Lecture 8

Schnirelmann's Theorem

Goldbach's conjecture asserts that any integer ≥ 4 can be expressed as the sum of two or three primes, depending on parity. Schnirelmann proved the following weaker result in 1933:

Theorem 1 (Schnirelmann) There is a bound k, such that every integer greater than 1 is the sum of at most k primes.

Asymptotic and Schnirelmann Density

A finite set is naturally measured by its cardinality. A set of reals is naturally measured its Lebesgue measure (I suppose non-measurable set exist, but we never meet them). There is however no similar universal way to measure and compare infinite sets of integers. The most naturally defined one is that of asymptotic density.

For a set $A \subseteq \mathbb{Z}$ we shall use the same letter to denote its counting function

$$A(x) := \#\{n \in A : 1 \leq n \leq x\}.$$

* We allow A to contain 0 and negative numbers, but they are not taken into account in the counting function.

For us the best universe to work with will be $\mathbb{Z}_{\geq 0}$, the non-negative integers.

Definition 1: The asymptotic density (in $\mathbb{N}$) of a set $A \subseteq \mathbb{Z}$ is defined by

$$\delta(A) := \lim_{x \to \infty} A(x)/x \text{ , if this limit exists.}$$

The upper & lower (asymptotic) densities are the corresponding upper and lower limits, respectively:

$$\overline{\delta}(A) := \limsup_{x \to \infty} A(x)/x \quad \& \quad \underline{\delta}(A) := \liminf_{x \to \infty} A(x)/x \text{ .}$$

Exercise (1):

(a) If $\underline{\delta}(A) > 0$, is there always a set $A' \subseteq A$ with $\delta(A') > 0$?

(b) Show that if $\underline{\delta}(A) + \underline{\delta}(B) > 1$, then $A+B$ contains all but finitely many positive integers.

(c) Let $\alpha, \beta, \gamma \in \mathbb{R}_{>0}$ with $\alpha + \beta \leq \gamma \leq 1$. Construct sets $A, B, C \subseteq \mathbb{N}$ such that $\delta(A) = \alpha$, $\delta(B) = \beta$ and $\delta(A+B) = \gamma$.

Definition 2: A set $A \subseteq \mathbb{Z}_{\geq 0}$ is a basis of finite order if $hA = \mathbb{Z}_{\geq 0}$ for some $h \in \mathbb{N}$, where $hA := \underbrace{A + \cdots + A}_{h \text{ times}}$.

(Recall that $A+B := \{a+b : a \in A, b \in B\}$.)

In otherwords, every element of $\mathbb{Z}_{\geq 0}$ can be expressed as the sum of h integers from A. Note that to be a basis, a set must contain 0 & 1.

Schnirelmann's Theorem $\iff$ $\mathcal{P} \cup \{0,1\}$ form a finite basis.

↑ all primes

Schnirelmann established that $\underline{\delta}(2\mathcal{P}) > 0$ (a result which in hindsight is not too difficult, later in this course we will show that in fact $\delta(2\mathcal{P}) = 1/2$); and every set (containing 0 & 1) with positive lower density form a finite basis.

To prove the second of these claims, Schnirelmann introduced a different notion of density.

Definition 3: The Schnirelmann density of a set $A \subseteq \mathbb{Z}_{\geq 0}$ is defined by

$$\sigma(A) := \inf_{x \in \mathbb{N}} A(x)/x .$$

* This is a much less natural concept that asymptotic density. For example, since $\sigma(A) = 0$ if $1 \notin A$, it follows that the Schnirelmann density of the odd integers is $\frac{1}{2}$, while the density of the even integers is 0.

Exercise (2): (a) Show that $\sigma(A) > 0 \iff 1 \in A$ & $\underline{\delta}(A) > 0$.

(b) $$\underline{\delta}(A) = \sup_n \sigma(A - n)$$

Theorem 2 (Schnirelmann) If $A \subseteq \mathbb{Z}_{\geq 0}$, with $0 \in A$ & $\sigma(A) > 0$, then A is a basis of finite order.

As noted above we will apply this theorem with $A = 2\mathcal{P} \cup \{0, 1\}$, we of course still has to establish that $\underline{\delta}(2\mathcal{P}) > 0$ (and Theorem 2).

Proof of Theorem 1 (assuming Theorem 2 & $\underline{\delta}(2\mathcal{P})>0$).

Since $\underline{\delta}(2\mathcal{P})>0$ it follows from Theorem 2 that the set $2\mathcal{P}\cup\{0,1\}$ is a basis of order h, for some $h\geq 1$. Thus for every integer $n\geq 2$,

$$n-2 = p_1+\cdots+p_{2m}+\underbrace{1+1+\cdots+1}_{\ell \text{ times}}$$

where the p_j are primes, and $m,\ell\in\mathbb{Z}_{\geq 0}$ with $m+\ell\leq h$.

Then

$$n = p_1+\cdots+p_{2m}+(\ell+2).$$

Since $\ell+2\geq 2$, it can be written as a sum of 2's and 3's, where the number of summands is at most $\frac{\ell+2}{2}\leq \frac{h}{2}+1$. This means that n has a representation as the sum of at most $2m+\frac{h}{2}+1\leq \frac{5h}{2}+1$ primes. Theorem 1 follows with $k=\frac{5h}{2}+1$. □

Proof that $\underline{\delta}(2\mathcal{P})>0$:

Let $R(N)$ denote the number of representation of N as the sum of two primes.

Lemma 1: $$\sum_{N\leq X} R(N) \gg \frac{X^2}{(\log X)^2}.$$

Proof: If p_1 & p_2 are primes such that $p_1, p_2\leq \frac{X}{2}$, then $p_1+p_2\leq X$ and

$$\sum_{N\leq X} R(N) \geq \pi(X/2)^2 \gg \frac{(X/2)^2}{(\log(X/2))^2} \gg \frac{X^2}{(\log X)^2}$$

by Chebyshev's theorem. □

Lemma 2: $\displaystyle\sum_{N\le x} R(N)^2 \ll \frac{x^3}{(\log x)^4}$.

Proof: Recall from Theorem 7.4 that

$$R(N) \ll \frac{N}{(\log N)^2}\cdot\prod_{p\mid N}\left(1+\frac{1}{p}\right) \le \frac{N}{(\log N)^2}\sum_{d\mid N}\frac{1}{d}.$$

Therefore

$$\sum_{N\le x} R(N)^2 \ll \frac{x^2}{(\log x)^4}\underbrace{\sum_{N\le x}\left(\sum_{d\mid N}\frac{1}{d}\right)^2}_{(*)}$$

and it suffice to show that $(*)=O(x)$. To do this we observe that

$$[d_1,d_2] \ge \max\{d_1,d_2\} \ge (d_1d_2)^{1/2}$$

and hence

$$\sum_{N\le x}\left(\sum_{d\mid N}\frac{1}{d}\right)^2 = \sum_{N\le x}\sum_{\substack{d_1\mid N\\ d_2\mid N}}\frac{1}{d_1d_2} = \sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\sum_{\substack{N\le x\\ d_1\mid N,\, d_2\mid N}} 1$$

$$\le \sum_{d_1,d_2\le x}\frac{1}{d_1d_2}\frac{x}{[d_1,d_2]}$$

$$\le x\sum_{d_1,d_2\le x}\frac{1}{(d_1d_2)^{3/2}} \le x\left(\sum_{d}\frac{1}{d^{3/2}}\right)^2 \ll x. \qquad \square$$

Theorem 3: $\delta(2\mathcal{P})>0$,

in particular $2\mathcal{P}(x)\gg x$ as $x\to\infty$.

Proof: It follows from Lemmas 1 & 2, together with Cauchy-Schwarz that

$$\frac{x^4}{(\log x)^4} \ll \left(\sum_{N\le x} R(N)\right)^2 = \left(\sum_{\substack{N\le x\\ R(N)>0}} R(N)\cdot 1\right)^2 \le \sum_{N\le x} R(N)^2 \underbrace{\sum_{\substack{N\le x\\ R(N)>0}} 1}_{=2\mathcal{P}(x)} \ll \frac{x^3}{(\log x)^4}\,2\mathcal{P}(x). \qquad \square$$

Proof of Theorem 2.

It remains for us to prove "Schnirelmann's basis theorem", namely Theorem 2. Schnirelmann deduced this result from the following inequality:

Lemma 3 (Schnirelmann's inequality) If $0 \in A$ and $1 \in B$, then

$$\sigma(A+B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Proof: Put $C = A+B$, we will estimate $C(n)$ for arbitrary $n \in \mathbb{N}$. Let

$$1 = b_1 < \cdots < b_k \leq n$$

be the elements of B in $\{1, \ldots, n\}$. Note that $k = B(n) \geq n\sigma(B)$ and since $0 \in A$ that these element are also in C. Further elements of C are given by

$$b_1 + (A \cap \{1, \ldots, b_2 - b_1 - 1\}),\ b_2 + (A \cap \{1, \ldots, b_3 - b_2 - 1\}),\ \ldots,$$

$$b_{k-1} + (A \cap \{1, \ldots, b_k - b_{k-1} - 1\}),\ b_k + (A \cap \{1, \ldots, n - b_k\}).$$

(the last block may be empty if $b_k = n$).

We can estimate the number of elements in a typical block by $A(m) \geq m\sigma(A)$ (even if $m = 0$) and hence

$$C(n) \geq k + \sigma(A)\left\{(b_2 - b_1 - 1) + (b_3 - b_2 - 1) + \cdots + (b_k - b_{k-1} - 1) + (n - b_k)\right\}$$

$$= k + \sigma(A)\,(n-k)$$

$$= \sigma(A)n + (1 - \sigma(A))\,n\,\sigma(B)$$

$$= \left(\sigma(A) + \sigma(B) + \sigma(A)\sigma(B)\right)n. \qquad \square$$

We can rewrite Schnirelmann's inequality in the symmetric form:

$$1-\sigma(A+B) \leq (1-\sigma(A))(1-\sigma(B)).$$

An iterated application then gives for any $h \in \mathbb{N}$ & A (containg 0&1)

$$1-\sigma(hA) \leq (1-\sigma(A))^h.$$

Notice that if $\sigma(A)>0$, then $(1-\sigma(A))^h \to 0$ as $h \to \infty$. We complement this inequality with the following easy

Lemma 4: If $0 \in A \cap B$ and $\sigma(A)+\sigma(B) \geq 1$, then $A+B \supseteq \mathbb{Z}_{\geq 0}$.

Proof (Pigeonhole Principle). Notice that $0 \in A \cap B \Rightarrow A \cup B \subseteq A+B$.

Suppose that $A+B \not\supseteq \mathbb{Z}_{\geq 0}$ and let n be the smallest natural number such that $n \notin A+B$. Then $n \notin A \cup B$, and A & $n-B$ are disjoint.

Let $C = A \cup (n-B)$, it follows that

$$n-1 \geq C(n-1) = A(n-1)+(n-B)(n-1) = A(n-1)+B(n-1) = A(n)+B(n) \geq (\sigma(A)+\sigma(B))n \geq n,$$

a contradiction. □

Proof of Theorem 2: Let $A \subseteq \mathbb{Z}_{\geq 0}$ with $0 \in A$ & $\sigma(A)>0$. If we take $h \in \mathbb{N}$ such that $(1-\sigma(A))^h \leq \frac{1}{2}$, then $\sigma(hA) \geq \frac{1}{2}$ & hence $\underbrace{2hA}_{=hA+hA} \supseteq \mathbb{Z}_{\geq 0}$

□

Note: The above argument estimates the order of the basis $(2h)$ by

$$\log 4 / \log(1-\sigma(A))^{-1} \leq \log 4 / \sigma(A).$$

Concluding Remarks

1. In Schnirelmann's inequality the role of the sets A & B is asymmetric: one must contain 0 while the other need not. This inequality can however be improved under the symmetric assumption $0 \in A \cap B$, which is also better suited for the repeated addition of the same set.

Theorem (Mann) If $0 \in A \cap B$, then $\sigma(A+B) \geq \min\{1, \sigma(A)+\sigma(B)\}$.

Thus if $0 \in A$, then $\sigma(hA) \geq \min\{1, h\sigma(A)\}$ and we obtain the following

Corollary: If $0 \in A$ & $\sigma(A) > 0$, then A has a basis of order $\leq 1/\sigma(A)$.

(I will prove Mann's Theorem in an additional short note - see webpage).

2. It is a result of Ramaré (1995) and Tao (2 weeks ago!!) respectively that every even natural number is the sum of at most 6 primes and that every odd integer > 1 is the sum of at most 5 primes.

Towards the end of this course we will establish:

Theorem (Vinogradov)

Let $R_3(N)$ denote the number of ways of writing N as an ordered sum of 3 primes. As $N \to \infty$ through the odd integers, we have

$$R_3(N) \sim \frac{1}{2} \prod_{p \nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p \mid N} \left(1 - \frac{1}{(p-1)^2}\right) \frac{N^2}{(\log N)^3}.$$

In particular, every sufficiently large odd integer is the sum of 3 primes.