LECTURE 1

Fundamental questions, concepts and techniques

1. Some motivating questions and our main groups of study

1.1. Some questions. Combinatorics is a subject in which one often wants to count things and classify structures, and as the title of this course suggests we shall be interested in doing this in settings where the operation of addition is somehow involved. Some of the questions we encounter will succumb to short, direct arguments, whereas we shall need to develop a fair bit of theory to deal with others. Below is a list of some questions of the types we shall be interested in; try to give some thought to how you might go about tackling them.

1) How large can a set $A \subseteq \{1, \dots, N\}$ be if A does not contain any solutions to the equation $a_1 + a_2 = a_3$ with $a_i \in A$?
2) How large can a set $A \subseteq \{1, \dots, N\}$ be if the only solutions to the equation $a_1 + a_2 = 2a_3$ with $a_i \in A$ are trivial, i.e., have $a_1 = a_2 = a_3$?
3) What if we take the equation $a_1 + a_2 = a_3 + a_4$ instead, where a solution is now considered trivial if $\{a_1, a_2\} = \{a_3, a_4\}$?

These questions concern the addition of individual elements of a set; the following set of questions involve adding whole sets: if $A, B \subseteq \mathbb{Z}$ we write $A+B = \{a+b : a \in A, b \in B\}$.

4) How small can $|A + A|$ be if $|A| = n$? How large can it be?
5) What can we say about A if $|A+A| < K|A|$ for some number K? What if $K = 2$?
6) What can we say about $A + A + A$ if $A \subseteq \{1, \dots, N\}$ and $|A| \geqslant \alpha N$?
7) What about $A + A$?

Of course one can answer many of these questions tautologically: if $|A + A| < K|A|$ then one can certainly say that $|A + A| < K|A|$. This is clearly not a very satisfactory answer; instead we shall aim to draw *interesting* conclusions. We shall also often want our answers to be *quantitative*—we would for example want to know how our conclusion depends on K for Question 5, or on α for Question 6.

By the end of the course you should be able to provide non-trivial answers to each of the above questions, as well as understand some of the fascinating methods that have been developed to tackle them.

1.2. Our main groups of study. Although the above questions were about sets of integers, with slight modifications they make sense in more general abelian groups. For example, if G is any abelian group then we may ask how small $|A + A|$ may be in terms of $|A|$ for finite sets $A \subseteq G$, and if G is finite then we may ask how large a subset A of G

can be without containing a solution to $a_1 + a_2 = a_3$ with $a_i \in A$. We shall study some questions in these more general settings, though in applications we shall be particularly interested in subsets of three families of groups:

- the integers $\mathbb{Z}$,
- the groups $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ of residues modulo N, and
- the additive groups $\mathbb{F}_q^n$ of vector spaces over finite fields.

The reason for singling out these families is that the first two are often the classical settings of interest for combinatorial and number-theoretical questions, and the third—in addition to being interesting in its own right—often provides a useful setting in which to think about proof-strategies, for many ideas can be implemented more cleanly there than in general. We shall see several examples of this throughout the course.

Meta-question 1.3. Which of Questions 1-7 above are 'easy' and which are 'hard'? How does the difficulty vary if we replace $\{1, \dots, N\}$ by $\mathbb{Z}_N$ or $\mathbb{F}_3^n$?

It turns out that Question 1 is relatively easy to answer for $\{1, \dots, N\}$; before doing so let us introduce a piece of terminology.

Definition 1.4. A subset A of an abelian group is said to be *sum-free* if there are no elements $a, b, c \in A$ such that $a + b = c$. In other words, A is sum-free if it does not contain the sum of any two of its elements.

For example, the set of odd numbers is a sum-free subset of $\mathbb{Z}$, and the set $\{3, 4, 5\}$ is a sum-free subset of $\mathbb{Z}_8$.

Theorem 1.5. *The largest size of a sum-free subset of* $\{1, \dots, N\}$ *is* $\lfloor \frac{N+1}{2} \rfloor$.

Proof. Suppose $A \subseteq \{1, \dots, N\}$ is sum-free and let $c = \max A$ be the largest element of A. The sets A and $c - A = \{c - a : a \in A\}$ are then disjoint subsets of $\{0, \dots, N\}$, and so certainly $2|A| \leqslant N + 1$. This gives the required upper bound. Since the set of odd numbers in $\{1, \dots, N\}$ attains this bound, we are done. □

This result, while pleasant, is in several ways rather unrepresentative of the majority of those we shall encounter. First, a short and direct argument gave us the answer, whereas in general we shall need to develop some quite substantial tools in order to get anywhere. Second, we were able to give an *exact* answer; for most questions we shall content ourselves with providing approximate answers, where the degree of approximation with which we are happy will depend on the context. Before we go on to discuss some questions of this type, let us give two further questions about sum-free sets that are worth thinking about in order to familiarise oneself with abelian groups other than the integers.

Question 1.6. How large a sum-free subset of $\mathbb{F}_2^n$ can you find? (Recall that $\mathbb{F}_2$ is the field of two elements $\{0, 1\}$, where $1 + 1 = 0$.)

Question 1.7. How large a sum-free subset of $\mathbb{Z}_N$ can you find when N is prime? What if we drop the prime requirement; what if N is even, say?

2. Operations on additive sets

The basic objects of study for us will be non-empty finite subsets of abelian groups; we shall sometimes refer to such sets as *additive sets*. In §1.1 we saw some questions about what happens when one forms the sum of two additive sets; in this section we shall try to get a better feel for such questions. Let us start with some important definitions.

Definition 2.1 (Additive set operations)**.** For two subsets A and B of an abelian group G, write

(i) $A+B = \{a+b : a \in A, b \in B\}$ for the *sumset* of A and B;
(ii) $A-B = \{a-b : a \in A, b \in B\}$ for the *difference set* of A and B;
(iii) $kA = \underbrace{A+A+\cdots+A}_{k \text{ copies}}$ for the *k-fold iterated sumset* of A, where $k \in \mathbb{N}$;
(iv) $-A = \{-a : a \in A\}$;
(v) $(-k)A = -(kA)$ for $k \in \mathbb{N}$;
(vi) $t+A = \{t\}+A$ for the *translate* of A by $t \in G$; and
(vii) $d \cdot A = \{da : a \in A\}$ for the *dilate* of A by $d \in \mathbb{Z}$.

Be careful not to confuse kA and $k \cdot A$; these sets will in general be very different. Note also that the notation $A-B$ will only be used in the above sense in this course; we shall write the set-theoretic difference of A and B as $A \setminus B$.

Example 2.2. Let $A = \{0, 1, \ldots, n-1\}$ be a set of integers. Then $A+A = \{0, 1, \ldots, 2n-2\}$ and $A-A = \{-(n-1), \ldots, -1, 0, 1, \ldots, n-1\}$. Thus $|A+A| = |A-A| = 2|A|-1$ for this example. Can you give other examples of sets with this property?

In general $A+A$ and $A-A$ may have quite different sizes, though there are relations between them as we shall see later on. Let us focus on $A+A$ for now. Could it be that there is a set of integers A such that $|A+A| \leqslant 2|A|-2$? The following result says that this is not possible: there is a minimum amount by which the sum of two sets of integers must grow compared to the summands.

Theorem 2.3. *Let A and B be additive sets of integers. Then $|A+B| \geqslant |A|+|B|-1$.*

Proof. Note that if X is a subset of an abelian group G, then $|t+X| = |X|$ for any $t \in G$: translation never affects the size of a set. (Can dilation affect the size of a set?) So by replacing A and B by translates if necessary, we may assume that $\max A = \min B = 0$. Hence $A+B$ consists of at least $|A|-1$ integers less than 0, at least $|B|-1$ integers greater than 0, and 0 itself. So $|A+B| \geqslant (|A|-1)+(|B|-1)+1$, as required. □

Exercise 2.4. Write out the above proof in full, without the "we may assume". Once familiar, this type of trick can save one a lot of time and writing.

In particular we have $|A+A| \geqslant 2|A|-1$ for any additive (that is, non-empty and finite) set A of integers. How large can $A+A$ be?

Exercise 2.5. Let $A = \{1, 2, 4, \ldots, 2^{n-1}\}$ be a set of integers. What is $|A+A|$?

Exercise 2.6. Suppose $A = \{0, 1, \ldots, n-1\}$ and $B = \{0, n, 2n, \ldots, (n-1)n\}$ are sets of integers. What is $A+B$? How does its size compare to those of A and B?

These exercises should convince you that $A+A$ (and $A+B$) can be substantially larger than A (and B); in fact $|A+A|$ can grow as a quadratic in $|A|$. We shall make this more precise later; for now we shall focus on for what types of sets $A+A$ can be *small* compared to A. In Example 2.2 we saw that intervals $\{0,1,\dots,n-1\}$ have comparatively small sumset; in fact their sumsets are as small as they could possibly be, by Theorem 2.3. This leads to some natural questions: what can one say about A if $|A+A| = 2|A|-1$; must A be 'similar to' an interval? What if $|A+A| \leqslant 4|A|$, or if $|A+A| \leqslant K|A|$ where K is some fixed constant (so that $|A+A|$ only grows linearly with $|A|$ and not quadratically)?

Definition 2.7. Let A be an additive subset of an abelian group. We write

$$\sigma[A] = \frac{|A+A|}{|A|}$$

for the *doubling constant* of A.

One is then faced with a basic question: what do sets with small doubling constant (or simply *small doubling*), say $\sigma[A] \leqslant K$, look like?[1] A moment's thought will reveal that if A is any set of integers and t, d are integers with $d \neq 0$, then the set $t + d \cdot A$ has the same doubling constant as A. Thus we must allow translates and dilates of sets with small doubling in any list of sets with small doubling. In particular, we must allow the following family.

Example 2.8. Write $[0,m] = \{0,1,\dots,m\}$. Any arithmetic progression $P = \{a, a+d, \dots, a+nd\} = a + d \cdot [0,n]$ has small doubling constant: $\sigma[P] = 2 - \frac{1}{|P|}$.

Furthermore, we must allow 'dense' subsets of sets with small doubling.

Example 2.9. Let $A \subseteq [0, 2n-1]$ be a set of n integers. Since $A+A \subseteq [0, 4n-2]$, we certainly have $|A+A| \leqslant 4|A|$. More generally, if $A \subseteq B$ are two finite subsets of an abelian group such that $|A| \geqslant \alpha|B|$ and $\sigma[B] \leqslant K$, then A has small doubling: $\sigma[A] \leqslant K/\alpha$.

(Note that the doubling constant will in general be larger for the subset; the point is, however, that if the density of the subset is fixed then so is the bound on the new doubling constant.)

Could it be that these examples give a complete description of sets with small doubling? Any such thoughts are dashed by the following example.

Example 2.10. Let $n \geqslant 2$ and $M \geqslant 100n$ be integers, and set

$$A = A_M = [0, n-1] + M \cdot [0, n-1] \subseteq \mathbb{Z}.$$

Then $|A| = n^2$ (why?) and $A+A = [0,2n-2] + M \cdot [0,2n-2]$ has size $(2n-1)^2 \leqslant 4|A|$; thus A has small doubling. Since M can be arbitrarily large, however, there is no fixed density α for which each set A_M can be considered to be a subset of an arithmetic progression P_M of size at least $\alpha|P_M|$. In particular, this family of examples is not covered by those given by Example 2.9 if one only considers dense subsets of arithmetic progressions.

Remark 2.11. This is really the example $[0, n-1] \times [0, n-1]$ from the group $\mathbb{Z}^2$: we have projected it to $\mathbb{Z}$ via the map $(x,y) \mapsto x + My$. We shall formalise this idea later using the notion of Freiman homomorphisms.

[1] Remember that we are after quantitative descriptions: the answer here should depend on K in such a way that it gives non-trivial information when K is a fixed number and $|A|$ is large.

Examples 'like this', allowing for higher dimensions, must thus also be added to our list of sets with small doubling (together with their dense subsets, of course). Quite remarkably, it turns out that we have now found essentially *all* examples of sets with small doubling: the precise statement is known as Freiman's theorem and will be one of the main results of the course. Its proof will be highly non-trivial, and we shall need to develop several powerful tools before we are able to tackle it.