# 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**

**2 Plünnecke's Theorem** **3**

**3 Covering** **7**

**Index** **7**

# 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 $\Phi$ 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 $A \subseteq Z$, $A \neq \emptyset$. The $G$ 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 $mA - nA \subseteq X + A$.*

**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 $A$.*