CHAPTER 1

PLÜNNECKE'S INEQUALITY

In this chapter we introduce the basic notation used throughout the course, and we establish some elementary, but important bounds. Do not be misled by the word 'elementary', as many of our arguments are elementary in the sense that they use only simple notions, but the arguments themselves can be very involved and long. However, in this first chapter we avoid the use of complicated reasoning.

Let Z be a commutative ring, and A and B are subsets of Z. Typically we work with the integers $\mathbb{Z}$, or the residue classes mod m, that is with $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, though sometimes with other rings and fields like $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{Z}^d$. In many cases we only need the additive group of the ring, or there is no ring at all, only a group written additively (the name 'additive combinatorics' comes from here). The *sumset* of A and B is defined by

$$A + B = \{x \in Z : \, x = a + b \text{ with some } a \in A,\, b \in B\}.$$

Typically we just write $A + B = \{a + b : \, a \in A,\, b \in B\}$ with the understanding that elements are not repeated in $A + B$. For $A + A$ we sometimes write $2A$. Similarly

$$\begin{gathered} kA = A + A + \cdots + A, \\ b + A = \{b\} + A = \{b + a : \, a \in A\}, \text{ a translate of } A, \\ A - B = \{a - b : \, a \in A,\, b \in B\}, \text{ the difference set }, \\ A \cdot B = \{ab : \, a \in A,\, b \in B\}, \text{ the product set }, \\ A/B = \{a/b : \, a \in A,\, b \in B\}, \text{ the quotient set }, \\ k \cdot A = \{k\} \cdot A = \{ka;\, a \in A\}, \text{ a dilate of } A. \end{gathered}$$

Note that with this convention $\mathbb{Z}/m\mathbb{Z}$ was an abuse of notation, from now on we use the short $\mathbb{Z}_m$ to denote the ring of residue classes mod m. Actually we do not plan to work in general groups or rings, always in one of the above list, but the reader is very welcome to double check the arguments if they can indeed be carried out in a more general context.

Theorem 1.1: Let A and B be two finite subsets of the real numbers $\mathbb{R}$. We have

$$|A| + |B| - 1 \le |A + B| \le |A||B|,$$

and equality can hold on both places. Moreover the lower bound is sharp (equality holds) iff (if and only if) A and B are arithmetic progressions of the same difference.

Proof: The upper bound is obvious and reflects the fact that as a worst case all sums in the form $a + b : \, a \in A,\, b \in B$ are different. This is indeed possible, for example, let

$$A = \{0, 1, \ldots, r - 1\}, \quad B = r \cdot \{0, 1, \ldots, s - 1\} = \{0, r, 2r, \ldots, (s - 1)r\},$$

and as is easily seen

$$A + B = \{0, 1, \ldots, rs - 1\}.$$

Let us concentrate on the lower bound. We can list the elements of the sets as

$$A = \{a_1 < a_2 < \cdots < a_r\}, \quad B = \{b_1 < b_2 < \cdots < b_s\}.$$

The next chain of inequalities contains well visibly $r + s - 1$ different elements of $A + B$.

$$a_1 + b_1 < a_1 + b_2 < a_1 + b_3 < \cdots < a_1 + b_s < a_2 + b_s < a_3 + b_s < \cdots < a_r + b_s\,.$$

This proves the lower bound and it is not hard to see that if $A = \{1, \ldots, r\}$ and $B = \{1, \ldots, s\}$ then $A + B = \{2, \ldots, r + s\}$. It is not hard to come up with several other chains of $r + s - 1$ different elements of $A + B$ in increasing order. For example,

$$a_1 + b_1 < a_2 + b_1 < a_2 + b_2 < a_2 + b_3 < \cdots < a_2 + b_s < a_3 + b_s < \cdots < a_r + b_s\,.$$

If $|A + B| = r + s - 1$ then the above two chains should be the same. The first terms of the chains, as well as the last $r - 1$ terms visibly agree, but the rest determines $s - 1$ equations, namely

$$\begin{aligned} a_1 + b_2 &= a_2 + b_1\,, \\ a_1 + b_3 &= a_2 + b_2\,, \\ &\vdots \\ a_1 + b_s &= a_2 + b_{s-1}\,. \end{aligned}$$

Rearranging these equations we arrive at

$$\begin{aligned} b_2 - b_1 &= a_2 - a_1\,, \\ b_3 - b_2 &= a_2 - a_1\,, \\ &\vdots \\ b_s - b_{s-1} &= a_2 - a_1\,. \end{aligned}$$

This means that the set B is indeed an arithmetic progression with difference $a_2 - a_1$. Either we can show a third chain of inequalities to cover the rest of the proof, but it is more elegant to argue that the roles of A and B are symmetric in the statement, we can interchange them to show that the set A is indeed an arithmetic progression with difference $b_2 - b_1$. This concludes the proof.

□

Theorem 1.2: Let $A_1, \ldots, A_k$, $k \geq 2$ be finite subsets of the real numbers $\mathbb{R}$. We have

$$|A_1| + \cdots + |A_k| - k + 1 \leq |A_1 + \cdots + A_k| \leq |A_1| \ldots |A_k|,$$

and equality can hold on both places. Moreover the lower bound is sharp iff $A_1, \dots, A_k$ are arithmetic progressions of the same difference.

Proof: This is a typical proof by induction. Note that the case $k = 2$ is precisely Theorem 1.1, and therefore this case is proved. We can suppose that $k > 2$, and that the statement is true for $k - 1$ and for 2. Let $A = A_1 + \cdots + A_{k-1}$ and $B = A_k$. First observe that $A + B = A_1 + \cdots + A_k$. Theorem 1.1 and the induction hypothesis say that

$$|A_1| + \cdots + |A_{k-1}| - k + 2 + |A_k| - 1 \leq |A| + |B| - 1 \leq |A + B| \leq |A||B| \leq |A_1| \dots |A_k|.$$

The two inequalities are therefore proved. Next observe that the only way to have equality in the lower bound is the following.

$$|A_1| + \cdots + |A_{k-1}| - k + 2 = |A_1 + \cdots + A_{k-1}| = |A|\,,$$
$$|A| + |B| - 1 = |A + B|\,.$$

By the induction hypothesis the first relation implies that $A_1, \dots, A_{k-1}$ are arithmetic progressions of the same difference, and therefore $A_1 + \cdots + A_{k-1} = A$ is also an arithmetic progression of the same difference, while the second relation implies that $B = A_k$ is also an arithmetic progression of the same difference.

□

Corollary 1.3: Let A be a finite subset of the real numbers $\mathbb{R}$, and $k \geq 2$ be an integer. We have

$$k|A| - k + 1 \leq |kA| \leq |A|^k,$$

moreover the lower bound is sharp iff A is an arithmetic progression.

□

The upper bound here is obviously not sharp unless $|A| = 1$, as $a_1 + a_2 = a_2 + a_1$, for example, and so not all sums can be different. We leave as an exercise to show that the sharp upper bound is $\binom{|A|+k-1}{k}$. It is a very interesting question to construct the largest set of integers $A \subset \{1, \dots, N\}$ such that $|A + A| = \binom{|A|+1}{2}$. Such an extremal set is called a 'Sidon set' and we plan to return to their study in Chapter 2.

Realize the main pattern of Corollary 1.3. It says if $A + A$ is smallest possible then A has a well defined structure, namely A should be an arithmetic progression. It was Gregori Freiman in the 1960's who recognized if $A + A$ is small, say $\leq C|A|$, then A still has a special structure, though not that strong as above. One of the main purpose of this course is to understand and to prove Freiman's structure theorem, but we do it only in Chapter 7. Right now we try to guess the result.

Our strategy is simply investigating examples. If A is a set of r members of an arithmetic progression of length $2r$, say, then $A + A$ is part of an arithmetic progression of length $4r - 1$, and thus $|A + A| \leq 4r - 1$. However, hoping that $|A + A| \leq C|A|$ implies that A is part of an arithmetic progression of length $C|A|/2$ is too optimistic.

Consider the following example. $A = \{0, 1, \dots, r - 2, N\}$ with $N > r - 2$ so $|A| = r$. One can easily see that $A + A = \{0, 1, \dots, 2r - 4\} \cup \{N, N + 1, \dots, N + r - 2\} \cup \{2N\}$. If $r - 2 < N \leq 2r - 4$ then $|A + A| = N + r \leq 3r - 4$, while if $N > 2r - 4$ then

$|A+A| = 3r-3$. In other words, we have found an example of a set A, which is r members of an $N+1\,(\leq 2r-3)$ elements arithmetic progression such that $|A+A| = N+r \leq 3r-4$, however we have also found an example of a set A such that $|A+A| = 3r-3$ but A can not be covered with any arithmetic progression of reasonable size. One can prove that the first part of this discovery is actually the extremal situation whenever $|A+A| \leq 3|A|-4$. For larger sumset, however, the arithmetic progression is no longer the underlining structure.

Next consider

$$Q = \{a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_d n_d : 0 \leq n_j < N_j \text{ for } j = 1, \ldots, d\},$$

where a_0, a_1, ... ,a_d are fixed real numbers (or integers, or ...) and N_1, N_2, ... ,N_d are integers ≥ 2. This is a *generalized arithmetic progression* of *dimension* $\dim(Q) = d$ and *volume* $\mathrm{vol}(Q) = N_1 \cdots N_d$. Obviously $|Q| \leq \mathrm{vol}(Q)$. Q is *proper* if all the above elements are different, in which case $|Q| = \mathrm{vol}(Q) = N_1 \cdots N_d$. Realize that $Q+Q$ is another generalized arithmetic progression, namely

$$Q+Q = \{2a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_d n_d : 0 \leq n_j < 2N_j - 1 \text{ for } j = 1, \ldots, d\}$$

(this is not necessary proper, even if Q was). Nevertheless $|Q+Q| \leq (2N_1-1)\cdots(2N_d-1)$ and if Q is proper then $|Q+Q| < 2^d|Q|$, so a proper generalized arithmetic progression is another example of small doubling. If $A \subset Q$, where Q is a generalized arithmetic progression and $\mathrm{vol}(Q) \leq C|A|$ with some constant $C \geq 1$ then since $A+A \subset Q+Q$, we have $|A+A| \leq |Q+Q| \leq 2^d \mathrm{vol}(Q) \leq C2^d|A|$. This is the ultimate example, as we will see in Chapter 7 that *if $A+A$ is 'small' then A is a 'large' subset of a generalized arithmetic progression of 'small' dimension and volume.*

Theorem 1.4: Let A, B and C be finite subsets of the real numbers. We have

$$|A-C||B| \leq |A-B||B-C|.$$

Proof: For all $d \in A-C$ we fix a representation $d = a_d - c_d$ where $a_d \in A$ and $c_d \in C$. We define a map between $(A-C)\times B$ and $(A-B)\times(B-C)$, namely a pair (d,b), where $d \in A-C$ and $b \in B$ is mapped to the pair $(a_d - b, b - c_d)$, where well visibly $a_d - b \in A-B$ and $b - c_d \in B-C$. We show that this map is injective, that is an image determines its unique inverse. Indeed, if (u,v) is an image under this map then $u+v$ should be d, and than a_d or c_d determine b by $b = a_d - u$ or $b = c_d + v$. Injectivity implies that the size of the image should be bigger than the size of the domain, which is precisely the stated inequality.

□

We want to stress (though this type of remarks are usually left to the reader) that Theorem 1.4 is valid in any group, we not even used commutativity in the proof. Actually, all statements from Corollary 1.5 to Theorem 1.11 below are valid for any commutative group with identical proof, and we will, indeed, use some of them in this more general setting. Another remark, one can recognize a kind of triangle inequality in this statement. Indeed, if we define

$$\Delta(A,B) = \log \frac{|A-B|}{\sqrt{|A||B|}}$$

then by Theorem 1.4 we have $\Delta(A,C) \le \Delta(A,B) + \Delta(B,C)$.

Finally putting $C = A$ and than $B = -A$ we get

Corollary 1.5:

$$|A - A| \le \frac{|A-B|^2}{|B|}, \text{ for all } B, \tag{1.1}$$

$$|A - A| \le \frac{|A+A|^2}{|A|}. \tag{1.2}$$

□

This last inequality (1.2) reads as if A has small doubling then $A - A$ is small as well. Similarly we can ask if $A - A$ is being small implies that $A + A$ is being small. This certainly follows if we can prove the *plus version* of Theorem 1.4. Note that there is a parity reason which blocks to get the plus version simply by changing the signs of some sets in Theorem 1.4. One can also ask if $A + B$ is being small implies that $A - B$ is being small. The answers for all these questions are affirmative, but we have to work a bit for it. We start with a lemma.

Lemma 1.6: Let A and B be finite subsets of the real numbers. If for a $c > 0$ we have

$$|A + B| = c|A|, \text{ while } |A' + B| \ge c|A'| \text{ for all } A' \subset A, \tag{1.3}$$

then for all finite subset C of the real numbers we have

$$|A + B + C| \le c|A + C|. \tag{1.4}$$

Proof: We use induction on the size of C. If $|C| = 1$, that is $C = \{x\}$ then

$$|A + B + x| = |A + B| = c|A| = c|A + x|,$$

thus the statement is obvious. Suppose now that the statement (1.4) is true for a non–empty set C, and let $x \notin C$ be an arbitrary real number, finally let $C' = C \cup \{x\}$. We prove the statement for C' as well. Study the right hand side of (1.4) first. We define

$$A' = \{a \in A : a + x \in A + C\} = A \cap (A + C - x) \subset A.$$

We have $A' + x = (A + x) \cap (A + C)$ and $A + C' = (A + C) \cup (A + x)$ and so

$$|A + C'| = |A + C| + |A + x| - |A' + x| = |A + C| + |A| - |A'|.$$

As $A' + x \subset A + C$ implies also $A' + B + x \subset A + B + C$ and so

$$A + B + C' = (A + B + C) \cup (A + B + x) = (A + B + C) \cup [(A + B + x) \setminus (A' + B + x)],$$

moreover

$$|A+B+C'| \le |A+B+C|+|A+B+x|-|A'+B+x| = |A+B+C|+|A+B|-|A'+B|.$$

We use the induction hypothesis (1,4) to estimate the first term on the right hand side, and the two conditions (1.3) to the other two terms, getting

$$|A+B+C'| \le c|A+C|+c|A|-c|A'| = c|A+C'|,$$

as is required to complete the induction.

□

There are two important consequences of this lemma. We can prove the sum version of the triangle inequality, Theorem 1.4, and we can prove Plünnecke's inequality.

Theorem 1.7: Let A, B and C be finite subsets of the real numbers. We have

$$|A+C||B| \le |A+B||B+C|.$$

Proof: Let $U \subset B$ a subset such that the ratio $|U+A|/|U| = c$ is minimal. We have for any $U' \subset U$ that $|U'+A|/|U'| \ge c$. The condition of Lemma 1.6 is satisfied for the choice

$$A \mapsto U, \quad B \mapsto A, \quad C \mapsto C,$$

getting

$$|U+A+C| \le c|U+C|.$$

Obviously we have $|A+C| \le |U+A+C|$, $|U+C| \le |B+C|$ and $c \le |A+B|/|B|$, as B itself is considered when the minimum is selected. The theorem follows from these last four inequalities.

□

Writing first $C = A$ and next $B = -A$ we get the companion of Corollary 1.5, namely we have

Corollary 1.8:

$$|A+A| \le \frac{|A+B|^2}{|B|}, \text{ for all } B, \tag{1.5}$$

$$|A+A| \le \frac{|A-A|^2}{|A|}. \tag{1.6}$$

□

Corollary 1.9:

$$|A-B| \le \frac{|A+B|^3}{|A||B|}, \tag{1.7}$$

$$|A+B| \le \frac{|A-B|^3}{|A||B|}. \tag{1.8}$$

Proof: Put B to C and $-A$ to B in Theorem 1.4 and use (1.6) of Corollary 1.8 to get

$$|A-B||A| \le |A+A||A+B| \le \frac{|A+B|^3}{|B|}.$$

The second inequality follows from this by putting $-B$ to B. □

Writing $C = (h-1)B$ to (1.4) we get $|A+hB| \le c|A+(h-1)B|$, and an induction gives the following result.

Corollary 1.10: Let A and B be finite subsets of the real numbers. If for a $c > 0$ we have

$$|A+B| = c|A|, \text{ while } |A'+B| \ge c|A'| \text{ for all } A' \subset A,$$

then for all positive integer h we have

$$|A+hB| \le c^h|A|.$$

□

Theorem 1.11: (Plünnecke) Let B be a finite subset of the real numbers, satisfying $|B+B| \le c|B|$ (or $|B-B| \le c|B|$). For all non–negative integers m and n we have

$$|mB-nB| \le c^{m+n}|B|.$$

Proof: Let $\emptyset \ne A \subset B$ (or $\emptyset \ne A \subset -B$) be one of the sets that minimizes the ratio $|A+B|/|A|$, and write $|A+B| = c'|A|$. Obviously $c' \le c$. By this definition $|A'+B| \ge c'|A'|$ for all $A' \subset A$, thus the conditions of Corollary 1.10 are satisfied. We have

$$|hB| \le |A+hB| \le (c')^h|A| \le c^h|B|,$$

proving the statement for the case of $m = 0$ or $n = 0$. For the general statement we appeal to Theorem 1.4. The roles are distributed as follows.

$$A \mapsto mB, \quad B \mapsto -A, \quad C \mapsto nB.$$

Theorem 1.4 and Corollary 1.10 imply that

$$|mB-nB||A| \le |A+mB||A+nB| \le (c')^m|A|(c')^n|A| \le c^{m+n}|B||A|,$$

and the theorem follows by simplifying with $|A|$.

□

If Q is a generalized arithmetic progression then any combination $mQ - nQ$ is small. Theorem 1.11 shows that if A has small doubling then the same is true for $mA - nA$. This is one indication to guess that small doubling implies some generalized arithmetic progression like behaviour.

We close this chapter with yet another argument. Not only this argument provides a different proof of Corollary 1.9, but it is interesting itself, and uses some important notions relevant in later chapters. First we introduce *representation functions*, whenever we speak about an operation with sets, like $A \pm B$, $A \cdot B$ or A/B, etc, we write

$$r_{A\pm B}(x) = \#\{(a,b) \in A \times B : \, x = a \pm b\},$$
$$r_{A\cdot B}(x) = \#\{(a,b) \in A \times B : \, x = ab\},$$
$$r_{A/B}(x) = \#\{(a,b) \in A \times B : \, x = a/b\}, \text{ etc.}$$

There are some fairly trivial observations about the first and second means of representation functions.

$$\sum_x r_{A+B}(x) = |A||B|,$$

and similarly with the other representation functions mentioned above.

$$\sum_x r_{A+B}(x)^2 = \#\{a_1 + b_1 = a_2 + b_2\} = \#\{a_1 - b_2 = a_2 - b_1\} =$$
$$= \#\{a_1 - a_2 = b_2 - b_1\} = \sum_x r_{A-B}(x)^2 = \sum_x r_{A-A}(x)\, r_{B-B}(x).$$

Theorem 1.12: Let A and B be finite subsets of the real numbers, and $x \in A + B$. We have

$$r_{A+B}(x) \le \frac{|A-B|^2}{|A+B|}.$$

Proof: It is very similar to the proof of Theorem 1.4. For any $s \in A + B$ we fix a representation $s = a_s + b_s$; $a_s \in A$, $b_s \in B$. We define an injective map from $R_x \times (A+B)$ to $(A - B) \times (A - B)$, where R_x denotes the set of representations of x as $x = a + b$: $a \in A$, $b \in B$, i.e. R_x is the set of such pairs (a, b). We map $((a, b), s) \in R_x \times (A + B)$ to $(a - b_s, a_s - b) \in (A - B) \times (A - B)$. This is indeed injective, if (u, v) is in the image then $s = x - u + v$ is determined, than a_s and b_s are determined, than $a = u + b_s$ and $b = a_s - v = x - a$ are determined. Any point in the image has a unique inverse, the statement of the theorem follows from comparing the size of the domain and the image. □

Lemma 1.13 (Cauchy–Schwarz inequality): For any finite sets of real numbers x_j, y_j we have

$$\Big(\sum x_j y_j\Big)^2 \le \sum x_j^2 \sum y_j^2.$$

Proof: We claimed and we prove the statement for finite sums, but it is actually true (with identical proof) for infinite sums or integrals as well, provided the appropriate convergence. Let us abbreviate $S = \sum x_j y_j / \sum y_j^2$, and consider the inequality

$$0 \le \sum (x_j - y_j S)^2 = \sum x_j^2 - 2S \sum x_j y_j + S^2 \sum y_j^2 = \sum x_j^2 - \frac{\left(\sum x_j y_j\right)^2}{\sum y_j^2},$$

and the lemma follows.

□

New proof of Corollary 1.9: After this preparation we can express the argument in a chain of equations and inequalities. We start with Lemma 1.13 and in due course we use Theorem 1.12 as well.

$$\begin{aligned}(|A||B|)^2 = \left(\sum_x r_{A-B}(x)\right)^2 \le |A-B| \sum_x r_{A-B}(x)^2 = \\ = |A-B| \sum_x r_{A+B}(x)^2 \le |A-B| \max_y r_{A+B}(y) \sum_x r_{A+B}(x) = \\ = |A||B||A-B| \max_y r_{A+B}(y) \le |A||B||A-B| \frac{|A-B|^2}{|A+B|},\end{aligned}$$

and the statement follows from a little rearrangement.

□

CHAPTER 2

SIDON SETS

Recall that in Chapter 1 we named a set A of integers a Sidon set if the sums $a_i + a_j$ were different for all $i \le j$. Finite Sidon sets are examples for a maximal $A + A$, however infinite Sidon sets are also interesting objects to study. The main problem here is to find *dense* Sidon sets, that is either for all integers $N \ge 1$ find the largest n such that there is a Sidon set $A \subset \{1, \dots, N\}$, $|A| = n$, this is the finite case, or to find an infinite Sidon set A of positive integers such that its counting function

$$A(x) = \sum_{\substack{a \le x \\ a \in A}} 1$$

is large in some sense. Obviously any subset of a Sidon set is a Sidon set again, especially any finite segment of an infinite Sidon set is a Sidon set, however, there are better finite constructions. It is possible to prove, that for all $\epsilon > 0$ and all (large) N there is a Sidon set $A \subset \{1, \dots, N\}$ with $|A| > (1 - \epsilon)\sqrt{N}$, while any infinite Sidon set A satisfies

$$\liminf_{x \to \infty} \frac{A(x)}{\sqrt{x}} = 0.$$

The first useful observation is that $a_i + a_j = a_k + a_\ell$ iff $a_j - a_k = a_\ell - a_i$, in other words all sums are different iff all differences (except 0) are different. If A is a Sidon set in $\{1, \dots, N\}$ then all nonzero differences are among $\{1, \dots, N-1\}$. So $|A| = n$ must satisfy

$$\binom{n}{2} \le N - 1, \quad n \le \sqrt{2N} + 1.$$

This is obviously an upper bound for any infinite Sidon set as well, $A(x) \le \sqrt{2x} + 1$. We will improve these bounds soon.

The next useful observation is that we can use the greedy algorithm to construct a Sidon set. We pick the elements of A one by one. Let $a_1 = 1$, $a_2 = 2$ and suppose we have already picked $a_1, \dots, a_n$, where $n \ge 2$. When choosing a_{n+1} we have to avoid some integers, namely $a_i + a_j - a_k$. (Some of these are not positive, and we avoid them automatically.) Nevertheless we have to avoid at most

$$\binom{n+1}{2} n < n^3$$

integers, so picking the smallest possible integer, it will satisfy $a_{n+1} \le n^3$. If $8 \le n^3 \le x < (n+1)^3$ then the first $n+1$ elements of this Sidon set is not bigger than x, that is $A(x) \ge n + 1 > x^{1/3}$. This naturally provides a Sidon set up to N with at least $N^{1/3}$

elements. It maybe surprising that improving the lower bound for the infinite case is very hard, but for the finite case it is not so.

Let p be an odd prime, and choose

$$a_k = 2pk + s_k, \text{ where } s_k \equiv k^2 \pmod{p},\ 1 \le s_k \le p-1,\ k = 1, \dots, p-1.$$

Clearly this is a set of $p-1$ integers below $2p^2$. We show that they form a Sidon set. Suppose that $a_i + a_j = a_k + a_\ell$, that is

$$2pi + s_i + 2pj + s_j = 2pk + s_k + 2p\ell + s_\ell,$$

or

$$2p(i + j - k - \ell) = s_k + s_\ell - s_i - s_j.$$

The right hand side is at most $2(p-1)$ in absolute value, while the left hand side is at least $2p$, unless it is zero. The above equation can only hold if both sides are zero, that is

$$i + j = k + \ell, \quad i^2 + j^2 \equiv k^2 + \ell^2 \pmod{p}.$$

This is the same as

$$j - k = \ell - i, \quad (j-k)(j+k) = j^2 - k^2 \equiv \ell^2 - i^2 = (\ell - i)(\ell + i) \pmod{p}.$$

We conclude that either $j - k = \ell - i = 0$ or $j + k \equiv \ell + i \pmod{p}$. In the first case $j = k$ and $i = \ell$, while the second case together with $j - k = \ell - i$ imply $j \equiv \ell \pmod{p}$ and $k \equiv i \pmod{p}$ and thus $j = \ell$ and $k = i$. In any case $a_i + a_j = a_k + a_\ell$ imply that the pairs $\{i, j\}$ and $\{k, \ell\}$ are the same. We have found a Sidon set of $p-1$ elements up to $2p^2$. The Prime Number Theorem claims that denoting the number of positive primes $p \le x$ by $\pi(x)$ we have

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1, \tag{2.1}$$

and it is an easy exercise to derive from here that for all $1 > \epsilon > 0$ and sufficiently large y there is a prime p satisfying $(1-\epsilon)y < p \le y$. With $y = \sqrt{N/2}$ the above construction provides a Sidon set of $(1-\epsilon)\sqrt{N/2}$ elements up to N.

Theorem 2.1: If $A \subset \{1, \dots, N\}$ is a Sidon set then

$$|A| \le N^{1/2} + N^{1/4} + 1.$$

Proof: Let us write $A = \{a_1 < a_2 < \cdots < a_n\}$. Remember that the differences $a_j - a_i$ are different for all $j > i$. Consider

$$S_1 =: \sum_{1 \le j \le n-1} (a_{j+1} - a_j) = a_n - a_1 \le N.$$

This sum is actually the sum of $n-1$ different integers, and as such, it is at least as big as the sum of the $n-1$ smallest positive integers. The upper bound coming from this argument does not go beyond our earlier knowledge. However, next we consider

$$S_2 =: \sum_{1\le j\le n-2} (a_{j+2}-a_j) = a_n + a_{n-1} - a_2 - a_1 \le 2N.$$

This sum is actually the sum of $n-2$ different integers, and they are also different from the previously considered $n-1$ differences. Since the sum of the two sets of differences are at least as big as the sum of the $2n-3$ smallest integers, we get

$$\frac{(2n-3)(2n-2)}{2} \le S_1 + S_2 \le 3N,$$

which leads to an improvement over the previous bound for n. Obviously we do not have to stop here. Consider

$$S_k =: \sum_{1\le j\le n-k} (a_{j+k}-a_j) = a_n + \cdots + a_{n-k+1} - a_k - \cdots - a_1 \le kN.$$

The number of differences in $S_1 + \cdots + S_k$ are exactly $(n-1) + \cdots + (n-k) = kn - k(k+1)/2 =: D$, and they are all different, their sum is at least as big as the sum of the D smallest integers. We have established the inequality

$$\frac{D(D+1)}{2} \le S_1 + \cdots + S_k \le (1 + \cdots + k)N,$$

and after further simplification

$$k(n - \frac{k+1}{2})^2 \le (k+1)N.$$

The optimal choice for k is given by the inequality

$$N^{1/4} \le k < N^{1/4} + 1,$$

and the last steps are

$$n \le \sqrt{(1+\frac{1}{k})N} + \frac{k+1}{2} \le \sqrt{N}(1+\frac{1}{2k}) + \frac{k+1}{2} \le N^{1/2} + N^{1/4} + 1.$$

□

This is obviously an upper bound for any finite segment of an infinite Sidon set,

Corollary 2.2: If A is an infinite Sidon set of positive integers, then

$$A(x) = \sum_{a\le x,\, a\in A} 1 \le x^{1/2} + x^{1/4} + 1.$$

□

Next we give a construction of a finite Sidon set of size near the upper bound in Theorem 2.1. There are several such constructions, they are all based on some properties of finite fields. We briefly summarize the necessary knowledge.
– For any prime power p^r there is a unique commutative field $\mathbb{F}_{p^r}$ of p^r elements.
– If $r|s$ then $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_{p^s}$.
– The multiplicative group of $\mathbb{F}_{p^r}$ is a cyclic group of order $p^r - 1$.

$\mathbb{F}_p$ is easy to understand, this is $\mathbb{Z}_p$, the ring of residue classes mod p, which is actually a field. From the Fermat–Euler theorem it is well know that $x^p = x$ for all elements of $\mathbb{Z}_p$. In general, $\mathbb{F}_{p^r}$ can be considered as the set of all solutions of the equation $x^{p^r} - x = 0$ (in an algebraic closure of $\mathbb{F}_p$).

Theorem 2.3: For every prime p there is a Sidon set $A \subset \{1, \dots, p^2 - 1\}$ with $|A| = p$.

Proof: Let $\theta \in \mathbb{F}_{p^2}$ be a generator of the multiplicative group of $\mathbb{F}_{p^2}$. This means

$$\mathbb{F}_{p^2} = \{0, \theta, \theta^2, \dots, \theta^{p^2-1} = 1\}.$$

Realize that we use $0, 1$ here as the zero and the unit elements of the finite field $\mathbb{F}_{p^2}$. The exponents are residue classes mod $p^2 - 1$, but we represent the classes with their least positive elements, and we select our set A from these exponents. $\mathbb{F}_p = \{c_1, \dots, c_p\}$ is a subfield of $\mathbb{F}_{p^2}$. Trivially θ is not an element of $\mathbb{F}_p$ as it is a generator of a bigger group, so $\theta + c_j \neq 0$. We are ready to define A, for every $j = 1, \dots, p$ there is an exponent a_j such that

$$\theta^{a_j} = \theta + c_j,$$

and let $A = \{a_1, \dots, a_p\}$ be the set of these exponents. This provides that A is indeed in the given range. Now suppose that $a_i + a_j = a_k + a_\ell$. We have

$$(\theta + c_i)(\theta + c_j) = \theta^{a_i}\theta^{a_j} = \theta^{a_i+a_j} = \theta^{a_k+a_\ell} = \theta^{a_k}\theta^{a_\ell} = (\theta + c_k)(\theta + c_\ell),$$

and after a little rearrangement we arrive at

$$\theta(c_i + c_j) + c_i c_j = \theta(c_k + c_\ell) + c_k c_\ell.$$

As θ is not in $\mathbb{F}_p$, it cannot be a solution of a linear equation with coefficients in $\mathbb{F}_p$, the only possibility is

$$c_i + c_j = c_k + c_\ell, \quad c_i c_j = c_k c_\ell. \tag{2,2}$$

Denoting the common value of the first equation with b and the common value of the second equation with d we can see that both sets $\{c_i, c_j\}$ and $\{c_k, c_\ell\}$ are the two solutions of the quadratic equation $X^2 - bX + d = 0$, the two sets must be the same. This implies that also $\{a_i, a_j\}$ must be the same as $\{a_k, a_\ell\}$. This concludes the proof.

□

For any (large) integer N we can find a prime p such that $(1 - \epsilon)\sqrt{N} < p \leq \sqrt{N}$ by (2.1).

Corollary 2.4: For any $1 > \epsilon > 0$ there is an N_0 such that for all $N \geq N_0$ there is a Sidon set $A \subset \{1, \dots, N\}$ with $|A| > (1 - \epsilon)\sqrt{N}$.

□

We close this chapter (and subject) with showing that finite segments of an infinite Sidon set must sometimes be much smaller than it is in Corollary 2.4.

Theorem 2.5: (Erdős) Let A be an infinite Sidon set of positive integers. We have

$$\liminf_{x\to\infty} \frac{A(x)}{\sqrt{\frac{40x}{\log x}}} \le 1.$$

Proof: We prove the theorem in the following equivalent form. For all integer $N \ge 2$ we have

$$\tau(N) =: \inf_{n\ge N} \frac{A(n)}{\sqrt{\frac{40n}{\log n}}} \le 1. \tag{2.3}$$

A simple consequence of the definition is that for all $n \ge N$

$$A(n) \ge \tau(N)\sqrt{\frac{40n}{\log n}}. \tag{2.4}$$

We fix an $N \ge 2$ and consider the elements $a \in A$ in the intervals $(k-1)N < a \le kN$ for all $k = 1, \dots, N$. The number of elements of A in this interval is $d(k) = A(kN) - A((k-1)N)$. The difference between two elements of the same interval is $< N$, and being a Sidon set, the differences of the different elements of A are all different. This implies

$$\sum_{\substack{k=1\\ d(k)>1}}^{N} \binom{d(k)}{2} < N,$$

and so we have

$$\sum_{k=1}^{N} d(k)^2 \le \sum_{\substack{k=1\\ d(k)\le 1}}^{N} 1 + 2\sum_{\substack{k=1\\ d(k)>1}}^{N} d(k)(d(k)-1) < 5N.$$

From the Cauchy–Schwarz inequality, Lemma 1.13, we conclude

$$\left(\sum_{k=1}^{N} \frac{d(k)}{\sqrt{k}}\right)^2 \le \sum_{k=1}^{N} d(k)^2 \sum_{k=1}^{N} \frac{1}{k} < 5N \sum_{k=1}^{N} \frac{1}{k}. \tag{2.5}$$

Recall Abel summation, which is a simple rearrangement of a finite sum. For arbitrary complex numbers $b_0, b_1, \dots, b_N$ and $c_1, \dots, c_{N+1}$ we have

$$\sum_{k=1}^{N} (b_k - b_{k-1})c_k = \sum_{k=1}^{N} b_k(c_k - c_{k+1}) + b_N c_{N+1} - b_0 c_1.$$

In the following long but straightforward computation we use this identity twice together with (2.4) and the estimate

$$\sqrt{k}-\sqrt{k-1}=\frac{1}{\sqrt{k}+\sqrt{k-1}}>\frac{1}{2\sqrt{k}}.$$

We have

$$\begin{aligned}\sum_{k=1}^{N}\frac{d(k)}{\sqrt{k}}=\sum_{k=1}^{N}\frac{A(kN)-A((k-1)N)}{\sqrt{k}}=\\ =\sum_{k=1}^{N}A(kN)\left(\frac{1}{\sqrt{k}}-\frac{1}{\sqrt{k+1}}\right)+\frac{A(N^2)}{\sqrt{N+1}}\geq\\ \geq\sum_{k=1}^{N}\tau(N)\sqrt{\frac{40kN}{\log kN}}\left(\frac{1}{\sqrt{k}}-\frac{1}{\sqrt{k+1}}\right)+\frac{\tau(N)\sqrt{\frac{40N^2}{\log N^2}}}{\sqrt{N+1}}\geq\\ \geq\tau(N)\sqrt{\frac{20N}{\log N}}\left(\sum_{k=1}^{N}\sqrt{k}(\frac{1}{\sqrt{k}}-\frac{1}{\sqrt{k+1}})+\frac{\sqrt{N}}{\sqrt{N+1}}\right)=\\ =\tau(N)\sqrt{\frac{20N}{\log N}}\sum_{k=1}^{N}\frac{\sqrt{k}-\sqrt{k-1}}{\sqrt{k}}\geq\tau(N)\sqrt{\frac{5N}{\log N}}\sum_{k=1}^{N}\frac{1}{k}.\end{aligned}$$

Finally writing this into (2.5) we establish

$$\tau(N)\leq\frac{\log N}{\sum_{k=1}^{N}\frac{1}{k}},$$

and (2.3), as well as the theorem follows from

$$\sum_{k\leq x}\frac{1}{k}>\int_1^x\frac{dt}{t}=\log x.$$

□

CHAPTER 3

SUMS OF RESIDUE CLASSES

Remember that the proof of Theorem 1.1 used the ordering of the real numbers. That proof certainly do not generalizes to finite groups, for example, to the group of residue classes. In this chapter we study this question, however, we only concentrate on getting a lower bound for the size of $A+B$ if A and B are subsets of the (additive) group of residue classes mod m. To describe all extremal cases is an open question in general, but is solved for $\mathbb{Z}_p$, the group of residue classes mod p, p being a prime (Vosper's Theorem). Although the proof is not particularly complicated, we do not spend time for working out the details.

Deriving the lower bound is especially simple when $|A|+|B|$ is large. Recall the general definition of representation functions, $r_{A+B}(z)$ denotes the number of pairs $(a,b) \in A \times B$ such that $z = a+b$.

Lemma 3.1: Let Z be a finite Abelian group, and let A and B be subsets of Z with $|A|+|B| \geq |Z|+t$. Then $r_{A+B}(z) \geq t$ for all $z \in Z$.

Proof: Consider the translates $z-B = \{z-b : b \in B\}$. Since

$$|Z| \geq |A \cup (z-B)| = |A| + |z-B| - |A \cap (z-B)| = |A| + |B| - |A \cap (z-B)|,$$

it follows that

$$|A \cap (z-B) \geq |A| + |B| - |Z| \geq t.$$

There exist (at least) t distinct elements $a \in A$ and t distinct elements $b \in B$ such that $a = z-b$, proving that $r_{A+B}(z) \geq t$. Since $z \in Z$ was arbitrary this concludes the lemma. □

The $t=1$ special case says that

Corollary 3.2: Let Z be a finite Abelian group, and let A and B be subsets of Z with $|A|+|B| > |Z|$. Then $A+B = Z$.

□

Next, following the footsteps of Freeman Dyson, the physicist, we introduce the *e–transform* of an ordered pair (A,B) of nonempty subsets of an Abelian group Z. Let $e \in Z$ be arbitrary, and define the e–transform of (A,B) as the pair $(A(e), B(e))$ of subsets of Z given by

$$A(e) = A \cup (B+e), \quad B(e) = B \cap (A-e).$$

We establish some simple properties of the e–transform.

Lemma 3.3: Let A and B be nonempty subsets of the (Abelian) group Z, and let e be any element of Z. We have

$$A(e) + B(e) \subset A + B, \tag{3.1}$$

$$A(e) \setminus A = e + (B \setminus B(e)), \tag{3.2}$$

$$|A(e)| + |B(e)| = |A| + |B|, \text{ if } A \text{ and } B \text{ are finite.} \tag{3.3}$$

Proof: To accept (3.1) realize that

$$A(e) + B(e) = (A + B(e)) \cup (B + e + B(e)) \subset (A + B) \cup (B + e + A - e) \subset A + B.$$

To prove (3.2) we observe that

$$A(e) \setminus A = (B + e) \setminus A = \{b + e : b \in B,\, b + e \notin A\} = \\ = e + \{b \in B : b \notin A - e\} = e + \{b \in B : b \notin B(e)\} = e + (B \setminus B(e)).$$

Finally for (3.3) note that clearly $A \subset A(e)$ and $B(e) \subset B$. For finite sets we have (using (3.2) in due course)

$$|A(e)| - |A| = |A(e) \setminus A| = |e + (B \setminus B(e))| = |B \setminus B(e)| = |B| - |B(e)|.$$

□

Theorem 3.4: Let $m > 1$ be fixed. If A and B are nonempty subsets of $\mathbb{Z}_m$ such that $0 \in B$, and $\gcd(b, m) = 1$ for all $b \in B \setminus \{0\}$, then

$$|A + B| \geq \min\{m,\, |A| + |B| - 1\}.$$

Proof: If $|A| + |B| - 1 \geq m$ then the statement follows from Corollary 3.2, we can suppose $|A| + |B| \leq m$. We prove by induction, if $|B| = 1$ then $|A + B| = |A| = |A| + |B| - 1$, the statement is true. Let $|B| \geq 2$ and we are going to prove the statement for B if it is true for any $B' \subset \mathbb{Z}_m$ with $|B'| < |B|$. We can select a $b \in B$, $b \neq 0$. Now $A + b \neq A$, otherwise starting from an arbitrary $a_0 \in A$ we find that $a_1 = a_0 + b \in A$, and $a_2 = a_1 + b = a_0 + 2b \in A$ and so on, all $a_0 + jb \in A$. Using that $\gcd(b, m) = 1$ we find $\mathbb{Z}_m \subset A$ which is not possible by $|A| + |B| \leq m$, $|B| \geq 2$. We can take an $e \in A$ such that $e + b \notin A$. We want to use the induction hypothesis for the pair $(A(e), B(e))$. As $A(e) \supset A$ and $0 \in B \cap (A - e)$ they are not empty, also $b \notin A - e$ so $B(e) \subsetneqq B$, we conclude using (3.3) and (3.1) that

$$|A| + |B| - 1 = |A(e)| + |B(e)| - 1 \leq |A(e) + B(e)| \leq |A + B|.$$

□

Theorem 3.5: (Cauchy–Davenport Theorem) Let p be a fixed prime . If A and B are nonempty subsets of $\mathbb{Z}_p$ then

$$|A + B| \geq \min\{p,\, |A| + |B| - 1\}.$$

Proof: Apply Theorem 3.4 with $B' = B - b$ for an arbitrary fixed element $b \in B$. The conditions are obviously satisfied.

□

Theorem 3.6: (Cauchy–Davenport Theorem) Let p be a fixed prime, and $h \geq 2$ be an integer. If $A_1, \ldots, A_h$ are nonempty subsets of $\mathbb{Z}_p$ then

$$|A_1 + \cdots + A_h| \geq \min\{p, |A_1| + \cdots + |A_h| - h + 1\}.$$

Proof: We prove by induction on h. The case $h = 2$ is precisely Theorem 3.5. Let $h \geq 3$, and suppose that the result is true for any $h-1$ subsets of $\mathbb{Z}_p$. Let $A_1 \ldots, A_h$ be nonempty subsets of $\mathbb{Z}_p$, and write $B = A_1 + \cdots + A_{h-1}$. By the induction hypothesis

$$|B| = |A_1 + \cdots + A_{h-1}| \geq \min\{p, |A_1| + \cdots + |A_{h-1}| - h + 2\},$$

and we have

$$\begin{aligned} |A_1 + \cdots + A_h| = |B + A_h| &\geq \min\{p, |B| + |A_h| - 1\} \geq \\ &\geq \min\{p, \min\{p, |A_1| + \cdots + |A_{h-1}| - h + 2\} + |A_h| - 1\} = \\ &= \min\{p, |A_1| + \cdots + |A_h| - h + 1\}. \end{aligned}$$

This completes the proof.

□

The Cauchy–Davenport theorem for $A = B$ claims that $|A + A| \geq \min\{p, 2|A| - 1\}$. It is a natural question to ask how this bound changes if we only add different elements of A. We (temporarily to the rest of this chapter) denote by $A \oplus A$ the set of sums $a + a'$ where $a, a' \in A$, $a \neq a'$. In case of Theorem 1.1, that is in the group of real numbers, one can quickly come up with the sharp lower bound $2|A| - 3$ by the very same method. It maybe surprising that the corresponding result for residue classes was conjectured by Erdős and Heilbronn in 1964 and was proved only 30 years later by Dias da Silva and Hamidoune, using rather complicated arguments. Here we include a different proof due to Alon, Nathanson and Ruzsa, we do it mainly to develop the polynomial method and to illustrate its use. The following lemma is the key step of the method. It is valid for polynomials over any field, but we claim and prove it only over the finite field of p elements, that is over the residue classes mod p.

Lemma 3.7: Let p be a prime, $h \geq 1$ be an integer, and $A_1, \ldots, A_h$ be nonempty subsets of $\mathbb{Z}_p$ with $|A_j| = k_j$. Let $f(x_1, \ldots, x_h)$ be a polynomial with coefficients in $\mathbb{Z}_p$ and of degree at most $k_j - 1$ in the variable x_j, for $j = 1, \ldots, h$. If $f(a_1, \ldots, a_h) = 0$ for all choices of $a_j \in A_j$, then $f(x_1, \ldots, x_h)$ is the zero polynomial.

Proof: We prove by induction on h. The case $h = 1$ is the *degree theorem*, that is a nonzero polynomial of degree n has at most n roots in a field. In the argument below $f = 0$ is understood in the given field, that is, it actually means $f \equiv 0 \pmod{p}$.

Let $h \geq 2$ and assume that the lemma is true for polynomials in less than h variables. We can write our polynomial according to the powers of x_h, that is

$$f(x_1, \ldots, x_h) = \sum_{j=0}^{k_h - 1} f_j(x_1, \ldots, x_{h-1}) x_h^j,$$

where for each $j = 0, \ldots, k_h - 1$ the polynomial $f_j(x_1, \ldots, x_{h-1})$ has degree at most $k_i - 1$ in the variable x_i. Fix an arbitrary

$$(a_1, \ldots, a_{h-1}) \in A_1 \times \cdots \times A_{h-1},$$

and write

$$g(x) = f(a_1, \ldots, a_{h-1}, x) = \sum_{j=0}^{k_h - 1} f_j(a_1, \ldots, a_{h-1}) x^j.$$

$g(x)$ is a polynomial of degree at most $k_h - 1$ such that $g(a_h) = 0$ for all $a_h \in A_h$. Since this counts k_h distinct roots, it follows that $g(x)$ is the zero polynomial, and so

$$f_j(a_1, \ldots, a_{h-1}) = 0$$

for all

$$(a_1, \ldots, a_{h-1}) \in A_1 \times \cdots \times A_{h-1}.$$

It follows from the induction hypothesis that $f_j(x_1, \ldots, x_{h-1})$ is the zero polynomial for all $j = 0, \ldots, k_h - 1$ and so $f(x_1, \ldots, x_h)$ is the zero polynomial as well.

□

Lemma 3.8: Let p be a prime and let A be a nonempty subset of $\mathbb{Z}_p$ with $|A| = k$. For every $m \geq 0$ there exist a polynomial $g_m(x)$ of degree at most $k - 1$ such that

$$g_m(a) = a^m, \text{ for all } a \in A.$$

Proof: This is a direct consequence of the usual Lagrange interpolation method. Another argument is the following. Consider the coefficients of $g_m(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1}$ as being variables. They must satisfy

$$\begin{aligned}
u_0 + u_1 a_1 + u_2 a_1^2 + \cdots + u_{k-1} a_1^{k-1} &= a_1^m, \\
u_0 + u_1 a_2 + u_2 a_2^2 + \cdots + u_{k-1} a_2^{k-1} &= a_2^m, \\
&\vdots \\
u_0 + u_1 a_k + u_2 a_k^2 + \cdots + u_{k-1} a_k^{k-1} &= a_k^m,
\end{aligned}$$

where $A = \{a_1, \ldots, a_k\}$. This is a system of k linear equations in the k unknowns $u_0, \ldots, u_{k-1}$, and it has a solution if the determinant of the coefficients is nonzero. The

lemma follows immediately from the observation that this determinant is a Vandermonde–determinant

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{k-1} \\ & & \vdots & & \\ 1 & a_k & a_k^2 & \dots & a_k^{k-1} \end{vmatrix} = \prod_{1 \le i < j \le k} (a_j - a_i) \neq 0.$$

□

Theorem 3.9: Let p be a prime number and let A and B be nonempty subsets of $\mathbb{Z}_p$ such that $|A| \neq |B|$. We have

$$|A \oplus B| \geq \min\{p,\, |A| + |B| - 2\}.$$

Proof: Let $|A| = k$ and $|B| = \ell$, and we can assume that $\ell < k \leq p$. We can also assume that $k + \ell - 2 \leq p$, because the case $k + \ell - 2 = p$ clearly implies the case $k + \ell - 2 > p$ by forgetting some elements of B, say. Writing $C = A \oplus B$, we have to prove $|C| \geq k + \ell - 2$. We prove by contradiction. Suppose $|C| \leq k + \ell - 3$, and let us choose $r \geq 0$ such that $r + |C| = k + \ell - 3$. We construct a polynomial in two variables, that is in $\mathbb{Z}_p[x, y]$, which vanishes on $A \times B$. We start by

$$f(x, y) = (x - y)(x + y)^r \prod_{c \in C} (x + y - c). \tag{3.5}$$

It has degree at most $1 + r + |C| = k + \ell - 2$ in both variables, as well as in total. That is, there exist coefficients $u_{m,n} \in \mathbb{Z}_p$ such that

$$f(x, y) = \sum_{m+n \leq k+\ell-2} u_{m,n} x^m y^n = (x - y)(x + y)^{k+\ell-3} + \text{ lower order terms.} \tag{3.6}$$

Using the binomial theorem we can read from here that the coefficient $u_{k-1,\ell-1}$ of the term $x^{k-1}y^{\ell-1}$ in $f(x, y)$ is actually

$$u_{k-1,\ell-1} = \binom{k + \ell - 3}{k - 2} - \binom{k + \ell - 3}{k - 1} = \frac{(k - \ell)(k + \ell - 3)!}{(k - 1)!(\ell - 1)!} \neq 0, \tag{3.7}$$

because $1 \leq \ell < k \leq p$ and $1 \leq k + \ell - 3 < p$. By Lemma 3.8, for every $m \geq k$ there is a polynomial $g_m(x)$ of degree at most $k - 1$ such that $g_m(a) = a^m$ for all $a \in A$, and similarly for every $n \geq \ell$ there is a polynomial $h_n(y)$ of degree at most $\ell - 1$ such that $h_n(b) = b^n$ for all $b \in B$. Writing these polynomials into (3.6) in place of x^m or y^n whenever $m \geq k$ or $n \geq \ell$ we arrive at a new polynomial $f^*(x, y)$ of degree at most $k - 1$ in x and at most $\ell - 1$ in y. If $(a, b) \in A \times B$ then by the construction and by (3.5) we have $f^*(a, b) = f(a, b) = 0$. Lemma 3.7 says that $f^*(x, y)$ must be the zero polynomial. On the other hand the highest degree term, $x^{k-1}y^{\ell-1}$ can only come from terms $u_{m,n}x^m y^n$ of (3.6), where $m \geq k - 1$ and $n \geq \ell - 1$. As $m + n \leq k + \ell - 2$ there is only one such term, namely $u_{k-1,\ell-1}x^{k-1}y^{\ell-1}$

itself, which is nonzero by (3.7), so $f^*(x, y)$ is not the zero polynomial. This contradiction proves the theorem.

□

Corollary 3.10: (The Erdős–Heilbronn conjecture) Let p be a prime and A be a nonempty subset of $\mathbb{Z}_p$. We have

$$|A \oplus A| \geq \min\{p, 2|A| - 3\}.$$

Proof: We can suppose that $|A| \geq 2$. Fix an arbitrary element of A, say a, and write $B = A \setminus \{a\}$. Obviously $A \oplus A = A \oplus B$ and Theorem 3.9 is applicable to the sets A, B, getting

$$|A \oplus A| = |A \oplus B| \geq \min\{p, |A| + |B| - 2\} = \min\{p, 2|A| - 3\}.$$

This completes the proof.

□

CHAPTER 4

ARITHMETIC PROGRESSIONS

Consider the following sets of integers.

$$X = \cup_{m=0}^{\infty}\{2^{2m} \leq n < 2^{2m+1}\},$$
$$Y = \cup_{m=1}^{\infty}\{2^{2m-1} \leq n < 2^{2m}\}.$$

Clearly $X \cup Y$ is a partition of the positive integers, that is, $X \cap Y = \emptyset$, $X \cup Y = \mathbb{N}$, where $\mathbb{N}$ denotes the set of positive integers. We can also think about a partition as a 2–coloring of $\mathbb{N}$, say X is the set of blue integers, Y is the set of red integers. Similarly partition into r disjoint sets is the same as r–coloring, the set of integers of the same color is a color class. As both X and Y contain arbitrarily long gaps, neither of them contains an infinite arithmetic progression. However, we have the following theorem.

Theorem 4.1: (van der Waerden, 1927) Let $k \geq 2$ and $r \geq 2$ be integers. For any r-coloring of the positive integers, at least one color class contains a k–term arithmetic progression.

We prove this theorem later in this chapter. Note that there are several other ways to state this theorem. For example, *let $r \geq 2$ be an integer. For any r–coloring of the positive integers, at least one color class contains arbitrarily long arithmetic progressions.* We can also finalize the statement. *Given integers $k \geq 2$ and $r \geq 2$, there exists a positive integer $N = N(k, r)$ such that for any r–coloring of the set $\{1, \ldots, N\}$, there is a monochromatic arithmetic progression of k–terms.* Here monochromatic means that all terms are in the same color class, they have the same color.

Edős and Turán conjectured that van der Waerden's theorem must be true for density reasons, that is any large subset of the integers should contain long arithmetic progressions. Their conjecture was proved by Szemerédi in 1975.

Theorem 4.2: (Szemerédi, 1975) Given an integer $k \geq 2$ and real number $1 > \delta > 0$, there is a positive integer $N(k, \delta)$ such that if $N \geq N(k, \delta)$ and $A \subset \{1, \ldots, N\}$, $|A| > \delta N$, then A contains a k–term arithmetic progression.

This is a deep theorem, one of the biggest achievement of mathematics. Although there are several different proofs by now, neither of them is suitable for this course. However, in Chapters 11 and 13 we prove the special cases $k = 3$ and $k = 4$. Theorem 4.2 is also one of the important ingredients in the following recent result of Green and Tao.

Theorem 4.3: For any $k \geq 2$, the set of positive primes contains a k–term arithmetic progression.

Needless to say, we do not prove this statement either. Not only the proof rests on Szemerédi's theorem, it also uses deep results from analytic number theory. As is well

known, the set of primes is not dense enough for a direct application of Theorem 4.2. There is another conjecture of Erdős, which (if true) implies Theorem 4.3.

Conjecture 4.4: If A is an infinite set of positive integers satisfying

$$\sum_{a\in A}\frac{1}{a}=\infty,$$

then A contains a k–term arithmetic progression for any $k\geq 2$.

At this point it is appropriate to discuss an early result, due to Schur. On one hand, Schur's theorem is interesting itself, it is not a consequence of van der Waerden's theorem, on the other hand, not only its proof is simple and elegant, but it gives some hint for the more complex argument coming after. Realize, that from density point of view the set of positive odd integers is a large set, it is half of the set of all integers. In spite of this, the equation $x+y=z$ cannot be solved in this large set. However, we have the following result.

Theorem 4.5: (Schur, 1916) Let $r\geq 1$ be an integer. For any r–coloring of $\mathbb{N}$ there is a monochromatic solution of $x+y=z$, that is a monochromatic triple $x,y,z\in\mathbb{N}$ such that $x+y=z$.

Proof: One can transform the problem to a somewhat more symmetric form by looking for a triple $a>b>c$ such that $x=a-b$, $y=b-c$, and $z=a-c$ are monochromatic. We prove the finalized version of this statement. *There is an $N(r)$ such that for all $N\geq N(r)$ and all r–coloring of the integers $\{1,\dots,N\}$, one can find integers $1\leq c<b<a\leq N$ such that $a-b$, $b-c$, and $a-c$ are monochromatic.*

Consider the complete graph on N vertices, and color the edge $\{a,b\}$ by the color of $|a-b|$. A monochromatic triangle $\{a,b,c\}$ is exactly what we want, if $a>b>c$ then $a-b$, $b-c$, and $a-c$ have the same color. The above statement than reads as follows. *There is an $N(r)$ such that for all $N\geq N(r)$ and all r–coloring of the complete graph on N vertices, one can find a monochromatic triangle.*

We prove by induction on r. The statement is trivial for $r=1$ with $N(1)=3$. Since the essential idea is already visible in the case of $r=2$, we work out that as well. Let $N\geq N(2)=2N(1)=6$. An arbitrary vertex a is the endpoint of $N-1\geq 5$ edges, they are 2–colored, so there are three edges of the same color, say red. Consider three vertices b,c,d attached to a with a red edge. If one of the edges $\{b,c\},\{c,d\},\{b,d\}$ is red, say $\{b,c\}$ is red, then $\{a,b,c\}$ is a red triangle, otherwise $\{b,c,d\}$ is a blue triangle.

Let $r\geq 2$ and suppose the statement is true for r with some $N(r)$. Let $N\geq N(r+1)=(r+1)(N(r)-1)+2$, and color the complete graph on N vertices by $r+1$ colors. An arbitrary vertex a is the endpoint of $N-1\geq(r+1)(N(r)-1)+1$ edges, there must be $N(r)$ of them in the same color, say red. Consider $N(r)$ vertices attached to a with a red edge. If there is a red edge between two of them, then a with that two vertices form a red triangle, otherwise the complete graph on that $N(r)$ vertices is colored with only r colors. By the induction hypothesis, it contains a monochromatic triangle. The proof is complete. It is recommended to compute $N(r)$ given by this proof, one gets a reasonable bound.

□

The arithmetic progression $\{a + jd : j = 0, \ldots, k-1\}$ is, in some sense, similar to an interval $\{1, \ldots, k\}$, indeed it is a dilate by d and translate by $a - d$. It is not hard to generalize van der Waerden's theorem into this direction. Theorem 4.1 follows from the theorem below by taking $S = \{1, \ldots, k\}$.

Theorem 4.6: (Grünwald) Let $r \geq 2$ be an integer and S be a finite nonempty set of positive integers. For any r–coloring of $\mathbb{N}$ there exist integers $a \geq 1$ and b such that $a \cdot S + b$ is monochromatic.

Proof: The proof is by induction on the size of S, but by no means can it be considered simple. For any finite set S of positive integers we state a claim, namely

A(S): for each $r \geq 2$ there is an $N(r)$ such that r–coloring of the integers, the set $\{1, \ldots, N\}$, $N \geq N(r)$ contains a monochromatic subset of the form $a \cdot S + b$ with some integers $a \geq 1$ and b.

The Theorem is proved if we prove A(S). We state another, rather different claim. For any finite set S of positive integers and an integer $n \geq 0$

B(S, n): for each $r \geq 2$ and $s \geq 1$ there is an $N(r, s)$ such that r–coloring of the integers, the set $\{1, \ldots, N\}$, $N \geq N(r, s)$ contains $n + 1$ monochromatic subsets, one for each $m = 0, \ldots, n$, of the form

$$T_m = \sum_{0 \leq j < m} a_j \cdot S + \left(\sum_{m \leq j \leq n} a_j \right) s + b,$$

with some integers $a_0 \geq 1, \ldots, a_n \geq 1$ and b.

Obviously, $N(r)$ in the statement A(S) depends on S as well, just like $N(r, s)$ in B(S, n) depends on S and n as well. The basic induction is that if we know A(S) then we want to know A($S \cup \{s\}$). The structure of the induction is as follows.
i. A(S) is trivially true for any one element set S, because any $a \cdot S + b$ is also one element, and thus monochromatic.
ii. We prove B(S, n) for every n by induction. The key step is that if we know A(S) and B(S, n) then we conclude B($S, n + 1$).
iii. B(S, n) for every n implies A($S \cup \{s\}$).

Next we work out ii. B($S, 0$) is trivial, we have to find a monochromatic $T_0 = a_0 s + b$ with some integers $a_0 \geq 1$ and b, but as T_0 is a single integer, it is always monochromatic. Although it is not necessary, let us check the claim B($S, 1$) as well. We have to find a monochromatic $T_0 = (a_0 + a_1)s + b$ and a monochromatic $T_1 = a_0 \cdot S + a_1 s + b$ simultaneously, with some integers $a_0, a_1 \geq 1$ and b. T_0 is still a single integer, and so monochromatic, we can concentrate on T_1. From A(S) we have a monochromatic $a' \cdot S + b'$, so we choose $a_0 = a'$, $a_1 = 1$ say, and $b = b' - s$. One can feel the difficulties, for $n = 2$ or more we have to point out the monochromatic property for three or more sets simultaneously, and only one of them is a singleton. This is the heart of the induction. Suppose that A(S) and B(S, n) are true and derive B($S, n + 1$). An S, s, and r–coloring of the integers are given. We refer to this coloring as the *original*. B(S, n) specifies an $N = N(r, s)$ such that

$\{1,\dots,N\}$ contains $n+1$ monochromatic subsets, one for each $m=0,\dots,n$, of the form

$$T_m=\sum_{0\le j<m} a_j\cdot S+\left(\sum_{m\le j\le n} a_j\right)s+b, \tag{2.1}$$

with some integers $a_0\ge 1,\dots,a_n\ge 1$ and b. We define an r'–coloring of the integers, namely the *new* color of u is the original color pattern of the interval $\{u+1,\dots,u+N\}$. Thus the number of new colors is $r'=r^N$, and u, v has the same new color if $u+j$, $v+j$ have the same original color for all $j=1,\dots,N$. Now $\mathrm{A}(S)$ specifies an $N'=N(r')$ such that $\{1,\dots,N'\}$ contains a (new) monochromatic $a'\cdot S+b'$ with some integers $a'\ge 1$ and b'. This means that for all $s'\in S$ the intervals $\{a's'+b'+1,\dots,a's'+b'+N\}$ have the same color pattern in the original r colors. For each $m=0,\dots,n$ that pattern has a monochromatic T_m described in (2.1), and thus it has the same color for all s', that is, we have a monochromatic $a'\cdot S+b'+T_m$ for all m. In more details, each line below is a monochromatic set, (but not all lines below have the same color).

$$\begin{gathered}
a'\cdot S+b'+(a_0+a_1+\dots+a_n)s+b,\\
a'\cdot S+b'+a_0\cdot S+(a_1+\dots+a_n)s+b,\\
a'\cdot S+b'+a_0\cdot S+a_1\cdot S+(a_2+\dots+a_n)s+b,\\
\vdots\\
a'\cdot S+b'+a_0\cdot S+a_1\cdot S+\dots+a_{n-1}\cdot S+a_ns+b.
\end{gathered}$$

Writing $a'_0=a'$, $a'_j=a_{j-1}$ for $j=1,\dots,n+1$, we got a monochromatic

$$T'_{m'}=\sum_{0\le j<m'} a'_j\cdot S+\left(\sum_{m'\le j\le n+1} a'_j\right)s+(b+b'),$$

for $m'=1,\dots,n+1$. Note that all these are subsets of $\{1,\dots,N'+N\}$. We have to add one more set for $m'=0$, which is the singleton

$$T'_0=\left(\sum_{0\le j\le n+1} a'_j\right)s+(b+b'),$$

and is trivially monochromatic, so $\mathrm{B}(S,n+1)$ follows. Note that this last subset is in $\{1,\dots,a's+b'+N\}$, and so $N(r,s)$ of $\mathrm{B}(S,n+1)$ satisfies $\le N+\max(N',a's+b')$, where $N=N(r,s)$ of $\mathrm{B}(S,n)$, $r'=r^N$, $N'=N(r')$ of $\mathrm{A}(S)$, and a',b' are the corresponding coefficients from $\mathrm{A}(S)$. This concludes ii.

Finally we work out iii. Suppose $\mathrm{B}(S,n)$ for all n. Especially for $n=r$ this says that there are $r+1$ monochromatic sets in the form of (2.1), and so there must be two of them

in the same color class, say $m = k, \ell$ with $k > \ell$. We can write the two sets as

$$T_\ell = \sum_{0 \le j < \ell} a_j \cdot S + \left(\sum_{\ell \le j < k} a_j \right) s + \left(\sum_{k \le j \le r} a_j \right) s + b,$$

$$T_k = \sum_{0 \le j < \ell} a_j \cdot S + \sum_{\ell \le j < k} a_j \cdot S + \left(\sum_{k \le j \le r} a_j \right) s + b.$$

That is $T_\ell \cup T_k$ is in one color class. Realize that this set is much bigger than what we actually need. Choosing an arbitrary $s_0 \in S$, one can easily see that

$$T_\ell \cup T_k \supset T = \left(\sum_{0 \le j < \ell} a_j \right) s_0 + \left(\sum_{\ell \le j < k} a_j \right) \cdot (S \cup \{s\}) + \left(\sum_{k \le j \le r} a_j \right) s + b$$

is monochromatic. Setting $a'' = a_\ell + \cdots + a_{k-1}$, and $b'' = (a_0 + \cdots + a_{\ell-1})s_0 + (a_k + \cdots + a_r)s + b$, we get that

$$T = a'' \cdot (S \cup \{s\}) + b''$$

is monochromatic, thus establishing $\mathrm{A}(S \cup \{s\})$. This completes the induction.

□

Theoretically it is possible to estimate $N(r)$ of $\mathrm{A}(S)$ from this proof, however it is not worth doing that, the result would be terribly weak. To get a reasonable bound for the finalized version of van der Waerden's theorem is a hard problem, and your best bet is the one, coming from the new quantitative version of Szemerédi's theorem due to Gowers. We discuss the main ingredients of Gowers' proof, and we details his method in the case of $k = 4$. The general case follows the same route but it is substantially more involved.

CHAPTER 5

SUM–PRODUCT ESTIMATES

In Chapters 1 and 3 we studied questions about the additive structure of integers, real numbers, or residue classes, actually we only used the additive groups of these rings or fields. Most of the results can be translated to the multiplicative structures as well, sometimes it is simply the application of the very same statement to the set $B = \{\log a : a \in A\}$. The reader is invited to check when this argument works.

In this chapter, however, we want to use both operations, and study the connection between them. If A is a finite set of positive real numbers, then $A + A$ is minimal for arithmetic progressions, Corollary 1.3. This translates as $A \cdot A$ is minimal for geometric progressions. Arithmetic progressions or geometric progressions are quite different from each other. This observation led Erdős and Szemerédi to conjecture that

Conjecture 5.1: (Erdős and Szemerédi) If A is a finite set of positive real numbers, $\epsilon > 0$ is a fixed real number, and $|A| = n > n_0(\epsilon)$, then

$$\max\{|A + A|, |A \cdot A|\} \geq n^{2-\epsilon}.$$

They themselves proved that a weaker lower bound is indeed true, namely there is a small real number $c > 0$ such that

$$\max\{|A + A|, |A \cdot A|\} \gg n^{1+c}.$$

Explicit values of c were computed by several mathematicians. Elekes made the first breakthrough when using incidence geometry he proved $c = 1/4$. Even simpler approach was discovered by Solymosi proving $c = 1/3$, the best result so far.

Theorem 5.2: (Solymosi) If A is a finite set of positive real numbers, and $|A| = n$, then

$$|A + A|^2 |A \cdot A| \geq \frac{4n^4}{5\lceil \log_2 n \rceil}.$$

Notice that in the case when $A + A$ is close to its minimum, say $|A + A| \leq n^{1+\epsilon}$ we get the conjectural lower bound for $|A \cdot A|$. In general, bounding the left hand side with $\max\{|A + A|, |A \cdot A|\}^3$ we immediately get (after numerical simplification)

Corollary 5.3: If A is a finite set of positive real numbers, and $|A| = n$, then

$$\max\{|A + A|, |A \cdot A|\} \gg \frac{n^{4/3}}{\log^{1/3} n}.$$

Proof of Theorem 5.2: Recall the notion and elementary properties of representation functions $r_{A \cdot A}$ and $r_{A/A}$ from the end of Chapter 1. We have

$$\sum_y r_{A \cdot A}(y) = n^2,$$

and the Cauchy–Schwarz inequality (Lemma 1.13) implies that

$$n^4 = \left(\sum_y r_{A\cdot A}(y)\right)^2 \le \left(\sum_y 1\right)\left(\sum_y r_{A\cdot A}(y)^2\right) = |A\cdot A|\sum_y r_{A\cdot A}(y)^2,$$

as only $y \in A\cdot A$ gives a non zero contribution to the sums. Remember also that

$$\sum_y r_{A\cdot A}(y)^2 = \sum_x r_{A/A}(x)^2,$$

because they compute the number of solutions of $ab = a'b'$ or $a/b' = a'/b$ in $a, b, a', b' \in A$, and the two equations are the same. We arrive at

$$n^4 \le |A\cdot A|\sum_x r_{A/A}(x)^2. \tag{5.1}$$

The second half of the proof is more tricky, and has geometric motivation. We will estimate the sum on the right hand side of (5.1) by means of $A + A$. The argument works only for approximately equal $r_{A/A}(x)$, therefore we start with splitting the sum accordingly. Let K be defined by

$$2^{K-1} \le n < 2^K. \tag{5.2}$$

Since $r_{A/A}(x) \le n$, we have

$$\sum_x r_{A/A}(x)^2 = \sum_{k=1}^{K} \sum_{2^{k-1}\le r_{A/A}(x)<2^k} r_{A/A}(x)^2. \tag{5.3}$$

Let us fix a $1 \le k \le K$ for which the inner sum is non empty. We arrange the quotients x counted in the k-th sum by increasing order, that is $\{x \in A/A : 2^{k-1} \le r_{A/A}(x) < 2^k\} = \{x_1 < x_2 < \cdots < x_m\}$. Consider $A \times A$ on the plane, the integer vectors (a, b) with coordinates from A. They are inside the first quadrant. The line $b = x_j a$ covers exactly $r_{A/A}(x_j)$ of them. With a little abuse of notation we refer to this line, more precisely to the half line in the first quadrant, simply as the *ray* x_j. Pick a vector (a, b) on the ray x_j and another vector (a', b') on the next ray x_{j+1}. Realize that their sum $(a + a', b + b')$ is in the sector defined by the two rays, indeed one can quickly check that

$$x_j = \frac{b}{a} < \frac{b+b'}{a+a'} < \frac{b'}{a'} = x_{j+1}.$$

Not only the vector $(u, v) = (a + a', b + b')$ is an element of $(A + A) \times (A + A)$, but (u, v) determines the two initial vectors, as is clear from the parallelogram rule of adding vectors. This provides the next inequality.

$$r_{A/A}(x_j)\, r_{A/A}(x_{j+1}) \le \#\{(u, v) \in (A + A) \times (A + A) : x_j < \frac{v}{u} < x_{j+1}\}.$$

As for different j–s these sectors are disjoint, we also have

$$\sum_{j=1}^{m-1} r_{A/A}(x_j)\, r_{A/A}(x_{j+1}) \le \#\{(u,v) \in (A+A)\times(A+A) :\ x_1 < \frac{v}{u} < x_m\}. \tag{5.4}$$

(5.4) and (5.3) are enough to prove the Theorem with a weaker constant, so the rest of the proof is only cosmetics. It is recommended to make the shortcut from here.

We define two more half lines x_0 and x_∞ (roughly corresponds to 0 and ∞) to include more vectors, and to handle the $m = 1$ case. Let a_0 be the least element of A. The ray x_0 covers the vectors (a, a_0), where a runs over all the first coordinates of the vectors on the ray x_1. In other words, it is the vertical projection of the ray x_1 to the horizontal line $b = a_0$. Similarly the ray x_∞ is the horizontal projection of the ray x_m to the vertical line $a = a_0$. Obviously these rays contain $r_{A/A}(x_1)$ or $r_{A/A}(x_m)$ vectors from $A \times A$. Adding the vectors of the ray x_0 to the vectors of the ray x_1 will result vectors (u, v) of $(A+A)\times(A+A)$ with $v/u < x_1$. Similarly adding the vectors of the ray x_m to the vectors of the ray x_∞ will result vectors (u, v) of $(A + A) \times (A + A)$ with $v/u > x_m$. Just like beforehand the vector (u, v) determines its origins. Thus we can complete (5.4) to

$$r_{A/A}(x_1)^2 + \sum_{j=1}^{m-1} r_{A/A}(x_j)\, r_{A/A}(x_{j+1}) + r_{A/A}(x_m)^2 \le |A + A|^2. \tag{5.5}$$

We finish with a little elementary calculus. One can check that for $1/2 < z < 2$ we have $z + 1/z < 5/2$, that is with $z = r/s$ we have $r^2 + s^2 < 5/2 \cdot rs$. Therefore by (5.5)

$$\sum_{j=1}^{m} r_{A/A}(x_j)^2 = \frac{1}{2}\, r_{A/A}(x_1)^2 + \sum_{j=1}^{m-1} \frac{r_{A/A}(x_j)^2 + r_{A/A}(x_{j+1})^2}{2} + \frac{1}{2}\, r_{A/A}(x_m)^2 \le$$

$$\le \frac{1}{2}\, r_{A/A}(x_1)^2 + \frac{5}{4} \sum_{j=1}^{m-1} r_{A/A}(x_j)\, r_{A/A}(x_{j+1}) + \frac{1}{2}\, r_{A/A}(x_m)^2 \le \frac{5}{4}\, |A + A|^2.$$

Writing to (5.3) and (5.1) we arrive at

$$n^4 \le \frac{5}{4}\, K |A \cdot A||A + A|^2.$$

Finally the theorem follows from $K < \lceil \log_2 n \rceil$.

□

Next we turn to the similar problem in the finite field $\mathbb{Z}_p$, that is in the field of residue classes mod p, a prime number. As in Chapter 3, we sometimes write $=$ rather than $\equiv$ mod p. We start with a couple of useful lemmas. We will use the exponential notation

$$e(x) = e^{2\pi i x} = \cos(2\pi x) + i \sin(2\pi x),$$

where $i = \sqrt{-1}$ is the imaginary unit, hence $e(x)$ is the complex number with absolute value of 1 and argument (angle) of $2\pi x$. We actually use discrete Fourier analysis, but for our purposes it is simplified to the relation

$$\frac{1}{p}\sum_{x\in\mathbb{Z}_p} e(\frac{nx}{p}) = \begin{cases} 1, \text{ if } n = 0, \\ 0, \text{ if } 0 \neq n \in \mathbb{Z}_p. \end{cases} \tag{5.6}$$

Indeed, the first statement is trivial and for $0 \neq n \in \mathbb{Z}_p$, nx runs over $\mathbb{Z}_p$ when x does the same. In this case the sum is the sum of p-th roots of unity, and it is zero. (One can also argue as this is a geometric sequence, and we know the sum formula.) We have Parseval identity, its proof is simply squaring out and applying (5.6).

Lemma 5.4: (Parseval identity) For any (complex) coefficients u_n we have

$$\frac{1}{p}\sum_{x\in\mathbb{Z}_p}\left|\sum_{n\in\mathbb{Z}_p} u_n e(\frac{nx}{p})\right|^2 = \sum_{n\in\mathbb{Z}_p}|u_n|^2.$$

□

Lemma 5.5: For any(complex) coefficients u_m and v_n, and for any $0 \neq x \in \mathbb{Z}_p$ we have the bound

$$\left|\sum_{m\in\mathbb{Z}_p}\sum_{n\in\mathbb{Z}_p} u_m v_n e(\frac{mnx}{p})\right| \leq \left(p\sum_{m\in\mathbb{Z}_p}|u_m|^2\sum_{n\in\mathbb{Z}_p}|v_n|^2\right)^{1/2}.$$

Especially for any subsets A and B of $\mathbb{Z}_p$ we have

$$\left|\sum_{a\in A}\sum_{b\in B} e(\frac{abx}{p})\right| \leq \sqrt{p\,|A||B|}.$$

Proof: This follows from the Cauchy–Schwarz inequality (Lemma 1.13), and from Parseval identity (Lemma 5.4). Indeed

$$\left|\sum_{m\in\mathbb{Z}_p}\sum_{n\in\mathbb{Z}_p} u_m v_n e(\frac{mnx}{p})\right|^2 \leq \left(\sum_{m\in\mathbb{Z}_p}|u_m|\left|\sum_{n\in\mathbb{Z}_p} v_n e(\frac{mnx}{p})\right|\right)^2 \leq$$

$$\leq \sum_{m\in\mathbb{Z}_p}|u_m|^2\sum_{m\in\mathbb{Z}_p}\left|\sum_{n\in\mathbb{Z}_p} v_n e(\frac{mnx}{p})\right|^2 = p\sum_{m\in\mathbb{Z}_p}|u_m|^2\sum_{n\in\mathbb{Z}_p}|v_n|^2.$$

□

Theorem 5.6: (Garaev) For any non empty subset $0 \notin A$ of $\mathbb{Z}_p$ we have

$$|A+A||A\cdot A| \geq \min\{\frac{p}{2}|A|,\ \frac{1}{4p}|A|^4\}.$$

Corollary 5.7: For any non empty subset $0 \notin A$ of $\mathbb{Z}_p$ we have

$$\max\{|A+A|, |A\cdot A|\} \gg \min\{\sqrt{p|A|},\ \frac{|A|^2}{\sqrt{p}}\}.$$

Note that these results are non trivial only when $|A|$ is substantially larger than $\sqrt{p}$. To derive a result in the form $\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+c}$ for smaller A is very deep already for a small $c>0$, beyond the level of this exposition.

Proof of Theorem 5.6: Let B be the set of the multiplicative inverses of A, that is $B = \{b = 1/a :\ a \in A\}$, or in another language, $B = \{b \in \mathbb{Z}_p :\ ba \equiv 1 \pmod p \text{ for some } a \in A\}$. Obviously $|B| = |A|$. (The condition $0 \notin A$ is required here.) We consider the number of solutions to

$$qb + a = s, \quad q \in A\cdot A,\ b \in B,\ a \in A,\ s \in A+A. \tag{5.7}$$

For any triple (a_1, a_2, a_3), $a_j \in A$ there is a solution to (5.7), namely $q = a_1a_2$, $b = 1/a_1$, $a = a_3$, and $s = a_2 + a_3$. These are all different solutions to (5.7) as a given solution (q, b, a, s) determines (a_1, a_2, a_3) by $a_1 = 1/b$, $a_2 = s - a$, and $a_3 = a$. This means that

$$|A|^3 \le \#\text{ solutions to (5.7)}. \tag{5.8}$$

Note that we do not have equality here, because there are solutions of different type as well. The theorem will follow from estimating the number of solutions to (5.7). By (5.6) we have

$$\frac{1}{p}\sum_{x\in\mathbb{Z}_p}\left(\sum_{q\in A\cdot A}\sum_{b\in B} e(\frac{qbx}{p})\right)\left(\sum_{a\in A} e(\frac{ax}{p})\right)\left(\sum_{s\in A+A} e(-\frac{sx}{p})\right) =$$

$$= \sum_{q\in A\cdot A}\sum_{b\in B}\sum_{a\in A}\sum_{s\in A+A}\frac{1}{p}\sum_{x\in\mathbb{Z}_p} e(\frac{(qb+a-s)x}{p}) = \#\text{ solutions to (5.7)}.$$

The most significant contribution comes from the 'major arc', the point $x = 0$, because for all other x the first function is small by Lemma 5.5. To estimate the rest of the sum over x, the 'minor arc' contribution, we use the Cauchy–Schwarz inequality and the Parseval identity.

$$\#\text{ of solutions to (5.7)} = \tag{5.9}$$

$$= \frac{|A||B||A+A||A\cdot A|}{p} + \frac{1}{p}\sum_{\substack{x\in\mathbb{Z}_p\\ x\neq 0}}\left(\sum_{q\in A\cdot A}\sum_{b\in B} e(\frac{qbx}{p})\right)\left(\sum_{a\in A} e(\frac{ax}{p})\right)\left(\sum_{s\in A+A} e(-\frac{sx}{p})\right) \le$$

$$\le \frac{|A||B||A+A||A\cdot A|}{p} + \frac{1}{p}\sum_{\substack{x\in\mathbb{Z}_p\\ x\neq 0}}\left|\sum_{q\in A\cdot A}\sum_{b\in B} e(\frac{qbx}{p})\right|\left|\sum_{a\in A} e(\frac{ax}{p})\right|\left|\sum_{s\in A+A} e(\frac{sx}{p})\right| \le$$

$$\le \frac{|A||B||A+A||A\cdot A|}{p} + \frac{1}{p}\sqrt{p|A\cdot A||B|}\,\sqrt{p|A|}\,\sqrt{p|A+A|},$$

because in the last step after using Lemma 5.5 for the first factor we can extend the sum over x to the whole $\mathbb{Z}_p$ and use the Cauchy–Schwarz inequality as follows.

$$\left(\sum_{x\in\mathbb{Z}_p}\left|\sum_{a\in A}e(\frac{ax}{p})\right|\left|\sum_{s\in A+A}e(\frac{sx}{p})\right|\right)^2 \le \sum_{x\in\mathbb{Z}_p}\left|\sum_{a\in A}e(\frac{ax}{p})\right|^2\sum_{x\in\mathbb{Z}_p}\left|\sum_{s\in A+A}e(\frac{sx}{p})\right|^2.$$

Recall that $|B|=|A|$, combining (5.8) and (5.9) we arrive at

$$|A|^2 \le \frac{1}{p}\,|A||A+A||A\cdot A| + \sqrt{p|A+A||A\cdot A|}.$$

Since at least one of the two terms on the right hand side must exceed half of the left hand side this concludes the proof of our theorem.

□

In the last part of this chapter we study the problem of representing $\mathbb{Z}_p$ as a sum like $B+\dots+B$ with a small number of terms. Without any special structure of the subset B one can not say too much. For example, if $B=\{1,2,\dots,n\}$ then we need more than p/n terms. However, if B has some multiplicative structure, then the situation improves a lot. We consider the case of $B=A\cdot A$. We will use Theorem 5.6 to show the following

Theorem 5.8: Let $0\notin A$ be a subset of $\mathbb{Z}_p$ with $|A|>\sqrt{2}\,p^{5/8}$. We have

$$(A+A)\cdot(A+A)+A\cdot A+A\cdot A=\mathbb{Z}_p.$$

Especially we have

$$A\cdot A+A\cdot A+A\cdot A+A\cdot A+A\cdot A+A\cdot A=6(A\cdot A)=\mathbb{Z}_p.$$

Proof: We want to show, that for all $r\in\mathbb{Z}_p$ the equation

$$r=s_1s_2+q_1+q_2,\quad s_i\in A+A,\ q_j\in A\cdot A, \tag{5.10}$$

can be solved. We use Fourier analysis again to express the number of solutions to (5.10). Indeed

$$\#\text{ of solutions to (5.10)} \;=\frac{1}{p}\sum_{x\in\mathbb{Z}_p}\left(\sum_{s_1\in A+A}\sum_{s_2\in A+A}e(\frac{s_1s_2x}{p})\right)\left(\sum_{q\in A\cdot A}e(\frac{qx}{p})\right)^2 e(-\frac{rx}{p}).$$

$x=0$ is the major arc, and contributes

$$\frac{|A+A|^2|A\cdot A|^2}{p}.$$

The rest of x is the minor arc. We estimate the first factor, the sum over s_1 and s_2, by Lemma 5.5, after that we extend the sum over x to the whole $\mathbb{Z}_p$ and apply the Parseval identity, Lemma 5.4. The contribution of the minor arcs is than bounded by

$$\le \max_{y\neq 0}\left|\sum_{s_1\in A+A}\sum_{s_2\in A+A} e(\frac{s_1s_2y}{p})\right| \frac{1}{p}\sum_{x\in\mathbb{Z}_p}\left|\sum_{q\in A\cdot A} e(\frac{qx}{p})\right|^2 \le \sqrt{p}\,|A+A|\,|A\cdot A|.$$

Therefore we have

$$\#\text{ of solutions to (5.10) } \ge \frac{|A+A|^2|A\cdot A|^2}{p} - \sqrt{p}\,|A+A|\,|A\cdot A| > 0,$$

whenever

$$|A+A|\,|A\cdot A| > p^{3/2}.$$

By Theorem 5.6 it is enough to provide that

$$\min\{\frac{p}{2}\,|A|,\ \frac{1}{4p}|A|^4\} > p^{3/2},$$

what follows from $|A| > \sqrt{2}\,p^{5/8}$.

□

There are several similar results, they vary according to the number of terms, the number of factors in one term, and the condition on $|A|$. The reader is invited to mimic the above proof to show that $4\,(A\cdot A) = \mathbb{Z}_p$ whenever $|A| > (2p)^{2/3}$. The starting equation to represent any $r\in\mathbb{Z}_p$ in the required form should be $r = sa + q_1 + q_2$, where $s\in A+A$, $a\in A$, and $q_j\in A\cdot A$. A deep result of Bourgain implies that for all $\delta > 0$ there are (large) integers n and N such that $NA^n = \mathbb{Z}_p$, whenever $|A| > p^\delta$. The dependence of n and N on δ is in the center of investigation in additive combinatorics.

CHAPTER 6

TECHNICAL PREPARATION: LATTICES

Minkowski's lattice geometry is a wonderful tool in different problems in number theory, including additive representations, Diophantine approximation, theory of quadratic forms, and many more. However, we restrict ourselves to develop just enough for our application to the proof of Freiman's theorem in Chapter 10. The interested reader is encouraged to study this beautiful subject from other sources, for example, J.W.S.Cassels, An Introduction to the Geometry of Numbers, Springer–Verlag, Berlin, 1959.

Our presentation depends on a lot of linear algebra, therefore a certain level of knowledge is expected. We review many statements without proofs, in the same time we detail the less well known theorems, like Mikowski's convex body theorems.

We work in the d–dimensional real Euclidean space $\mathbb{R}^d$. Let $\mathbf{a}_1, \dots, \mathbf{a}_d$ be a basis, that is, be linearly independent. The abelian group Λ generated by these vectors is the set of vectors of the form

$$u_1\mathbf{a}_1 + \cdots + u_d\mathbf{a}_d, \quad u_1, \dots, u_d \in \mathbb{Z}.$$

This is a *lattice*, and the set of linearly independent vectors $\mathbf{a}_1, \dots, \mathbf{a}_d$ is a basis of the lattice. A lattice is a *discrete* subgroup of $\mathbb{R}^d$, and any discrete subgroup of $\mathbb{R}^d$, if it contains d linearly independent vectors, is a lattice.

For example, the standard basis of $\mathbb{R}^d$ is the set of vectors $\mathbf{e}_1, \dots, \mathbf{e}_d$, where

$$\begin{aligned} \mathbf{e}_1 &= (1, 0, 0, \dots, 0) \\ \mathbf{e}_2 &= (0, 1, 0, \dots, 0) \\ &\vdots \\ \mathbf{e}_d &= (0, 0, 0, \dots, 1) \end{aligned}$$

The integer lattice $\mathbb{Z}^d$ is the lattice with basis $\mathbf{e}_1, \dots, \mathbf{e}_d$. If $\mathbf{b}_1, \dots, \mathbf{b}_d$ are d linearly independent vectors in a lattice Λ, then there exists a basis $\mathbf{a}_1, \dots, \mathbf{a}_d$ for Λ such that each of the vectors $\mathbf{b}_j$ is of the form

$$\mathbf{b}_j = \sum_{i=1}^{j} v_{ij}\mathbf{a}_i, \quad v_{ij} \in \mathbb{Z}. \tag{6.1}$$

Notice that in this representation $\mathbf{b}_j$ is expressed from $\mathbf{a}_1, \dots, \mathbf{a}_j$ only.

The basis of a lattice is not uniquely determined by the lattice. For example, not only $(1, 0)$ and $(0, 1)$ generates $\mathbb{Z}^2$ but also $(7, 5)$ and $(4, 3)$, as one can easily check. The vectors $\mathbf{a}_1, \dots, \mathbf{a}_d$ and $\mathbf{b}_1, \dots, \mathbf{b}_d$ generate the same lattice iff there is a $d \times d$ unimodular matrix

$U = (u_{ij})$ (a matrix with integer entries and determinant $\det(U) = \pm 1$, the inverse of an unimodular matrix is also unimodular) such that

$$\mathbf{b}_j = \sum_{i=1}^{d} u_{ij}\mathbf{a}_i.$$

Let $\mathbf{a}_1, \ldots, \mathbf{a}_d$ be vectors of $\mathbb{R}^d$, and let

$$\mathbf{a}_j = \sum_{i=1}^{d} a_{ij}\mathbf{e}_i$$

for $j = 1, \ldots, d$, where $a_{ij} \in \mathbb{R}$ are the coordinates of $\mathbf{a}_j$ with respect to the standard basis of $\mathbb{R}^d$. The $d \times d$ matrix $A = (a_{ij})$ is the *matrix of the vectors* $\mathbf{a}_1, \ldots, \mathbf{a}_d$. They are linearly independent iff $\det(A) \neq 0$.

The *determinant of the lattice* Λ is defined by

$$\det(\Lambda) = |\det(A)|,$$

where A is the matrix of a basis of Λ. This is independent of the choice of the basis as the matrices of any two bases are connected by an unimodular matrix, and we refer to the product rule of determinants.

The next important notion is the *fundamental parallelopiped* of the lattice Λ with respect to the basis $\mathbf{a}_1, \ldots, \mathbf{a}_d$, it is defined by

$$F(\Lambda) = F(\Lambda; \mathbf{a}_1, \ldots, \mathbf{a}_d) =: \left\{ \sum_{i=1}^{d} x_i\mathbf{a}_i : 0 \leq x_i < 1,\ i = 1, \ldots, d \right\} \subset \mathbb{R}^d.$$

The volume of a fundamental parallelopiped is

$$\mathrm{vol}(F(\Lambda)) = \det(\Lambda),$$

and such, it is independent of the choice of the basis (but not the fundamental parallelopiped itself). Every vector in $\mathbb{R}^d$ has a unique representation as the sum of a lattice vector and an element in the fundamental parallelopiped, $\mathbb{R}^d = \Lambda + F(\Lambda)$. A fundamental parallelopiped contains only one lattice point, the origin in one of the corners.

A set K in $\mathbb{R}^d$ is convex if, for every pairs of vectors $\mathbf{a}, \mathbf{b} \in K$, the line segment $(1-t)\mathbf{a} + t\mathbf{b}$, $0 \leq t \leq 1$ also belongs to K. A body in $\mathbb{R}^d$ is a bounded open set. We shall consider only nonempty convex bodies K with positive volume $\mathrm{vol}(K)$. For a real number $\lambda \geq 0$ we define (actually we have defined)

$$\lambda \cdot K = \{\lambda\,\mathbf{a} : \mathbf{a} \in K\}.$$

Notice that $\mathrm{vol}(\lambda \cdot K) = \lambda^d \mathrm{vol}(K)$. The set K is *symmetric* if $\mathbf{a} \in K$ implies that $-\mathbf{a} \in K$. A symmetric convex body contains the origin.

Lemma 6.1: (Blichfeldt) Let Λ be a lattice in $\mathbb{R}^d$ and K be a body in $\mathbb{R}^d$ with volume $\mathrm{vol}(K) > \det(\Lambda)$. Then there exist vectors $\mathbf{a} \neq \mathbf{b}$ in K such that $\mathbf{a} - \mathbf{b} \in \Lambda$.

Proof: We fix a fundamental parallelopiped F of the lattice Λ. We have $\mathrm{vol}(F) = \det(\Lambda) < \mathrm{vol}(K)$. Since K is bounded and Λ is discrete, there exist only finitely many lattice points $\mathbf{u} \in \Lambda$ with $K \cap (\mathbf{u} + F) \neq \emptyset$. Since $\mathbb{R}^d = \cup_{\mathbf{u}\in\Lambda}(\mathbf{u} + F)$, it follows that $K = \cup_{\mathbf{u}\in\Lambda}(K \cap (\mathbf{u} + F))$, and we have

$$\mathrm{vol}(F) < \mathrm{vol}(K) = \sum_{\mathbf{u}\in\Lambda} \mathrm{vol}(K \cap (\mathbf{u} + F)) = \sum_{\mathbf{u}\in\Lambda} \mathrm{vol}((K - \mathbf{u}) \cap F).$$

Since obviously $(K - \mathbf{u}) \cap F \subset F$, it follows that the sets $(K - \mathbf{u}) \cap F$ cannot be pairwise disjoint, and so there exist distinct lattice points $\mathbf{u}_1 \neq \mathbf{u}_2$ such that $(K-\mathbf{u}_1)\cap(K-\mathbf{u}_2) \neq \emptyset$ That means there exist distinct vectors $\mathbf{a} \neq \mathbf{b}$ in K such that $\mathbf{a} - \mathbf{u}_1 = \mathbf{b} - \mathbf{u}_2$, and this conclude the proof as $\mathbf{a} - \mathbf{b} = \mathbf{u}_1 - \mathbf{u}_2 \in \Lambda$.

□

Theorem 6.2: (Minkowski) Let Λ be a lattice in $\mathbb{R}^d$, and let K be a symmetric convex body in $\mathbb{R}^d$ with volume $\mathrm{vol}(K) > 2^d \det(\Lambda)$. Then K contains a lattice point different from the origin.

Proof: Let $K' = (1/2) \cdot K$ be the shrunk to half of K. Then K' is a symmetric convex body with

$$\mathrm{vol}(K') = \frac{\mathrm{vol}(K)}{2^d} > \det(\Lambda).$$

It follows from Lemma 6.1 that there exist vectors $\mathbf{a}' \neq \mathbf{b}'$ in K' such that $\mathbf{a}' - \mathbf{b}' \in \Lambda$. Obviously $\mathbf{a} = 2\mathbf{a}'$ and $\mathbf{b} = 2\mathbf{b}'$ are in K, moreover $-\mathbf{b}$ is in K and

$$\frac{1}{2}\,\mathbf{a} + \frac{1}{2}\,(-\mathbf{b}) = \mathbf{a}' - \mathbf{b}' \in K \cap \Lambda$$

since K is symmetric and convex.

□

The *successive minima* of the convex body $\mathbf{0} \in K$ with respect to the lattice $\Lambda \subset \mathbb{R}^d$ are a sequence of real numbers $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d$, and defined by

$$\lambda_k = \inf\{\lambda > 0 :\ \lambda \cdot K \text{ contains } k \text{ linearly independent vectors of } \Lambda\}.$$

Because K is an open set, it follows that $\lambda_k \cdot K$ contains at most $k-1$ linearly independent vectors of Λ, while $\lambda_k \cdot \overline{K}$ contains at least k linearly independent vectors of Λ. Not exactly $k-1$ and k because the boundary of $\lambda_k \cdot K$ can contain several linearly independent lattice vectors. (Here $\overline{K}$ is the closure of K.)

Theorem 6.2 can be reformulated as: *Let Λ be a lattice in $\mathbb{R}^d$, and let K be a symmetric convex body in $\mathbb{R}^d$ with volume* $\mathrm{vol}(K) \geq 2^d \det(\Lambda)$. *Then $\overline{K}$ contains a lattice point different from the origin.*

Theorem 6.3: (Minkowski's second theorem) Let K be a symmetric convex body in $\mathbb{R}^d$, and let Λ be a lattice in $\mathbb{R}^d$. Let $\lambda_1, \ldots, \lambda_d$ be the successive minima of K with respect to the lattice Λ. We have

$$\lambda_1 \cdots \lambda_d \operatorname{vol}(K) \leq 2^d \det(\Lambda).$$

Proof: A rigorous proof is somewhat complex and lengthy, and therefore we omit. Here we present a short, heuristic argument, why the theorem holds. (%) will indicate that a claim needs more explanation, or even some more precision. Some of those claims are studied in the homework problems in more details.

An alternative, maybe more practical way of seeing the successive minima, which also identify a natural basis of $\mathbb{R}^d$, is the following. For a sufficiently small λ, $\lambda \cdot \overline{K}$ contains only one lattice vector, the origin, because Λ is a discrete group. By increasing λ we magnify $\overline{K}$ until it hits another lattice vector. This defines λ_1 and we choose one such vector as $\mathbf{b}_1$. We magnify $\overline{K}$ further, until it hits a lattice vector, linearly independent from $\mathbf{b}_1$. This defines λ_2 and we choose one such vector as $\mathbf{b}_2$. We keep doing this, λ_d is the minimal factor of magnification to hit a lattice vector, linearly independent of $\mathbf{b}_1, \ldots, \mathbf{b}_{d-1}$ and we choose one such vector as $\mathbf{b}_d$. Note that magnifying further sometimes means no more magnification, in one step we can hit several linearly independent lattice vectors. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_d$ is a basis of $\mathbb{R}^d$ as being d linearly independent vectors, but not necessary a basis of Λ, they may span a *sublattice* of Λ (%).

Now magnify K by a factor λ_j in the direction of $\mathbf{b}_j$ for all $j = 1, \ldots, d$. In other words we define

$$K^* = \{\sum_{j=1}^{d} \lambda_j x_j \mathbf{b}_j : \sum_{j=1}^{d} x_j \mathbf{b}_j \in K\}.$$

K^* is a symmetric convex body (%) with volume $\operatorname{vol}(K^*) = \lambda_1 \cdots \lambda_d \operatorname{vol}(K)$ (%). Moreover K^* contains no lattice point other than the origin (but there are d linearly independent lattice points, and some other lattice points as well, on the boundary of K^*) (%). Theorem 6.2 implies that $\operatorname{vol}(K^*) \leq 2^d \operatorname{vol}(\Lambda)$, thus proving the theorem.

□

Remark: Theorem 6.3 implies Theorem 6.2. Indeed, we have $\lambda_1^d \operatorname{vol}(K) \leq \lambda_1 \ldots \lambda_d \operatorname{vol}(K)$ $\leq 2^d \operatorname{vol}(\Lambda)$ by Theorem 6.3. Together with $\operatorname{vol}(K) > 2^d \operatorname{vol}(\Lambda)$ this implies $\lambda_1 < 1$, which is equivalent to the fact that there is already a lattice vector, other than the origin, in K.

As a typical application of Minkowski's theorems we give a proof of Dirichlet's approximation theorem. The reader is invited to recover the original proof of Dirichlet which is based on the box principle. $\|y\|$ denotes the distance of y to the nearest integer.

Lemma 6.4: Let $k \geq 1$ be an integer and $\alpha_1, \ldots, \alpha_k$ be real numbers. For any integer $Q \geq 1$ there is an integer $1 \leq q \leq Q^k$ such that

$$\|q\alpha_j\| \leq \frac{1}{Q}, \text{ for all } j = 1, \ldots, k.$$

Proof: We define a lattice $\Lambda \subset \mathbb{R}^{k+1}$ by the following matrix.

$$\Lambda = \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_k \\ & 1 & & \\ & & \vdots & \\ & & & 1 \end{pmatrix} \mathbb{Z}^{k+1} = \begin{pmatrix} \mathbf{u}_0 \\ \mathbf{u}_1 \\ \vdots \\ \mathbf{u}_k \end{pmatrix} \mathbb{Z}^{k+1},$$

and we define a symmetric convex body K, actually K is a rectangle, by

$$K = \{(x_0, \dots x_k) : |x_0| < Q^k + 1, \, |x_j| < \frac{1}{Q}, \, j = 1, \dots, k\}.$$

Obviously $\mathrm{vol}(\Lambda) = 1$ and $\mathrm{vol}(K) = 2^{k+1}(Q^k + 1)/Q^k > 2^{k+1}\mathrm{vol}(\Lambda)$, and according to Theorem 6.2, K contains a non–trivial lattice point, say it belongs to the integer vector $(q, -a_1, \dots, -a_k)$, that is $q\mathbf{u}_0 - a_1\mathbf{u}_1 - \cdots - a_k\mathbf{u}_k \in K$. Being in K determines an inequality for each coordinates, namely $|q| < Q^k + 1$ and $|q\alpha_j - a_j| < 1/Q$ for all $j = 1, \dots, k$. Note that $q = 0$ is impossible, and without loss of generality we can suppose $1 \le q \le Q^k$, this proves the statement.

□

CHAPTER 7

FREIMAN'S THEOREM

In this chapter we prove Freiman's theorem. In the 1960's he recognized, if $A+A$ is small, then A has a special structure, it is a subset of a not much bigger generalized arithmetic progression of small dimension. The original proof was long and complicated, but in the 1990's Ruzsa and Bilu independently found more accessible proofs. Our presentation is based on Ruzsa's work.

Remember the definition of a generalized arithmetic progression, given in Chapter 1.

$$Q = \{a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_d n_d : 0 \le n_j < N_j \text{ for } j = 1, \dots, d\}, \tag{7.1}$$

where a_0, a_1, ... ,a_d are fixed real numbers (or integers, or residue classes, or vectors, or ...) and N_1, N_2, ... ,N_d are integers ≥ 1. This is a *generalized arithmetic progression* of *dimension* $\dim Q = d$ and *volume* $\mathrm{vol}(Q) = N_1 \cdots N_d$. Obviously $|Q| \le \mathrm{vol}(Q)$. Q is *proper* if all the above elements are different, in which case $|Q| = \mathrm{vol}(Q) = N_1 \cdots N_d$. Realize that $Q+Q$ is another generalized arithmetic progression, namely

$$Q+Q = \{2a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_d n_d : 0 \le n_j < 2N_j - 1 \text{ for } j = 1, \dots, d\}$$

(which is not necessary proper, even if Q is proper). Nevertheless $|Q+Q| \le (2N_1 - 1) \cdots (2N_d - 1) \le 2^d \mathrm{vol}(Q)$ and if Q is proper then $|Q+Q| < 2^d |Q|$. Simply speaking, a generalized arithmetic progression has small doubling, and so has any large subset of it. This result is ready to reverse.

Theorem 7.1: (Freiman, Ruzsa) Let A be a finite subset of the integers, and $C \ge 2$. If $|A+A| \le C|A|$ then there is a generalized arithmetic progression Q such that

$$A \subset Q, \quad \mathrm{vol}(Q) \le F(C)|A|, \quad \dim Q \le d(C), \tag{7.2}$$

with explicitly calculable functions $F(C)$ and $d(C)$.

Remark 7.2: Following closely our proof one can derive explicit bounds, namely $d(C) \le e^{O(C^{48})}$ and $F(C) \le e^{e^{O(C^{48})}}$. These are worse with one exponential compared to recent results, for example $d(C) \le C$ and $F(C) \le e^{O(C^2 \log C)}$ are proved.

We return later to the proof of Theorem 7.1 as it is split into smaller steps, first we prove these steps one by one. All the steps, as well as the completion of the proof require much ingenuity, our main ingredients are, among others, Fourier analysis (as is used in Chapter 5), geometry of numbers (Chapter 6), and Plünnecke's inequality, Theorem 1.11.

Theorem 7.3: (Bogolyubov, Ruzsa) Let N be a (large) prime, $0 < \alpha < 1$ be a real number, and $A \subset \mathbb{Z}_N$, $|A| = \alpha N$. Then $2A - 2A$ contains a proper generalized arithmetic progression of $\dim \le \alpha^{-2}$ and $\mathrm{vol} \ge (\alpha^2/4)^{\alpha^{-2}} N$.

Proof: Let us define (the Fourier coefficients)

$$\hat{A}(r) = \sum_{a\in A} e\big(\frac{ar}{N}\big),$$

and let $\mathcal{R}$ be the set where $\hat{A}(r)$ is big.

$$\mathcal{R} =: \{r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \alpha^{3/2}N\}.$$

Parseval identity (Lemma 5.4) gives the opportunity to estimate the size of $\mathcal{R}$, indeed we have

$$\alpha N^2 = N|A| = \sum_{r\in\mathbb{Z}_N} |\hat{A}(r)|^2 \geq \sum_{r\in\mathcal{R}} |\hat{A}(r)|^2 \geq |\mathcal{R}|\alpha^3 N^2,$$

and so

$$|\mathcal{R}| \leq \frac{1}{\alpha^2}. \tag{7.3}$$

We are going to study the representation function $r_{2A-2A}(x)$ and we will see that there is a generalized arithmetic progression (with parameters described above) on which $r_{2A-2A}(x) > 0$. The number of solutions of an additive equation can be expressed by means of the Fourier coefficients (actually by (5.6)), thus we have

$$r_{2A-2A}(x) = \frac{1}{N}\sum_{r\in\mathbb{Z}_N} |\hat{A}(r)|^4 e\big(\frac{rx}{N}\big) = \frac{1}{N}\sum_{r\in\mathbb{Z}_N} |\hat{A}(r)|^4 \cos\big(2\pi\frac{rx}{N}\big), \tag{7.4}$$

where we took the real part, as the left hand side is obviously real. We restrict ourselves to special residue classes x, namely those with

$$\Big\|\frac{rx}{N}\Big\| \leq \frac{1}{4}, \tag{7.5}$$

for all $r \in \mathcal{R}$. (Recall that $\|y\|$ denotes the distance of y to the nearest integer.) As $\cos(2\pi\frac{rx}{N}) \geq 0$ for all such x and all $r \in \mathcal{R}$, we have

$$r_{2A-2A}(x) \geq \frac{1}{N}|\hat{A}(0)|^4 - \frac{1}{N}\sum_{r\notin\mathcal{R}} |\hat{A}(r)|^4 >$$
$$> \frac{1}{N}|\hat{A}(0)|^4 - \frac{1}{N}\big(\alpha^{3/2}N\big)^2 \sum_{r\in\mathbb{Z}_N} |\hat{A}(r)|^2 = \alpha^4 N^3 - \alpha^3 N\alpha N^2 = 0.$$

In other words, $2A - 2A$ contains all $x \in \mathbb{Z}_N$ for which (7.5) holds with every $r \in \mathcal{R}$. Such a set is called a *Bohr neighborhood*, and are extensively studied. We are going to show that a Bohr neighborhood contains a generalized arithmetic progression. (Note that Lemma 6.4 provide a true arithmetic progression of length $N^{1/|\mathcal{R}|} \geq N^{\alpha^2}$ in this set of x.)

This is the place where the geometry of numbers enters the picture. Let $d = |\mathcal{R}|$ and let $r_1, \dots, r_d$ be a fixed set of representatives of the residue classes $\mathcal{R}$. Let $\mathbf{r} = (r_1, \dots, r_d)$ be the integer vector composed from the elements of $\mathcal{R}$. Coordinates here and below are understood in the standard orthogonal basis of $\mathbb{R}^d$. Finally let

$$\Lambda = N \cdot \mathbb{Z}^d + \mathbf{r} \cdot \mathbb{Z} = \{(a_1 N + b r_1, \dots, a_d N + b r_d) : \, a_j, b \in \mathbb{Z}\} \subset \mathbb{Z}^d \subset \mathbb{R}^d.$$

Λ is a lattice, and $\det(\Lambda) = N^{d-1}$. To see this, note that Λ is a subgroup, and that $N \cdot \mathbb{Z}^d$ is a subgroup of Λ. Obviously $\det(N \cdot \mathbb{Z}^d) = N^d$, and a fundamental parallelopiped of $N \cdot \mathbb{Z}^d$ is the cube with side N. It contains exactly N points of Λ, namely $0 \cdot \mathbf{r}, 1 \cdot \mathbf{r}, \dots, (N-1) \cdot \mathbf{r}$ after each coordinates are reduced to the least nonnegative residue mod N. Thus N translates of a fundamental parallelopiped of Λ fill the N sided cube completely (mod N, that is you may have to cut and paste pieces).

Next let $K = \{(u_1, \dots, u_d) : \, |u_j| < 1\}$ be a symmetric, convex body with $\mathrm{vol}(K) = 2^d$. Let $0 < \lambda_1 \le \lambda_2 \le \cdots \le \lambda_d$ be the sequence of successive minima of K with respect to Λ. As in the sketch of the proof of Theorem 6.3 (Minkowski's second theorem), there are linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_d$ of Λ such that $\mathbf{b}_j$ is on the boundary of $\lambda_j \cdot K$, that is all coordinates of $\mathbf{b}_j$ is bounded in absolute value by λ_j. But $\mathbf{b}_j \in \Lambda$ as well, so $\mathbf{b}_j = s_j \cdot \mathbf{r} + \mathbf{v}_j$ where $0 \le s_j < N$ is an integer, while $\mathbf{v}_j \in N \cdot \mathbb{Z}^d$ is an integer vector, all its coordinates are multiples of N. Moreover

$$\left\| \frac{s_j \mathbf{r}}{N} \right\| = \left\| \frac{\mathbf{b}_j}{N} \right\| \le \frac{\lambda_j}{N}, \tag{7.6}$$

where the above relations are understood coordinatewise.

We are in the position to define our generalized arithmetic progression P.

$$P = \{a_1 s_1 + \cdots + a_d s_d : \, |a_j| \le \frac{N}{4d\lambda_j}\}.$$

If $x \in P$ then $x = a_1 s_1 + \cdots + a_d s_d$ and

$$\left\| \frac{x\mathbf{r}}{N} \right\| \le \sum_{j=1}^{d} |a_j| \left\| \frac{s_j \mathbf{r}}{N} \right\| \le \sum_{j=1}^{d} \frac{N}{4d\lambda_j} \, \frac{\lambda_j}{N} = \frac{1}{4},$$

and so $x \in 2A - 2A$, indeed $P \subset 2A - 2A$. We show that P is proper. Suppose that $x = x'$ where $x = a_1 s_1 + \cdots + a_d s_d \in P$ and $x' = a'_1 s_1 + \cdots + a'_d s_d \in P$, that is $0 = (a_1 - a'_1) s_1 + \cdots + (a_d - a'_d) s_d$. Thus (relations are understood coordinatewise) we have

$$\mathbf{0} = (\sum (a_j - a'_j) s_j) \cdot \mathbf{r} = \sum (a_j - a'_j)(\mathbf{b}_j - \mathbf{v}_j) \equiv \sum (a_j - a'_j) \mathbf{b}_j \pmod{N}.$$

Since all coordinates of $\mathbf{b}_j$ is bounded by λ_j, and $|a_j - a'_j| \le N/(2d\lambda_j)$ we have that all coordinates of $\sum (a_j - a'_j) \mathbf{b}_j$ is bounded by $N/2$, and as all coordinates are divisible by N,

they are equal to 0. That is $\sum(a_j - a'_j)\mathbf{b}_j = \mathbf{0}$, and from the linear independence of the vectors $\mathbf{b}_j$ we conclude $a_j - a'_j = 0$ for all j.

Finally we estimate the volume of P. Since Theorem 6.3 implies $\lambda_1 \dots \lambda_d \operatorname{vol}(K) \leq 2^d \det(\Lambda)$, and since any interval of the form $(-y, y)$ contains at least y integers, we have that

$$\operatorname{vol}(P) \geq \prod_{j=1}^{d} \frac{N}{4d\lambda_j} \geq \left(\frac{N}{4d}\right)^d \frac{\operatorname{vol}(K)}{2^d \det(\Lambda)} = \left(\frac{1}{4d}\right)^d N.$$

With (7.3) this concludes the proof.

□

We want to establish connection between $\mathbb{Z}$ and $\mathbb{Z}_N$. To this end we introduce the notion of a k–isomorphism (also called Freiman isomorphism).

Definition 7.4: Let $k \geq 2$ be an integer, and $A \subset Z_1$ and $B \subset Z_2$, where Z_1 and Z_2 are two (additive) abelian groups. A bijection $\phi : A \to B$ is a k–isomorphism if

$$a_1 + \dots + a_k = a'_1 + \dots + a'_k \text{ iff } \phi(a_1) + \dots + \phi(a_k) = \phi(a'_1) + \dots + \phi(a'_k).$$

Note that ϕ is not necessarily defined on the whole group Z_1, not alone on $a_1 + \dots + a_k$, when it is not in A. A k–isomorphism is an ℓ–isomorphism as well, for all $\ell < k$. Obviously the inverse of a k–isomorphism is a k–isomorphism, and $|A| = |B|$. The 2–isomorphic image of a (proper) generalized arithmetic progression is a (proper) generalized arithmetic progression of the same dimension and volume. This follows from the repeated application of the fact that $a_1 - a_2 = a_3 - a_4$ iff $a_1 + a_4 = a_2 + a_3$ iff $\phi(a_1) + \phi(a_4) = \phi(a_2) + \phi(a_3)$ iff $\phi(a_1) - \phi(a_2) = \phi(a_3) - \phi(a_4)$. If B is a $k(m+n)$–isomorphic image of A then $mB - nB$ is a k–isomorphic image of $mA - nA$. Indeed, the map $\phi : A \to B$ induces a map $\phi^* : mA - nA \to mB - nB$ by

$$\phi^*(a_1 + \dots + a_m - a_{m+1} - \dots - a_{m+n}) = \phi(a_1) + \dots + \phi(a_m) - \phi(a_{m+1}) - \dots - \phi(a_{m+n}),$$

since ϕ is an $(m+n)$–isomorhism, this is well defined, and since ϕ is a $k(m+n)$–isomorhism, this is a k–isomorphism.

Theorem 7.5: (Ruzsa's embedding theorem) Let $k \geq 2$ be an integer and let $A \subset \mathbb{Z}$ be a finite set of integers. If $N > 2|kA - kA|$ is a prime, then there is a subset $A' \subset A$ and a k–isomorphism $\phi : A' \to B \subset \mathbb{Z}_N$, where $|A'| \geq |A|/k$.

Proof: With simple terms, any subset A of the integers contains a rather "big" subset A', such that A' has a k–isomorphic image B in $\mathbb{Z}_N$, where N is a well chosen not too large prime. We construct this isomorphism in four steps.

First step. We choose a prime $p > k(\max A - \min A)$, and map the elements of A into the residue classes of $\mathbb{Z}_p$, they represent. This is a k–isomorphism, because $L =: k \min A \leq a_1 + \dots + a_k \leq k \max A < L + p$ and two such integers are equal iff they are congruent mod p.

Second step. For an integer $1 \leq q \leq p-1$ we map $a \in \mathbb{Z}_p$ to $qa \in \mathbb{Z}_p$. This is a k–isomorphism, obviously. Our aim with this step is to shuffle the image of A in $\mathbb{Z}_p$ to

a more uniform position. Let us denote the image of A after these two isomorphisms by $A_q \subset \mathbb{Z}_p$.

Third step. We map $A_q \subset \mathbb{Z}_p$ to their least non negative residues in $\mathbb{Z}$. This is not a k–isomorphism, obviously. However, there is an interval of length p/k containing at least $|A|/k$ images of A_q, we denote these images by $A_q'' \subset \mathbb{Z}$, and we denote the pre–image of A_q'' by $A_q^* \subset A_q \subset \mathbb{Z}_p$. Note that $M =: \min A_q'' \le \max A_q'' < M + \frac{p}{k}$, our map is a k–isomorphism between A_q^* and A_q'' for the same reason as in the first step.

Fourth step. We choose a prime $N > 2|kA - kA|$, and map the elements of A_q'' into B_q, the reside classes of $\mathbb{Z}_N$, they represent. This is not a k–isomorphism usually, however we show that there is a q for which this is. To this end we compute the number of bad choices for the role of q. The inverses of the first three isomorphisms define $A_q' \subset A$, the isomorphic image of A_q'' in A. We have $|A_q'| > |A|/k$. We denote the composition of all four maps by ϕ, that is $\phi : A_q' \to B_q \subset \mathbb{Z}_N$. q is a bad choice if there are

$$0 \neq c = a_1 + \cdots + a_k - a_1' - \cdots - a_k' \in kA_q' - kA_q' \subset kA - kA,$$

such that

$$\phi(a_1) + \cdots + \phi(a_k) - \phi(a_1') - \cdots - \phi(a_k') \equiv 0 \pmod N$$

in B_q. Especially, the number of different choices for c is bounded by $\le |kA - kA|$. The images of $a_1, \ldots, a_k'$ in $A_q'' \subset \mathbb{Z}$ after the first three isomorphisms are $c_1, \ldots, c_k'$ respectively. They satisfy

$$r =: c_1 + \cdots + c_k - c_1' - \cdots - c_k' \equiv qa_1 + \cdots + qa_k - qa_1' - \cdots - qa_k' = qc \not\equiv 0 \pmod p,$$

the last because of A_q^* is isomorphic to A_q', and we also conclude $0 < |r| < p$, while

$$r = c_1 + \cdots + c_k - c_1' - \cdots - c_k' \equiv \phi(a_1) + \cdots + \phi(a_k) - \phi(a_1') - \cdots - \phi(a_k') \equiv 0 \pmod N.$$

From this last congruence (and the bound for the size of r), the number of choices for r is at most $\le 2(p-1)/N$. From the previous congruence $q \equiv r/c \pmod p$, and so the number of different choices for a bad q is bounded by

$$\le \frac{2(p-1)}{N} |kA - kA| < p - 1,$$

there must be a q for which ϕ is a k–isomorphism. Let $A' = A_q'$ and $B = B_q$ with such a q. This concludes the proof of our theorem.

□

Keeping applications in mind we prove a slightly more general (not really) result namely

Theorem 7.6: Let $n \ge 1$ be an integer and A be a finite subset of $\mathbb{Z}^n$, and $C \ge 2$. If $|A + A| \le C|A|$ then there is a generalized arithmetic progression Q of integer vectors such that

$$A \subset Q, \quad \mathrm{vol}(Q) \le F(C)|A|, \quad \dim Q \le d(C), \tag{7.2}$$

with explicitly calculable functions $F(C)$ and $d(C)$.

Proof: After a translation we can suppose that

$$A \subset \{0, \dots, M-1\}^n,$$

with a large M. Let D be the 16–isomorphic image of A in $\mathbb{Z}$ under the map $(a_1, \dots, a_n) \mapsto a_1 + a_2(16M) + \dots + a_n(16M)^{n-1}$. Note that $|A| = |D|$ and $|8A - 8A| = |8D - 8D|$. Theorem 1.11 (Plünnecke's inequality) implies that $|8A - 8A| \le C^{16}|A|$. Note that it is enough to use Plünnecke inequality on the $D \subset \mathbb{Z}$ side. We fix a prime N satisfying $2C^{16}|A| < N \le 4C^{16}|A|$. Theorem 7.5 implies that there is a $D' \subset D$ and an 8–isomorphism $\phi : D' \to B \subset \mathbb{Z}_N$, where $|D'| \ge |A|/8$. Let $A' \subset A$ be the pre–image of D' in $\mathbb{Z}^n$. Note that B is an 8–isomorphic image of A', and $|B| = |D'| = |A'| \ge |A|/8 \ge N/(32C^{16}) =: \alpha N$. Theorem 7.3 (Bogolyubov) implies that there is a proper generalized arithmetic progression $P \subset 2B - 2B$ with $\dim P \le \alpha^{-2}$ and $\mathrm{vol}(P) \ge (\alpha^2/4)^{\alpha^{-2}} N$. The (inverse) isomorphic image of P is a proper generalized arithmetic progression $P' \subset 2A' - 2A' \subset 2A - 2A$ with the same dim and vol. We write $\dim P' = \delta \le \alpha^{-2}$ and $\mathrm{vol}(P') = \gamma|A| \ge (\alpha^2/4)^{\alpha^{-2}} N \ge 2C^{16}(\alpha^2/4)^{\alpha^{-2}}|A|$. Note also that $\gamma|A| = \mathrm{vol}(P') \le |2A - 2A| \le C^4|A|$.

Let $S \subset A$ be maximal to the property that the sets $\mathbf{s} + P'$ are pairwise disjoint for all $\mathbf{s} \in S$. Obviously $|S||P'| = |S + P'|$, moreover $S + P' \subset A + P' \subset 3A - 2A$ and by Plünnecke's inequality again, we have

$$|S| \le \frac{|3A - 2A|}{|P'|} \le \frac{C^5|A|}{\mathrm{vol}(P')} = \frac{C^5}{\gamma}.$$

From the maximality of S, for all $\mathbf{a} \in A$ there is an $\mathbf{s} \in S$ such that $(\mathbf{a} + P') \cap (\mathbf{s} + P') \ne \emptyset$. This means that $\mathbf{a} + \mathbf{u}_1 = \mathbf{s} + \mathbf{u}_2$ where $\mathbf{u}_1, \mathbf{u}_2 \in P'$, that is $\mathbf{a} = \mathbf{u}_2 - \mathbf{u}_1 + \mathbf{s}$ and so

$$A \subset P' - P' + S \subset Q,$$

where, if $P' = \{\mathbf{a}_0 + \mathbf{a}_1 n_1 + \dots + \mathbf{a}_\delta n_\delta : 0 \le n_j < N_j\}$ then

$$Q = \{\sum_{j=1}^{\delta} \mathbf{a}_j n_j + \sum_{\mathbf{s} \in S} \mathbf{s}\epsilon_s : |n_j| < N_j,\ 0 \le \epsilon_s < 2\},$$

is a generalized arithmetic progression with $\dim Q = \delta + |S|$ and $\mathrm{vol}(Q) \le 2^\delta \gamma |A| 2^{|S|}$. This completes the proof.

□

It is recommended to follow closely the proof in order to compute how the parameters α, δ, γ , and $|S|$ depends solely on C, finally to find an expression for $d(C)$ and $F(C)$.

These bounds can be significantly improved by the following observation, due to Chang (2002). The poor bounds in the above argument come from the enormous size of S, we will improve it by replacing S and Q above to a much smaller S' and a somewhat bigger Q'. We use an iterative method. Let $S_0 = S$ and $Q_0 = Q$ be as in the last paragraph of

the proof, and let $m > C$ be an integer chosen later. If S_j and Q_j are constructed then do the following. If $|S_j| \le m$ then we stop and let this j is denoted by J. If $|S_j| > m$ then select any subset $T_j \subset S_j$ with $|T_j| = m$ and let $Q_{j+1} = T_j + Q_j$. (Ignore the fact that these are not anymore generalized arithmetic progressions.) Nevertheless we select $S_{j+1} \subset A$ in the same way, that is a maximal set with $s + Q_{j+1}$ are pairwise disjoint. We have $|S_{j+1}||Q_{j+1}| = |S_{j+1} + Q_{j+1}|$. Note that this also imply (from the previous step) that $m|Q_j| = |T_j||Q_j| = |T_j + Q_j| = |Q_{j+1}|$, and by induction $|Q_j| = m^j|Q|$. On the other hand $Q_{j+1} \subset S_j + Q_j \subset A + Q_j \subset \cdots \subset (j+1)A + Q \subset (j+3)A - 2A$. By Plünnecke's inequality $|S_j| \le |S_j + Q_j|/|Q_j| \le (C/m)^j\, C^5|A|/|Q|$, since this is decreasing to 0 as j increases, we have to stop at some J. From the same computation we have $m^J|Q| = |Q_J| \le C^{J+4}|A|$, that is $(m/C)^J \le C^4/\gamma$.

From the construction

$$A \subset S_J + Q_J - Q_J \subset S_J + \sum_{j=0}^{J-1} (T_j - T_j) + Q - Q,$$

which is a generalized arithmetic progression of $\dim = |S_J| + mJ + \delta \le (m+1)J + \alpha^{-2}$ and $\mathrm{vol} \le 2^{|S_J|} 3^{mJ} \gamma |A|$. The reader is invited to fill up the details in this argument, to find the optimal choice of m, and to trace through for getting the bounds of $d(C)$ and $F(C)$.

CHAPTER 8

A STATISTICAL RESULT

Let Z be an additive abelian group ($\mathbb{Z}$, for example), $A \subset Z$ and $B \subset Z$ are finite subsets. Suppose there are "many" additive quadruples in the form $a_1 + b_1 = a_2 + b_2$, that is there are many solutions to this equation, where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Is this a severe condition on A and B?

Alternatively let $G \subset A \times B$, and $S = \{a + b : (a, b) \in G\}$. The best way to view G is that G is the set of the edges of a bipartity graph on the two vertex sets A and B, as disjoint vertex sets, (even if they are not disjoint as subsets of Z). Than S is the set of the sums of the two vertices along each edges of G. Suppose that $|S|$ is "small" while $|G|$ is "large". Is this a severe condition on A and B?

In this chapter we prove that they indeed imply that A and B have to have some "weak" structure. There is a family of statements of this kind. We have already expressed the basic condition in two forms, and the results also vary according to the precise meaning of the words "many", "small", "large" and "weak" above. The results follow the scheme, that there are "large" subsets $A' \subset A$ and $B' \subset B$ such that the complete sum set $A' + B' = \{a + b : a \in A', b \in B'\}$ is "small". Roughly speaking, partial information on the sum set imply the existence of subsets with complete information. One can now appeal to the structure theorem of Freiman (Chapter 7) to describe A' and B' more precisely.

Theorem 8.1: Let Z be an additive abelian group, $A \subset Z$, $B \subset Z$, $G \subset A \times B$, and $S = \{a + b : (a, b) \in G\}$. If $|A|, |B|, |S| \leq N$ and $|G| = \alpha N^2$ then there are $A' \subset A$ and $B' \subset B$ such that

$$(8.1) \qquad \text{i.) } |A' + B'| \leq \frac{2^{15}}{\alpha^5} N, \quad \text{ii.) } |A'|, |B'| \geq \frac{\alpha}{8} N, \quad \text{iii.) } |(A' \times B') \cap G| \geq \frac{\alpha^2}{32} N^2.$$

Theorem 8.2 Let Z be an additive abelian group, $A \subset Z$, $B \subset Z$, and $|A|, |B| \leq N$. If there are $\geq 2\alpha N^3$ solutions to the equation $a_1 + b_1 = a_2 + b_2$, in $a_1, a_2 \in A$ and $b_1, b_2 \in B$, then there are $A' \subset A$ and $B' \subset B$ such that

$$\text{i.) } |A' + B'| \leq \frac{2^{15}}{\alpha^5} N, \quad \text{ii.) } |A'|, |B'| \geq \frac{\alpha}{8} N.$$

First we show that Theorem 8.2 follows from Theorem 8.1 by the use of a simple averaging argument. Suppose that the condition of Theorem 8.2 holds and remember the definition from Chapter 1, $r_{A+B}(n) = \#\{n = a + b : a \in A, b \in B\} \leq N$, moreover let $S = \{n : r_{A+B}(n) \geq \alpha N\}$. Note that $\sum r_{A+B}(n) = |A||B| \leq N^2$. We have

$$2\alpha N^3 \leq \sum_{a_1+b_1=a_2+b_2} 1 = \sum_n r_{A+B}(n)^2 = \sum_{n \in S} r_{A+B}(n)^2 + \sum_{n \notin S} r_{A+B}(n)^2 \leq$$
$$\leq N \sum_{n \in S} r_{A+B}(n) + \alpha N \sum_{n \notin S} r_{A+B}(n) \leq N \sum_{n \in S} r_{A+B}(n) + \alpha N^3.$$

If S is so abundant that $|S| > N$ then we can drop a few elements to reach $|S| = N$ and still maintain that $\sum_{n\in S} r_{A+B}(n) \geq \alpha N^2$. Finally let $G = \{(a,b) : a+b \in S\}$, $|G| = \sum_{n\in S} r_{A+B}(n)$ and the conditions of Theorem 8.1 are satisfied.

□

Actually, the whole proof of Theorem 8.1 is no more than the repeated use of this same averaging argument, so we state it here independently.

Lemma 8.3: Let S be any set with $|S| \leq N$ and $f : S \to \mathbb{R}$ be any function with $f(s) \leq M$.

$$\text{If} \quad \sum_{s\in S} f(s) \geq \alpha MN, \quad \text{and} \quad S' = \{s \in S : f(s) \geq \frac{\alpha}{2}M\}$$

$$\text{then} \quad \sum_{s\in S'} f(s) \geq \frac{\alpha}{2}MN \quad \text{and} \quad |S'| \geq \frac{\alpha}{2}N. \tag{8.2}$$

Proof: One can verify (8.2) in a few lines just copying the above argument.

$$\alpha MN \leq \sum_{s\in S} f(s) = \sum_{s\in S'} f(s) + \sum_{s\notin S'} f(s) \leq \sum_{s\in S'} f(s) + \frac{\alpha}{2}M|S|,$$

$$\frac{\alpha}{2}MN \leq \sum_{s\in S'} f(s) \leq M|S'|.$$

□

Proof of Theorem 8.1: Any a resp. b with or without subscript or superscript will always denote elements of A resp. B. Our plan is the following. If we can write

$$a + b = (a + b') - (a' + b') + (a' + b) \tag{8.3}$$

such that all three terms on the RHS are sums from S, and in addition we have $\gg N$ such choices of a' and $\gg N$ such choices of b' then we have $\gg N^2$ representations

$$a + b = s_1 - s_2 + s_3.$$

They can be the same for different pairs a, b, but they are certainly different for different values of $a+b$. As there are no more than N^3 different three–tuples of elements of S, this prevents us to have too many different values of $a + b$. Of course, we have to restrict our choice of a and b to provide the numerous representations of the required manner, but this is the only thing we have to concentrate on.

We define a bipartity graph G_1 as is described earlier. That is the left hand side vertex set A_1 is identified with A, the right hand side vertex set B_1 is identified with B and a, b are connected with an edge if $(a, b) \in G$. Our strategy is to reduce this graph step by step by dropping vertices and/or edges to gain better properties. The subsequent graphs,

as well as its set of edges will be denoted by G_n, and the corresponding vertex sets by A_n and B_n. We do not go further than G_4.

The most important constituents of our graphs are R_a resp. R_b, the set of vertices on the other side connected to a resp. b, we call them the "shadow" of a resp. the shadow of b. Note that R_a and R_b depend of the actual graph, we have to follow their changes with some care.

Note that $|R_a| \le N$ and we have that

$$\sum_{a\in A} |R_a| = |G_1| = |G| = \alpha N^2,$$

define $A_2 = \{a \in A : |R_a| \ge \frac{\alpha}{2}N\}$, the set of vertices with big shadows. We do not touch the other side, $B_2 = B_1 = B$. (8.2) implies that

$$|G_2| = \sum_{a\in A_2} |R_a| \ge \frac{\alpha}{2}N^2, \quad |R_a| \ge \frac{\alpha}{2}N \text{ in } G_2. \tag{8.4}$$

The next reduction, still on the A side, is the most delicate step of the whole process. Remember our goal, (8.3). We want that the three terms on the right hand side correspond to edges in G_2. Now, if a and b are fixed and we picked an $a' \in R_b$, then any choice of $b' \in R_a \cap R_{a'}$ will work. This justify the following definition, let $\gamma > 0$ be a real number, chosen later, and

$$Y = \{(a, a') \in A_2 \times A_2 : |R_a \cap R_{a'}| \le \gamma N\} \tag{8.5}$$

be the set of "unfriendly" pairs with poorly intersecting shadows. We expect that $|Y|$ is small if γ is small enough. On one hand

$$\sum_{(a,a')\in Y} |R_a \cap R_{a'}| \le \gamma N|Y| \le \gamma N^3, \tag{8.6}$$

on the other hand (note that $b \in R_a \Leftrightarrow a \in R_b \Leftrightarrow (a, b) \in G_2$) we have

$$\sum_{(a,a')\in Y} |R_a \cap R_{a'}| = \sum_{(a,a')\in Y} \sum_{b\in R_a\cap R_{a'}} 1 = \sum_{b\in B} |(R_b \times R_b) \cap Y|. \tag{8.7}$$

(8.6) and (8.7) together say that on average there are not too many unfriendly pairs in shadows. A good candidate for A_3 is a well chosen R_b, but we have to provide several things simultaneously.

We have from (8.4) that

$$\sum_{b\in B_2} |R_b| = |G_2| \ge \frac{\alpha}{2}N^2.$$

Writing $B^* = \{b \in B : |R_b| \ge \frac{\alpha}{4}N\}$, we get from our standard averaging argument (8.2) that

$$\sum_{b\in B^*} |R_b| \ge \frac{\alpha}{4}N^2. \tag{8.8}$$

Now suppose that for every $b \in B^*$ we have

$$|(R_b \times R_b) \cap Y| > \frac{4\gamma}{\alpha} N|R_b|. \tag{8.9}$$

From (8.6), (8.7), (8.8) and (8.9) we get a contradiction, indeed

$$\gamma N^3 \le N \sum_{b\in B^*} \frac{4\gamma}{\alpha}|R_b| < \sum_{b\in B^*} |(R_b \times R_b) \cap Y| \le \gamma N^3.$$

At least once the contrary of (8.9) should be true, there is a $b \in B$ such that choosing $A_3 = R_b$, $B_3 = B_2 = B$ we have

$$|(A_3 \times A_3) \cap Y| \le \frac{4\gamma}{\alpha} N|A_3|, \quad |A_3| \ge \frac{\alpha}{4}N, \quad |G_3| \ge \frac{\alpha}{2}N|A_3|. \tag{8.10}$$

The last estimate is a consequence of the fact that all R_a is big in A_3 by (8.4). For simplifying notation we write $|A_3| = \rho N$, so (8.10) is actually

$$|(A_3 \times A_3) \cap Y| \le \frac{4\gamma\rho}{\alpha} N^2, \quad |A_3| = \rho N, \quad |G_3| \ge \frac{\alpha\rho}{2}N^2, \quad \frac{\alpha}{4} \le \rho \le 1. \tag{8.11}$$

Note that the (later) choice of γ cannot depend on ρ as the choice of A_3 depends on γ.

A_3 is still not perfect, some elements can have many unfriendly counterparts. Let $\delta > 0$ be chosen soon, and let $A_4 = \{a \in A_3 : \#\{a' \in A_3 : (a, a') \in Y\} \le \delta N\}$ be the set of friendly elements, elements with only a few unfriendly counterparts. Trivially

$$\frac{4\gamma\rho}{\alpha} N^2 \ge |(A_3 \times A_3) \cap Y| = \sum_{a\in A_3} \sum_{\substack{a'\in A_3 \\ (a,a')\in Y}} 1 \ge \sum_{a\notin A_4} \sum_{\substack{a'\in A_3 \\ (a,a')\in Y}} 1 \ge \delta N|A_3 \setminus A_4|,$$

$$|A_4| = |A_3| - |A_3 \setminus A_4| \ge \rho N - \frac{4\gamma\rho}{\alpha\delta} N = \frac{\rho}{2}N, \quad \text{if} \quad \delta = \frac{8\gamma}{\alpha}.$$

Still keeping $B_4 = B_3 = B$, for all $a \in A_4$ we have from (8.4) that

$$\#\{a' \in A_4 : (a, a') \in Y\} \le \frac{8\gamma}{\alpha} N, \quad |A_4| \ge \frac{\rho}{2}N, \quad |G_4| \ge \frac{\alpha\rho}{4}N^2. \tag{8.12}$$

There is no more reduction, we choose $A' = A_4$ and $B' = \{b \in B : |R_b| \ge \frac{\alpha\rho}{8}N\}$. Note that $|R_b| \le |A_4| \le |A_3| = \rho N$ and that

$$\sum_{b\in B} |R_b| = |G_4| \ge \frac{\alpha\rho}{4}N^2,$$

so our averaging argument (8.2) (this time with $M = \rho N$) implies that

$$\sum_{b\in B'} |R_b| \ge \frac{\alpha\rho}{8}N^2, \quad |B'| \ge \frac{\alpha}{8}N. \tag{13}$$

The first is a bound for the number of edges connecting A' and B', they are all edges of the original G, so we have by the last inequality of (8.11) that

$$|(A' \times B') \cap G| \geq \frac{\alpha\rho}{8} N^2 \geq \frac{\alpha^2}{32} N^2,$$

which is (8.1.iii.). Also (8.12) and (8.13) prove (8.1.ii.). Now we can complete the plan as is described in the beginning of the proof. Note that we are working in G_4 so R_a and R_b refer to this stage.

Fix any pair of elements $a \in A'$ and $b \in B'$. By the choice of B', the shadow of b is big, $|R_b| \geq \frac{\alpha\rho}{8} N$, while the number of unfriendly counterparts of a is small, $\#\{a' \in A_3 : (a, a') \in Y\} \leq \frac{8\gamma}{\alpha} N$. This is less than half of the shadow if

$$\frac{8\gamma}{\alpha} \leq \frac{1}{2}\frac{\alpha\rho}{8} \quad \Leftrightarrow \quad \gamma \leq \frac{\alpha^2\rho}{128} \quad \Leftarrow \quad \gamma = \frac{\alpha^3}{512}.$$

For all of those friendly a' we have a choice of $|R_a \cap R_{a'}| \geq \gamma N = \frac{\alpha^3}{512} N$ different $b' \in B$. Collecting these bounds we get that the number of different edge–triples (a, b'), (a', b'), and (a', b) in G_4 is at least

$$\#\{a'\}\#\{b'\} \geq \frac{\alpha\rho}{16} N\gamma N \geq \frac{\alpha^5}{2^{15}} N^2. \tag{8.14}$$

Thus for every pair a, b the number of representations

$$a + b = (a + b') - (a' + b') + (a' + b) = s_1 - s_2 + s_3, \tag{8.15}$$

with $s_1, s_2, s_3 \in S$ is by (8.14) at least

$$\#\{a'\}\#\{b'\} \geq \frac{\alpha^5}{2^{15}} N^2.$$

They can be the same for different pairs a, b, but they are certainly different for different values of $a + b$. Since there are no more than $|S|^3 \leq N^3$ different three–tuples of s_1, s_2, s_3, we arrive at (8.1.i.), that is

$$|A' + B'| \leq \frac{\#\text{ of three–tuples in } S}{\#\text{ of representations of } a + b \text{ in (8.15)}} \leq \frac{N^3}{\frac{\alpha^5}{2^{15}} N^2} = \frac{2^{15}}{\alpha^5} N.$$

□

These type of results play a crutial role in the recent argument of Gowers to prove a quantitative Szemerédi's theorem. We illustrate some of the diverse applications in the next chapter, and describe Gowers' argument in the last three chapters. As we have already mentioned, there are many more variations of Theorem 8.1. They basically differ by the type of conclusions. One can ask if partial information about sums imply full information about differences in large subsets, (in contrast to Theorem 8.1, where the full information

is derived from sums to sums). In a wide selection of applications $A = B$, and we want to conclude an $A' \subset A$ with $A' + A'$ is small, (in contrast to Theorem 8.1, where we conclude two, possibly different sets $A', B' \subset A$ with $A' + B'$ is small). Little more generally one can ask information from $A + B$ to $A' \pm A'$. Plünnecke's inequality makes possible to connect the sizes of $A' \pm B', A' \pm A'$, however, an application blows the exponents. It is sometimes more economical to modify the above proof to the new situations. It is a recommended exercise to improve the quantitative aspects of the following corollaries, by adopting the proof of Theorem 8.1. Doing so one can run into an interesting parity problem. For example, $a_1 - a_2 = (a_1 + b) - (a + b) + (a + b') - (a_2 + b')$, however, $a_1 + a_2$ cannot be expressed as a combination of sums from $A + B$. Some estimates are considerable more difficult than others (similarly to the case of Theorem 1.4 and Theorem 1.7).

Corollary 8.4: Let Z be an additive abelian group, $A \subset Z$, $B \subset Z$, $|A|, |B| \leq N$. If either $G \subset A \times B$, $|G| = \alpha N^2$, and $S = \{a + b : (a, b) \in G\}$, $|S| \leq N$, or if there are $\geq 2\alpha N^3$ solutions to the equation $a_1 + b_1 = a_2 + b_2$, in $a_1, a_2 \in A$ and $b_1, b_2 \in B$, then there is an $A' \subset A$ such that

$$\text{i.) } |A' \pm A'| \leq \frac{2^{33}}{\alpha^{11}} N, \quad \text{ii.) } |A'| \geq \frac{\alpha}{8} N.$$

Proof: An application of Theorem 8.1 or Theorem 8.2 provides an $A' \subset A$ and $B' \subset B$ such that

$$\text{i.) } |A' + B'| \leq \frac{2^{15}}{\alpha^5} N, \quad \text{ii.) } |A'|, |B'| \geq \frac{\alpha}{8} N.$$

Either of Corollary 1.5 and Corollary 1.8 than imply that

$$|A' \pm A'| \leq \frac{|A' + B'|^2}{|B'|} \leq \big(\frac{2^{15}}{\alpha^5} N\big)^2 \big(\frac{\alpha}{8} N\big)^{-1} = \frac{2^{33}}{\alpha^{11}} N.$$

□

Corollary 8.5: Let Z be an additive abelian group, $A \subset Z$, $B \subset Z$, $G \subset A \times B$, and $S = \{a + b : (a, b) \in G\}$. If $|A|, |B|, |S| \leq N$ and $|G| = \alpha N^2$ then there is an $A' \subset A$ and a $B' \subset B$ such that

$$\text{i.) } |A' - B'| \leq \frac{2^{51}}{\alpha^{17}} N, \quad \text{ii.) } |A'|, |B'| \geq \frac{\alpha}{8} N, \quad \text{iii.) } |(A' \times B') \cap G| \geq \frac{\alpha^2}{32} N^2.$$

Proof: An application of Theorem 8.1 provides an $A' \subset A$ and $B' \subset B$ such that

$$\text{i.) } |A' + B'| \leq \frac{2^{15}}{\alpha^5} N, \quad \text{ii.) } |A'|, |B'| \geq \frac{\alpha}{8} N, \quad \text{iii.) } |(A' \times B') \cap G| \geq \frac{\alpha^2}{32} N^2.$$

Corollary 1.9 implies

$$|A' - B'| \leq \frac{|A' + B'|^3}{|A'||B'|} \leq \big(\frac{2^{15}}{\alpha^5} N\big)^3 \big(\frac{\alpha}{8} N\big)^{-2} = \frac{2^{51}}{\alpha^{17}} N.$$

□

CHAPTER 9

SOME APPLICATIONS

Erdős conjectured that a set of integers that contains many three–term arithmetic progressions must contain a long arithmetic progression as well. He may believed to prove Szemerédi's theorem in this line. In the first half of this section, we apply Corollary 8.4 (the statistical result), Theorem 7.1 (Freiman's theorem), and Theorem 4.2 (Szemerédi's theorem) to prove this statement. Note that Theorem 4.2 is stated without proof in Chapter 4. A full proof is beyond the scope of this course, but in Chapter 13 we detail the case of $k = 4$.

Theorem 9.1: Let $\alpha > 0$ and $k \geq 3$. If A is a set of $N \geq N_0(\alpha, k)$ integers that contains at least αN^2 distinct three–term arithmetic progressions, then A contains a k–term arithmetic progression.

Proof: Let A be a set of integers with $|A| = N$. We define a set $G \subset A \times A$. For each non–trivial three–term arithmetic progression a, b, c in A, we put the pair (a, c) into G. We have $|G| \geq \alpha N^2$. Let $S = \{a + c : (a, c) \in G\}$. A three–term arithmetic progression a, b, c satisfies $a + c = 2b$, that is $a + c \in 2 \cdot A$, hence $|S| \leq |2 \cdot A| = N$. Corollary 8.4 (with $A = B$) yields to an $A' \subset A$ with

$$|A'| \geq \frac{\alpha}{8} N, \quad |A' + A'| \leq \frac{2^{33}}{\alpha^{11}} N \leq \frac{2^{36}}{\alpha^{12}} |A'|.$$

Next Theorem 7.1 yields to a generalized arithmetic progression Q such that

$$A' \subset Q = \{a_0 + a_1 n_1 + \cdots + a_d n_d : 0 \leq n_j < N_j \text{ for } j = 1, \ldots, d\},$$
$$N_1 \cdots N_d = \mathrm{vol}(Q) \leq F(C)|A'|, \quad d = \dim Q \leq d(C),$$

where $C = 2^{36}/\alpha^{12}$. We can assume without loss of generality that

$$\max(N_1, \ldots, N_d) = N_d, \quad N_d \geq |A'|^{1/d},$$

since $A' \subset Q$ implies $|A'| \leq N_1 \cdots N_d \leq N_d^d$. Let $\mathcal{V}$ be the set of lattice points

$$\mathbf{v} = (n_1, \ldots, n_{d-1}) \in \mathbb{Z}^{d-1}, \quad 0 \leq n_j < N_j \text{ for } j = 1, \ldots, d-1.$$

Obviously $|\mathcal{V}| = N_1 \cdots N_{d-1}$. For each $\mathbf{v} \in \mathcal{V}$, the set

$$\mathcal{L}(\mathbf{v}) = \{a_0 + a_1 n_1 + \ldots a_{d-1} n_{d-1} + a_d n_d : 0 \leq n_d < N_d\}$$

is an arithmetic progression of length N_d, and $Q = \cup_{\mathbf{v} \in \mathcal{V}} \mathcal{L}(\mathbf{v})$. Thus $A' \subset Q$ means $A' = \cup_{\mathbf{v} \in \mathcal{V}} (\mathcal{L}(\mathbf{v}) \cap A')$, and so

$$\frac{1}{F(C)} N_1 \cdots N_d \leq |A'| \leq \sum_{\mathbf{v} \in \mathcal{V}} |\mathcal{L}(\mathbf{v}) \cap A'|.$$

There is at least one $\mathbf{v} \in \mathcal{V}$ with

$$|\mathcal{L}(\mathbf{v}) \cap A'| \geq \frac{1}{F(C)} N_d.$$

Let us fix one such $\mathbf{v}$, and define

$$B = \{0 < n \leq N_d : a(n) =: a_0 + a_1 n_1 + \dots a_{d-1} n_{d-1} + a_d(n-1) \in A'\}.$$

Since $|B| \geq N_d/F(C)$, by Szemerédi's theorem B contains an arithmetic progression of length k whenever $N_d \geq N(k, \delta)$ with $\delta = 1/F(C)$, and this follows from

$$\frac{\alpha}{8} N \geq N(k, \delta)^d,$$

where the parameters C, δ, d are all functions of α in Theorem 7.1. If $b_1, \dots, b_k$ is a non–trivial arithmetic progression in B then $a(b_1), \dots, a(b_k)$ is a non–trivial arithmetic progression in $A' \subset A$, and we are done.

□

Next we apply Corollary 8.5 to the Kakeya problem. This problem can be studied both in the real Euclidean space or in finite fields; for simplicity we treat with the finite field case only.

Let p be an odd prime, and $\mathbb{Z}_p$ be the finite field of p elements, the field of residue classes mod p. For a fixed integer $n \geq 2$ we consider $\mathbb{Z}_p^n$, the n– dimensional vector space over $\mathbb{Z}_p$. A *line* in $\mathbb{Z}_p^n$ is any set $\mathcal{L}$ of the form

$$\mathcal{L} = \{\mathbf{x} + t\mathbf{v} : t \in \mathbb{Z}_p\},$$

where $\mathbf{x} \in \mathbb{Z}_p^n$ and $\mathbf{v} \in \mathbb{Z}_p^n \setminus \{0\}$; we refer to $\mathbf{v}$ as the *direction* of $\mathcal{L}$, though this direction is only defined up to scalar multiplication by non–zero residue classes. There are $(p^n - 1)/(p-1) > p^{n-1}$ directions. A set $E \subset \mathbb{Z}_p^n$ which contains a line in every direction is called a *Besicovitch set*. (The Euclidean Besicovitch set contains a unit interval in every direction. There are Besicovitch sets of zero measure, and the Kakeya conjecture claims that any Besicovitch set has *Hausdorff dimension* n; it can have zero measure, but it is big.)

The corresponding finite field Kakeya conjecture asserted that

$$|E| \geq c(n, \epsilon) p^{n-\epsilon},$$

for every $\epsilon > 0$ and some $c(n, \epsilon) > 0$. In other words, Besicovitch sets are conjectured to fill up practically all of $\mathbb{Z}_p^n$. The conjecture is recently proved in the stronger form $|E| \gg p^n$, using the polynomial method introduced in Chapter 3. We give the proof later in this chapter. Unfortunately this proof cannot be transferred to the Euclidean case. We start with weaker results that can be transferred (although we skip the transference).

First we prove an easy estimate, which motivates the deeper developments. Fix a Besicovich set E. For every $u \in \mathbb{Z}_p$, consider the *horizontal plane* $\mathbb{Z}_p^{n-1} \times \{u\}$, and let E_u denote the *horizontal slice*

$$E_u =: E \cap (\mathbb{Z}_p^{n-1} \times \{u\}).$$

We obviously have

$$\sum_{u \in \mathbb{Z}_p} |E_u| = |E|,$$

so the average size of $|E_u|$ is $|E|/p$. There must be at least two values of u for which $|E_u| \leq 2|E|/p$. By an affine transformation, we may assume those values are 0 and 1, that is $|E_0|, |E_1| \leq 2|E|/p$. Now consider the lines in E. For every $\mathbf{w} \in \mathbb{Z}_p^{n-1}$, there must be a line, $\mathcal{L}_{\mathbf{w}}$ with direction $(\mathbf{w}, 1)$ that lies in E. This line intersects E_0 at some point $a(\mathbf{w}) \in E_0$, and intersects E_1 at another point $b(\mathbf{w}) \in E_1$. Clearly $b(\mathbf{w}) - a(\mathbf{w}) = t(\mathbf{w}, 1) = (\mathbf{w}, 1)$ by comparing the last coordinates. Thus to each $\mathbf{w} \in \mathbb{Z}_p^{n-1}$ we can associate a pair $(a(\mathbf{w}), b(\mathbf{w})) \in E_0 \times E_1$ of points, so that the line across them lies in E and has direction $(\mathbf{w}, 1)$. Since two different points determine exactly one line, all these pairs are distinct, so their number is p^{n-1}. On the other hand, their number is bounded by

$$p^{n-1} \leq |E_0 \times E_1| = |E_0||E_1| \leq \frac{4|E|^2}{p^2}.$$

This yield to the inequality

$$|E| \geq \frac{1}{2}\, p^{\frac{n+1}{2}}.$$

Anything better than this bound is non–trivial. We are going to use Corollary 8.5 to improve upon this (for large dimensions n). Note that the exponents in Corollary 8.5 are not the best obtainable, the result below can be improved with the same method, and can be further improved with a different method.

Theorem 9.2: Let p be an odd prime and $n \geq 2$ be an integer. Every Besicovitch set E in $\mathbb{Z}_p^n$ has size

$$|E| \geq \frac{1}{25}\, p^{\frac{19n+18}{37}}.$$

Proof: We fix a Besicovitch set E, and again, we consider the slices E_u. We have

$$\frac{8|E|}{p}\, |\{u \in \mathbb{Z}_p : |E_u| > \frac{8|E|}{p}\}| < \sum_{u \in \mathbb{Z}_p} |E_u| = |E|,$$

and so

$$|\{u \in \mathbb{Z}_p : |E_u| \leq \frac{8|E|}{p}\}| > \frac{7}{8}\, p.$$

In particular, we can find a non–trivial arithmetic progression u, $u + r$, $u + 2r$ such that $|E_u|, |E_{u+r}|, |E_{u+2r}| \leq 8|E|/p$. By an affine transformation we may suppose that $u = 0, r = 1/2$, thus we have $|E_0|, |E_{1/2}|, |E_1| \leq N =: 8|E|/p$.

As before, we consider the lines in E. For every $\mathbf{w} \in \mathbb{Z}_p^{n-1}$, there must be a line, $\mathcal{L}_{\mathbf{w}}$ with direction $(\mathbf{w}, 1)$ that lies in E. This line intersects E_0 at some point $a(\mathbf{w}) \in E_0$, and intersects E_1 at another point $b(\mathbf{w}) \in E_1$. Clearly $b(\mathbf{w}) - a(\mathbf{w}) = t(\mathbf{w}, 1) = (\mathbf{w}, 1)$ by comparing the last coordinates, while the midpoint $(a(\mathbf{w}) + b(\mathbf{w}))/2$ lies in $E_{1/2}$. Thus to each $\mathbf{w} \in \mathbb{Z}_p^{n-1}$ we can associate a pair $(a(\mathbf{w}), b(\mathbf{w})) \in E_0 \times E_1$ of points, so that the line across them lies in E and has direction $(\mathbf{w}, 1)$. Since two different points determine exactly one line, all these pairs are distinct, so their number is p^{n-1}. We set $G = \{(a(\mathbf{w}), b(\mathbf{w})); \mathbf{w} \in \mathbb{Z}_p^{n-1}\}$, and in fact, since all differences $b - a$ for $(a, b) \in G$ are different, we have

$$|\{b - a : (a, b) \in G\}| = p^{n-1}, \text{ while } |\{a + b : (a, b) \in G\}| = |E_{1/2}| \leq N.$$

Write $\alpha =: p^{n-1}/N^2 = p^{n+1}/(64|E|^2)$, so that $|G| = \alpha N^2$. We can apply Corollary 8.5, and we get $A' \subset E_0$ and $B' \subset E_1$ such that

$$|A' - B'| \leq \frac{2^{51}}{\alpha^{17}} N.$$

However, since all the differences in G are different, using iii.) from Corollary 8.5 we arrive at

$$\frac{\alpha^2}{32} N^2 \leq |G \cap (A' \times B')| \leq |A' - B'|,$$

and the two inequalities together yield (with some numerical simplification) that

$$\alpha^{19} N \leq 2^{56}, \quad |E| \geq \frac{1}{25} p^{\frac{19n+18}{37}}.$$

□

Theorem 9.3: Let p be an odd prime and $n \geq 2$ be an integer. Every Besicovitch set E in $\mathbb{Z}_p^n$ has size

$$|E| \geq \binom{n + p - 1}{n} \geq \frac{p^n}{n!}.$$

Proof: We prove by contradiction. Suppose E is a Besicovitch set satisfying $|E| < \binom{n+p-1}{n}$. There is a non–zero polynomial $F(\mathbf{x}) \in \mathbb{Z}_p[x_1, \ldots, x_n]$ of degree at most $p - 1$ such that $F(\mathbf{x}) = 0$ for all $\mathbf{x} \in E$. This follows from solving a system of linear equations, where the unknowns are the coefficients of $F(\mathbf{x})$, and there is an equation for each points $\mathbf{x} \in E$. The number of unknowns is exactly the number of monomials $x_1^{k_1} \cdots x_n^{k_n}$ with $0 \leq k_1 + \cdots + k_n \leq p - 1$, and this is exactly $\binom{n+p-1}{n}$, bigger than the number of equations.

Write $F(\mathbf{x}) = \sum_{i=0}^{p-1} F_i(\mathbf{x})$, where F_i is the homogeneous part of degree i of F. Fix an arbitrary direction $\mathbf{v} \in \mathbb{Z}_p^n$, there is a point $\mathbf{b}$ such that the line $\{\mathbf{b} + t\mathbf{v}\} \in E$, which means $F(\mathbf{b} + t\mathbf{v}) = 0$ for all $t \in \mathbb{Z}_p$. For a fixed $\mathbf{b}$ and $\mathbf{v}$ the left hand side is a polynomial in t of degree at most $p - 1$ with p zeros, it must be the zero polynomial. All its coefficients are zero, in particular the coefficient of the highest degree term t^{p-1} is zero. It is easy to

see that this coefficient is $F_{p-1}(\mathbf{v})$. Since $\mathbf{v}$ was arbitrary, $F_{p-1}(\mathbf{v}) = 0$ for all $\mathbf{v}$, it is the zero polynomial by Lemma 3.7. In other words $F(\mathbf{x})$ is of degree $p-2$ at most, and we can repeat the above argument. Again, for an arbitrary direction $\mathbf{v} \in \mathbb{Z}_p^n$, there is a point $\mathbf{b}$ such that $F(\mathbf{b} + t\mathbf{v}) = 0$ for all $t \in \mathbb{Z}_p$. The coefficient of highest degree term t^{p-2} is zero, which is $F_{p-2}(\mathbf{v}) = 0$ for all $\mathbf{v}$. This must be the zero polynomial, $F(\mathbf{x})$ is of degree $p-3$ at most, and so on, $F(\mathbf{x})$ itself is the zero polynomial. This is a contradiction.

□

CHAPTER 10

TECHNICAL PREPARATION: THE EXPONENTIAL FUNCTION

In this chapter we discuss a certain property of the exponential function $e(x) = e^{2\pi ix}$. Namely, we will show that $e(\alpha n)$, and similarly $e(\alpha n^2)$, is nearly constant on stretches of residue classes of some well chosen moduli. We only concentrate on the results we want to use later, and we do not discuss the background of these results. However, there is a beautiful subject behind our arguments, the theory of uniform distribution. A sequence $a_1, a_2, \dots$ of real numbers is uniformly distributed (mod 1) if every subinterval $[u, v)$ of $[0, 1]$ contains the right proportion of the sequence, that is

$$\lim_{N\to\infty} \frac{1}{N} \#\big\{n \le N : \, u \le \{a_n\} < v\big\} = v - u.$$

Here $\{a\} = a - \lfloor a \rfloor$ is the fractional part of the real number a. It was Hermann Weyl, who connected this property to the exponential function. He proved that the sequence $a_1, a_2, \dots$ of real numbers is uniformly distributed (mod 1) if and only if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} e(ka_n) = 0,$$

for all fixed integer $k \neq 0$. The interested reader can try to prove Weyl's theorem, as well as to prove the uniform distribution of the sequences $\{\alpha n\}$, $n \in \mathbb{N}$ or $\{\alpha n^2\}$, $n \in \mathbb{N}$, where α is any fixed irrational number. The best reading in the subject is the book L. Kuipers, H. Niederreiter, Uniform distribution of sequences, John Wiley & Sons, New York, 1974.

Lemma 10.1: Let $P \subset \mathbb{Z}_N$ be an arithmetic progression of $R \le N$ elements. We can partition P into arithmetic progressions P_j of size $|P_j| = R^{1/4} + O(1)$ such that (for all j)

$$\left| e\left(\frac{a\ell}{N}\right) - e\left(\frac{a\ell'}{N}\right) \right| \le \frac{2\pi}{R^{1/4}}, \tag{10.1}$$

whenever $\ell, \ell' \in P_j$.

Proof: Note that the number of subprogressions $M = R^{3/4} + O(R^{1/2})$. Without loss of generality we may suppose that $P = \{1, \dots, R\}$. From Dirichlet's approximation theorem (Lemma 6.4, $k = 1$), there is a rational number b/q, $(b, q) = 1$, $q \le R^{1/2}$ such that

$$\left| \frac{a}{N} - \frac{b}{q} \right| < \frac{1}{qR^{1/2}}. \tag{10.2}$$

Split the set $\{1,\dots,R\}$ into residue classes mod q, and split all residue classes into $R^{3/4}/q+O(1)$ intervals of length $R^{1/4}+O(1)$. They are the arithmetic progressions P_j, we only have to show (10.1). If $\ell,\ell'\in P_j$ then $\ell-\ell'=kq$, $|k|\le R^{1/4}$. We rewrite (10.2) as

$$\frac{a}{N}=\frac{b}{q}+\frac{\Theta}{qR^{1/2}},\ |\Theta|<1,$$

and we arrive at

$$\left|e\left(\frac{a\ell}{N}\right)-e\left(\frac{a\ell'}{N}\right)\right|=\left|e\left(\frac{a(\ell-\ell')}{N}\right)-1\right|=\left|e\left(\frac{akq}{N}\right)-1\right|=\left|e\left(\frac{\Theta k}{R^{1/2}}\right)-1\right|.$$

(10.1) follows from the inequality $|e(x)-1|\le 2\pi|x|$.

□

More effort is needed to get a similar result with a quadratic polynomial $a\ell^2+b\ell$ in place of the linear polynomial $a\ell$ of Lemma 10.1. We start with an estimate of the classical Gauss sum, what we will use to prove a result, similar to Dirichlet's approximation theorem, but with rational numbers of square denominator.

Lemma 10.2: For $(2a,N)=1$ we have

$$\left|\sum_{m\in\mathbb{Z}_N}e\left(\frac{am^2+bm}{N}\right)\right|=\sqrt{N},$$

moreover in general we have

$$\left|\sum_{m\in\mathbb{Z}_N}e\left(\frac{am^2+bm}{N}\right)\right|\le\sqrt{(2a,N)\,N}.$$

Proof: Let S be the sum on the left hand side, and we compute its square.

$$\begin{aligned}|S|^2&=\sum_{m_1\in\mathbb{Z}_N}\sum_{m_2\in\mathbb{Z}_N}e\left(\frac{a(m_1^2-m_2^2)+b(m_1-m_2)}{N}\right)=\\&=\sum_{h\in\mathbb{Z}_N}\sum_{m_2\in\mathbb{Z}_N}e\left(\frac{ah(2m_2+h)+bh}{N}\right)=\sum_{h\in\mathbb{Z}_N}e\left(\frac{ah^2+bh}{N}\right)\sum_{m\in\mathbb{Z}_N}e\left(\frac{2ahm}{N}\right).\end{aligned}$$

The Lemma follows from the fact that the inner sum is N when $N|2ah$ and 0 when $N\nmid 2ah$. The former is equivalent to $\frac{N}{(2a,N)}|h$ which happens exactly for $(2a,N)$ choices of h.

□

Lemma 10.3: Let α be any real number. For any $0<\epsilon<1/3$ and $Q\ge Q_0(\epsilon)$, there is a rational number c/q^2 such that $q\le Q$ and

$$\left|\alpha-\frac{c}{q^2}\right|<\frac{1}{q^2Q^{1/3-\epsilon}}. \tag{10.3}$$

Proof: Note that we no longer claim $(c,q)=1$. Better results than the stated are known, namely Heilbronn proved 1/2, and recently Zaharescu proved 4/7 in place of 1/3 in (10.3).

We start with Dirichlet's approximation theorem used for a parameter R (the optimal choice is going to be $R \approx Q^{4/3}$). Like in (10.2) there is a rational number a/r, $(a,r)=1$, $r \le R$ such that

$$\left|\alpha - \frac{a}{r}\right| < \frac{1}{rR}.$$

If $r \le Q$ then simply choose $q=r$ and $c=ar$ getting

$$\left|\alpha - \frac{c}{q^2}\right| < \frac{1}{rR} \le \frac{Q}{q^2 R}. \tag{10.4}$$

If $Q < r \le R$ then we look for a solution to

$$aq^2 \equiv \ell \pmod{r}, \quad q \le Q, \quad |\ell| \le L. \tag{10.5}$$

Suppose we have a solution to (10.5). (The optimal choice is going to be $L \approx r/Q^{1/3}$.) This means that $aq^2 - cr = \ell$ with some integer c, and we have

$$\left|\alpha - \frac{c}{q^2}\right| \le \left|\alpha - \frac{a}{r}\right| + \frac{|aq^2 - cr|}{q^2 r} < \frac{1}{rR} + \frac{L}{q^2 r} \le \frac{1}{q^2}\left(\frac{Q}{R} + \frac{L}{r}\right). \tag{10.6}$$

We detect M, the number of solutions to (10.5) by trigonometric sums, as we did while proving Theorem 5.6. We have

$$M = \frac{1}{r}\sum_{x \in \mathbb{Z}_r}\sum_{q \le Q}\sum_{|\ell| \le L} e\left(\frac{(aq^2-\ell)x}{r}\right) = \frac{1}{r}\sum_{x \in \mathbb{Z}_r}\sum_{q \le Q} e\left(\frac{aq^2 x}{r}\right)\sum_{|\ell| \le L} e\left(\frac{-\ell x}{r}\right). \tag{10.7}$$

The term $x=0$ contributes $Q(2L+1)/r$. For the remaining $0 < |x| \le r/2$ we estimate the two inner sums individually. The last sum is a geometric sequence and we have

$$\left|\sum_{|\ell| \le L} e(\frac{\ell x}{r})\right| = \left|\frac{e(\frac{(2L+1)x}{r}) - 1}{e(\frac{x}{r}) - 1}\right| = \left|\frac{\sin(\pi\frac{(2L+1)x}{r})}{\sin(\pi\frac{x}{r})}\right| \le \frac{r}{2|x|}, \tag{10.8}$$

by $|\sin \pi y| \ge 2|y|$ if $|y| \le \frac{1}{2}$. As for the sum over q, we relate it to Lemma 10.2. Note that $Q < r$ and $(a,r)=1$. We have

$$\left|\sum_{q \le Q} e\left(\frac{aq^2 x}{r}\right)\right| = \frac{1}{r}\left|\sum_{y \in \mathbb{Z}_r}\sum_{m \in \mathbb{Z}_r}\sum_{q \le Q} e\left(\frac{am^2 x}{r}\right) e\left(\frac{(m-q)y}{r}\right)\right| \le$$

$$\le \frac{1}{r}\sum_{y \in \mathbb{Z}_r}\left|\sum_{m \in \mathbb{Z}_r} e\left(\frac{axm^2 + ym}{r}\right)\right|\left|\sum_{q \le Q} e\left(\frac{-qy}{r}\right)\right|.$$

The last sum is a geometric sequence again, and estimated by (10.8), while the sum over m is estimated by Lemma 10.2. We get

$$\left|\sum_{q\le Q} e\left(\frac{aq^2x}{r}\right)\right| \le \frac{1}{r}\sqrt{(2ax,r)\,r}\,Q + \frac{1}{r}\sum_{0<|y|\le r/2}\sqrt{(2ax,r)\,r}\frac{r}{2|y|} \le \sqrt{(2x,r)\,r}(1+\log r).$$

Writing back everything to M, we arrive at

$$\left|M - \frac{Q(2L+1)}{r}\right| \le \frac{1}{r}\sum_{0<|x|\le r/2}\sqrt{(2x,r)\,r}(1+\log r)\frac{r}{2|x|} \le r^{1/2+\epsilon},$$

where the last inequality follows from the estimate

$$\sum_{x\le r}\frac{\sqrt{(x,r)}}{x} \le r^{\epsilon}, \tag{10.9}$$

which is discussed in Appendix 1. The required solution to (10.5) is granted if $QL \ge r^{3/2+\epsilon}$, that is $L \approx r^{3/2+\epsilon}/Q$. Finally (10.4) and (10.6) guarantee

$$\left|\alpha - \frac{c}{q^2}\right| \le \frac{1}{q^2}\left(\frac{Q}{R} + \frac{r^{1/2+\epsilon}}{Q}\right) < \frac{1}{q^2Q^{1/3-\epsilon}},$$

if $r \le R \approx Q^{4/3}$.

□

Lemma 10.4: Let $P \subset \mathbb{Z}_N$ be an arithmetic progression of $L \le N$ elements. We can partition P into arithmetic progressions P_j of size $|P_j| = L^{1/40} + O(1)$ such that (for all j)

$$\left|e\left(\frac{a\ell_1^2 + b\ell_1}{N}\right) - e\left(\frac{a\ell_2^2 + b\ell_2}{N}\right)\right| \le \frac{4\pi}{L^{1/40}}, \tag{10.10}$$

whenever $\ell_1, \ell_2 \in P_j$.

Proof: Note that the number of subprogressions $M \approx L^{39/40}$. Needless to say, the exponent $1/40$ is a comfortable choice, but not an optimal one. Without loss of generality we may suppose that $P = \{1, \dots, L\}$. From Lemma 10.3 there is a rational number c/q^2, $q \le L^{7/10}$ such that ($\epsilon = 1/120$)

$$\left|\frac{a}{N} - \frac{c}{q^2}\right| < \frac{1}{q^2L^{9/40}}, \quad \frac{a}{N} = \frac{c}{q^2} + \frac{\Theta}{q^2L^{9/40}}, \tag{10.11}$$

where $|\Theta| \le 1$. Split the set $\{1, \dots, L\}$ into residue classes mod q, and split all residue classes into $L^{9/10}/q + O(1)$ intervals of length $L^{1/10} + O(1)$. These arithmetic progressions

are denoted by Q_i with $i = 1, \dots, I$, $I \approx R^{9/10}$. For any fixed i, Q_i looks like $\{qm + v : m \le R_i = L^{1/10} + O(1)\}$. We can write $\ell = qm + v$ and

$$\frac{a\ell^2 + b\ell}{N} = \frac{a(qm+v)^2 + b(qm+v)}{N} =$$
$$= \frac{aq^2m^2}{N} + \frac{(2aqv + bq)m + av^2 + bv}{N} =$$
$$= cm^2 + \frac{\Theta m^2}{L^{9/40}} + \frac{(2aqv + bq)m + av^2 + bv}{N},$$

or, writing $a' = 2aqv + bq$

$$\left| e\left(\frac{a\ell_1^2 + b\ell_1}{N}\right) - e\left(\frac{a\ell_2^2 + b\ell_2}{N}\right)\right| =$$
$$= \left| e\left(\frac{a'm_1}{N} + \frac{\Theta m_1^2}{L^{9/40}}\right) - e\left(\frac{a'm_2}{N} + \frac{\Theta m_2^2}{L^{9/40}}\right)\right| \le$$
$$\le \left| e\left(\frac{a'm_1}{N}\right) - e\left(\frac{a'm_2}{N}\right)\right| + \frac{2\pi R_i^2}{L^{9/40}}.$$

Now Lemma 10.1 says that Q_i can be split into M_i arithmetic progressions of length $R_i^{1/4} + O(1) = L^{1/40} + O(1)$ such that in each of these arithmetic progressions

$$\left| e\left(\frac{a'm_1}{N}\right) - e\left(\frac{a'm_2}{N}\right)\right| \le \frac{2\pi}{R_i^{1/4}} \le \frac{2\pi}{L^{1/40}}.$$

This proves the Lemma.

□

It is important to stress that the arithmetic progressions guaranteed by Lemma 10.1 and 10.4 are in $\mathbb{Z}_N$ and not in $\mathbb{Z}$. For example, although it does not look like, the set $\{1, 2, 8\}$ is a 3–term arithmetic progression mod 13 (with difference 7). Our last statement claims, that such sets can further split to get genuine arithmetic progressions. The argument is very similar to the proof of Lemma 10.1.

Lemma 10.5: Let $P \subset \mathbb{Z}_N$ be an arithmetic progression of $R \le N$ elements. We can partition P into $\le 3R^{1/2}$ genuine arithmetic progressions, each are $\subset \{1, \dots, N\}$.

Proof: Let the progression P be $\{am + b : m = 1, \dots, R\}$. By Dirichlet's approximation theorem we find a rational number c/q with $(c, q) = 1$ and $q \le R^{1/2}$ such that

$$\left|\frac{a}{N} - \frac{c}{q}\right| \le \frac{1}{qR^{1/2}}, \quad aq = cN + t, \quad |t| \le \frac{N}{R^{1/2}}.$$

Split P into q progressions according to the residue of m mod q. Thus $P_j = \{a(q\ell + j) + b : 1 \le q\ell + j \le R\}$ for $j = 1, \dots, q$. Thanks to the choice of q we also have $P_j = \{t\ell + aj + b\}$ with the same condition on the range of ℓ. Since $t\ell$ changes at most $\le |t|R/q \le NR^{1/2}/q$, P_j intersects at most $2 + R^{1/2}/q$ intervals of the form $\{kN+1, \dots, (k+1)N\}$, and so P_j can be split into that many genuine arithmetic progressions $\subset \{1, \dots, N\}$. Thus P itself can be split into at most $\le 2q + R^{1/2} \le 3R^{1/2}$ genuine arithmetic progressions $\subset \{1, \dots, N\}$.

□

CHAPTER 11

ARITHMETIC PROGRESSIONS OF LENGTH 3

In this chapter we prove the $k = 3$ case of Szemerédi's theorem. The proof is originated from the circle method, developed by Hardy and Littlewood in the 1910's and later elaborated by many mathematicians. We list some of the important milestones along this development.

- Waring problem, for each integer $k \geq 2$ there is an integer $s = s(k)$ such that every positive integer is a sum of at most s positive k–powers. (This was first proved by Hilbert, later Hardy and Littlewood developed the circle method to give a different proof.)
- Ternary Goldbach problem, every sufficiently large odd integer is a sum of three primes. (Vinogradov)
- There are infinitely many 3–term arithmetic progressions in primes. (van der Corput)
- Statistical binary Goldbach problem, almost all even integer is a sum of two primes. (Chudakov)
- $k = 3$ case of Szemerédi's theorem, a dense set of integers contains 3–term arithmetic progressions. (Roth)
- If A is dense, then $A - A$ contains infinitely many squares. (Sárközy)

One can look for the background of the circle method in Fourier analysis, we instead reduce the explanation to the simple fact that the integral of the sin and cos functions over a full period is zero. This immediately implies for any integer n that

$$\int_0^1 e(n\alpha)\, d\alpha = \begin{cases} 1 \text{ if } n = 0, \\ 0 \text{ if } n \neq 0. \end{cases} \tag{11.1}$$

This integral is an excellent tool to test if an integer is zero or not, for example, if $a+c-2b$ is zero or not, that is if the integers a, b, c form a 3–term arithmetic progression or not. The name of the method reflects that this integral is over the unit circle, if we consider it on the complex plane. Suppose we wish to prove van der Corput's result, that is the infinitude of 3–term arithmetic progressions in primes. For a (large) number N we define

$$P(\alpha) = \sum_{p \leq N} e(p\alpha), \tag{11.2}$$

where the sum is over the primes. We start with the integral

$$S =: \int_0^1 (P(\alpha))^2 P(-2\alpha)\, d\alpha = \int_0^1 \sum_{p_1 \leq x} e(p_1\alpha) \sum_{p_3 \leq N} e(p_3\alpha) \sum_{p_2 \leq N} e(-2p_2\alpha)\, d\alpha =$$

$$= \sum_{p_1 \leq N} \sum_{p_2 \leq N} \sum_{p_3 \leq N} \int_0^1 e((p_1 + p_3 - 2p_2)\alpha)\, d\alpha = \sum_{p_1+p_3=2p_2,\, p_j \leq N} 1.$$

S counts the 3–term arithmetic progressions in primes $\leq N$, including the $\pi(N)$ trivial progressions $p_1 = p_2 = p_3$. We have to compute this integral. There are just enough analytic information about $P(\alpha)$ to compute an asymptotic estimate to the integral, for example, the primes are uniformly distributed in the reduced residue classes mod q, resulting an asymptotic expansion of $P(a/q)$ for small q. Another argument results an upper bound of $P(\alpha)$ for all α not close to a rational number with small denominator. This makes the method so delicate, the integral is split into *major arcs*, where $P(\alpha)$ is big, around rational numbers with small denominator, and into *minor arcs*, where it is small. A detailed proof uses several deep results from analytic number theory.

The case of Roth theorem is somewhat different. Suppose that $A \subset \{1, \dots, N\}$ is a big set, and imagine that p runs over the elements of A in (11.2). S counts the 3–term arithmetic progressions in A (including the $|A|$ trivial ones). However, we know very little about the function $P(\alpha)$ this time. Nevertheless we can try to follow the above pattern and we can trace the arcs, where our function is big. It is a little easier to do that in discrete points, so (11.1) is changed to (for simplicity N is a big prime)

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} e(\frac{nx}{N}) = \begin{cases} 1, \text{ if } n \equiv 0 \pmod{N}, \\ 0, \text{ if } n \not\equiv 0 \pmod{N}. \end{cases} \tag{11.3}$$

Introducing the Fourier coefficient of A (instead of $P(\alpha)$ above)

$$\widehat{A}(x) = \sum_{a \in A} e(\frac{ax}{N}), \tag{11.4}$$

the expression to study is the following.

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} \left(\widehat{A}(x)\right)^2 \widehat{A}(-2x) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} \sum_{a_1 \in A} e(\frac{a_1 x}{N}) \sum_{a_3 \in A} e(\frac{a_3 x}{N}) \sum_{a_2 \in A} e(\frac{-2a_2 x}{N}) =$$

$$= \sum_{a_1 \in A} \sum_{a_2 \in A} \sum_{a_3 \in A} \frac{1}{N} \sum_{x \in \mathbb{Z}_N} e(\frac{(a_1 + a_3 - 2a_2)x}{N}) = \sum_{a_1 + a_3 \equiv 2a_2 \, (N), \, a_j \in A} 1.$$

Rather than the genuine 3–term arithmetic progressions, this counts the mod N progressions in A. This is a small problem, there are several ways to remedy. The bigger problem is that we cannot estimate $\widehat{A}(x)$ at all, if we know nothing about the distribution of A. For example, in Chapter 5 we have used the circle method (though we did not call it like this), in the proof of Theorem 5.6, the single point $x = 0$ played the role of 'major arcs', while Lemma 5.5 provided the necessary upper bound on the 'minor arcs'. Obviously, this is no help here, nothing like Lemma 5.5 can be proved for the Fourier coefficient of a general set A. The ingenious idea of Roth is, that either $x = 0$ is the only 'major arc' again, or there should be some irregularity in the distribution of A, and one can find a (long) arithmetic progression in which the density of A is substantially bigger than that of in $\{1, \dots, N\}$.

After this long preparation we can move to the detailed proof.

Theorem 11.1: (Roth, 1953) Let $\delta > 0$ be given. There is an $N(\delta)$ such that any set of integers $A \subset \{1, \dots, N\}$, $|A| \geq \delta N$ contains non trivial 3–term arithmetic progressions if $N \geq N(\delta)$.

Proof: We can suppose that $|A| = \delta N$, and that N is a prime (actually, any odd integer serves equally well). Let B be the set of odd or even elements of A, whichever is more numerous. Obviously $|B| \geq \frac{\delta}{2}N$. $\widehat{A}(x)$ is the Fourier coefficient of A defined in (11.4), and similarly

$$\widehat{B}(x) = \sum_{a\in B} e(\frac{ax}{N}).$$

Suppose that $a_1, a_3 \in B$, $a_2 \in A$. Since $a_1 + a_3 \equiv 0 \pmod 2$, we know that $a_1 + a_3 \equiv 2a_2 \pmod N$ implies $a_1 + a_3 - 2a_2 \equiv 0 \pmod{2N}$. However $-2N < a_1 + a_3 - 2a_2 < 2N$, and we conclude that $a_1 + a_3 = 2a_2$. That is

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\Big(\widehat{B}(x)\Big)^2\widehat{A}(-2x) = \sum_{a_1+a_3=2a_2,\, a_1,a_3\in B,\, a_2\in A} 1 \leq \sum_{a_1+a_3=2a_2,\, a_j\in A} 1.$$

The term $x = 0$ contribute to the left hand side

$$\frac{|B|^2|A|}{N} \geq \frac{\delta}{2}|A||B|,$$

while the rest contribute at most

$$\max_{y\neq 0}|\widehat{A}(y)|\,\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\Big|\widehat{B}(x)\Big|^2 = |B|\,\max_{y\neq 0}|\widehat{A}(y)|$$

by Parseval identity (Lemma 5.4). If we suppose that

$$\max_{y\neq 0}|\widehat{A}(y)| \leq \frac{\delta^2}{4}N = \frac{\delta}{4}|A| \tag{11.5}$$

then we conclude that

$$\sum_{a_1+a_3=2a_2,\, a_j\in A} 1 \geq \frac{\delta}{2}|A||B| - \max_{y\neq 0}|\widehat{A}(y)||B| \geq \frac{\delta}{4}|A||B| \geq \frac{\delta^3}{8}N^2. \tag{11.6}$$

The lower bound in (11.6) is bigger than $|A| = \delta N$ (when N is sufficiently large), the number of trivial 3–term arithmetic progressions, thus Theorem 11.1 is proved in case of (11.5) holds true. Note that (11.6) represents the expected lower bound (up to the constant multiple of 1/8).

We turn to the opposite case, where there is a residue class $y \neq 0$ such that $|\widehat{A}(y)| > \frac{\delta^2}{4}N$. With a little cosmetics we can claim this as

$$|\sum_{n\in\mathbb{Z}_N}\big(A(n)-\delta\big)e(\frac{yn}{N})| > \frac{\delta^2}{4}N, \quad \text{where} \quad A(n) = \begin{cases} 1 \text{ if } n \in A, \\ 0 \text{ if } n \notin A. \end{cases} \tag{11.7}$$

Note that in usual terms, $\widehat{A}(x)$ is the Fourier coefficient of the function $A(n)$. Since $\mathbb{Z}_N$ is an arithmetic progression of N elements, Lemma 10.1 says that $\mathbb{Z}_N$ can be split into

$M = N^{3/4} + O(N^{1/2})$ arithmetic progressions P_j of length $N^{1/4} + O(1)$ such that $e(yn/N)$ changes $\le 2\pi N^{-1/2}$ on each of them. By triangle inequality

$$\frac{\delta^2}{4}N < |\sum_j \sum_{n\in P_j} \big(A(n)-\delta\big)e(\frac{yn}{N})| \le \sum_j |\sum_{n\in P_j} \big(A(n)-\delta\big)e(\frac{yn}{N})| \le$$
$$\le \sum_j |\sum_{n\in P_j} \big(A(n)-\delta\big)| + \sum_{n\in\mathbb{Z}_N} \frac{2\pi}{N^{1/4}} \le \sum_j |\sum_{n\in P_j} \big(A(n)-\delta\big)| + 2\pi N^{3/4}.$$

As we trivially have (this is why we set $|A| = \delta N$)

$$\sum_j \sum_{n\in P_j} \big(A(n)-\delta\big) = \sum_{n\in\mathbb{Z}_N} \big(A(n)-\delta\big) = |A| - \delta N = 0,$$

we conclude that

$$\frac{\delta^2}{5}N < \sum_j \left(|\sum_{n\in P_j} \big(A(n)-\delta\big)| + \sum_{n\in P_j} \big(A(n)-\delta\big) \right).$$

Now $|X| + X = 0$ if $X \le 0$, while $|X| + X = 2X$ if $X \ge 0$, and we find a j such that

$$\sum_{n\in P_j} \big(A(n)-\delta\big) > \frac{\delta^2 N}{10M} > \frac{\delta^2}{11}N^{1/4}. \tag{11.8}$$

Note that P_j is an arithmetic progression mod N. By Lemma 10.5 we can split P_j into at most $K = 3|P_j|^{1/2} \le 4N^{1/8}$ genuine arithmetic progressions $Q_k \subset \{1,\dots,N\}$. Some of them can be too short, say $\mathcal{G}$ is the collection of those with length $\ge N^{1/16}$, while $\mathcal{B}$ is the collection of those with length $< N^{1/16}$. Obviously

$$\sum_{Q_k\in\mathcal{B}} \sum_{n\in Q_k} \big(A(n)-\delta\big) \le \sum_{Q_k\in\mathcal{B}} |Q_k| \le KN^{1/16} \le 4N^{3/16},$$

and we get that

$$\sum_{Q_k\in\mathcal{G}} \sum_{n\in Q_k} \big(A(n)-\delta\big) \ge \frac{\delta^2}{12} \sum_{Q_k\in\mathcal{G}} |Q_k|.$$

This means that there is an arithmetic progression Q_k with length $\ge N^{1/16}$ such that $|A\cap Q_k| = \sum_{n\in Q_k} A(n) \ge (\delta + \frac{\delta^2}{12})|Q_k|$. If we write $Q_k = \{a + \ell b : \ell = 1,\dots,N_1\}$ and define $A_1 = \{\ell : a+\ell b \in A\cap Q_k\} \subset \{1,\dots,N_1\}$, $|A_1| = \delta_1 N_1$ then $N_1 \ge N^{1/16}$ and $\delta_1 \ge \delta(1+\frac{\delta}{12})$, moreover if R is an arithmetic progression (of any length) in A_1 then $a + b\cdot R$ is an arithmetic progression of the same length in A. We have better chance when we repeat the whole argument with A_1, as δ_1 is substantially bigger than δ. If it is still not conclusive then we find an

$$A_2 \subset \{1,\dots,N_2\}, \quad \delta_2 \ge \delta_1(1+\frac{\delta_1}{12}) \ge \delta(1+\frac{\delta}{12})^2, \quad N_2 \ge N_1^{1/16} \ge N^{(1/16)^2},$$

and so on. After j steps we find an

$$A_j \subset \{1, \dots, N_j\}, \quad \delta_j \geq \delta(1 + \frac{\delta}{12})^j, \quad N_j \geq N^{(1/16)^j}.$$

However, this is not possible for large j, for example, if $j \geq \frac{12}{\delta^2}$ then trivially

$$\delta_j \geq \delta(1 + \frac{\delta}{12})^j \geq \delta(1 + \frac{j\delta}{12}) \geq 1 + \delta$$

and this is not consistent with $N_j > N_0$. That is, for some $j \leq \frac{12}{\delta^2}$, A_j must satisfy (11.5) and so (11.6) with a large N.

□

We summarize the structure of the proof. If the Fourier coefficients of $A(n) - \delta$ are all small, then we have the expected number of 3–term arithmetic progressions. If not, that is (11.5) is not true, than A has a certain *linear bias*, namely $A(n) - \delta$ correlates with $e(yn/N)$, this is reflected in the inequality (11.7). Finally this linear bias implies irregular distribution of A, this is reflected in the density increment as expressed in (11.8). An iteration closes the proof. For k–term arithmetic progressions we have to introduce the Gowers' uniformity norms, they will take the role of the Fourier coefficients (Chapter 12). If the U^{k-1} norm of $A(n) - \delta$ is small, then we have the expected number of k–term arithmetic progressions. If not, than A has a certain *higher order bias*, that is $A(n) - \delta$ shows a weak correlation with $e(\Psi(n)/N)$ where $\Psi(n)$ is a polynomial over $\mathbb{Z}_N$ of degree $k - 2$. Finally this higher order bias leads to irregular distribution of A, eventually leads to density increment. (Chapter 13 discusses the case of $k = 4$.)

The above proof makes possible to express $N(\delta)$. Note, that N_j is still a (small) power of N if δ is fixed, however tracing the speed of the diminishing of N_j one can even let δ be a function of N. It is highly recommended to double check the last steps of the calculation to prove that *any set of integers $A \subset \{1, \dots, N\}$ contains non trivial 3–term arithmetic progressions if*

$$|A| \geq \frac{CN}{\log \log N},$$

with a sufficiently large constant C.

The best result in this direction is due to Sanders and proves the same result with

$$|A| \gg \frac{N(\log \log N)^C}{\log N},$$

with some explicit large constant C. On the other hand examples are known for a set $A \subset \{1, \dots, N\}$ with no 3–term arithmetic progression and size

$$|A| \geq \frac{N}{e^{c\sqrt{\log N}}}.$$

The first such example is due to Behrend and worked out in the homework problems. Recent constructions are improvements only on the numerical value of c.

CHAPTER 12

GOWERS' NORMS

Let N be a (large) prime, $A \subset \mathbb{Z}_N$ be a set of residue classes mod N, and $A(n)$ is the indicator function of the set A. The number of 3–term arithmetic progressions in A can be computed by evaluating

$$S = \sum_n \sum_d A(n)A(n+d)A(n+2d), \tag{12.1}$$

or k–term arithmetic progressions by

$$S_k = \sum_n \sum_d A(n)A(n+d)\cdots A(n+(k-1)d).$$

Here, and throughout the last chapters every sums are over $\mathbb{Z}_N$ unless otherwise specified. It was Tim Gowers who recognized the connection between (12.1) and the following average

$$U = \frac{1}{N^3} \sum_a \sum_b \sum_c A(a)A(a+b)A(a+c)A(a+b+c).$$

One term in this sum consists of a product of four copies of the function $A(n)$ taken on the vertices of a 2–dimensional cube, and U is the average over all such cubes. Before the systematic work, let us see the connection between S and U, that needs no more than a couple of Cauchy–Schwarz inequalities. To follow better what we do, we generalize S slightly. Let $f_j : \mathbb{Z}_N \to \mathbb{C}$ be three functions satisfying $|f_j(n)| \le 1$, and we study

$$S = \sum_n \sum_d f_1(n)f_2(n+d)f_3(n+2d),$$
$$U(f) = \frac{1}{N^3} \sum_a \sum_b \sum_c f(a)\overline{f(a+b)f(a+c)}f(a+b+c).$$

We start estimating S by a Cauchy–Schwarz inequality where n is 'out' and d is 'in'.

$$|S|^2 \le \left(\sum_n |f_1(n)| \left|\sum_d f_2(n+d)f_3(n+2d)\right|\right)^2 \le N \sum_n \left|\sum_d f_2(n+d)f_3(n+2d)\right|^2 =$$
$$= N \sum_n \sum_{d_1} \sum_{d_2} f_2(n+d_1)f_3(n+2d_1)\overline{f_2(n+d_2)f_3(n+2d_2)}.$$

We have got rid of f_1 and we can get rid of f_2 with another application of the Cauchy–Schwarz inequality. We do that after a change of variables $d_1 = u$, $n+d_1 = v$, $n+d_2 = v+w$, and so $n + 2d_1 = u + v$, $n + 2d_2 = u + v + 2w$. We have

$$|S|^2 \le N \sum_u \sum_v \sum_w f_2(v) f_3(u+v) \overline{f_2(v+w) f_3(u+v+2w)} \le$$

$$\le N \sum_v \sum_w |f_2(v) \overline{f_2(v+w)}| \Big| \sum_u f_3(u+v) \overline{f_3(u+v+2w)} \Big|,$$

$$|S|^4 \le N^4 \sum_v \sum_w \Big| \sum_u f_3(u+v) \overline{f_3(u+v+2w)} \Big|^2 =$$

$$= N^4 \sum_v \sum_w \sum_{u_1} \sum_{u_2} f_3(u_1+v) \overline{f_3(u_1+v+2w) f_3(u_2+v)} f_3(u_2+v+2w).$$

Another change of variables come, $u_1 + v = a$, $2w = b$, $u_2 + v = a + c$, and so $u_1 + v + 2w = a + b$, $u_2 + v + 2w = a + b + c$, moreover we keep the variable u_1, however, nothing depends on u_1 any more, so we arrive at

$$|S|^4 \le N^5 \sum_a \sum_b \sum_c f_3(a) \overline{f_3(a+b) f_3(a+c)} f_3(a+b+c) = N^8 \, U(f_3). \tag{12.2}$$

Especially $U(f)$ is non–negative and real, whatever the function f is, and we have proved that $|S| \le N^2 \, U(f_3)^{1/4}$. Actually, by symmetry or by different choices of the 'in' and 'out' roles in the Cauchy–Schwarz inequalities one can prove $|S| \le N^2 \, U(f_2)^{1/4}$ or $|S| \le N^2 \, U(f_1)^{1/4}$ as well.

Another interesting relation is the following. Recall the Fourier coefficients of the function $f(n)$

$$\widehat{f}(x) = \sum_n f(n) e(\frac{xn}{N}).$$

We can compute the fourth moment of the Fourier coefficients by (11.1)

$$\frac{1}{N} \sum_x |\widehat{f}(x)|^4 = \sum_{n_1+n_2=n_3+n_4} f(n_1) f(n_2) \overline{f(n_3) f(n_4)} = \tag{12.3}$$

$$= \sum_a \sum_b \sum_c f(a) \overline{f(a+b) f(a+c)} f(a+b+c) = N^3 \, U(f),$$

where we made a change of variables $n_1 = a$, $n_3 = a + b$, $n_4 = a + c$, and so $n_2 = a + b + c$.

Now we can argue for Roth theorem as follows. Let $f_1(n) = f_2(n) = B(n)$, $f_3(n) = A(n) - \delta = f(n)$ where $|A| = \delta N$ and $B \subset A$ is chosen appropriately (this is a little cosmetics, we have seen such a choice in Chapter 11, and we give another later, the purpose is to provide that mod N arithmetic progressions are actually genuine arithmetic progressions). We have by (12.2) that

$$\left| \sum_n \sum_d B(n) B(n+d) A(n+2d) - \delta |B|^2 \right| \le N^2 \, U(f)^{1/4} \le c \, \delta^3 N^2,$$

if $U(f) \le c^4\,\delta^{12}$. Note that trivially $U(f) \le 1$ since it is an average of a bounded function, so if it is somewhat smaller than trivially, then we have the right number of 3–term arithmetic progressions in A (by choosing $c > 0$ small enough in terms of the proportion of B in A). If this is not the case, that is $U(f)$ is big, then by (12.3) and by Parseval identity we get

$$c^4\,\delta^{12} < U(f) = \frac{1}{N^4}\sum_x |\widehat{f}(x)|^4 \le \frac{1}{N^3}\max_y |\widehat{f}(y)|^2 \frac{1}{N}\sum_x |\widehat{f}(x)|^2 =$$

$$= \frac{1}{N^3}\max_y |\widehat{f}(y)|^2 \sum_n |A(n) - \delta|^2 \le \frac{1}{N^2}\max_y |\widehat{f}(y)|^2,$$

and as $\widehat{f}(0) = 0$, there is an $y \neq 0$ such that $|\widehat{f}(y)| > c^2\,\delta^6\,N$. This is exactly as (11.7), we have traced the liner bias, one can complete the proof of Roth theorem just like in Chapter 11. We can handle the general case in the very same frame. The key step is the generalization of $U(f)$.

First we fix notation and notion. Any functions are of the type $f : \mathbb{Z}_N \to \mathbb{C}$, $|f| \le 1$, and we refer them as bounded functions. The Fourier coefficients of such a function are defined by (11.1), that is

$$\widehat{f}(x) = \sum_n f(n) e(\frac{xn}{N}).$$

The 'derivative', or 'difference' function is defined by a parameter $z \in \mathbb{Z}_N$ as

$$\triangle(f, z)(n) = f(n)\overline{f(n+z)}.$$

The U^k norm of such a function is defined by

$$\|f\|_{U^1}^2 = \frac{1}{N^2}\sum_a \sum_b f(a)\overline{f(a+b)},$$

$$\|f\|_{U^2}^4 = \frac{1}{N^3}\sum_a \sum_b \sum_c f(a)\overline{f(a+b)f(a+c)}f(a+b+c),$$

$$\|f\|_{U^3}^8 = \frac{1}{N^4}\sum_a \sum_b \sum_c \sum_d f(a)\overline{f(a+b)f(a+c)f(a+d)}\times$$

$$\times f(a+b+c)f(a+b+d)f(a+c+d)\overline{f(a+b+c+d)},$$

$$\vdots$$

$$\|f\|_{U^k}^{2^k} = \frac{1}{N^{k+1}}\underbrace{\sum_a \sum_b \cdots \sum_z}_{k+1} \underbrace{f(a)\cdots f(a+b+\cdots+z)}_{2^k}.$$

One term in the multiple sum is the product of 2^k copies of f or $\overline{f}$ taken at the vertices of a cube of dimension k, while the sum is taken over all such cubes. We say that a is the

corner of the cube, and $b, c, \dots, z$ are the sides. f or $\overline{f}$ appears according to the position of the vertices, formally it is f if its argument is a vertex of even number of steps away from the corner a, while it is $\overline{f}$ if its argument is a vertex of odd number of steps away from the corner a. We are going to use the word that $\|f\|_{U^k}$ is the Gowers U^k uniformity norm, actually $\|f\|_{U^1}$ is not a norm, as we see soon, and we do not justify the triangle inequality either, so strictly speaking we do not prove that $\|f\|_{U^k}$ is a norm for $k \geq 2$, although they are.

Lemma 12.1: We have the following relations.

$$\|f\|_{U^1}^2 = \left| \frac{1}{N} \sum_a f(a) \right|^2, \tag{12.4}$$

$$\|f\|_{U^2}^4 = \frac{1}{N^4} \sum_x |\widehat{f}(x)|^4, \tag{12.5}$$

$$\|f\|_{U^k}^{2^k} = \frac{1}{N} \sum_z \|\triangle(f,z)\|_{U^{k-1}}^{2^{k-1}}, \tag{12.6}$$

$$0 \leq \|f\|_{U^1} \leq \|f\|_{U^2} \leq \dots \leq \|f\|_{U^k} \leq \dots. \tag{12.7}$$

Proof: (12.4) trivially follows from the definition. Note that this shows, the U^1 uniformity norm is not a norm, it can be zero without f is identically zero. (12.5) is already proved in (12.3). (12.6) follows from the definition directly, but it is not so visible. Observe that a cube of dimension k with corner a and sides $b, c, \dots, z$ is actually the union of two cubes of dimension $k-1$, one with corner a and sides $b, c, \dots, y$, while the other with corner $a+z$ and sides $b, c, \dots, y$. Another view is that the second cube is the former cube translated with z. We can couple the factors $f(V)$ and $\overline{f(V+z)}$ into $\triangle(f,z)(V)$, where V is a vertex of even steps away from the corner a, or the factors $\overline{f(W)}$ and $f(W+z)$ into $\overline{\triangle(f,z)(W)}$, where W is a vertex of odd steps away from the corner a. We illustrate this process in the $k=3$ case, the one we are going to use in Chapter 13.

$$\begin{aligned}
\|f\|_{U^3}^8 = \frac{1}{N^4} \sum_a \sum_b \sum_c \sum_d f(a)\overline{f(a+b)f(a+c)f(a+d)} \times \\
\times f(a+b+c)f(a+b+d)f(a+c+d)\overline{f(a+b+c+d)} = \\
= \frac{1}{N} \sum_d \frac{1}{N^3} \sum_a \sum_b \sum_c \Big(f(a)\overline{f(a+d)} \Big) \Big(\overline{f(a+b)} f(a+b+d) \Big) \times \\
\times \Big(\overline{f(a+c)} f(a+c+d) \Big) \Big(f(a+b+c)\overline{f(a+b+c+d)} \Big) = \\
= \frac{1}{N} \sum_d \frac{1}{N^3} \sum_a \sum_b \sum_c \triangle(f,d)(a)\overline{\triangle(f,d)(a+b)\triangle(f,d)(a+c)}\triangle(f,d)(a+b+c) = \\
= \frac{1}{N} \sum_d \|\triangle(f,d)\|_{U^2}^4.
\end{aligned}$$

As for(12.7) the left most inequality follows from (12.4), for the rest we have to show that $\|f\|_{U^{k-1}} \le \|f\|_{U^k}$ which is equivalent to

$$\left(\|f\|_{U^{k-1}}^{2^{k-1}}\right)^2 \le \|f\|_{U^k}^{2^k}. \tag{12.8}$$

We estimate the left hand side of (12.8) with an application of the Cauchy–Schwarz inequality, where the corner of the cubes, a is 'in' and all sides are 'out'.

$$\left|\frac{1}{N^k}\underbrace{\sum_a\sum_b\cdots\sum_y}_{k}\underbrace{f(a)\cdots f(a+b+\cdots+y)}_{2^{k-1}}\right|^2 \le$$

$$\le \frac{N^{k-1}}{N^{2k}}\underbrace{\sum_b\sum_c\cdots\sum_y}_{k-1}\left|\sum_a\underbrace{f(a)\cdots f(a+b+\cdots+y)}_{2^{k-1}}\right|^2 =$$

$$= \frac{1}{N^{k+1}}\underbrace{\sum_{a_1}\sum_{a_2}\sum_b\cdots\sum_y}_{k+1}\underbrace{f(a_1)\cdots f(a_1+b+\cdots+y)}_{2^{k-1}}\underbrace{\overline{f(a_2)}\cdots\overline{f(a_2+b+\cdots+y)}}_{2^{k-1}}.$$

Writing $a_1 = a$ and $a_2 = a + z$ we get (12.8).

□

Lemma 12.2: For any $k \ge 2$

$$\left|\sum_n\sum_d f_1(n)f_2(n+d)\cdots f_k(n+(k-1)d)\right| \le N^2 \min_{j=1,\dots,k}\|f_j\|_{U^{k-1}}.$$

Proof: For $k = 2$ this is immediate from (12.4). For $k = 3$ we proved this statement in (12.2), although we do not need that here. The general statement follows by induction. We write S for the left hand side, and we start with an application of the Cauchy–Schwarz inequality

$$|S|^2 = \left|\sum_n\sum_d f_1(n)f_2(n+d)\cdots f_k(n+(k-1)d)\right|^2 \le$$

$$\le N\sum_n\left|\sum_d f_2(n+d)f_3(n+2d)\cdots f_k(n+(k-1)d)\right|^2 =$$

$$= N\sum_n\sum_{d_1}\sum_{d_2} f_2(n+d_1)f_3(n+2d_1)\cdots f_k(n+(k-1)d_1)\times$$

$$\times\overline{f_2(n+d_2)f_3(n+2d_2)\cdots f_k(n+(k-1)d_2)}.$$

We write $d_1 = d$, $n + d_1 = m$ and $d_2 - d_1 = b$. Observe that

$$f_2(n+d_1)\overline{f_2(n+d_2)} = \triangle(f_2, b)(m),$$
$$f_3(n+2d_1)\overline{f_3(n+2d_2)} = \triangle(f_3, 2b)(m+d),$$
$$\vdots$$
$$f_k(n+(k-1)d_1)\overline{f_k(n+(k-1)d_2)} = \triangle(f_k, (k-1)b)(m+(k-2)d).$$

When we write this into the above inequality we can use the induction hypothesis for every fixed b getting (somewhere in the chain of inequalities we estimate the minimum over j with any individual j, we write $(j-1)b = z$, we use $k-2$ Cauchy–Schwarz inequalities, or just one use of Hölder inequality, and we use (12.6))

$$|S|^2 \le N \sum_b \left(\sum_m \sum_d \triangle(f_2, b)(m)\triangle(f_3, 2b)(m+d)\cdots\triangle(f_k, (k-1)b)(m+(k-2)d) \right) \le$$
$$\le N \sum_b \left(N^2 \min_{j=2,\dots,k} \|\triangle(f_j, (j-1)b)\|_{U^{k-2}} \right) \le N^3 \sum_b \|\triangle(f_j, (j-1)b)\|_{U^{k-2}} \le$$
$$\le N^3 (N)^{1-\frac{1}{2^{k-2}}} \left(\sum_z \|\triangle(f_j, z)\|_{U^{k-2}}^{2^{k-2}} \right)^{\frac{1}{2^{k-2}}} = N^4 \left(\|f_j\|_{U^{k-1}}^{2^{k-1}} \right)^{\frac{1}{2^{k-2}}}.$$

We get $|S| \le N^2 \|f_j\|_{U^{k-1}}$ and this is true for all $j = 2, \dots, k$, so this is true for the smallest of them. To include $j = 1$ as well, one can do the same analysis, but start with rewriting the sum $n + (k-1)d \mapsto n$ and $-d \mapsto d$ resulting

$$S = \sum_n \sum_d f_k(n) f_{k-1}(n+d)\cdots f_1(n+(k-1)d)$$

and thus we get $|S| \le N^2 \|f_j\|_{U^{k-1}}$ for all $j = 1, \dots, k-1$. The statement follows.

□

Lemma 12.3: For any $k \ge 2$, and $A \subset \{1, \dots, N\}$ we define $B = \{a \in A : \frac{k-2}{2k-3} N < a \le \frac{k-1}{2k-3} N\}$. If there are $n, d \in \mathbb{Z}_N$, $a_0, a_1 \in B$ and $a_2, \dots, a_{k-1} \in A$ such that $n + jd \equiv a_j \pmod N$ for $j = 0, \dots, k-1$ then $a_0, \dots, a_{k-1}$ form a genuine k–term arithmetic progression.

Proof: We can restrict ourselves to the case when $0 < n, d \le N$ and so $0 < n + d \le 2N$. Thus the congruence $n + d \equiv a_1 \pmod N$ leaves only two possibilities open, namely either $\frac{k-2}{2k-3} N < n + d \le \frac{k-1}{2k-3} N$ or $N + \frac{k-2}{2k-3} N < n + d \le N + \frac{k-1}{2k-3} N$. Similarly the congruence $n \equiv a_0 \pmod N$ implies $\frac{k-2}{2k-3} N < n \le \frac{k-1}{2k-3} N$. These inequalities imply in the first case that $0 < d \le \frac{1}{2k-3} N$ and in the second case $N - \frac{1}{2k-3} N < d \le N$. Moreover for all $j = 1, \dots, k-1$ we have in the first case that $\frac{k-2}{2k-3} N < n + jd \le \frac{k-1}{2k-3} N + \frac{j-1}{2k-3} N \le N$,

and in the second case $0 \leq \frac{k-2}{2k-3} N - \frac{j-1}{2k-3} N < n + j(d-N) \leq \frac{k-1}{2k-3} N$. Finally the congruence conditions imply that for all $j = 0, \ldots, k-1$, in the first case $a_j = n + jd$ and in the second case $a_j = n + j(d-N)$. In either case $a_0, \ldots, a_{k-1}$ form a genuine k–term arithmetic progression.

□

CHAPTER 13

ARITHMETIC PROGRESSIONS OF LENGTH 4

Theorem 13.1: (Szemerédi, 1969) Let $\delta > 0$ be given. There is an $N(\delta)$ such that any set of integers $A \subset \{1, \dots, N\}$, $|A| \geq \delta N$ contains non trivial 4–term arithmetic progressions if $N \geq N(\delta)$.

Proof: We can suppose that N is a prime and $|A| = \delta N$. We use the notation of Chapter 12, especially $A(n)$ is the indicator function of A (defined on $\mathbb{Z}_N$) and $f(n) = A(n) - \delta$. We follow the proof of Tim Gowers, and the interested reader is invited to check the details of the remaining cases ($k \geq 5$) in his original paper [W. T. Gowers, A new proof of Szemerédi's theorem, Geom. Funct. Anal. **11** (2001), 465–588.]. As we see soon, the case $k = 4$ is substantially more involved as the case $k = 3$. The general case can be attacked in the present way, but again, some more difficulties rise.

The points $\frac{2}{5}N$ and $\frac{3}{5}N$ splits A into three parts, A_1, B, and A_2, where B consists of the elements of A in the central interval. Either $|B| \geq \frac{1}{9}\delta N$ or one of A_1 and A_2 has $\geq \frac{4}{9}\delta N$ elements. In the latter case there is an arithmetic progression P (an interval actually) of length $\frac{2}{5}N$ such that $|A \cap P| \geq \frac{10}{9}\delta |P|$. As in Chapter 11, this density increment cannot be repeated too many times, sooner or later the first case must hold, and we can suppose it holds immediately, that is $|B| \geq \frac{1}{9}\delta N$. Let $B(n)$ be the indicator function of the set B (defined on $\mathbb{Z}_N$).

We are interested in computing

$$S =: \sum_n \sum_d B(n)B(n+d)A(n+2d)A(n+3d). \tag{13.1}$$

Lemma 12.3 says that, if $S > |B|$ then A contains a genuine non–trivial 4–term arithmetic progression. Lemma 12.2 relates S to the U^3 and U^2 norms of the function $f(n)$, more precisely

$$\left| \sum_n \sum_d B(n)B(n+d)A(n+2d)A(n+3d) - \delta^2 |B|^2 \right| \leq \tag{13.2}$$

$$\leq \left| \sum_n \sum_d B(n)B(n+d)A(n+2d)f(n+3d) \right| + \delta \left| \sum_n \sum_d B(n)B(n+d)f(n+2d) \right| \leq$$

$$\leq N^2 \|f\|_{U^3} + \delta N^2 \|f\|_{U^2}.$$

Since $\|f\|_{U^2} \leq \|f\|_{U^3}$ by (12.7) of Lemma 12.1, and since $\delta^2 |B|^2 \geq \frac{1}{81}\delta^4 N^2$, which is the expected number of 4-term arithmetic progressions in A, $\|f\|_{U^3} \leq \frac{1}{200}\delta^4$ implies

$$S = \sum_n \sum_d B(n)B(n+d)A(n+2d)A(n+3d) \geq \frac{1}{500}\delta^4 N^2.$$

It remains to study the opposite case, that is if

$$\|f\|_{U^3} \geq \frac{\delta^4}{200}. \tag{13.3}$$

Note that we have seen in Chapter 12 and 11 how a big U^2 norm leads to density increment. However, it is possible to construct an example to show that the U^2 norm can be small while the U^3 norm is big. The real difficulty of the proof is to find some weak structure in A derived from (13.3).

Lemma 12.1, more precisely (12.6) implies that

$$\sum_z \|\triangle(f,z)\|_{U^2}^4 \geq \left(\frac{\delta^4}{200}\right)^8 N = \frac{\delta^{32}}{2560000000000000000} N. \tag{13.4}$$

Unfortunately we are forced to compute several estimates like this later on. To simplify the exposition, we introduce a notation. $X \ll Y$ abbreviates that there is an absolute constant $C > 0$ such that $|X| \leq CY$. It is indeed practical, for example, $2\pi X + \sqrt{X} \sin X \ll X$. The exponent of δ also grow very fast in these estimates, and we do not want to keep track of it, we will simply write δ^c for any explicitly calculable power of δ. With this convention (13.4) reads like

$$\sum_z \|\triangle(f,z)\|_{U^2}^4 \gg \delta^c N, \tag{13.4}$$

of course, c is not a fixed number, it can be different at each occurrence.

Lemma 8.3, the simple averaging argument says, that there is a subset $\mathcal{Z} \subset \mathbb{Z}_N$, such that $|\mathcal{Z}| \gg \delta^c N$ and

$$\|\triangle(f,z)\|_{U^2} \gg \delta^c, \quad \text{for all} \quad z \in \mathcal{Z}. \tag{13.5}$$

Exactly as in Chapter 12, this implies that for all $z \in \mathcal{Z}$ there is a $y = \phi(z)$ such that

$$|\widehat{\triangle(f,z)}(y)| \gg \delta^c N, \quad \text{for all} \quad z \in \mathcal{Z},\, y = \phi(z). \tag{13.6}$$

Of course, given z there can be several y satisfying (13.6), in that case just fix any of them as $\phi(z)$. Surprisingly enough, this flexibility of choosing the values of the function ϕ will not block us to prove that ϕ is 'almost' a linear function.

We have from (13.6) that ($f(x)$ is real valued this time, and once we write $y = x + u$)

$$\begin{aligned}
\delta^c N^3 &\ll \sum_{z\in\mathcal{Z}} |\widehat{\triangle(f,z)}(\phi(z))|^2 = \\
&= \sum_{z\in\mathcal{Z}} \sum_x \sum_y f(x)f(x+z)f(y)f(y+z)e\left(\frac{(x-y)\phi(z)}{n}\right) = \\
&= \sum_x \sum_u f(x)f(x+u) \sum_{z\in\mathcal{Z}} f(x+z)f(x+u+z)e\left(\frac{u\phi(z)}{N}\right) \leq \\
&\leq \sum_x \sum_u \left| \sum_{z\in\mathcal{Z}} \triangle(f,u)(x+z)e\left(\frac{u\phi(z)}{N}\right)\right|.
\end{aligned}$$

Temporarily we fix u and consider the sum over x and z only. Our plan is to completely get rid of f, that is of $\triangle(f,u)$ by a couple of Cauchy–Schwarz inequalities.

$$T_u^2 =: \left(\sum_x \left|\sum_{z\in\mathcal{Z}} \triangle(f,u)(x+z)e\left(-\frac{u\phi(z)}{N}\right)\right|\right)^2 \leq$$

$$\leq N\sum_x \left|\sum_{z\in\mathcal{Z}} \triangle(f,u)(x+z)e\left(-\frac{u\phi(z)}{N}\right)\right|^2 =$$

$$= N\sum_x \sum_{z_1\in\mathcal{Z}}\sum_{z_2\in\mathcal{Z}} \triangle(f,u)(x+z_1)\triangle(f,u)(x+z_2)e\left(\frac{u\phi(z_1)-u\phi(z_2)}{N}\right).$$

For fixed z_1 and z_2 we write the sum over x in the following (strange) form using (11.3), the circle method

$$\sum_x \triangle(f,u)(x+z_1)\triangle(f,u)(x+z_2) =$$

$$= \frac{1}{N}\sum_v\sum_w\sum_t \triangle(f,u)(v)\triangle(f,u)(w)e\left(\frac{t(v-w+z_1-z_2)}{N}\right) =$$

$$= \frac{1}{N}\sum_t \left|\sum_v \triangle(f,u)(v)e(\frac{tv}{N})\right|^2 e\left(\frac{tz_1-tz_2}{N}\right).$$

Putting back into its place we arrive at

$$T_u^{=} \left(\sum_x \left|\sum_{z\in\mathcal{Z}} \triangle(f,u)(x+z)e\left(-\frac{u\phi(z)}{N}\right)\right|\right)^2 \leq$$

$$\leq \sum_t \left|\sum_v \triangle(f,u)(v)e(\frac{tv}{N})\right|^2 \sum_{z_1\in\mathcal{Z}}\sum_{z_2\in\mathcal{Z}} e\left(\frac{tz_1-tz_2+u\phi(z_1)-u\phi(z_2)}{N}\right).$$

This inequality is of the form $T_u^2 \leq \sum_t |V_t|^2 Z_{t,u}$, while we are interested in an upper bound of $\sum_u T_u$. Trivially $|V_t| \leq N$, and some more Cauchy–Schwarz inequalities lead to

$$\delta^c N^3 \ll \sum_u T_u \leq \left(N\sum_u T_u^2\right)^{1/2} \leq \left(N\sum_u\sum_t |V_t|^2 Z_{t,u}\right)^{1/2} \leq$$

$$\leq \left(N^2\sum_u\sum_t |V_t||Z_{t,u}|\right)^{1/2} \leq N\left(\sum_u\sum_t |V_t|^2 \sum_u\sum_t |Z_{t,u}|^2\right)^{1/4}.$$

The first sum over u is simply N, moreover by Parseval identity

$$\sum_t |V_t|^2 = \sum_t \left|\sum_v \triangle(f,u)(v)e(\frac{tv}{N})\right|^2 = N\sum_v |\triangle(f,u)(v)|^2 \leq N^2,$$

and finally we conclude that

$$\delta^c N^5 \ll \sum_u \sum_t |Z_{t,u}|^2 = \sum_u \sum_t \left| \sum_{z_1 \in \mathcal{Z}} \sum_{z_2 \in \mathcal{Z}} e\left(\frac{tz_1 - tz_2 + u\phi(z_1) - u\phi(z_2)}{N} \right) \right|^2 =$$

$$= \sum_u \sum_t \sum_{z_1,z_2,z_3,z_4 \in \mathcal{Z}} e\left(\frac{t(z_1 - z_2 - z_3 + z_4) + u(\phi(z_1) - \phi(z_2) - \phi(z_3) + \phi(z_4))}{N} \right) =$$

$$= N^2 \#\{z_1, z_2, z_3, z_4 \in \mathcal{Z} : \, z_1 + z_4 = z_2 + z_3, \, \phi(z_1) + \phi(z_4) = \phi(z_2) + \phi(z_3)\}.$$

We have (with renumbering the variables)

$$\delta^c N^3 \ll \#\{z_1, z_2, z_3, z_4 \in \mathcal{Z} : \, z_1 + z_2 = z_3 + z_4, \, \phi(z_1) + \phi(z_2) = \phi(z_3) + \phi(z_4)\}. \tag{13.7}$$

It is a straightforward task to prove that if $\phi(z_1)+\phi(z_2) = \phi(z_3)+\phi(z_4)$ whenever $z_1+z_2 = z_3+z_4$ for all $z_1, z_2, z_3, z_4 \in \mathbb{Z}_N$ then $\phi(z) = 2\lambda z + \mu$ is a linear function. But we do not know it for 'all', we only know for 'many', this is the situation discussed in Chapter 8, and we can only conclude that $\phi(z)$ is linear in a 'big' set.

Let $\Gamma = \{(z, \phi(z)); \, z \in \mathcal{Z}\} \subset \mathbb{Z}_N^2$, that is Γ is an additive set possessing many additive quadruples by (13.7), just like in Theorem 8.2. As in Corollary 8.4, we know that there is a subset $\Gamma' \subset \Gamma$ such that

$$|\Gamma' + \Gamma'| \ll \frac{N}{\delta^c}, \quad |\Gamma'| \gg \delta^c N.$$

Think about Γ' as a subset of $\{1, \dots, N\}^2 \subset \mathbb{Z}^2$ by representing any residue class with its smallest non–negative residue. Γ' satisfies

$$|\Gamma' + \Gamma'| \le C|\Gamma'|, \quad \text{where} \quad C \ll \frac{1}{\delta^c}.$$

Freiman's theorem, Theorem 7.6 (we only need the second statement), provides an arithmetic progression P_0 such that $|\Gamma' \cap P_0| \gg \delta^c |P_0|$, and $|P_0| \gg \delta^c N^{\delta^c}$. From now on we again think about Γ' and P_0 as pairs of residue classes, and let P be the arithmetic progression defined by the first coordinates of P_0. Note that trivially $|P| \ge |\mathcal{Z} \cap P| \gg \delta^c |P|$ and $|P| \gg \delta^c N^{\delta^c}$. This means that there are $(a, b), (c, d) \in \mathbb{Z}_N^2$ such that $(z, \phi(z)) = (a, b) + \ell(c, d)$ for all ℓ with $z = a + \ell c \in \mathcal{Z}$, and than $\phi(z) = b + \ell d = b + (z - a)d/c = 2\lambda z + \mu$ for all $z \in \mathcal{Z} \cap P$. Eventually we conclude that

$$\sum_{z \in P} |\widehat{\triangle(f, z)}(2\lambda z + \mu)|^2 \ge \sum_{z \in \mathcal{Z} \cap P} |\widehat{\triangle(f, z)}(2\lambda z + \mu)|^2 \gg \delta^c N^2 |\mathcal{Z} \cap P| \gg \delta^c N^2 |P|.$$

Carry out the square on the left hand side, it becomes

$$\sum_{z \in P} \sum_x \sum_y f(x) f(x + z) f(y) f(y + z) e\left(\frac{(2\lambda z + \mu)(y - x)}{N} \right). \tag{13.8}$$

We write $x+u+w$ for y, where $w\in P$ and $u\in\mathbb{Z}_N$, we can do that in exactly $|P|$ ways, thus (13.8) becomes

$$\frac{1}{|P|}\sum_x\sum_u\sum_{z\in P}\sum_{w\in P} f(x)f(x+z)f(x+u+w)f(x+u+w+z)e\left(\frac{(2\lambda z+\mu)(u+w)}{N}\right).$$

We conclude that there is a u, what we fix, such that

$$\sum_x\left|\sum_{z\in P}\sum_{w\in P} f(x+z)f(x+u+w)f(x+u+w+z)e\left(\frac{2\lambda zw+2\lambda uz+\mu w}{N}\right)\right|\gg$$

$$\gg \delta^c N|P|^2. \tag{13.9}$$

Next we separate the variables w and z by writing $2\lambda zw=\lambda(z+w)^2-\lambda w^2-\lambda z^2$. For any fixed x we first investigate the inner sums of (13.9). We write

$$g_1(z)=f(x+z)e\left(\frac{-\lambda z^2+2\lambda uz}{N}\right),\quad g_2(w)=f(x+u+w)e\left(\frac{-\lambda w^2+\mu w}{N}\right),$$
$$g_3(z+w)=f(x+u+(z+w))e\left(\frac{\lambda(z+w)^2}{N}\right).$$

Note that these functions depend on x as well. g_1 and g_2 are defined on P, while g_3 is defined on $P+P$. For other values of z, w or $v=z+w$ we set these functions equal to zero. (13.9) reads as

$$\sum_x\left|\sum_z\sum_w g_1(z)g_2(w)g_3(z+w)\right|\gg\delta^c N|P|^2. \tag{13.10}$$

Using (11.3), the Cauchy–Schwarz inequality, and the Parseval identity the inner sum can be transformed to

$$\left|\sum_z\sum_w g_1(z)g_2(w)g_3(z+w)\right|=$$
$$=\left|\sum_z\sum_w\sum_v g_1(z)g_2(w)g_3(v)\frac{1}{N}\sum_t e\left(\frac{zt+wt-vt}{N}\right)\right|=$$
$$=\frac{1}{N}\left|\sum_t\widehat{g_1}(t)\widehat{g_2}(t)\widehat{g_3}(-t)\right|\le\max_t|\widehat{g_1}(t)|\left(\frac{1}{N}\sum_t|\widehat{g_2}(t)|^2\right)^{1/2}\left(\frac{1}{N}\sum_t|\widehat{g_3}(t)|^2\right)^{1/2}\le$$
$$\le\max_t|\widehat{g_1}(t)|(|P||P+P|)^{1/2}\le\sqrt{2}|P|\max_t|\widehat{g_1}(t)|.$$

Writing this back to (13.10) we arrive at

$$\sum_x\max_t\left|\sum_{z\in P}f(x+z)e\left(\frac{-\lambda z^2+(2\lambda u+t)z}{N}\right)\right|\gg\delta^c N|P|.$$

For every x we pick up a $t = t_x$, where the maximum is taken. Further we change the variable $z = n - x$, where $n \in P + x$, finally we write $-\lambda z^2 + (2\lambda u + t)z = -\lambda n^2 + (2\lambda x + 2\lambda u + t)n - \lambda x^2 - 2\lambda ux - tx = -\lambda n^2 + \nu_x n - \eta_x$ with some ν_x and η_x, though this latter one is irrelevant. We have

$$\sum_x \left| \sum_{n \in P+x} (A(n) - \delta) e\left(\frac{-\lambda n^2 + \nu_x n}{N}\right) \right| \gg \delta^c N |P|.$$

This relation corresponds to (11.7), which led to density increment in Chapter 11. There are two major differences, this time we have a quadratic bias rather than linear, and not on $\mathbb{Z}_N$ but only on $P+x$, though in average over all x. Nevertheless, we finish the proof in a similar manner. $P + x$ is an arithmetic progression of length $L = |P + x| \gg \delta^c N^{\delta^c}$. Lemma 10.4 says that $P + x$ can be split into $M \approx L^{39/40}$ arithmetic progressions $P_{j,x}$ of length $L^{1/40} + O(1)$ such that $e\big((-\lambda n^2 + \nu_x n)/N\big)$ changes $\le 4\pi L^{-1/40}$ on each of them. By triangle inequality

$$\begin{aligned}
\delta^c N|P| &\ll \sum_x |\sum_{j=1}^{M} \sum_{n \in P_{j,x}} \big(A(n) - \delta\big) e(\frac{-\lambda n^2 + \nu_x n}{N})| \le \\
&\le \sum_x \sum_{j=1}^{M} |\sum_{n \in P_{j,x}} \big(A(n) - \delta\big) e(\frac{-\lambda n^2 + \nu_x n}{N})| \le \\
&\le \sum_x \sum_{j=1}^{M} |\sum_{n \in P_{j,x}} \big(A(n) - \delta\big)| + \sum_x \sum_{n \in P+x} \frac{4\pi}{L^{1/40}} \le \\
&\le \sum_x \sum_{j=1}^{M} |\sum_{n \in P_{j,x}} \big(A(n) - \delta\big)| + 4\pi N |P|^{39/40}.
\end{aligned}$$

Moreover we trivially have (remember $|A| = \delta N$)

$$\sum_x \sum_{j=1}^{M} \sum_{n \in P_{j,x}} \big(A(n) - \delta\big) = \sum_x \sum_{n \in P+x} \big(A(n) - \delta\big) = |P||A| - \delta |P| N = 0,$$

and we conclude, as we did in Chapter 12, that

$$\delta^c N|P| \ll \sum_x \sum_{j=1}^{M} \sum_{n \in P_{j,x}} \big(A(n) - \delta\big).$$

There is a choice of j, x such that

$$\delta^c L^{1/40} \ll \sum_{n \in P_{j,x}} \big(A(n) - \delta\big).$$

Note that $P_{j,x}$ is an arithmetic progression mod N. By Lemma 10.5 we can split $P_{j,x}$ into $K \leq 3|P_{j,x}|^{1/2} \leq 4L^{1/80}$ genuine arithmetic progressions $Q_k \subset \{1, \dots, N\}$. Some of them can be too short, say $\mathcal{G}$ is the collection of those with length $\geq L^{1/160}$, while $\mathcal{B}$ is the collection of those with length $< L^{1/160}$. Obviously

$$\sum_{Q_k \in \mathcal{B}} \sum_{n \in Q_k} \big(A(n) - \delta\big) \leq \sum_{Q_k \in \mathcal{B}} |Q_k| \leq K L^{1/160} \leq 4L^{3/160},$$

and we get that

$$\sum_{Q_k \in \mathcal{G}} \sum_{n \in Q_k} \big(A(n) - \delta\big) \gg \delta^c \sum_{Q_k \in \mathcal{G}} |Q_k|.$$

There is an arithmetic progression Q_k with length $\geq L^{1/160} \gg \delta^c N^{\delta^c}$ such that $|A \cap Q_k| = \sum_{n \in Q_k} A(n) \geq (\delta + \epsilon\delta^c)|Q_k|$, where ϵ (small) and c (big) are now fixed positive absolute constants. This density increment in a relatively long arithmetic progression is enough to finish our Theorem, exactly as we finished the proof of Theorem 11.1 (Roth).

APPENDIX 1

THE DIVISOR FUNCTION

In this Appendix we discuss some well–known properties of $d(n)$, the divisor function. Our main intention is to prove the estimate (10.9) that we used in Chapter 10.

First we show that $d(n)$ grows slower than any (small) power of n. We use the fact that the divisor function is multiplicative with $d(p^\alpha) = \alpha + 1$. For a fixed $\epsilon > 0$ we define $F(n) = d(n)/n^\epsilon$, which is also a multiplicative function. Consider, for a moment, $g(\alpha) = F(p^\alpha) = (\alpha+1)/p^{\epsilon\alpha}$ as a function of the real variable α. We determine the maximum of $g(\alpha)$ by differential calculus.

$$g'(\alpha) = \frac{1 - (\alpha+1)\,\epsilon \log p}{p^{\epsilon\alpha}}.$$

This shows that $g(\alpha)$ is increasing while $\alpha + 1 \le \frac{1}{\epsilon \log p}$ and decreasing while $\alpha + 1 \ge \frac{1}{\epsilon \log p}$, moreover

$$g(\alpha) \le \frac{2}{p^\epsilon} \le 1, \text{ for } p \ge 2^{1/\epsilon},$$

and in general

$$g(\alpha) \le \frac{p^\epsilon}{e\epsilon \log p}.$$

We conclude that

$$F(n) \le \prod_{p|n,\, p<2^{1/\epsilon}} \frac{p^\epsilon}{e\epsilon \log p} \le \prod_{p<2^{1/\epsilon}} \frac{p^\epsilon}{e\epsilon \log p} = C_\epsilon.$$

We have proved that

$$d(n) \le C_{\epsilon/2}\, n^{\epsilon/2} \le n^\epsilon, \tag{A.1}$$

the last inequality is valid for $n \ge n_0(\epsilon)$. Note that with slightly more effort one can prove the optimal upper bound $d(n) \le 2^{(1+\epsilon)\log n/\log\log n}$.

Next we turn to the proof of (10.9), that is for $r \ge r_0(\epsilon)$ we have

$$\sum_{m\le r} \frac{\sqrt{(m,r)}}{m} \le r^\epsilon.$$

As this is a rather crude estimate, we can be generous. For example, we start with the trivial relation $\sqrt{n} \le \sum_{d|n} \sqrt{d}$, and we finish with an application of (A.1).

$$\sum_{m\le r} \frac{\sqrt{(m,r)}}{m} \le \sum_{m\le r} \frac{1}{m} \sum_{d|(m,r)} \sqrt{d} = \sum_{d|r} \sqrt{d} \sum_{m\le r,\, d|m} \frac{1}{m} =$$

$$= \sum_{d|r} \frac{1}{\sqrt{d}} \sum_{n\le r/d} \frac{1}{n} \le \sum_{d|r} \frac{1}{\sqrt{d}} \big(1 + \log \frac{r}{d}\big) \le (1+\log r) d(r) \le r^\epsilon.$$