Combinatorial Number Theory

Martin Henk

based on lecture notes of Terence Tao
and the book by
Terence Tao and Van H. Vu *Additive Combinatorics*

Contents

1 Basics

1.1 Notation. *Let A, B subsets of an Abelian group Z.*

i) $A + B = \{a + b : a \in A,\, b \in B\}$.

ii) $A - B = \{a - b : a \in A,\, b \in B\}$.

iii) $kA = \underbrace{A + A + \ldots + A}_{k \text{ times}}$, $k \in \mathbb{Z}_{\geq 1}$.

iv) $t + B = \{t\} + B$ *for* $t \in Z$.

1.2 Proposition. *Let $A \subset \{1, \ldots, N\}$ such that $a + a' \notin A$ for all $a, a' \in A$, i.e., A is a sumfree subset of $\{1, \ldots, N\}$. Then $|A| \leq \lfloor \frac{N+1}{2} \rfloor$.*

1.3 Proposition. *Let $A, B \subset \mathbb{Z}$ be finite. Then $|A + B| \leq |A|\,|B|$.*

1.4 Proposition. *Let $A, B \subset \mathbb{Z}$ be finite. Then $|A + B| \geq |A| + |B| - 1$.*

1.5 Definition [Torsion-free]. *An Abelian group is caleld* torsion-free *if for all $x \in Z \setminus \{0\}$ and all $m \in \mathbb{Z}_{\geq 1}$ it holds $m\,x \neq 0$.*

1.6 Remark. *We will need the fact that each fnitely generated torsion-free group is isomorphic to a lattice.*

1.7 Definition [Freiman isomorphism]. *Let $A \subseteq Z$, $A' \subseteq Z'$ subsets of Abelian group Z, Z', and let $k \geq 2$. A* Freiman isomorphism of order k *is a bijective map $\Phi : A \to B$ such that for all $a_1, \ldots, a_k \in A$ and $a'_1, \ldots, a'_k \in A'$*

$$\sum_{i=1}^{k} \Phi(a_i) = \sum_{i=1}^{k} \Phi(a'_i) \Longleftrightarrow \sum_{i=1}^{k} a_i = \sum_{i=1}^{k} a'_i.$$

1.8 Remark.

i) *If Φ is a Freiman isomorphism of order k then also of order $k' \leq k$.*

ii) *The composition of Freiman isomorphisms is again a Freiman isomorphism.*

iii) *Let $\Phi : A \to A'$ be a Freiman isomorphism, and let $U_1, U_2 \subset A$. Then $|U_1 + U_2| = |\Phi(U_1) + \Phi(U_2)|$.*

1.9 Lemma. *Let $A \subseteq Z$ be a finite subset of an Abelian torsion free group. For every $k \geq 2$ exists a Freiman isomorphism $\Phi : A \to \Phi(A) \subseteq \mathbb{Z}$.*

1.10 Theorem. *Let $A, B \subseteq Z$ be finite subsets of an Abelian torsion free group Z. Then $|A + B| \geq |A| + |B| - 1$.*

1.11 Remark. *Let $A, B \subseteq \mathbb{Z}/N\mathbb{Z}$. Then $|A+B| \geq \max\{|A|, |B|\}$ which is best possible as a (non-trivial) subgroup shows.*

1.12 Theorem [Cauchy-Davenport]. *Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ for a prime p. Then $|A+B| \geq \max\{|A|+|B|-1, p\}$.*

1.13 Lemma. *Let $A, B \subseteq Z$ be finite subsets of an Abelian group Z. Then the following statements are equivalent:*

i) $|A+B| = |A|$.

ii) $|A-B| = |A|$.

iii) $|A+mB-nB| = |A|$ *for all* $m, n \in \mathbb{Z}_{\geq 0}$, $(m,n) \neq (0,0)$.

iv) $|A+mB-nB| = |A|$ *for a pair* $m, n \in \mathbb{Z}_{\geq 0}$ *with* $(m,n) \neq (0,0)$.

v) *There exists a subgroup $U \leq G$ such that B is a subset of a coset w.r.t. U and A is the union of cosets w.r.t. U.*

1.14 Lemma. *Let $A, B, C \subseteq Z$ be finite subsets of an Abelian group Z. Then*

$$|A-B| \leq \frac{|A+C|\,|B+C|}{|C|}.$$

1.15 Corollary. *Let $A, B, A\prime, B' \subseteq Z$ be finite subsets of an Abelian group Z.*

i) *If $|A+B| = |A|$ and $|A'+B| = |A'|$. Then $|A \pm A'| \leq |A||A'|/|B|$.*

ii) *If $|A+B| = |A| = |A+B'|$ then $|B \pm B'| \leq |A|$.*

2 Plünnecke's Theorem

2.1 Theorem [Plünnecke]. *Let Z be an Abelian group, let $A, B \subseteq Z$ be finite, and let $K \geq 1$ such that $|A+B| \leq K|A|$. Then there exists a $A' \subseteq A$, $A' \neq \emptyset$, such that*

$$|A' + B + B| \leq K^2 |A'|$$

2.2 Definition [Plünnecke Graph]. *Let Z be an Abelian group. A graph $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ is called an* Plünnecke graph (of depth 2) *with vertices $V_0 \cup V_1 \cup V_2 \subset Z$ and directed edges $E_{0\to1} \cup E_{1\to2}$ if every edge $E_{0\to1}$ starts in V_0 and ends in V_1, every edge $E_{1\to2}$ starts in V_1 and ends in V_2 and the following* Plünnecke property *is fulfilled:*

$$\begin{aligned} &\text{if } a \to a+b \in E_{0\to1} \text{ and } a+b \to a+b+c \in E_{1\to2} \\ &\text{then } a \to a+c \in E_{0\to1} \text{ and } a+c \to a+b+c \in E_{1\to2}. \end{aligned} \tag{Pp}$$

2.3 Remark. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be Plünnecke graph.*

i) *Each $a \to a+b \in E_{0\to1}$ induced an injection between $\{a+b \to a+b+c \in E_{1\to2}\}$ (all edges of $E_{1\to2}$ starting in $a+b$ and $\{a \to a+c \in E_{0\to1}\}$ (all edges of $E_{0\to1}$ emanating from a).*

ii) *Each $d \to c+d \in E_{1\to2}$ induced an injection between $\{d-b \to d \in E_{0\to1}\}$ (all edges of $E_{0\to1}$ ending in d and $\{-b+c+d \to c+d \in E_{0\to1}\}$ (all edges of $E_{1\to2}$ ending inc + d).*

iii) *We may always assume that the sets V_i are pairwise disjunct.*

2.4 Definition. *Let $G = (V, E)$ be a graph. For $V' \subseteq V$ let $G(V') = \{v \in V : \exists\, v' \in V' \text{ with } (v, v') \in E\}$ be all nodes which can be reached via a path of length 1 starting in V'. Recursively, $G^k(V')$ be all nodes which can be reached via a path of length k starting in V'.*

2.5 Remark. *With respect to finite subsets $A, B \subseteq Z$ of an Abelian group Z we consider the following* Plnnecke graph *$G(A, B) = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$, where $V_0 = A$, $V_1 = A + B$, $V_2 = A + B + B$ and $E_{0\to1} = \{a \to a+b : a \in A,\, b \in B\}$ and $E_{1\to2} = \{a+b \to a+b+c : a \in A,\, b, c \in B\}$. In terms of the graph $G(A, B)$, Theorem 2.1 says:*
Suppose $|V_1| \leq K\,|V_0|$ then there exists a nonempty subset $A' \subseteq V_0$ such that

$$G^2(A') \leq K^2\,|A'|.$$

2.6 Lemma [Menger's theorem]. *Let $G = (V, E)$ be a directed graph. For subsets $V_0, V_1 \subset V$ let* $\mathrm{maxflow}(V_0, V_1)$ *be the maximal number of vertex disjoint paths from V_0 to V_1, and let* $\mathrm{mincut}(V_0, V_1)$ *be the minimal number of vertices which have to be removed from V such that V_0 and V_1 are disconnected. Then*

$$\mathrm{maxflow}(V_0, V_1) = \mathrm{mincut}(V_0, V_1).$$

First, we prove Remark 2.5 for arbitrary Plünnecke graphs in the case $K = 1$. More precisely,

2.7 Proposition. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with $|V_1| < |V_0|$. Then there exists a nonempty subset $A' \subseteq V_0$ such that $G^2(A') < |A'|$.*

2.8 Definition [Magnification Ratio]. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with respect to a group Z.*

i)
$$\mathrm{D}(G) = \min_{A'\subseteq V_0,\, A'\neq\emptyset} \frac{|G^2(A')|}{|A'|}$$
is called magnification ratio *of the graph.*

ii) *Let $\overline{G} = (\overline{V_0}, \overline{V_1}, \overline{V_2}, \overline{E}_{0\to1}, \overline{E}_{1\to2})$ be another Plünnecke graph with respect to a group $\overline{Z}$. The Cartesian product*
$$G \times \overline{G} = (V_0 \times \overline{V_0}, V_1 \times \overline{V_1}, V_2 \times \overline{V_2}, E_{0\to1} \times \overline{E}_{0\to1}, E_{1\to2} \times \overline{E}_{1\to2})$$
is a Plünnecke graph with respect to $Z \times \overline{Z}$. Here the product of two edges $a \to b$ and $\overline{a} \to \overline{b}$ is just $(a, \overline{a}) \to (b, \overline{b})$.

2.9 Remark.

i) *Proposition 2.7 says: if $|V_1| < |V_0|$ then $\mathrm{D}(G) < 1$.*

ii) *Let $Z = \mathbb{Z}^k$, $A = \{0\}$, $B = \{e_1, \dots, e_k\}$, where e_i denotes the i-th unit vector. The Plünnecke graph $G(A, B)$ is denoted by G_k and it is*
$$\mathrm{D}(G_k) = \frac{k(k+1)}{2}.$$
For the associated reflected graph $G_k^\intercal$ (all edges are reversed) we find $\mathrm{D}(G_k^\intercal) = \frac{2}{k(k+1)}$.

2.10 Lemma. *Let $G, \overline{G}$ be Plünnecke graphs. Then*
$$\mathrm{D}(G \times \overline{G}) = \mathrm{D}(G) \cdot \mathrm{D}(\overline{G}).$$

2.11 Proposition. *Let $G = (V_0, V_1, V_2, E_{0\to1}, E_{1\to2})$ be a Plünnecke graph with $|V_1| < K\,|V_0|$, $K \geq 1$. Then $\mathrm{D}(G) \leq K^2$, i.e., there exists a nonempty subset $A' \subseteq V_0$ such that $G^2(A') \leq K^2\,|A'|$.*

Observe, Proposition 2.11 implies Theorem 2.1.

2.12 Corollary. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \leq K\,|A|$ for some $K \geq 1$. For any $n \in \mathbb{N}$ there exists $A_n \subseteq A$, $A_n \neq \emptyset$, such that*
$$|A_n + nB| \leq K^{c_n}\,|A_n|,$$
where c_n depends only on n (in fact, it can be shown that $c_n = n$ works).

2.13 Corollary [Sumset Estimate]. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \le K\,|A|$ for some $K \ge 1$. For any $n, m \in \mathbb{N}$ we have*

$$|nB - mB| \le K^{c_{n,m}}\,|A|,$$

where $c_{n,m}$ depends only on n and m.

2.14 Corollary. *Let A, B finite subsets of an Abelian group Z and let $|A+B| \le K\,|A|$ for some $K \ge 1$. Let $\delta \in (0,1)$. Then there exists $A' \subseteq A$ with $|A'| \ge (1-\delta)|A|$ and*

$$|A' + B + B| \le \frac{2\,K^2}{\delta}\,|A| \quad \left(\le \frac{2\,K^2}{\delta(1-\delta)}\,|A'|\right).$$

2.15 Proposition. *There exist subsets $A, B \subset \mathbb{Z}^2$ with $|A| \sim n^2$, $|B| \sim n$, such that $|A+B| \sim n^2$, but $|A+B+B| \sim n^3$.*

3 Covering

3.1 Lemma [Ruzsa's quotient lemma]. *Let A, B finite subsets of an Abelian group Z. Then there exists a set $X \subseteq Z$ with $|X| \leq \frac{|A+B|}{|A|}$ such that $B \subseteq X + A - A$, i.e., B is covered by at most $\frac{|A+B|}{|A|}$ translates of $A - A$.*

3.2 Corollary. *If $|A+A| \sim |A|$ then $nA-mA$ can be covered by $O(1)$ translates of $A - A$.*

3.3 Lemma. *Let Z be a finite Abelian group and let $A \subseteq Z$, $A \neq \emptyset$. Then G can be covered by $O(\frac{|Z|}{|A|} \log |Z|)$ translates of A, i.e., there exists $X \subseteq Z$, $|X| \in O(\frac{|Z|}{|A|} \log |Z|)$ such that $G = X + A$.*

3.4 Lemma [Improved quotient lemma]. *Let A, B finite subsets of an Abelian group Z. Then there exists a set $X \subseteq Z$ with $|X| \leq 2\frac{|A+B|}{|A|}$ such that B is covered by $X + A - A$ at least $\frac{|A|}{2}$ times, i.e., for every $y \in B$ there are at least $\frac{|A|}{2}$ triplets $(x, a, a') \in X + A - A$ such that $y = x + a - a'$.*

3.5 Theorem. *Let A be a finite subset of an Abelian group Z such that $|A + A| \sim |A|$. For any fixed $n, m \geq 0$ there exists a set $X_{n,m} \subseteq Z$ with $|X_{n,m}| \in O(\log |A|)$ such that $mA - nA \subseteq X_{n,m} + A$.*

3.6 Proposition. *There exist finite subsets A, B of an Abelian group Z such that $|A + B| \sim |A|$, but $|A - B| \geq |A|^{2-\log 6/\log 7}$.*

3.7 Proposition. *Let A, B finite subsets of an Abelian group Z such that $|A + B| \sim |A|$. Then for every $\epsilon > 0$ there exists a subset $A' \subseteq A$ such that $|A'| \sim |A|$ and $|A' - B| \leq C_\epsilon |A|^{1+\epsilon}$.*

3.8 Proposition. *For any integer $n \geq 1$ there exist finite subsets A, B of an Abelian group Z such that $|A + B| \sim |A| \sim C^n$, $|B| \sim n$, but $|A' - B| \geq n|A'|$ for all non-empty subsets of A.*

4 Freiman's theorem

4.1 Definition. *Let A, A' be subsets of an Abelian group Z.*

i) *$A' \subseteq A$ is called a* refinement *of A if $|A'| \sim |A|$.*

ii) *A' is a called a* small convolution *of A if there exists an $X \subseteq Z$ with $|X| = O(1)$ and $A' = X + A$.*

4.2 Remark. *Let A be a finite subset of an Abelian group Z which is essentially closed under addition, i.e., $|A + A| \sim |A|$.*

i) *If A' is a refinement of A then $|A' + A'| \sim |A'|$.*

ii) *If A' is* a small convolution *of A then $|A' + A'| \sim |A'|$.*

iii) *If Φ is a Freiman Isomorphism of order $k \geq 2$ then $|\Phi(A)+\Phi(A)| \sim |\Phi(A)|$.*

4.3 Theorem [Finite Torsion]. *Let Z be an Abelian group of Torsion $r < \infty$. Let $A \subseteq Z$ with $|A + A| \sim |A|$. Then A is a refinement of a subgroup $U \leq Z$.*

4.4 Definition [Generalized arithmetic progression].

i) *Let $N = (N_1, \ldots, N_d) \in \mathbb{N}^d$ and let $[0, N] = \{n \in \mathbb{Z}^d : 0 \leq n_i \leq N_i,\ 1 \leq i \leq d\}$. d is called the* rank *of the* box *$[0, N]$, and $|[0, N]| = \prod_{i=1}^{d}(N_i + 1)$ is called the* (discrete) volume *of the box $[0, N]$.*

ii) *Let Z be an Abelian group, let $\Phi : \mathbb{Z}^d \to Z$ be an affine homomorphism, and let $[0, N] \subset \mathbb{Z}^d$ be a box of rank d. The image $\Phi([0, N])$ is called a* (generalized) arithmetic progression *of* dimension *d,* length *N and volume $|[0, N]|$. If $\Phi|_{[0,N]}$ is injective the progression is called* proper.

4.5 Remark. *With the notation as above let $\Phi(0) = a$ and $\Phi(e_i) = v_i$, $1 \leq i \leq d$, where e_i are the unit vectors of $\mathbb{Z}^d$. Then*

$$\Phi([0, N]) = \left\{ a + \sum_{i=1}^{d} n_i\, v_i : 0 \leq n_i \leq N_i,\ 1 \leq i \leq d \right\},$$

and a is called base point *and v_i are called* basis vectors *of the arithmetic progression $\Phi([0, N])$.*

4.6 Proposition. *Let Z be an Abelian group, $\Phi : \mathbb{Z}^d \to Z$ be a Freiman isomorphism of order (at least) 2, and let $[0, N] \subset \mathbb{Z}^d$ be a box. Then $\Phi([0, N])$ is essentially closed under addition, i.e., $|\Phi([0, N]) + \Phi([0, N])| \sim |\Phi([0, N])|$.*

4.7 Theorem [Freiman]. *Let Z be a torsion-free Abelian group, and let $A \subset Z$ be essentially closed under addition, i.e., $|A + A| \sim |A|$. Then A is a refinement of a small convolution of a proper generalized arithmetic progression P of bounded rank, i.e., there exists a set $X \subset Z$, $X = O(1)$, with $A \subseteq X + P$, and $|A| \sim |X + P| \sim |P|$.*

4.8 Lemma. *Let A be a finite subset of a torison-free Abelian group Z. Let $n, N \in \mathbb{N}$ such that $2\,|nA - nA| < N$. Then there exists a subset $A' \subseteq A$ with $|A'| \geq |A|/n$ and a Freiman isomorphism $\Phi : A' \to B \subset \mathbb{Z}/N\,\mathbb{Z}$ of order n.*

4.9 Lemma. *Let $N \in \mathbb{N}$, $A \subseteq \mathbb{Z}/N\,\mathbb{Z}$ with $|A| \sim N$ and $|A + A| \sim |A|$. Then the set $2A - 2A$ contains a generalized proper arithmetic progression P of bounded rank with $|P| \sim N$.*

4.10 Definition. *Let Z be an Abelian (additive) group. Let $e : Z \times Z \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$ be a map such that*

i) $e(x + x', y) = e(x, y)e(x', y)$ *and* $e(x, y + y') = e(x, y)e(x, y')$

ii) *for all x (or y) $\in Z \setminus \{0\}$ exists y (or x) $\in Z \setminus \{0\}$ such that $e(x, y) \neq 1$.*

e is called a bi-character.

4.11 Remark.

i) $e(0, y) = e(x, 0) = 1$, $e(x, -y) = e(-x, y) = \overline{e(x, y)}$.

ii) *For $\mathbb{Z}/N\mathbb{Z}$ the function $e(x, y) : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to S^1$ with $e(x, y) = e^{2\pi\,\mathrm{i}\,xy/N}$ is a bi-character.*

iii) *Let e_1, e_2 be bi-characters with respect to groups Z_1, Z_2. Then $e_1 \otimes e_2 : (Z_1 \times Z_2) \times (Z_1 \times Z_2)$ with $(e_1 \otimes e_2)(x_1 \times x_2, y_1, \times y_2) = e_1(x_1, y_1) \cdot e_2(x_2, y_2)$, $x_1, y_1 \in Z_1$, $x_2, y_2 \in Z_2$, is a bi-character on $Z_1 \times Z_2$.*

iv) *Every finite Abelian group has a bi-character.*

4.12 Lemma. *Let Z be a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Then*

$$\frac{1}{|Z|} \sum_{x \in Z} e(x, y)\overline{e(x, y')} = \delta_{y,y'} \quad \text{and} \quad \frac{1}{|Z|} \sum_{y \in Z} e(x, y)\overline{e(x', y)} = \delta_{x,x'},$$

where $\delta_{x,y} = 1$ if $x = y$ and 0 otherwise.

4.13 Remark. *Let $\mathbb{C}^Z$ be the set of all complex-valued functions on Z. For $f, g \in \mathbb{C}^Z$ let*

$$\langle f, g \rangle_Z = \frac{1}{|Z|} \sum_{x \in Z} f(x)\,\overline{g(x)}.$$

i) *$\langle \cdot, \cdot \rangle$ is an inner product on $\mathbb{C}^Z$.*

ii) *$e(\cdot, y)$, $y \in Z$, form an orthonormal system.*

iii) *Let $f \in \mathbb{C}^Z$. Then*

$$f = \sum_{y \in Z} \langle f, e(\cdot, y) \rangle_Z\, e(\cdot, y).$$

4.14 Definition [Fourier transform]. *Let $f \in \mathbb{C}^Z$, where Z is a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Then $\widehat{f} : Z \to \mathbb{C}$ with*

$$\widehat{f}(y) = \langle f, e(\cdot, y)\rangle_Z = \frac{1}{|Z|} \sum_{x \in Z} f(x)\, \overline{e(x,y)}$$

is called the Fourier transform *of f.*

4.15 Theorem. *Let Z be a finite Abelian group, and let $e : Z \times Z \to S^1$ be a bi-character. Let $f \in \mathbb{C}^Z$.*

i) $f(x) = \sum_{y \in Z} \widehat{f}(y)\, e(x,y)$ (Fourier inversion formula)

ii) $\frac{1}{|Z|} \sum_{x \in Z} f(x)\overline{g(x)} = \sum_{y \in Z} \widehat{f}(y)\, \overline{\widehat{g}(y)}$ (Plancherel formula)

iii) $\frac{1}{|Z|} \sum_{x \in Z} |f(x)|^2 = \sum_{y \in Z} |\widehat{f}(y)|^2$ (Parseval relation)

4.16 Definition [Convolution]. *Let $f, g \in \mathbb{C}^Z$. Then $f \star g \in \mathbb{C}^Z$ with*

$$f \star g(x) = \frac{1}{|Z|} \sum_{y \in Z} f(y)\, g(x-y)$$

is called convolution *of f and g.*

4.17 Lemma.

i) $\widehat{f \star g}(y) = \widehat{f}(y)\, \widehat{g}(y)$.

ii) *Let $\tilde{f}(x) = \overline{f(-x)}$. Then $\widehat{\tilde{f}}(y) = \overline{\widehat{f}(y)}$.*

4.18 Proposition. *Let $A \subseteq Z$ with characteristic function χ_A, and let $c = |A|/|Z|$. Then*

i) $\sum_{y \in Z} |\widehat{\chi_A}(y)|^2 = c$.

ii) $|\widehat{\chi_A}(y)| \le c$.

iii) *Let $\epsilon \in (0,1]$. Then $|\{y \in Z : |\widehat{\chi_A}(y)| \ge \epsilon\, c\}| \le \epsilon^{-2} \frac{1}{c}$.*

iv) $\sum_{y \in Z} |\widehat{\chi_A}(y)|^4 \le c^3$.

4.19 Lemma. *Let $A \subseteq Z$ with characteristic function χ_A, let $c = |A|/|Z|$ and $|A + A| \le K\, |A|$. Then*

i) $\chi_A \star \chi_A(x) \neq 0$ *if and only if* $x \in A + A$.

ii) $\sum_{y \in Z} |\widehat{\chi_A}(y)|^4 \ge c^3\, K^{-1}$.

iii) *Let*

$$\Lambda = \left\{ y \in Z : |\widehat{\chi_A}(y)| \geq \frac{c}{2\sqrt{K}} \right\}.$$

Then $|\Lambda| \leq 4K\, c^{-1}$ *and*

$$\sum_{y\in\Lambda} |\widehat{\chi_A}(y)|^4 \geq \frac{3}{4} \sum_{y\in Z} |\widehat{\chi_A}(y)|^4.$$

4.20 Remark. *Let* $f(x) = \chi_A \star \chi_A \star \chi_{-A} \star \chi_{-A}$. *Then* $f(x) \neq 0$ *if and only if* $x \in 2\,A - 2\,A$, *and it holds* $\widehat{f}(y) = |\widehat{\chi_A}(y)|^4$.

4.21 Lemma. *Let* $A \subseteq Z$, $|A|/|Z| = c$, *and let* $|A + A| \leq K\,|A|$. *Let*

$$\Lambda = \left\{ y \in Z : |\widehat{\chi_A}(y)| \geq \frac{c}{2\sqrt{K}} \right\} \text{ and}$$
$$X = \left\{ x \in Z : |e(x,y) - 1| < \frac{1}{4} \text{ for all } y \in \Lambda \right\}.$$

Then $X \subseteq 2A - 2A$.

4.22 Theorem [Gowers-Walters]. *Let* Z *be a torsion-free Abelian group. Then every generalized arithmetic progression in* Z *with bounded rank is the refinement of a proper generalized arithmetic progression bounded rank.*

4.23 Corollary [Freiman's theorem without small convolutions]. *Let* Z *be a torsion-free Abelian group, and let* $A \subset Z$ *with* $|A + A| \sim |A|$. *Then* A *is a refinement of a proper generalized arithmetic progression* P *of bounded rank, i.e.,* $A \subseteq P$ *and* $|A| \sim |P|$.

4.24 Lemma. *Let* $\Lambda \subset \mathbb{R}^d$ *be a lattice (discrete subgroup) containing* d *linearly independent vectors* $s_1, \ldots, s_d$. *Then there exists* $b_1, \ldots, b_d \in \Lambda$ *such that for* $1 \leq k \leq d$

$$\operatorname{lin}\{s_1, \ldots, s_k\} \cap \Lambda = \{z_1\, b_1 + \cdots z_k\, b_k : z_i \in \mathbb{Z}\} = (b_1, \ldots, b_k)\mathbb{Z}^k.$$

4.25 Corollary. *Let* $\Lambda \subset \mathbb{R}^d$ *be a lattice of rank* k. *Then there exists* $b_1, \ldots, b_k \in \Lambda$ *such that* $\Lambda = (b_1, \ldots, b_k)\,\mathbb{Z}^k$.

4.26 Definition. *Let* $\Lambda \subset \mathbb{R}^d$ *be a lattice.* $v \in \Lambda$ *is called* irreducible *or* primitive *if* $\lambda\, v \notin \Lambda$ *for all* $\lambda \in (0,1)$.

4.27 Corollary. *Let* $\Lambda \subset \mathbb{R}^d$ *be a lattice of rank* k *and let* $v \in \Lambda$ *be irreducible. Then there exists a lattice* Λ' *of rank* $k-1$ *such that* $\Lambda = \mathbb{Z}\, v \oplus \Lambda'$.

5 Partial Sums

5.1 Lemma. *Let X, Y be finite sets and let $f : X \to Y$. Then*

$$|\{(x, x') \in X \times X : f(x) = f(x')\}| \geq |X|^2/|Y|.$$

5.2 Lemma. *Let X, Y be finite sets and let $f : X \to Y$. Let*

$$Y_p = \left\{ y \in Y : |\{x \in X : f(x) = y\}| \geq \frac{1}{2}\frac{|X|}{|Y|} \right\}.$$

Then

$$|\{x \in X : f(x) \in Y_p\}| \geq \frac{1}{2}|X|.$$

5.3 Definition. *Let $A, B \subseteq Z$ subsets of a group Z, and let $G \subseteq A \times B$. The set*

$$A \overset{G}{+} B = \{a + b : (a, b) \in G\}$$

is called partial sum set *and*

$$A \overset{G}{-} B = \{a - b : (a, b) \in G\}$$

partial difference set.

5.4 Proposition. *Let $A, B \subseteq Z$ with $|A| \gg |B|$ and $|A + B| \sim |A|$. Then there exists a subset $G \subseteq A \times B$ with $|G| \sim |A \times B|$ and $|A \overset{G}{-} B| \sim |A|$.*

5.5 Theorem [Balog-Szemerédi-Gowers]. *Let $A, B \subseteq Z$ be finite sets, and let $G \subseteq A \times B$ such that*

$$|G| \geq |A||B|/K \text{ and } |A \overset{G}{+} B| \leq K'|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$$

for some constants $K \geq 1$, $K' > 0$. Then there exists subsets $A' \subseteq A$, $B' \subseteq B$ such that

$$|A'| \geq \frac{1}{4\sqrt{2}K}|A|, \quad |B'| \geq \frac{1}{4K}|B| \quad \text{and } |A' + B'| \leq 2^{12}K^5(K')^3\,|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}.$$

5.6 Lemma. *Let $G(A, B, E)$ be a bipartite Graph with edges $|E| \geq |A||B|/K$ for some $K \geq 1$. For any $\epsilon \in (0, 1)$ there exists a subset $A' \subseteq A$ such that*

$$|A'| \geq \frac{1}{\sqrt{2}K}|A|,$$

and such that at least $(1 - \epsilon)$ of the pairs a, a' of A' are connected by at least $\frac{\epsilon}{2K^2}|B|$ paths of length 2 in $G(A, B, E)$.

5.7 Corollary. *Let $G(A, B, E)$ be a bipartite Graph with edges $|E| \geq |A||B|/K$ for some $K \geq 1$. Then there exists $A' \subseteq A$, $B' \subseteq B$ with $|A'| \geq \frac{1}{4\sqrt{2}K}|A|$, $|B'| \geq \frac{1}{4K}|B|$ such that all $(a', b') \in A' \times B'$ are connected by at least $\frac{1}{2^{12}K^5}|A||B|$ paths of length 3 in $G(A, B, E)$.*

5.8 Theorem* [Bourgain]. *Let $A, B \subseteq Z$ finite with $|A|, |B| \leq N$, and let $G \subseteq A \times B$ with $|G| \geq N^2/K$ such that $|A \overset{G}{+} B| \leq N$. Then there exist $A' \subseteq A$, $B' \subseteq B$ with $|G \cap (A' \times B')| \geq K^{-9}N^2$ and $|A' - B'| \leq (K^{13}/N)|G \cap (A' \times B')|$.*

5.9 Definition [Kakeya Problem].

i) *A Kakeya set in $\mathbb{R}^n$ is a compact set $E \subset \mathbb{R}^n$, such that E contains for every direction $v \in \mathbb{R}^n$ a segement of length 1 in this direction, i.e., for every $v \in \mathbb{R}^n$, $|v|_2 = 1$, there exists an $a \in \mathbb{R}^n$ such that $\{a + t\,v : t \in [0,1]\} \subset E$. It is conjectured that these sets have Hausdorff and Minkowski dimension n.*

ii) *Finite Fields: Let $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, p prime and large, and let $n \geq 2$. For a given $a \in \mathbb{F}^n$, $v \in \mathbb{F}^n \setminus \{0\}$ the set $L(a,v) = \{a + t\,v : t \in \mathbb{F}\}$ is called a line in direction v. $E \subseteq \mathbb{F}^n$ is called a* Kakeya set *in $\mathbb{F}^n$, if for every $v \in \mathbb{F}^n \setminus \{0\}$ there exists a $a \in \mathbb{F}^n$ such that $L(a,v) \subset E$. It is (was) conjectured that $|E| \geq c(n,\epsilon)\,|\mathbb{F}|^{n-\epsilon}$ for any $\epsilon > 0$.*

5.10 Proposition. *Let $E \subseteq \mathbb{F}^n$ be a Kakeya set. Then $|E| \geq \frac{1}{2}|\mathbb{F}|^{\frac{n+1}{2}}$.*

5.11 Proposition. *Let $p \geq 3$, and let $E \subseteq \mathbb{F}^n$ be a Kakeya set. Then $|E| \geq \frac{1}{100}|\mathbb{F}|^{\frac{13n+12}{25}}$.*

5.12 Lemma. *Let $g \in \mathbb{F}[x_1, \ldots, x_n]$ with $\mathrm{grad}(g) \leq |\mathbb{F}| - 1$ and $g \not\equiv 0$. Then there exists a $y \in \mathbb{F}^n$ with $g(y) \neq 0$.*

5.13 Lemma [Schwartz-Zippel]. *Let $g \in \mathbb{F}[x_1, \ldots, x_n]$ with $\mathrm{grad}(g) = d$ and $g \not\equiv 0$. Then*

$$|\{x \in \mathbb{F}^n : g(x) = 0\}| \leq d\,|\mathbb{F}|^{n-1}.$$

5.14 Lemma. *Let $E \subseteq \mathbb{F}^n$ with $|E| < \binom{n+d}{d}$. Then there exists a $P \in \mathbb{F}[x_1, \ldots, x_n]$, $\mathrm{grad}P \leq d$, $P \not\equiv 0$ and $P(x) = 0$ for all $x \in E$.*

5.15 Lemma. *Let $E \subseteq \mathbb{F}^n$ be a Kakeya set and let $P \in \mathbb{F}[x_1, \ldots, x_n]$ with $\mathrm{grad}P \leq |\mathbb{F}| - 1$ and $P(x) = 0$ for all $x \in E$. Then $P \equiv 0$.*

5.16 Theorem [Divr]. *Let $E \subseteq \mathbb{F}^n$ be a Kakeya set. Then*

$$|E| \geq \binom{|\mathbb{F}| + n - 1}{n} = \frac{|\mathbb{F}|^n}{n!} + O(|\mathbb{F}|^{n-1}).$$

5.17 Definition.

i) *A graph $G = (V, E)$ is called complete if $(v, v') \in E$ for all $v, v' \in V$, $v \neq v'$.*

ii) *An edge k-coloring of a graph $G = (V, E)$ is a partitioning of E into k different (color-) classes $E_1, \ldots, E_k$.*

iii) *Let $E_1, \dots, E_k$ be a k-coloring of $G = (V, E)$. A subgraph $G' = (V', E')$ is called E_j-monochrom if $E' \subseteq E_j$.*

5.18 Definition [Ramsey numbers]. *Let $m, n \geq 1$. The* Ramsey number *$R(n, m)$ is the smallest number such for any 2-coloring E_{blue}, E_{red} of a complete graph with at least $R(n, m)$ vertices there exist either a complete E_{blue}-monochrom subgraph with n vertices or a complete E_{red}-monochrom subgraph with m vertices.*

5.19 Theorem [Ramsey]. $R(n, m) \leq \binom{n+m-2}{n-1}$.

5.20 Remark. *The bound is sharp for some small values of n, m. For instance, $R(3, 3) = 6$.*

5.21 Corollary. *Let $m \geq 2$ and let $n_1, \dots, n_m \in \mathbb{N}_{\geq 1}$. There exists a number $R(n_1, \dots, n_m; m)$, such that for any m-coloring $E_1, \dots, E_m$ of a complete graph with at least $R(n_1, \dots, n_m; m)$ vertices there exists a $j_* \in \{1, \dots, m\}$ and a E_{j_*}-monochrom complete subgraph with n_{j_*} vertices.*

5.22 Theorem [Schur]. *Let $m, k \in \mathbb{N}_{\geq 1}$. There exists a number $N = N(m, k)$ such that for a any partition $[1, N] = A_1 \cup A_2 \cup \dots \cup A_m$ into m subsets at least one of the A_j contains a subset of the form*

$$\{x_1, \dots, x_k, x_1 + \dots + x_k\}.$$

In fact, we can choose $N(m, k) = R(k + 1, \dots, k + 1; m)$ (cf. Corollary 5.21).

5.23 Corollary. *Let $n \geq 2$. There exists a $s(n) \in \mathbb{N}$ such that for all primes $p > s(n)$ the congruence*

$$x^n + y^n \equiv z^n \bmod p$$

has as non-trivial solution (p is not a divisor of xyz).

5.24 Proposition. *Let $m, n \in \mathbb{N}_{\geq 1}$ and let $1 \leq s \leq m$. There exists an integer $\overline{d} = \overline{d}(n, m, s) \geq 1$ such that for any partition*

$$[0, n-1]^{\overline{d}} = E_1 \cup \dots \cup E_m$$

into m non-empty subsets E_i there exist either $j_* \in \{1, \dots, m\}$, $a \in [0, n-1]^{\overline{d}}$ and $v \in [0, 1]^{\overline{d}} \setminus \{0\}$ with

$$a + [0, n-1] \cdot v \subseteq E_{j_*},$$

or there exist s distinct classes $E_{j_1}, \dots, E_{j_s}$, $a \in [0, n-1]^{\overline{d}}$ and $v_i \in [0, 1]^{\overline{d}} \setminus \{0\}$, $1 \leq i \leq s$ such that

$$a + [1, n-1] \cdot v_i \subseteq E_{j_i},\ 1 \leq i \leq s.$$

5.25 Theorem [Hales-Jewett]. *Let $m, n \in \mathbb{N}_{\geq 1}$. There exists an integer $\overline{d} = \overline{d}(n,m) \geq 1$ such that for any partition $[0, n-1]^{\overline{d}} = E_1 \cup \cdots \cup E_m$ into m non-empty subsets E_i there exist a $j_* \in \{1, \ldots, m\}$, $a \in [0, n-1]^{\overline{d}}$ and $v \in [0,1]^{\overline{d}} \backslash \{0\}$ with*

$$a + [0, n-1] \cdot v \subseteq E_{j_*}.$$

5.26 Theorem [van der Waerden]. *Let Z be an arbitrary additive group, and let $m, k \in \mathbb{N}_{\geq 1}$. There exists a number $N = N(m,k)$ such that for a any given proper arithmetic progression P of length N and any partition $P = A_1 \cup A_2 \cup \cdots \cup A_m$ of P into m color classes, at least one of the A_j containes a monochromatic proper arithmetic sub-progression $P' \subseteq P$ of length k.*

6 Arithmetic progressions of length 3

6.1 Theorem* [Szemerédi (1975), Fürstenberg (1977), ..., Gowers(2001)]. *Let $\delta \in (0,1]$. There exist absolute constants C_k, c_k sucht that for $N \in \mathbb{N}$ with $\ln\ln N \geq (C_k/\delta)^{c_k}$, any set $A \subseteq [1,N]$ of size $|A| \geq \delta N$ contains a proper arithmetic progression of length k.*

6.2 Theorem [Roth 1953]. *Let $\delta \in (0,1]$. There exists an absolute constant C sucht that for $N \in \mathbb{N}$ with $\ln\ln N \geq C/\delta$, any set $A \subseteq [1,N]$ of size $|A| \geq \delta N$ contains a proper arithmetic progression of length 3, i.e., there exists $a,b,c \in A$, $a<b<c$, with $a+c=2b$.*

6.3 Remark.

i) *In the following we will always assume $|A| = \delta N$ and $A \subseteq \{0,\dots,N-1\}$.*

ii) *Some (slightly renormalized) facts on Fourier transforms on the group $\mathbb{Z}_N = \mathbb{Z}/NZ$ (see Chapter 4). For $f : \mathbb{Z}_N \to \mathbb{C}$ the function $\widehat{f}(y) = \sum_{x=0}^{N-1} f(x)\,\mathrm{e}^{2\pi\mathrm{i}\frac{xy}{N}}$ is the Fourier-transform of f, and we have*

i) $\widehat{f}(0) = \sum_x f(x)$, ii) $|\widehat{f}(y)| \leq \sum_x |f(x)|$,

iii) *for $f \star g(x) = \sum_{t=0}^{N-1} f(t)g(x-t)$ it is $\widehat{f\star g}(y) = \widehat{f}(y)\widehat{g}(y)$ and so*

$$|\widehat{f}(y)|\,|\widehat{g}(y)| \leq \sum_x \left|\sum_t f(t)g(x-t)\right|,$$

iv) $\sum_x |f(x)|^2 = \frac{1}{N}\sum_y |\widehat{f}(y)|^2$, v) $\frac{1}{N}\sum_{x=0}^{N-1} \mathrm{e}^{2\pi\mathrm{i}\frac{xy}{N}} = \begin{cases} 1, & y \equiv 0 \bmod N, \\ 0, & \text{otherwise} \end{cases}$

6.4 Notation. *An arithmetic progression in $\mathbb{Z}_N$ will be denoted as $\mathbb{Z}_n$-progression, whereas an arithmetic progression in $\mathbb{Z}$ is called a $\mathbb{Z}$-progression. Let*

i) *$S = |\{a,b,c \in A : a+c = 2b\}|$, i.e., 3-term $\mathbb{Z}$-progressions in A.*

ii) *$S_0 = |\{a,b,c \in A : a+c \equiv 2b \bmod N\}|$, i.e., 3-term $\mathbb{Z}_N$-progressions in A.*

Then $S_0 \geq S$. Furthermore, we denote by χ_A the characteristic function of A.

6.5 Remark. *Let $|A| = \delta N$.*

i) $\widehat{\chi_A}(0) = \delta\, N$.

ii)

$$S_0 = \sum_{a,b,c\in A} \frac{1}{N}\sum_{x=0}^{N-1} \mathrm{e}^{2\pi\mathrm{i}\frac{a+b-2c}{N}} = \delta^3\, N^2 + \frac{1}{N}\sum_{x=1}^{N-1} \widehat{\chi_A}(x)^2\widehat{\chi_A}(-2x).$$

Here $\delta^3\, N^2$ is the expected number of 3-term $\mathbb{Z}_N$ arithmetic progressions if each element in A is chosen randomly (and independently) with probability δ.

6.6 Definition. *A is called* ϵ-uniform *(or* suitable random*) if* $|\widehat{\chi_A}(s)| \leq \epsilon N$ *for all* $s \in \mathbb{Z}_N \setminus \{0\}$.

6.7 Remark.

i) *Ler A be ϵ-uniform with $\epsilon \leq \delta^2/2$, then $S_0 \geq \delta^3 N^2/2$.*

ii) *Let $M_A = A \cap [n/3, 2N/3)$. Every 3-term $\mathbb{Z}_N$-progression $a + c \equiv 2b \mod N$ with $a, b \in M_A$ is a 3-term $\mathbb{Z}$-progression.*

6.8 Lemma. *Let A be ϵ-uniform with $\epsilon \leq \delta^2/8$ and let $|M_A| \geq \frac{|A|}{4}$. Then $S \geq \frac{1}{32}\delta^3 N^2$.*

6.9 Proposition. *If A does not contain any non-trivial 3-term $\mathbb{Z}$ progression, then one of the following conditions must hold:*

i) $N \leq 32/\delta^2$

ii) *A is not ϵ-uniform for all $\epsilon \leq \delta^2/8$.*

iii) *There exists a $\mathbb{Z}$-progression P with $|P| \geq N/3$ and $|A \cap P| \geq (\delta + \delta/8)|P|$.*

6.10 Notation. *A $\mathbb{Z}_N$ progression P of successive distance d is called* non-overlapping *if $|P|\, d \leq N$.*

6.11 Lemma. *Let B' be a non-overlapping $\mathbb{Z}_N$ progression with $|A \cap B'| \geq (\delta + \epsilon')|B'|$. Then there exists a $\mathbb{Z}$-progression P with $|P| \geq \frac{1}{2}\epsilon'|B'|$ and $|A \cap P| \geq (\delta + \frac{1}{2}\epsilon')|P|$.*

6.12 Lemma. *Let $s \in \mathbb{Z}_N$, $s \neq 0$, with $|\widehat{\chi_A}(s)| \geq \epsilon N$. Then there exists a non-overlapping $\mathbb{Z}_N$-progression B' with $|B'| \geq \sqrt{N}/4$ and $|A \cap B'| \geq (\delta + \frac{1}{4}\epsilon)|B'|$.*

6.13 Corollary. *Let A be not ϵ-uniform. Then there exists a $\mathbb{Z}$-progression P with $|P| \geq \frac{\epsilon}{32}\sqrt{N}$ and $|A \cap P| \geq (\delta + \frac{1}{8}\epsilon)|P|$.*

6.14 Corollary. *Let $N > 32/\delta^2$. Then either A contains a non-trivial 3-term $\mathbb{Z}$-progression, or there exists a $\mathbb{Z}$-progression $P \subseteq \{0, \cdots, N-1\}$ with*

$$|P| \geq \frac{\delta^2}{256}\sqrt{N} \text{ and } |A \cap P| \geq (\delta + \frac{1}{64}\delta^2)|P|.$$

6.15 Theorem [Behrend, 1946]. *There exists an $A \subset [1, N]$ of size*

$$|A| \geq \frac{1}{\mathrm{e}^{c\sqrt{\ln N}}} N$$

containing no non-trivial 3-term arithmetic progression. Here c is an absolute constant.

Index