p$* , Acta Arithmetica **155** (2012), 41–51.

- 
- [35] W. M. Schmidt, *Equations over finite fields: an elementary approach*, vol. 536, Springer, 2006.
  - [36] A. Selberg, *Collected papers, volume II*, Springer, Berlin-Heidelberg, 1991.
  - [37] I. Shkredov, *Sumsets in quadratic residues*, Acta Arithmetica **164** (2014), 221–243.
  - [38] R. C. Vaughan, *Some applications of Montgomery’s sieve*, Journal of Number Theory **5** (1973), 64–79.
  - [39] A. Weil, *On some exponential sums*, Proceedings of the National Academy of Sciences **34** (1948), no. 5, 204–207.

# Index of Notation

$(\mathcal{M}; \mathcal{P}', \Omega)$	a sifted set, page 3
$\gg$	relation between functions in terms of growth, page 4
$\ll$	relation between functions in terms of growth, page 4
$\mathbf{1}_A$	indicator function of the set $A$ , page 7
$\ \cdot\ _{\mathbb{R}/\mathbb{Z}}$	distance to the nearest integer, page 4
$\mathbb{N}$	the positive integers, page 3
$\omega(\cdot)$	number of distinct prime factors, page 67
$\mathcal{P}$	the prime numbers, page 3
$\pi(\cdot)$	number of primes in $[1, \cdot]$ , page 16
$\sim$	relation between functions in terms of growth, page 16
$\varphi$	Euler's totient function, page 16
$\mathbb{Z}$	the integers, page 4
$e(\cdot)$	$e(t) = \exp(2\pi it)$ , page 3
$H(a_0; a_1, \dots, a_d)$	$d$ -dimensional Hilbert cube, page 56
$O(\cdot)$	relation between functions in terms of growth, page 4
$X \triangle Y$	symmetric difference of the sets $X$ and $Y$ , page 15
$d(\cdot)$	divisor function, page 19