Addative Combinatorics

March 20, 2009

Books: There is really only one book in this field, *Addative Combinatorics* by T. Tao and V. H. Vu. This is very expensive, and while it makes a good reference work, is not ideal for first-time learning of the material; it is therefore recommended only for the reader who is considering a PhD in the field. Printed notes for the course will be made available on the lecturer's website following the lectures they relate to; also, the lecturer intends to write a book of the course, in collaboration with Gowers, though this will probably differ substantially from the lectures.

Notation: We use the "Big Oh, little oh" notation used throughout analysis. Suppose we have two functions, $f, g : \mathbb{N} \to \mathbb{C}$ (say; sometimes $\mathbb{R}$). We say $f(n) = O(g(n))$ to mean there is an absolute constant C such that $|f(n)| \leq Cg(n)$ for n sufficiently large. We say $f(n) = o(g(n))$ if, for any $\epsilon > 0$, we have $|f(n)| \leq \epsilon g(n)$ provided $n \geq N_0(\epsilon)$. Occasionally the absolute constant C, or $N_0(\epsilon)$, may depend on some other parameters $k_1, k_2, \ldots$; this will be indicated using subscripts, e.g. $kn^2 = O_k(n^2)$.

C, c always denote absolute positive constants, whose value could be worked out explicitly if one wished; we always have $0 < c < 1 < C$ [this seems to be false in the case of c]. Different instances of this notation can and frequently will denote different absolute constants, even on the same line. Again there will sometimes be subscripts indicating dependence on other parameters.

If X is a finite set and $f : X \to \mathbb{C}$ is a function, write $\mathbb{E}_{x \in X} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$ (it is traditional to use this rather than summing in this field; it tends to require fewer junk constants in our expressions). $e(\theta)$ always means $e^{2\pi i \theta}$. Finally $\|x\|_{\frac{\mathbb{R}}{\mathbb{Z}}}$ denotes the absolute value of the fractional part of x, e.g. $\|0.9\|_{\frac{\mathbb{R}}{\mathbb{Z}}} = 0.1$.

1 Roth's Theorem on Progressions of Length 3

Theorem (Roth, 1953): Suppose N is sufficiently large and $A \subset \{1, \ldots, N\}$ has $|A| \geq \frac{cN}{(\log \log N)^{\frac{1}{5}}}$. Then A contains a non-trivial 3-term arithmetic progression (AP), i.e. a triple $x, x+d, x+2d$ with $d \neq 0$.

Remark: The key point of this is that $(\log \log N)^{\frac{1}{5}} \to \infty$, hence e.g. if $|A| \geq \frac{N}{100}$ then, provided N is sufficiently large, A contains a 3-term AP. Also, the original proof of this theorem gives $\log \log N$ where this proof has $(\log \log N)^{\frac{1}{5}}$, but we wish to use an argument which generalizes more smoothly to longer APs.

The overall proof strategy is the dentsity increment strategy; the key is the following proposition:

Proposition (Density increment step): Suppose $0 < \alpha < 1$ and $N > C\alpha^{-c}$. Suppose that P is a [arithmetic] progression of length N. Suppose that $A \subset P$ has cardinality at least αN. Then at least one of the following holds: i) A contains at least $\frac{1}{10}\alpha^3 N^2$ nontrivial 3-term APs (and hence at least one), ii) There is another progression (actually a subprogression) P' with $|P'| \geq N^{\frac{1}{3}}$ such that, writing $A' = A \cap P'$, we have $\frac{|A'|}{|P'|} = \alpha' \geq \alpha + c\alpha^6$.

Deduction of Roth's Theorem from this: Suppose $A \subset \{1, \ldots, N\}$, $|A| = \alpha|N|$ and that A contains no nontrivial 3APs. (Try to) apply the preceding proposition repeatedly, obtaining a sequence $P_0, P_1, \ldots$ of progressions ($P_0 = \{1, \ldots, N\}$) together with sets $A_i := A \cap P_i$ such that, writing $\alpha_i = \frac{|A_i|}{|P_i|}$, we have $|P_i| \geq N^{(\frac{1}{3})^i}$ and $\alpha_{i+1} \geq \alpha_i + c\alpha_i^6$. Note that after $\frac{c}{\alpha^5}$ steps of this iteration, α has already doubled; after another $\frac{c}{(2\alpha)^5}$ steps we've reached 4α and so on. The density becomes > 1 after $\frac{c}{\alpha^5}$ steps, which is clearly nonsense. So it can't have been valid to keep applying the proposition; the condition $|P_i| > C\alpha_i^{-c}$ must be violated for some $i \leq \frac{C}{\alpha^5}$. Note however that $\alpha_i \geq \alpha$ and $|P_i| \geq N^{(\frac{1}{3})^{\frac{C}{\alpha^5}}}$. Therefore $N^{(\frac{1}{3})^{\frac{C}{\alpha^5}}} \leq C\alpha^{-c}$. Taking logs, $(\frac{1}{3})^{\frac{C}{\alpha^5}} \log N \leq \log(C\alpha^{-c})$; taking logs again, $-\frac{C}{\alpha^5} + \log\log N \leq \log\log(C\alpha^{-c})$. Hence $\log\log N \leq \log\log(C\alpha^{-c}) + \frac{c}{\alpha^5} \leq \frac{c'}{\alpha^5}$ and thus $\alpha \leq C(\log\log N)^{-\frac{1}{5}}$ as claimed.

An interpretation of the proposition: there are essentially two types of sets $A \subset \{1, \ldots, N\}$: "random" sets, which are essentially a random scattering of points and will by chance include many 3APs, and "structured" sets, which are essentially unions of some series of intervals. These may not contain (many) 3APs, but they will contain these interval subsets where the density is much higher than that of A. The proposition draws a formal distinction between these two types of set.

Proof of the density increment proposition: By rescaling P, we may wlog take $P = \{1, \ldots, N\}$. (This affects neither the density of A nor the count of 3APs in A.) First, an ugly technical manouver: let N' be a prime (actually, we only need an odd number) of size $\sim 10N$ (actually, we only need larger than $2N$) and consider A as a subset of $\frac{\mathbb{Z}}{N'\mathbb{Z}}$, which we shall call G. Write $\tilde{A}$ for the copy of A inside G. Observe that the number of 3APs in $\tilde{A}$ is the same as the number in A since there are no "wraparound" issues. Henceforth we shall drop the tildes and think of A as a subset of $\frac{\mathbb{Z}}{N'\mathbb{Z}} = G$.

Notation: Let $f_1, f_2, f_3 : G \to \mathbb{C}$ be functions. Write $AP_3(f_1, f_2, f_3) = \mathbb{E}_{x,d \in G} f_1(x) f_2(x+d) f_3(x+2d)$. In particular, $AP_3(1_A, 1_A, 1_A)$ (1_A being the characteristic function of A, $1_A(x) = 1$ if $x \in A$, 0 otherwise) $= \frac{1}{(N')^2}$ times the number of 3APs in A, including the trivial ones (x, x, x).

Define the <u>balanced function</u> $f = 1_A - \alpha 1_{[n]}$ (where $[n] = \{1, \ldots, N\} \subset G$). We can see $\alpha 1_{[n]}$ as in some sense representing a "random set of size $|A|$", though of course it is not the characteristic function of any specific set. We'll compare $AP_3(1_A, 1_A, 1_A)$ with $AP_3(\alpha 1_{[n]}, \alpha 1_{[n]}, \alpha 1_{[n]})$.

Lemma: Suppose $0 < \alpha < 1$ and $N > C\alpha^{-c}$. Suppose that $A \subset \{1, \ldots, N\} \subset G$ has cardinality αN and at most $\frac{1}{10}\alpha^3 N^2$ non-trivial 3-term APs. Then there are 1-bounded functions (i.e. functions whose absolute value is always ≤ 1) g_1, g_2, g_3, at least one of which is the balanced function f of A, such that $|AP_3(g_1, g_2, g_3)| \geq c\alpha^3$: Write $1_A = f + \alpha 1_{[N]}$. Now AP_3 is trilinear, so we can expand $AP_3(1_A, 1_A, 1_A)$ as a sum of eight terms - a main term $AP_3(\alpha 1_{[N]}, \alpha 1_{[n]}, \alpha 1_{[n]})$ and seven terms of the form $AP_3(g_1, g_2, g_3)$ with at least one of the g_i being f. The main term is $\frac{\alpha^3}{(N')^2}$ times the number of 3-term APs in $\{1, \dots, N\}$; this is easy to calculate but we only need a crude bound: if we choose $x, d \leq \frac{N}{3}$ then $x, x+d, x+2d$ all lie in $\{1, \dots, N\}$, and so the number of 3-term APs in $\{1, \dots, N\}$ si at least $\frac{N^2}{9}$. Thus the main term is $\geq \frac{\alpha^3}{0}(\frac{N}{N'})^2$. On the other hand, by assumption $AP_3(1_A, 1_A, 1_A) \leq \frac{\alpha^3}{10}(\frac{N}{N'})^2 + (\frac{N}{N'})^2$ (the second term here being for the trivial 3APs); if c is chosen appropriately this is certainly at most $\frac{10\alpha^2}{99}(\frac{N}{N'})^2$. By the triangle inequality, at least one of the other seven terms is then at least $\frac{1}{7}(\frac{1}{9} - \frac{10}{99})\alpha^3(\frac{N}{N'})^2 \geq c\alpha^3$, as required.

The Gowers u^2-norm

There is a family of norms, the Gowers u^k-norms, defined for functions $f : G \to \mathbb{C}$, where G is any (finite) abelian group. (Generally, the Gowers u^k norm is useful when studying $(k+1)$APs).

Definition: Let $f : G \to \mathbb{C}$ be a function. Then we define $\|f\|_{u^2} = (\mathbb{E}_{x,h_1,h_2 \in G} f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2))^{\frac{1}{4}}$.

Remarks: i) The quantity whose fourth root is being taken is real and nonnegative; we shall see this as a byproduct of the proof of the next lemma. 2) This is a valid norm; in particular $\|f+g\|_{u^2} \leq \|f\|_{u^2} + \|g\|_{u^2}$. We shall not use this fact in the course; it may be proven on the example sheet.

The relation between Gowers norms and 3APs is given by a so-called "generalised von Neumann theorem":

Lemma (Generalised VN): Let $f_1, f_2, f_3 : G \to \mathbb{C}$ be 1-bounded functions. Then $|AP_3(f_1, f_2, f_3)| \leq \|f_i\|_{u^2}$ for $i = 1, 2, 3$.

Observation (Cauchy-Schwartz inequality): Let $b : G \to \mathbb{C}$ be a 1-bounded function and let $F : G \times G \to \mathbb{C}$ be another function. Then $|\mathbb{E}_{x,y \in G} b(x)F(x,y)| \leq (\mathbb{E}_{x,y,y' \in G} F(x,y)\overline{F(x,y')})^{\frac{1}{2}}$: Apply C-S in its usual form $(\mathbb{E}_x \alpha_x \beta_x \leq (\mathbb{E}_x |\alpha_x|^2)^{\frac{1}{2}} (\mathbb{E}_x |\beta_x|^2)^{\frac{1}{2}})$ with $\alpha_x = b(x), \beta_x = \mathbb{E}_y F(x,y)$.

Proof of generalised von Neumann theorem: The key is to rewite $AP_3(f_1, f_2, f_3)$ so that Cauchy-Schwartz can be used. We shall do the case $i = 1$; the other two are very similar. Note that $AP_3(f_1, f_2, f_3) = \mathbb{E}_{x,y \in G} f_1(2x-y)f_2(x)f_3(y)$: since N' is odd, the triple $2x-y, x, y$ ranges over all 3-term APs once each. Applying C-S once we get $|AP_3(f_1, f_2, f_3)|^2 \leq \mathbb{E}_{x,y,y'} f_1(2x-y)\overline{f_1(2x-y')}f_3(y)\overline{f_3(x')}$ (since $|f_2(x)| \leq 1$); applying C-S once more, observing that $|f_3(y)\overline{f_3(y')}| \leq 1$, we obtain $|AP_3(f_1, f_2, f_3)|^4 \leq \mathbb{E}_{x,x',y,y'} f_1(2x-y)\overline{f_1(2x-y')f_1(2x'-y)}f_1(2x'-y')$. But as x, x', y, y' range over G, the quadruple $2x-y, 2x-y', 2x'-y, 2x'-y'$ ranges over parallelograms, covering each precisely N' times. So the RHS here is precisely $\|f_1\|_{u^2}^4 = \mathbb{E}_{x,h^1,h^2} f_1(x)\overline{f_1(x+h_1)f_1(x+h_2)}f_1(x+h_1+h_2)$ $(\star)$.

Remark: It has come to our attention that $(\star)$ is real and nonnegative.

Corollary: Suppose $0 < \alpha < 1, A \subset \{1, \dots, N\}, |A| = \alpha N$ and A has at most $\frac{1}{10}\alpha^3 N^2$ non-trivial 3APs. Suppose also $N > C\alpha^{-c}$ and let $f = 1_A - \alpha 1_{[N]}$ be the balanced function of A (recall this is defined on $G = \frac{\mathbb{Z}}{N'\mathbb{Z}}$. Then the Gowers u^2-norm $\|f\|_{u^2} \geq c\alpha^3$.

An inverse theorem for the u^2-norm

So far we have been "shifting the hard part": we have some property of A which we don't really understand, but can use it to prove that A has some other property - but we don't really understand this, either. What can we say about f if $\|f\|_{u^2} \geq \delta$?

The discrete fourier transform: Suppose $f : G \to \mathbb{C}$ is a function ($G = \frac{\mathbb{Z}}{N'\mathbb{Z}}$, though some of our comments apply to general abelian groups). Then we define, for $r \in \frac{\mathbb{Z}}{N'\mathbb{Z}}$, $\widehat{f}(r) := \mathbb{E}_{x\in G} f(x)e(\frac{-rx}{N'})$ (recall $e(y) = e^{2\pi iy}$).

Lemma (Basic properties of the FT): Let $f, g : G \to \mathbb{C}$. Then i) $\|\widehat{f}\|_2 = \|f\|_2$ where $\|f\|_2 := (\mathbb{E}_{x\in G}|f(x)|^2)^{\frac{1}{2}}$, $\|\widehat{f}\|_2 := (\sum_{r\in G} |\widehat{f}(r)|^2)^{\frac{1}{2}}$. (For now, the reader may simply view these as definitions. The difference comes from the fact that one of our copies of G here is actually $\widehat{G}$, the dual group; an abelian group is always isomorphic to its dual, but this does not carry over to the [measure?] on the group. More on this later). ii) If we define the convolution $f \star g(x) := \mathbb{E}_{y\in G} f(y)g(x-y)$ then $\widehat{f \star g} = \widehat{f}\widehat{g}$. (If $f = 1_A, g = 1_B$ then $\text{supp}(f \star G) = A + B = \{a + b : a \in A, b \in B\}$; this is part of "what convolutions are for", which is poorly explained in the tripos). iii) $\|f\|_{u^2} = \|\widehat{f}\|_4 := (\sum_{r\in G} |\widehat{f}(r)|^4)^{\frac{1}{4}}$. i) is a very easy consequence of the identity $\mathbb{E}_{x\in G} e(\frac{(r-s)x}{N'}) = \delta_{r,s}$ (i.e. 1 if $r = s$, 0 otherwise); this is "orthogonality of characters", or this case can be verified quite directly by summing the GP; making this a complete proof is an exercise, as is the even easier part ii). For iii), one could check this directly by computation, but this would not give us a good sense of "why" it is true. Note that $\|f\|_{u^2}^4 = \|f \star f\|_2^2$: the RHS here is $\|f \star f\|_2^2 = \mathbb{E}_x|\mathbb{E}_y f(y)f(x-y)|^2 = \mathbb{E}_{x,y,y'} f(y)f(x-y)\overline{f(y')f(x-y')}$. But as x, y, y' range over G, the quadruple $y, x-y, y', x-y'$ ranges over the parallelograms used to define u^2.

Proposition (inverse theorem for the u^2 norm): Let $0 < \delta < 1$ and suppose $f : G \to \mathbb{C}$ is a 1-bounded function ($|f(x)| \leq 1$). Suppose $\|f\|_{u^2} > \delta$. Then there is some $r \in \frac{\mathbb{Z}}{N'\mathbb{Z}}$ such that $|\mathbb{E}_{x\in\frac{\mathbb{Z}}{N'\mathbb{Z}}} f(x)e(-\frac{rx}{N'})| \geq \delta^2$ (Exercise: show the "converse"; one cannot prove an exact converse to this, we will "lose a little in the powers of δ". See the firstexample sheet). The conclusions correspond to $\|\widehat{f}\|_\infty \geq \delta^2$. The assumption that $\|f\|_{u^2} > \delta$ implies, by part iii) of the above lemma, that $\|\widehat{f}\|_4 \geq \delta$. But $\|\widehat{f}\|_4^4 \leq \|\widehat{f}\|_2^2\|\widehat{f}\|_\infty^2$ (an instance of $\sum_{i=1}^m a_i^2 \leq (\max_i a_i)\sum_{i=1}^m a_i$, which is valid for real nonnegative a_i: take $a_r = |\widehat{f}(r)|^2$). But $\|\widehat{f}\|_2 = \|f\|_2 \leq 1$. Therefore $\|\widehat{f}\|_\infty \geq \delta^2$, as required.

Combining this with the above corollary we get:

Corollary: Suppose $0 < \alpha < 1, A \subset \{1, \ldots, N\}, |A| = \alpha N$ and A has at most $\frac{1}{10}\alpha^3N^2$ nontrivial 3APs. Let $f = 1_A - \alpha$ (yes, this is different from the balanced function we had before). Then there is some $\theta \in \mathbb{R}$ such that $|\sum_{x\in\{1,\ldots,N\}} f(x)e(-\theta x)| \geq c\alpha^6 N$.

Note: $\frac{\mathbb{Z}}{N'\mathbb{Z}}$ has disappeared; it has served its purpose.

Remark: Applying the inverse theorem for u^2 to the corollary at the start of the lecture gives some $r \in \frac{\mathbb{Z}}{N'\mathbb{Z}}$ such that $|\mathbb{E}_{x\in\frac{\mathbb{Z}}{N'\mathbb{Z}}} f(x)e(-\frac{rx}{N'}| \geq c\alpha^6$. Now take $\theta = \frac{r}{N'}$, note that $\text{Supp}(f) \subset \{1, \ldots, N\}$ and change the $\mathbb{E}$ into a $\sum$.

This looks a bit like the required "density increment" proposition: recall we wanted a progression $P \subset \{1, \ldots, N\}$ with $|P| \geq N^{\frac{1}{3}}$ such that $\sum_{x\in P} f(x) \geq c\alpha^6|P|$ (trivially equivalent to $|A \cap P| \geq (\alpha + c\alpha^6)|P|$.

Lemma (Dirichlet) (This is the lemma for which the pigeonhole principle was invented) Let $\theta \in \mathbb{R}$ and let $0 < \delta < 1$. Then there is a positive integer d, $1 \le d \le \frac{1}{\delta}$ such that $\|\theta d\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \le \delta$: let $L = \lfloor \frac{1}{\delta} \rfloor$ and consider the numbers $0, \theta, 2\theta, \ldots, L\theta$ (mod 1). By Dirichlet's Principle of the Pigeons, some two of these, say $j\theta, j'\theta$, differ by at most $\frac{1}{L+1} \le \delta$. Then $d := |j - j'|$ gives the lemma.

Lemma: Suppose $0 < \eta < 1$ and $N > C\eta^{-6}$. Then we can partition $\{1, \ldots, N\}$ into progressions $P_1, \ldots, P_k$, each of length at least $N^{\frac{1}{3}}$, such that $\sup_{x,x' \in P} |e(\theta x) - e(\theta x')| \le \eta \forall i$: take $\delta = \frac{1}{20}\eta N^{-\frac{1}{3}}$ in the previous lemma. We can find a $d \le \frac{1}{\delta}$, thus in particular $d \le \sqrt{N}$, such that $\|\theta d\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \le \delta$. Let P be any progression with common difference d and length $\le 2N^{\frac{1}{3}}$. Then $\sup_{x,x' \in P} |e(\theta x) - e(\theta x')| \le 2N^{\frac{1}{3}} |e(\theta d) - 1|$ (by the triangle inequality). But it is easy to see that $|e(t) - 1| = 2|\sin \pi t| \le 2\pi \|t\|_{\frac{\mathbb{R}}{\mathbb{Z}}}$. Hence $\sup_{x,x' \in P} |e(\theta x) - e(\theta x')| \le 4\pi N^{\frac{1}{3}} \delta \le \eta$ (since $4\pi < 20$). It is quite easy to see (if fiddly to prove) that, if N is large, we may partition $\{1, \ldots, N\}$ into progressions with common difference d and lengths between $N^{\frac{1}{3}}$ and $2N^{\frac{1}{3}}$.

Now recall that $|\sum_{x=1}^{N} f(x)e(\theta x)| \ge c\alpha^6 N$. For the rest of the proof, we shall fix this value of c. Apply the preceding lemma with $\eta = \frac{c\alpha^6}{2}$ (this is valid so long as $N > C'\alpha^{-36}$), to get progressions $P_1, \ldots, P_k$. We certainly have $\sum_{i=1}^{k} |\sum_{x \in P_i} f(x)e(\theta x)| \ge c\alpha^6 \sum_{i=1}^{k} |P_i|$ ($= c\alpha^6 N$) (†). On the other hand, by the triangle inequality the LHS $\sum_{i=1}^{k} |\sum_{x \in P_i} f(x)e(\theta x)| \le \sum_{i=1}^{k} |\sum_{x \in P_i} f(x)| + \frac{c\alpha^6}{2} \sum_{i=1}^{k} |P_i|$. Comparing with (†) we see that $\sum_{i=1}^{k} |\sum_{x \in P_i} f(x)| \ge \frac{c\alpha^6}{2} \sum_{i=1}^{k} |P_i|$. How do we get rid of the mod signs? We use a cute trick, likely due to Gowers: Note $\sum_{i=1}^{k} \sum_{x \in P_i} f(x) = 0$. Adding, we obtain $\sum_{i=1}^{k} (|\sum_{x \in P_i} f(x)| + \sum_{x \in P_i} f(x)) \ge \frac{c\alpha^6}{2} \sum_{i=1}^{k} |P_i|$. By the pigeonhole principle there is some $P = P_i$ such that $|\sum_{x \in P} f(x)| + \sum_{x \in P} f(x) \ge \frac{c\alpha^6}{2}|P|$, so $\sum_{x \in P} f(x) \ge \frac{c\alpha^6}{4}|P|$. It is easy to see that this implies (in fact, is equivalent to) $|A \cap P| \ge (\alpha + \frac{c\alpha^6}{4})|P|$. But by construction $|P| \ge N^{\frac{1}{3}}$ and hence we have completed the proof of the density increment proposition, and hence of Roth's Theorem.

2 Sumsets

Suppose that $A, B, C, \ldots$ are sets in some ambient abelian group. Then we define $A + B = \{a + b : a \in A, b \in B\}, A - B = \{a - b : a \in A, b \in B\}, A + B + C = \{a + b + c : a \in A, b \in B, c \in C\}$ etc. We can express various famous results and conjectures of number theory in this form, e.g. if $S = \{0, 1, 4, 9, 16, \ldots\}$ then Lagrange is $4S = S + S + S + S = \mathbb{N}$ ($4S$ is obvious notation). The Goldbach conjecture is that if $\mathcal{P} = \{3, 5, 7, 11, \ldots\}$ then $\mathcal{P} + \mathcal{P} = \{$even numbers $\ge 6\}$. Fermat's Last Theorem can also be written this way.

We write $\sigma[A, B] = \frac{|A+B|}{|A|^{\frac{1}{2}} |B|^{\frac{1}{2}}}$, a normalized version of the cardinality of $A + B$. $\sigma[A] := \sigma[A, A] = \frac{|A+A}{|A|}$, the doubling constant of A. We can see this as measuring "how close A is to being a group"; the reader may verify $\sigma[A] \ge 1$ with equality iff A is a coset of a (finite) subgroup [of the ambient group].

Proposition (Ruzsa triangle inequality): Let U, V, W be finite sets in some ambient abelian group. Then $|U||V - W| \le |U - V||U - W|$. This is an inequality without a constant on either side, which are often (but not always) easy to prove; we'll exhibit an injection $\psi : U\times(V-W) \to (U-V)\times(U-W)$. For each $d \in V-W$ choose elements $\alpha(d) \in V, \beta(d) \in W$ such that $\alpha(d) - \beta(d) = d$. Define $\psi(u,d) = (u-\alpha(d), u-\beta(d)$; if $\psi(u,d) = \psi(u',d')$ then $u-\alpha(d) = u'-\alpha(d'), u-\beta(d)-u'-\beta(d')$; subtracting, $\alpha(d) - \beta(d) = \alpha(d') - \beta(d')$ i.e. $d = d'$, and hence $u = u'$.

One may rearrange the Ruzsa triangle inequality in the form $\log \frac{|V-W|}{|V|^{\frac{1}{2}}|W|^{\frac{1}{2}}} \leq \log \frac{|U-V|}{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}} + \log \frac{|U-W|}{|U|^{\frac{1}{2}}|W|^{\frac{1}{2}}}$; if we define the "Ruzsa distance" between A and B to be $d(A,B) := \log \frac{|A-B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}$ then this becomes a "genuine" triangle inequality: $d(V,W) \leq d(U,V) + d(U,W)$. However, note that this is not a valid metric; in particular, $d(A,A)$ is not usually 0; while it is possible to form a metric space by "quotienting out" this, doing so only serves to obfuscate matters.

Often it is useful to supplement the Ruzsa triangle inequality with the following estimate:

Proposition (We shall call this Ruzsa's second inequality): $d(U,-V) \leq 3d(U,V)$ (Written out explicitly, $|U+V| \leq \frac{|U-V|^3}{|U||V|}$): if $x \in U-V$, write $r(x) = \#\{(u,v) : u-v = x\}$; similarly for $x \in U+V$, $s(x) = \#\{(u,v) : u+v = x\}$. Supposing that $|U-V|$ is small, we shall find an x such that $s(x)$ is large: observe that $\sum_x r(x) = \sum_x s(x) = |U||V|$. Furthermore, $\sum_x r(x)^2 = \sum_x s(x)^2$, since both quantities are equal to the number of solutions to $u_1 + v_1 = u_2 + v_2$ or equivalently $u_1 - v_2 = u_2 - v_1$ for $u_1, u_2 \in U, v_1, v_2 \in V$ (cf "additive energy", seen later in this course). But by the Cauchy-Schwartz inequality, $\sum_x r(x)^2 \geq \frac{1}{|U-V|}(\sum_x r(x))^2$ (To see this, we have $\sum_x r(x) = \sum_x r(x)1_{U-V}(x) \leq (\sum_x r(x)^2)^{\frac{1}{2}}(\sum_x 1_{U-V}(x)^2)^{\frac{1}{2}})$, $\geq \frac{|U|^2|V|^2}{|U-V|}$. Therefore $\sum_x s(x)^2 \geq \frac{|U|^2|V|^2}{|U-V|}$. Since $\sum_x s(x) = |U||V|$ there is some x such that $s(x) \geq \frac{|U||V|}{|U-V|}$.

Let $S = \{(u,v) \in U \times V : u+v = x\}$; thus $|S| \geq \frac{|U||V|}{|U-V|}$ ($\star$). Consider the map $\phi : S \times (U+V) \to (U-V) \times (U-V)$ defined by: for each $w \in U+V$ select $\alpha(w) \in U, \beta(w) \in V$ such that $w = \alpha(w)+\beta(w)$ and define $\phi(u,v,w) = \phi((u,v),w) = (u-\beta(w), \alpha(w)-v)$. We claim that ϕ is injective: suppose $\phi(u,v,w) = \phi(u',v',w')$. Then $u+v = u'+v' = x$. Hence $w = (u+v) - (u-\beta(w)) + (\alpha(w)-v) = (u'+v') - (u'-\beta(w')) + (\alpha(w')-v') = w'$; it is now easy to show $u = u', v = v'$ as well. It follows that $|S||U+V| \leq |U-V|^2$; by ($\star$), it follows that $|U+V| \leq \frac{|U-V|^3}{|U||V|}$, as required.

Remark: also $d(U,V) \leq 3d(U,-V)$ by replacing V with $-V := \{-v : v \in V\}$.

Ruzsa calculus: Suppose K is a parameter and X, Y are real quantities. We will use "rough notation at scale K": $X \lesssim Y$ means $X \leq CK^C Y$ for some absolute constant C; $X \approx Y$ means $X \lesssim Y$ and $Y \lesssim X$; they are "the same up to powers of K". If A, B are sets in some ambient abelian group then we write $A \sim B$ to mean $|A-B| \approx |A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$; note that we do not generally have $A \sim A$.

Proposition (Ruzsa Calculus): Let $U, V < W$ be sets in some ambient abelian group. Let K be a scale; we use rough notation at scale K. i) If $U \sim V$ then $|U-V| \approx |U| \approx |V|$; also $\sigma[U], \sigma[V] \approx 1$ and $U \sim -V$. ii) If $U \sim V$ and $V \sim W$ then $U \sim W$. iii) Suppose $(\exists V :)$ $U \sim V$ and $\sigma[W] \approx 1$. Suppose also that there is an x such that $|U \cap (x+W)| \approx |U| \approx |W|$. Then $U \sim W$ (of course $x + W = \{x + w : w \in W\}$. iv) Suppose $\sigma[U], \sigma[W] \approx 1$ and that there is an x such that $|U \cap (x+W)| \approx |U| \approx |W|$. Then $U \sim W$

For i), note that if $|U-V| \leq K|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$ then, since $|U-V| \leq |U||V|$, we get

$|U| \le K^2|V|$ and $|V| \le K^2|U|$. Hence if $U \sim V$ then $|U| \approx |V| \approx |U-V|$. The rest of i) and ii) follow immediately from the Ruzsa triangle inequality and Ruzsa's second inequality. For iii), wlog take $x = 0$ (otherwise just translate W; this will still be equivalent to U as U- a translated W is just a translated $U - W$). Further $W \sim W$ since $\sigma[W] \approx 1$ means $W \sim -W$ and acigarettespply i). Now by the Ruzsa triangle inequality once more, together with the inclusions $U \cap W \subset U, W$, we obtain $|U \cap W||U-W| \le |(U\cap W) - U||(U \cap W) - W| \le |U-U||W-W|$. But $|U \cap W| \approx |U-U| \approx |W-W| \approx |U| \approx |W|$ and hence $|U-W| \lesssim |U|, |W|$. iv) is immediate from iii), since $\sigma[U] \approx 1 \Leftrightarrow U \sim (-U)$ (we will need both versions iii),iv) of the assumptions, so include both separately).

Ruzsa's Third Inequality: Proposition: Let U, V, W be finite sets in some ambient abelian group. Suppose that $d(U,V), d(V,W) \le \log K$ (i.e. $|U-V| \le K|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$ etc.) (then $d(U,W)$ is also small). Then $|U+V+W| \le CK^C|U|^{\frac{1}{3}}|V|^{\frac{1}{3}}|W|^{\frac{1}{3}}$. Remark: In the "Ruzsa" calculus notation, this is the result that if $U \sim V \sim W$ then $U + V \sim W$ (and permutations therof). Proof: We shall use the Ruzsa calculus notation (fairly sparingly). We claim there is a set S such that $U + V \sim S$; once this is established, Ruzsa calculus implies $\sigma[U+V] \approx 1$ ($\star$). For $x \in U - W$, write $r(x)$ for the number of pairs $u \in U, w \in W$ with $x = u - w$. Then $\sum_x r(x) = |U||W|$ and $|U - W| \approx |U| \approx |W|$. Hence there is some x with $r(x) \gtrsim |U| \approx |W|$. But $r(x) = |U \cap (W+x)|$; indeed, if $t = u = w + x$ then $x = u - w$. Therefore there is some x such that $|U \cap (W+x)| \gtrsim |U|$. Adding an arbitrary $v \in V$ we get $|(U+v) \cap (W+x+v)| \ge |U|$ hence certainly $|(U+V) \cap (W+\tilde{x})| \gtrsim |U|$ (where $\tilde{x} = x + v$). Finally note that $U \sim W \Rightarrow \sigma[W] \approx 1$ and hence by part iv) of the Ruzsa calculus we have $U + V \sim W$ as required.

It remains to prove the claim. Suppose $\frac{|U+V|}{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}} = L$. Then certainly $L \approx 1$ (in fact $L \le K^3$) by Ruzsa's second inequality. Define S to be the set of "popular sums" in $U+V$: $S = \{x \in U + V : s(x) \ge \frac{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}}{2L}\}$, with $s(x)$ being the number of pairs u, v with $u + v = x$ as before.

We claim S is quite large. By the same application of C-S we used in the proof of Ruzsa II, we have $\sum_x s(x)^2 \ge \frac{|U|^{\frac{3}{2}}|V|^{\frac{3}{2}}}{L}$. Also $\sum_x s(x) = |U|V|$. Therefore $\sum_{x \notin S} s(x)^2 \le \max_{x \notin S} s(x) \sum_x s(x) \le \frac{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}}{2L}|U||V|$. Thus $\sum_{x \in S} s(x)^2 \ge \frac{|U|^{\frac{3}{2}}|V|^{\frac{3}{2}}}{2L}$. But manifestly $s(x) \le \min(|U|, |V|) \le |U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$ and therefore $|S| \ge \frac{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}}{2L}$ (†); there are "lots of popular sums".

We claim that $U + V \sim (-S)$, i.e. that $|U + S + V|$ is small. Suppose that $x = u + s + v \in U + S + V$. Then s can be written in $\ge \frac{1}{2L}|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$ ways as $u' + v'$; for each, $x = u + u' + v' + v = (u + v') + (u' + v)$. Thus x is a sum of two elements of $U + V$ is $\ge \frac{1}{2L}|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$ ways. It follows that $\frac{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}}{2L}|U + S + V| \le |U+V|^2$, which implies that $|U + S + V| \le \frac{2L|U+V|^2}{|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}} = 2L^3|U|^{\frac{1}{2}}|V|^{\frac{1}{2}}$. Since $L \approx 1$ it follows that $U + V \sim (-S)$, as claimed.

Remarks: One can iterate Ruzsa III to "get control over" sums of more than three sets.

Corollary: Suppose A is a subset of some abelian group with $\sigma[A] = \frac{|A+A|}{|A|} \le K$. Then for any nonnegative integers r, s, not both zero, there is some constant $\gamma(r,s)$ such that $|rA - sA| \le (CK)^{\gamma(r,s)}|A|$.

(Later in the course, we shall need a slightly stronger version of this: Corollary: If $\sigma(A) \le K$ and k, l are nonnegative integers not both zero, then

$|kA - lA| \leq K^{C(k+l)}|A|$: By Ruzsa 3 and Ruzsa calculus we have $|2A - A| \leq K^C|A|$. Applying the Ruzsa triangle inequality with $U = A, V = (k-1)A, W = A - A$ we obtain $|A||kA - A| \leq |(k-1)A - A||2A - A|$ and hence by induction on k, $|kA - A| \leq k^{Ck}|A|$. Applying the Ruzsa triangle inequality once more, with $U = A, V = kA, W = lA$ we have $|A||kA - lA| \leq |kA - A||lA - A| \leq K^{C(k+l)}|A|^2$, as required.)

Before these cunning arguments were found, it was necessary in this course to spend around three lectures proving: Theorem (Plünecker-Ruzsa Inequalities): If $\sigma[A] \leq K$ then $|rA - sA| \leq K^{r+s}|A|$. The proof is given in Nathanson's second book on additive number theory; it is long, involves a substantial amount of graph theory, and unlike everything else we have seen so far in this course, is hard to adapt to general (nonabelian) groups.

3 Structure theory of set addition

What can we say about the structure of "approximate groups"? Let $K \geq 1$ be a fixed parameter (e.g. 100) and suppose $A \subset G$ is a finite set in some ambient abelian group G such that $\sigma[A] \leq K$ (i.e. $|A + A| \leq K|A|$. Can we say anything more specific/precise about A? Even as described here this is an ongoing research area; for G nonabelian this is essentially a field made up entirely of open problems. The answer is simpler in some groups G than in others, and turns out to be relatively hard for $G = \mathbb{Z}$.

3.1 The finite field model

We take $G = \mathbb{F}_2^\omega$, the vector space of countably infinite sequences over $\mathbb{F}_2$ (i.e. sequences of 0s and 1s, with addition taken modulo 2). Many results of this subject are easier in this or similar settings.

Theorem (Ruzsa): Suppose $A \subset \mathbb{F}_2^\omega$ is a finite set with $\sigma[A] \leq K$. Then there is a vector subspace $V \leq \mathbb{F}_2^\omega$ with $A \subset V$ and $|V| \leq \exp(CK^C)|A|$.

Rk: If $V \leq \mathbb{F}_2^\omega$ is a finite (or finite-dimensional) subspace and $A \subset V$ with $|A| = \alpha|V|$ then $A + A \subset V + V = V$, whence $\sigma[A] \leq \frac{1}{\alpha}$. Hence, apart from the dependence on the parameters, being "economically contained in a subspace" is a precise characterisation of those sets with small doubling.

Proof: Let $X \subset 3A$ be such that the translates $A + x : x \in X$ are disjoint, and which is maximal with this property. Now the disjoint union $\bigcup_{x \in X}(A + x)$ is contained in $4A$, a set of cardinality $\leq CK^C|A|$ by Ruzsa III ($\leq K^4|A|$ if you believe Plunnecke-Ruzsa). Suppose $y \in 3A$; since X was chosen maximal we must have $(A + y) \cap (A + x) \neq \emptyset$ for some $x \in X$, which implies $y \in 2A + x$. Since y was arbitrary, $3A \subset 2A + X$. Repeatedly adding A to both sides, $4A \subset 3A + X \subset 2A + 2X$ etc.; $\langle A \rangle \subset 2A + \langle X \rangle$ (where $\langle S \rangle$ means the subspace of $\mathbb{F}_2^\omega$ spanned by S). The set on the right has size $\leq |2A|2^{|X|}$ (here we use the 2-torsion extensively; there is no way we could do anything like this in $\mathbb{Z}$), $\leq K|A|2^{CK^C}$, so $\langle A \rangle$ is a subspace as required.

3.2 Approximate subgroups of $\mathbb{Z}$ and the Freiman-Ruzsa theorem

There is a substantial catalogue of approximate subgroups of $\mathbb{Z}$. Example 1: $A = \{a, a+d, \ldots, a+(n-1)d\}$ an arithmetic progression has $|A+A| = 2n-1$. This is the smallest possible size of $|A+A|$ for $|A| = n$: write $A = \{a_1, \ldots, a_n\}$ with $a_1 < \cdots < a_n$, then $A+A$ contains the strictly increasing sequence $a_1 + a_1, a_1 + a_2, \ldots, a_1 + a_n, a_2 + a_n, \ldots, a_n + a_n$. Exercise: APs are the only sets A for which this is exact. Example 2: If $\sigma[A] = K$ and $A' \subset A$ with $|A'| = \alpha|A|$ then $\sigma[A'] \leq \frac{K}{\alpha}$ - the notion of approximate groups is weakly hereditary. Combining this with example 1 gives us many approximate groups in $\mathbb{Z}$, but there are some genuinely different ones:

Definition: Suppose $x_0, \ldots, x_d \in \mathbb{Z}$ and $L_1, \ldots, L_d \geq 1$ are positive integers. Then the set $P := \{x_0 + l_1 x_1 + \cdots + l_d x_d : 0 \leq l_i < L_i\}$ is a generalized arithmetic progression (GAP) or dimension d and size $L_1 \ldots L_d$. If the sums $x_0 + l_1 x_1 + \cdots + l_d x_d$ are all distinct (in which case the size really is $|P|$) we say P is Proper. This should be thought of as the projection of a "box" or "grid" down onto a 1D line.

Example 3: If P is a proper GAP of dimension d then $\sigma[P] \leq 2^d$. Example 4: combine examples 2 and 3.

Theorem (Freiman-Ruzsa) (Usually known as Freiman) (these bounds due to Chang): Suppose $A \subset \mathbb{Z}$ has $\sigma[A] \leq K$. Then there is a GAP P with $\dim(P) \leq CK^C$ and $\text{size}(P) \leq \exp(CK^C)|A|$, such that $A \subset P$ (one can guarantee that P is proper, though the proof is somewhat tedious; with that, this result becomes an if and only if).

3.3 Freiman homomorphisms

Let $s \geq 2$ be an integer, G an abelian group and A a subset therof. Let H be another abelian group and $\phi : A \to H$ a map. We say ϕ is a Freiman s-homomorphism if $a_1 + \cdots + a_s = a'_1 + \cdots + a'_s \Rightarrow \phi(a_1) + \cdots + \phi(a_n s) = \phi(a'_1) + \cdots + \phi(a'_s)$. We say ϕ is a Freiman s-isomorphism (onto its image) if there is an inverse $\phi^{-1} : \phi(A) \to A$ which is also a Freiman s-homomorphism. Example 1: If $\phi : G \to H$ is a group homomorphism then ϕ induces a Freiman s-homomorphism on any set A, for any s. Example 2: $A = \{1, 10, 100, 1000\}, B = \{1, 100, 10000, 1000000\}$: any bijection between A, B is a Freiman 2-isomorphism (Freiman isomorphisms tell us that in some sense "the addative structures are the same"; here it is because "there is no additive structure"). Example 3: $\phi : \{0,1\}^n \subset \mathbb{Z}^n \to \mathbb{F}_2^n$ is a bijection and a Freiman 2-homomorphism, but not a Freiman isomorphism.

Lemma (Basic Properties of Freiman Homomorphisms) (Some parts may be left as exercises): i) If $\phi : A \to H$ is a Freiman s-homomorphism and $s' \leq s$ then ϕ is also a s'-homomorphism ii) If $\phi : A \to H$ is a Freiman s-homomorphism and k, l non-negative integers, not both 0, with $s \geq k + l$, then ϕ induces a well-defined map $\tilde{\phi} : kA - lA \to H$ via $\tilde{\phi}(a_1 + \cdots + a_k - a'_1 - \cdots - a'_l) = \phi(a_1) + \cdots + \phi(a_k) - \phi(a'_1) - \cdots - \phi(a'_l)$. Further $\tilde{\phi}$ is a Freiman s'-homomorphism for any $s' \leq \frac{s}{k+l}$. iii) i) and ii) remain true if we replace "homomorphism" with "isomorphism" iv) Suppose P is a GAP of dimension d and $\pi : P \to \pi(P)$ is a Freiman 2-homomorphism. Then $\pi(P)$ is a GAP of dimension d. v) Suppose $A \subset \frac{\mathbb{Z}}{m\mathbb{Z}}$ is contained inside a subinterval of $\{1, \ldots, m\} \hookrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$ of length at most $\frac{m}{s}$. Then the "unfolding map" $\psi : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \{1, \ldots, m\}$ is a Freiman s-homomorphism.

vi) The composition of two Freiman s-homomorphisms is another Freiman s-homomorphism; likewise for isomorphisms. Most parts of this are trivial exercises; for iv), suppose $P = \{x_0 + l_1x_1 + \cdots + l_dx_d : 0 \le l_i < L_i\}$. Let $\pi(x_0) = y_0, \pi(x_i + x_0) = y_i + y_0$ for $i = 1, \dots, d$. Then we claim $\pi(x_0 + l_1x_1 + \cdots + l_dx_d) = y_0 + l_1y_1 + \cdots + l_dy_d \forall 0 \le l_i < L_i$; clearly this gives the result. We prove this claim by induction on $l_1 + \cdots + l_d$; the claim is trivial when this is [0 or] 1. Then for the inductive step note that we can find $(l'_1, \dots, l'_d), (l''_1, \dots, l''_d)$ in $\mathbb{Z}^d$ such that $(0, \dots, 0) + (l_1, \dots, l_d) = (l'_1, \dots, l'_d) + (l''_1, \dots, l''_d)$. Then induct using $x_0, x_0 + \sum l_ix_i, x_0 + \sum l'_ix_i$ and $x_0 + \sum l''_ix_i$.

Proposition (Ruzsa's "model" lemma): Let $s \ge 2$ be an integer, $A \subset \mathbb{Z}$ finite, $p > |sA - sA|$ prime. Then there is $A' \subset A$ with $|A'| \ge \frac{|A|}{s}$ which is Freiman s-isomorphic to a subset of $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Corollary: Suppose $A \subset \mathbb{Z}$ has $\sigma[A] \le K$. Then there is a prime $p \le K^C|A|$ and a set $A' \subset A$, $|A'| \ge \frac{1}{8}|A|$, which is Freiman 8-isomorphic to a subset of $\frac{\mathbb{Z}}{p\mathbb{Z}}$: by Ruzsa calculus, $|8A - 8A| \le K^c|A|$. By Bertrand's postulate there is at least one prime p with $|8A - 8A| < p \le 2|8A - 8A|$. (We could easily have stated this with s in place of 8, but 8 is the version we shall need in the proof of Freiman-Ruzsa).

Proof of Proposition: By translating A if necessary, we may wlog assume all its elements are positive integers. Take a huge prime $q >>> \max(A)$ and consider the chain of maps $\mathbb{Z} \xrightarrow{\pi_q} \frac{\mathbb{Z}}{q\mathbb{Z}} \xrightarrow{\lambda} \frac{\mathbb{Z}}{q\mathbb{Z}} \xhookrightarrow{\psi} \mathbb{Z} \xrightarrow{\pi_p} \frac{\mathbb{Z}}{p\mathbb{Z}}$, where π_p, π_q are projections, ψ is the unwrapping map and λ is dilation (i.e. multiplication) by $\lambda \in (\frac{\mathbb{Z}}{q\mathbb{Z}})^\times$. Note taht π_q, π_p, λ are group homomorphisms, and hence Freiman homomorphisms at any order. ψ is a Freiman s-homomorphism when restricted to any subinterval $I_j \subset \frac{\mathbb{Z}}{q\mathbb{Z}}$ of the form $[\frac{j}{s}q, \frac{j+1}{s}q)$, by v) of the previous proposition. By the pigeonhole principle there is a set $A' \subset A$, $|A'| \ge \frac{|A|}{s}$ such that $\lambda \circ \pi_q(A')$ is contained inside some I_j, so the composition $\varphi := \pi_p \circ \psi \circ \lambda \circ \pi_q$ is then a Freiman s-homomorphism when restricted to A' (which is actually dependent on λ, $A'(\lambda)$, but this is irrelevant). If it is not a Freiman s-isomorphism, there must be some $a_1, \dots, a_s, a'_1, \dots, a'_s$ such that $a_1 + \cdots + a_s \ne a'_1 + \cdots + a'_s$ but $\varphi(a_1) + \cdots + \varphi(a_s) = \varphi(a'_1) + \cdots + \varphi(a'_s)$, a condition that can be written as $(\lambda(a_1 + \cdots + a_s - a_1 - \cdots - a_s) \mod q) \mod p = 0$, i.e. $(\lambda d \mod q) \mod p = 0$, for some $d \in (sA - sA) \setminus \{0\}$. For any fixed such d, $\lambda d \mod q$ ranges over $[1, \dots, q-1] \subset \frac{\mathbb{Z}}{q\mathbb{Z}}$ as λ ranges over $(\frac{\mathbb{Z}}{q\mathbb{Z}})^\times$. Of these numbers, at most $\frac{q-1}{p}$ are divisible by p; hence, provided that $p > |sA - sA|$, there is at least one λ such that none of the $\lambda d \mod q$, $d \in sA - sA$, is divisible by p; choose that λ and we are done.

Bogolyubov's Lemma

Suppose $r_1, \dots, r_k \in \frac{\mathbb{Z}}{p\mathbb{Z}}$, p prime; we want to "think of these as frequencies". Let $R = \{r_1, \dots, r_k\}$.

Definition: The Bohr set $B(R, \epsilon) = \{x \in \frac{\mathbb{Z}}{p\mathbb{Z}} : \|\frac{rx}{p}\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \le \epsilon \forall r \in R\}$. (The lecturer likes to think of this as: each r defines a character $\chi_r : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}^\star$ via $\chi_r(x) = e(\frac{rx}{p})$. Then $B(R, \epsilon)$ is the pullback under $(\chi_{r_1}, \dots, \chi_{r_k})$ of a small "cube" in the torus $(S^1)^k \subset \mathbb{C}^k$. This definition makes sense for an arbitrary G, not just $\frac{\mathbb{Z}}{p\mathbb{Z}}$). We say $k = |R|$ is the dimension of the Bohr set and $\epsilon > 0$ is the width.

Proposition (Bogolyubov's Lemma): Let $S \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ be of size αp, where $0 < \alpha < 1$. Then there is a Bohr set $B(R, \epsilon)$, of dimension $\leq \frac{4}{\alpha^2}$ and width $\geq \frac{1}{10}$, contained in $2S - 2S$: Recall the (discrete) Fourier transform: if $f : \frac{\mathbb{Z}}{p\mathbb{Z}} \to \mathbb{C}$ is a function an $r \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ a "frequency", $\widehat{f(r)} := \mathbb{E}_{x \in \frac{\mathbb{Z}}{p\mathbb{Z}}} f(x)e(\frac{-rx}{p})$. We've shown Parseval's identity: $||f||_2 = (\mathbb{E}_x|f(x)|^2)^{\frac{1}{2}} = ||\widehat{f}||_2 = (\sum_r |\widehat{f(r)}|^2)^{\frac{1}{2}}$. Recall $f \star g(x) = \mathbb{E}_y f(y)g(x-y)$ and $\widehat{f \star g} = \widehat{fg}$. Note that if $f = 1_U, g = 1_V$ then the support of $f \star g$ is precisely $U + V$. We shall also need the inversion formula, which allows us to recover f from $\widehat{f}$: $f(x) = \sum_r \widehat{f(r)}e(\frac{rx}{p})$, as can be proven very easily using the orthogonality relations.

To prove the lemma, define $f(x) = 1_S \star 1_S \star 1_{-S} \star 1_{-S}(x)$ (where of course $-S = \{-s : s \in S\}$). Noting that $\widehat{1_{-S}}(r) = \overline{\widehat{1_S}}(r)$, we have $\widehat{f(r)} = |\widehat{1_S}(r)|^4$. Hence, by the inversion formula, $f(r) = \sum_r |\widehat{1_S}(r)|^4 e(\frac{rx}{p})$ $(\star)$.

Let R be the set of all $r \neq 0$ such that $|\widehat{1_S}(r)| \geq \frac{\sigma^{\frac{3}{2}}}{2}$. It follows from Parseval's identity, together with teh observation taht $||1_S||_2 = \sigma^{\frac{1}{2}}$, than $|R| \leq \frac{4}{\sigma^2}$. We claim $f(x) > 0$ whenever $x \in B(R, \frac{1}{10})$; this suffices to complete the argument, since the support of f is precisely $2S - 2S$.

To prove the claim, first take real parts of $(\star)$, obtaining $f(x) = \sum_r |\widehat{1_S}(r)|^4 \cos \frac{2\pi rx}{p}$. We split this sum into three parts: the term $r = 0$ contributes σ^4. If $x \in B(R, \frac{1}{10})$ and $r \in R$ then $\cos \frac{2\pi rx}{p} \geq 0$, and so the sum of terms with $r \in R$ is ≥ 0. Finally, $\sum_{r \notin R \cup \{0\}} |\widehat{1_S}(r)|^4 \cos \frac{2\pi rx}{p} \geq -\sum_{r \notin R \cup \{0\}} |\widehat{1_S}(r)|^4 \geq -\frac{\sigma^3}{4} \sum_{r \notin R \cup \{0\}} |\widehat{1_S}(r)|^2$ (as $|\widehat{1_S}(r)| < \frac{\sigma^{\frac{3}{2}}}{2}$ on this set) $\leq -\frac{\sigma^4}{4}$ by Parseval's identity. So for $x \in B(R, \frac{1}{10})$, $f(x) \geq \sigma^4 + 0 - \frac{\sigma^4}{4} > 0$ as required.

Geometry of Numbers

This is a much-hated part of the course; it has been described as a subject which went out of fashion in England in the 1950s, and elsewhere considerably earlier. We will be interested in centrally symmetric convex bodies $K \subset \mathbb{R}^d$, i.e. for which if $x, y \in K$ then $\frac{x+y}{2}, -x \in K$. Note these are precisely the unit balls of norms on $\mathbb{R}^d$. A lattice is a discrete subgroup of $\mathbb{R}^d$, i.e. any $B(x, r)$ contains only finitely many points of it. We say a lattice Λ is nondegenerate if it generates $\mathbb{R}^d$ as a vector space over $\mathbb{R}$.

This is a somewhat abstract definition. It turns out that any non-degenerate lattice Λ has an integral basis $v_1, \ldots, v_d$, meaning that $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_d$; some prefer to use this as a definition. The determinant $\det \Lambda$ is defined to be the determinant of the column matrix $(v_1 \ldots v_d)$, or equivalently the volume of the "fundamental parallelepiped" spanned by $v_1, \ldots, v_d$; this is independent of the choice of $v_1, \ldots, v_d$. (Note: If $(v_1, \ldots, v_d), (v'_1, \ldots, v'_d)$ are two integral bases, there will be a $M \in SL_d(\mathbb{Z})$ such that $(v_i) = M(v'_i)$.

Lemma (Blichfeldt's Lemma): Let K be any measurable subset of $\mathbb{R}^d$ and Λ a non-degenerate lattice. Suppose $\mathrm{vol}(K) > \det \Lambda$. Then there are distinct $x, y \in K$ with $x - y \in \Lambda$. The proof is by a "volume-packing" argument. By considering $K \cap B(0, R)$ for suitably large R, we may assume K is bounded. Suppose the conclusion is false; then for every $t \in \mathbb{R}^d$, $\sum_x 1_K(x+t)1_\Lambda(x) \leq 1$. Let $R' >>> R$ and average this over $t \in B(0,R')$: $\sum_x 1_\Lambda(x)\frac{1}{\mathrm{vol}(B(0,R'))}\int_{B(0,R')} 1_K(x+t)dt \leq 1$ $(\star)$. If $x \in B(0, R'-R)$ then the integral here is simply $\mathrm{vol}(K)$ (also, although we shall not need this, it is 0 for $x \notin B(0, R'+R)$. Hence the LHS is at least $\frac{\mathrm{vol}(K)}{\mathrm{vol}(B(0,R'))}\sum_x 1_\Lambda(x)1_{B(0,R'-R)}(x)$. However, as $r \to \infty$, $\frac{1}{\mathrm{vol}(B(0,r))}\sum_x 1_\Lambda(x)1_{B(0,r)}(x) \to \frac{1}{\det\Lambda}$ (although "obvious", this result is fiddly to prove; we do so by tiling using fundamental parallelepipeds for Λ). Also $\lim_{R'\to\infty}\frac{\mathrm{vol}(B(0,R'-R))}{\mathrm{vol}(B(0,R'))} = 1$. Combining all these observations with $(\star)$ we have $\frac{\mathrm{vol}(K)}{\det(\Lambda)} \leq 1$, a contradiction, and so the result.

Minkowski's Second Theorem

Let $K \subset \mathbb{R}^d$ be a centrally symmetric convex body and Λ a non-degenerate lattice. For $k = 1, \dots, d$, let λ_k be the infinum of all λ such that the dilate λK contains k linearly independent elements of Λ. The λ_k are called the successive minima of K wrt Λ. Note that if K is closed then $\lambda_k K$ itself will contain k linearly independent vectors in Λ.

Pick an arbitrary $b_1 \neq 0 \in \Lambda_1\overline{K} \cap \Lambda$, then pick $b_2 \in \lambda_2\overline{K} \cap \Lambda$ such that $\dim_{\mathbb{R}} \mathrm{span}(b_1, b_2) = 2$, and so on; we obtain a basis for $\mathbb{R}^d$ consisting of vectors $b_1, \dots, b_d \in \Lambda$. This is called a directional basis (for K wrt Λ).

Remark: $b_1, \dots, b_d$ need not form an integral basis for Λ: consider $d = 5, \Lambda = \mathbb{Z}^d \oplus (\frac{1}{2}, \dots, \frac{1}{2}), K = B(0,1)$ the Euclidean ball of radius 1 about the origin. (The directional basis will simply be the standard basis for $\mathbb{R}^5$, which does not include the "half"-points of the lattice $(\frac{1}{2}, \dots, \frac{1}{2}), (\frac{3}{2}, \frac{1}{2}, \dots, \frac{1}{2})$ etc.).

Theorem (Minkowski's Second Theorem): $\lambda_1, \dots, \lambda_d \mathrm{vol}(K) \leq 2^d \det\Lambda$: wlog take K open (this is simply a convenience for later on). Let $b_1, \dots, b_d$ be a dorectional basis. Define maps $\varphi_j : K \to K$ by setting $\varphi_j(x)$ to be the centre of gravity of the $j-1$-dimensional slice of K parallel to $b_1, \dots, b_{j-1}$ and containing x. Define $\varphi : K \to \mathbb{R}^d$ by $\varphi(x) := \sum_{j=1}^d (\lambda_j - \lambda_{j-1})\varphi_j(x)$ where λ_0 is taken to be 0 (the lecturer freely admits to not understanding what is really going on here). For a given $x \in \mathbb{R}^d$ write $x = x_1b_1 + \dots + x_db_d$. Writing $\varphi_j(x) = \sum_{i=1}^d c_{ij}(x)b_i$ we see that $c_{ij}(x) = x_i$ if $i \geq j$ and depends only on $x_j, \dots, x_d$ if $j > i$. It follows from this that $(\varphi(x))_i = \lambda_i x_i + \psi_i(x_{i+1}, \dots, x_d)$, from which it follows immediately that $\mathrm{vol}(\varphi(K)) = \lambda_1 \dots \lambda_d \mathrm{vol}(K)$, since the Jacobian of φ is upper-triangular with $\lambda_1, \dots, \lambda_d$ along the diagonal, so has determinant $\lambda_1 \dots \lambda_d$.

Suppose that $\lambda_1 \dots \lambda_d \mathrm{vol}(K) > 2^d \det\Lambda$. Then $\mathrm{vol}(\varphi(K)) > \det(2\Lambda)$ (where $2\Lambda = \{2\lambda : \lambda \in \Lambda\}$) and hence by Blichfeldt there are distinct $x, y \in K$ such that $\frac{\varphi(x)-\varphi(y)}{2} \in \Lambda$. Let k be maximal such that $x_k \neq y_k$. Then $\frac{\varphi(x)-\varphi(y)}{2} = \sum_{i=1}^d (\lambda_i - \lambda_{i-1})\frac{\varphi_i(x)-\varphi_i(y)}{2} = \sum_{i=1}^k (\lambda_i - \lambda_{i-1})\frac{\varphi_i(x)-\varphi_i(y)}{2}$ by considering the expressions for φ_i relative to our basis $b_1, \dots, b_d$. HOwever, $\varphi_i(x), \varphi_i(y) \in K$ by convexity of K, whence $\frac{\varphi_i(x)-\varphi_i(y)}{2} \in K$ by central symmetry and convexity, and so $\sum_{i=1}^k (\lambda_i - \lambda_{i-1})\frac{\varphi_i(x)-\varphi_i(y)}{2} \in \lambda_k K$ by convexity. Hence $\frac{\varphi(x)-\varphi(y)}{2} \in \lambda_k K \cap \Lambda$. But by assumption, the kth coordinate relative to $b_1, \dots, b_d$ is $\frac{x_k - y_k}{2} \neq 0$ and so $\lambda_k K \cap \Lambda$ contains k independent elements of $\mathbb{R}^k$. Hence so does $(\lambda_k - \epsilon)K \cap \Lambda$, since K is open, but this contradicts the definition of λ_k.

For a more conceptually clear proof which sadly yields a looser inequality: by an Affine transformation we may wlog consider the lattice to be $\mathbb{Z}^d$. By

John's Theorem K contains an ellipsoid with a large proportion of its volume; then finding many points of $\mathbb{Z}^d$ inside an ellipsoid is easy.

We will use Minkowski's Second Theorem to locate a large GAP inside a Bohr set.

Proposition: Let p be a prime and let $R \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ be a set of k "frequencies" (elements). Let $\epsilon < \frac{1}{2}$. Then the Bohr set $B(R, \epsilon)$ contains a (proper) GAP of dimension k and size at least $(\frac{\epsilon}{k})^k p$: Suppose $R = \{r_1, \ldots, r_k\}$. Consider the lattice $\Lambda = p\mathbb{Z}^k + \mathbb{Z}(r_1, \ldots, r_k)$; since p is prime, this is equal to the direct sum $p\mathbb{Z}^k \oplus \{0, \ldots, p-1\}(r_1, \ldots, r_k)$, and hence it is not hard to convince oneself (if, again, fiddly to actually prove) that $\det \Lambda = p^{k-1}$.

Let $K \subset \mathbb{R}^k$ be the l^∞-ball $\{x : \|x\|_\infty \leq \epsilon\}$ i.e. $\{x : |x_1|, \ldots, |x_k| \leq \epsilon\}$. Let $b_1, \ldots, b_k$ be a directional basis (for Λ wrt K) and let $\lambda_1, \ldots, \lambda_k$ be the successive minima. We have $\|b_i\|_\infty \leq \epsilon \lambda_i$. Set $L_i := \lceil \frac{p}{\lambda_i k} \rceil$. Then for $0 \leq l_i < L_i$, $\|l_1 k_1 + \cdots + l_k b_k\|_\infty \leq \sum_{i=1}^k \frac{p}{\lambda_i k} \times \lambda_i \epsilon = \epsilon p$ $(\star)$.

Since b_i lies in Λ, we have $b_i = x_i(r_1, \ldots, r_k) \mod p$, where $0 \leq xi < p$; by slight abuse of notation we consider $x_i \in \frac{\mathbb{Z}}{p\mathbb{Z}}$. Then $(\star)$ implies that $\|\frac{(l_1 x_1 + \cdots + l_k x_k) r_j}{p}\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \epsilon$ whenever $0 \leq l_i < L_i$; that is, $l_1 x_1 + \cdots + l_k x_k \in B(R, \epsilon)$. The size of this progression is $L_1 \ldots L_k \geq \frac{1}{k^k} \frac{p^k}{\lambda_1 \ldots \lambda_k}$. But by Minkowski II $\lambda_1 \ldots \lambda_k (2\epsilon)^k \leq 2^k p^{k-1}$ and so this is $\geq (\frac{\epsilon}{k})^k p$, as claimed.

We also claimed that this progression P is proper: suppose $l_1 x_1 + \cdots + l_k x_k = l'_1 x_1 + \cdots + l'_k x_k \mod p$. Then $b := (l_1 - l'_1) b_1 + \cdots + (l_k - l'_k) b_k$ lies in $p\mathbb{Z}^k$. However $\|b\|_\infty \leq \sum_{i=1}^k \frac{p}{\lambda_i k} \lambda_i \epsilon \leq \epsilon p$. But $\epsilon < \frac{1}{2}$ and so $b = 0$, and hence $l_i = l'_i \forall i = 1, \ldots, k$.

Chang's Covering Lemma

Lemma: Suppose that $A \subset \mathbb{Z}$ and $\sigma[A] \leq K$. Suppose also that $2A - 2A$ contains a proper GAP P, of dimension d and size $\eta|A|$. Then A is contained in a GAP of dimension at most $d + CK^C \log \frac{1}{\eta}$ and size at most $2^d \eta^{-CK^C}|A|$: Let L be a quantity to be chosen later (of the form CK^C). Set $P_0 = P$; pick a maximal $R_0 \subset A$ such that the translates $P_0 + r_0, r_0 \in R_0$ are disjoint. If $|R_0| \leq L$ then stop, otherwise pick $S_0 \subset R_0, |S_0| = L$, and define $P_1 := P_0 + S_0$. Pick $R_1 \subset A$ maximal such that the translates $P_1 + r_1, r_1 \in R_1$ are all disjoint. If $|R_1| \leq L$, stop; otherwise pick $S_1 \subset R_1, |S_1| = L$ and set $P_2 := P_1 + S_1$, and so on.

We claim that this algorithm terminates in good time for an appropriately chosen L. Suppose it runs for t steps, then $|P_t| = |P_0||S_0| \ldots |S_{t-1}| \geq \eta|A|L^t$. On the other hand, since $P_0 \subset 2A - 2A$ and each S is a subset of A, $P_t \subset (t+2)A - 2A$, hence $|P_t| \leq K^{C(t+4)}|A|$. Choosing $L = K^{2C}$, say, it is easy to see that $t \leq C \log \frac{1}{\eta}$.

Suppose the algorithm stops at the tth step (and we now have $t \leq C \log \frac{1}{\eta}$). This means there is a set $R_t \subset A$ such that $|R_t| \leq L$, the translates $P_t + r_t$ are disjoint for $r_t \in R_t$, and R_t is maximal wrt this property. Hence if $x \in A$ then $(P_t + x) \cap (P_t + r_t) \neq \emptyset$ for some $r_t \in R_t$, which means that $A \subset P_t - P_t + R_t \subset P - P + (S_0 - S_0) + \cdots + (S_{t-1} - S_{t-1}) + R_t$ (†).

Now given a set S, we may place $S - S$ very crudely inside a progression by $\overline{S} := \{\sum_{s \in S} \epsilon_s s : \epsilon_s \in \{-1, 0, 1\}\}$ with sidelength 3 and dimension $|S|$. Similarly R_t lies inside a GAP of dimension $|R_t|$ and size $2^{|R_t|}$. Returning to (†), A has been placed inside a GAP of dimension $\leq d + \sum_{i=0}^{t-1} |S_i| + |R_t| \leq d + CK^C \log \frac{1}{\eta}$.

The size of this GAP is at most $|P-P|(\prod_{i=0}^{t-1} 3^{|S_i|})2^{|R_t|}$. Noting that P is proper we have $|P-P| \leq 2^d|P|$; also, since $P \subset 2A-2A$, we have $|P| \leq CK^C|A|$. Putting this together with the bounds $|S_i|, |R_t| \leq L$ and $t \leq C\log\frac{1}{\eta}$, we get that the size of this GAP is $\leq 2^d\eta^{-CK^C}|A|$, as required.

Conclusion of proof of Freiman-Ruzsa: 1) Suppose $\sigma(A) \leq K$. By Ruzsa's model lemma, $\exists A' \subset A, |A'| \geq \frac{1}{8}|A|$, such that A' is 8-isomorphic to a set $S \subset \frac{\mathbb{Z}}{p\mathbb{Z}}, |S| \geq cK^{-c}p$. 2) $2S-2S$ contains a Bohr set of dimension $\leq CK^C$ and width $\frac{1}{10}$ (Bogolyubov). 3) That Bohr set contains a proper GAP P of dimension $\leq CK^C$ and size $\geq \exp(-cK^c)|A|$. 4) By "basic properties of Freiman isomorphisms", $2A'-2A'$ is Freiman 2-isomorphic to $2S-2S$. So $2A-2A$ contains a progression $\tilde{P}$, $\dim\tilde{P} \leq CK^C$, of size $\geq \exp(-cK^c)|A|$. 5) Chang's covering lemma implies A is contained in a GAP Q with $\dim Q \leq CK^C$ and $|Q| \leq e^{CK^C}|A|$.

Additive Energy and the Bolog-Szeverédi-Gowers Theorem

(The name of this theorem is a bit unwieldy; a similar result was first proven by Bolog-Szererédi, but gave impractically large bounds; the first polynomial bounds were given by Gowers).

Definition: Suppose A, B are finite sets in some abelian group. Then the (normalized) additive energy $\omega_+(A,B)$ (the notation is original to this course) is the number of solutions to $a_1+b_1 = a_2+b_2$ with $a_1, a_2 \in A, b_1, b_2 \in B$, divided by $|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$.

Remark: $0 \leq \omega_+(A,B) \leq 1$: to see the latter, note that the number of solutions to $a_1+b_1 = a_2+b_2$ is $\leq |A|^2|B|$ since there is at most one solution for each $(a_1, a_2, b_1) \in A \times A \times B$; similarly it is $\leq |A||B|^2$ and thus $\leq$ the geometric mean $|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$.

Recall we wrote $\sigma[A,B] = \frac{|A+B|}{|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}}$. There is a close connection between having small sumset and large additive energy. One direction of this connection is very easy: if the sumset is small then the additive energy is large:

Lemma: Suppose $\sigma[A,B] \leq K$. Then $\omega_+(A,B) \geq \frac{1}{K}$: Write $r(x)$ for the number of pairs $(a,b) \in A \times b$ with $a+b = x$. Then $\sum_x r(x) = |A||B|$ and $\sum_x r(x)^2$ is the number of solutions to $a_1+b_1 = a_2+b_2$, i.e. $|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}\omega_+(A,B)$. Note further that $r(x)$ is supported on $A+B$ and so, by Cauchy-Schwartz, $\sum_x r(x)^2 \geq \frac{1}{|A+B|}(\sum_x r(x))^2$; this quickly leads to the result.

The most obvious attempt to form a converse fails: for example, let $A = A_1 \cup A_2$ where $A_1 = \{1, \ldots, \frac{n}{2}\}$ and $A_2 = \{x_1, \ldots, x_{\frac{n}{2}}\}$ is arbitrary (and sparse). Then $\omega_+(A,A) \geq \frac{1}{100}$ but typically $\sigma[A] \sim cn$. (Informally, if we add some random points to a set, this won't affect the additive energy much, but can greatly increase the doubling).

Theorem (Balog-Szeverédi-Gowers): Suppose A, B are sets in some abelian group and $\omega_+(A,B) \geq \frac{1}{K}$. Then there exist $A' \subset A, B' \subset B$ with $|A'| \geq cK^{-C}|A|, |B'| \geq cK^{-C}|B|$ and with $\sigma[A',B'] \leq CK^C$.

Paths of length 3

We shall deduce B-S-G (quite straightforwardly) from the following graph-theoretic lemma:

Lemma: Suppose G is a bipartite graph on vertex sets V, W, $|V| = |W| = n$, and suppose G has αn^2 edges, $0 < \alpha \leq 1$. Then there are sets $V' \subset V, W' \subset W$ with $\frac{|V'|}{|V|}, \frac{|W'|}{|W|} \geq c\alpha^C$ such that there are at least $c\alpha^C n^2$ paths of length 3 in G between any $x \in V'$ and any $y \in W'$ (the lecturer thinks, but is not sure, that there is a stronger result where we can find paths of length 3 in the induced graph on $V' \cup W'$, but we shall not need that and the proof is doubtless much harder).

The heart of the proof is the following lemma about paths of length 2:

Lemma: Suppose G is a bipartite graph on $V \cup W$, $|V| = |W| = n$ with αn^2 edges. Let $0 < \eta < 1$ be a further parameter. Then there is a set $V' \subset V, |V'| \geq \frac{\alpha n}{2}$, such that $\forall_\eta$ pairs $(v_1, v_2 \in V' \times V'$ (where $\forall_\eta$ means for a proportion $(1 - \eta)$ - "for all except η many") there are at least $\frac{\eta\alpha^2}{2}n$ paths of length 2 (in G) between v_1 and v_2: For $v \in V$, write $N(v)$ for the set of all vertices in W adjacent to V, and similarly $N(w)$. By double-counting, $\sum_{w \in W} \sum_{v \in V} 1_{vw \in E(G)} = \alpha n^2$. Hence, by Cauchy-Schwartz, $\sum_{w \in W} \sum_{v,v' \in V} 1_{vw \in E(G)} 1_{v'w \in E(G)} \geq \alpha^2 n^3$, or in other words $\sum_{v,v' \in V} |N(v) \cap N(v')| \geq \alpha^2 n^3$ $(\star)$. Call v, v' very unfriendly if $|N(v) \cap N(v')| \leq \frac{\eta\alpha^2}{2}n$, i.e. if there are fewer than $\frac{\eta\alpha^2}{2}n$ paths of length 2 between v and v'. Let $S \subset V \times V$ be the set of very unfriendly pairs. Then it follows from $(\star)$ that $\sum_{v,v' \in V}(\eta - 1_{(v,v') \in S})|N(v) \cap N(v')| \geq \frac{\eta\alpha^2 n^3}{2}$. This may be rewritten as $\sum_{w \in W} \sum_{v,v' \in V}(\eta - 1_{(v,v') \in S}) 1_{vw \in E(G)} 1_{v'w \in E(G)} \geq \frac{\eta\alpha^2 n^3}{2}$. In particular there is at least one w such that $\sum_{v,v' \in V}(\eta - 1_{(v,v') \in S}) 1_{vw \in E(G)} 1_{v'w \in E(G)} \geq \frac{\eta\alpha^2 n^2}{2}$. Define $V' := N(w)$. Just the fact that the preceding expression is ≥ 0 tells us that $\forall_\eta$ pairs $(v_1, v_2) \in V' \times V'$, $(v_1, v_2) \notin S$, so there are $\frac{\eta\alpha^2}{2}n$ paths of length 2 between them. Also, ignoring the contribution from S completely, we have $\sum_{v,v' \in V} 1_{vw \in E(G)} 1_{v'w \in E(G)} \geq \frac{\alpha^2 n^2}{2}$, i.e. $|N(w)|^2 \geq \frac{\alpha^2 n^2}{2}$. Thus $|V'| \geq \frac{\alpha n}{\sqrt{2}} \geq \frac{\alpha n}{2}$, as claimed.

Gowers' original proof of this result was along similar lines; he was using random selection from w though, and so had to pick 5 elements $w_1, \ldots, w_5$ and then set V' to be the intersection of their neighbourhoods $N(w_1) \cap \cdots \cap N(w_5)$. Here we have been able to pick a "clever" w by "letting linearity of expectation do all the work for us".

Proof of the paths of length 3 lemma: The number of edges enmating from vertices in V with degree $\leq \frac{\alpha n}{2}$ is at most $\frac{\alpha n^2}{2}$; deleting these, we still have $\geq \frac{\alpha n^2}{2}$ edges. Henceforth, "edge" shall refer only to those edges which remain after this deletion. Let $\eta > 0$ be a parameter to be chosen later and applythe paths of length 2 lemma; this gives us $V' \subset V, |V'| \geq \frac{\alpha n}{4}$ such that $\forall_\eta$ pairs $(v_1, v_2) \in V' \times V'$ there are $\geq \frac{\eta\alpha^2}{8}n$ common neighbours of v_1, v_2 in W. Now a silly technical point (we want to just delete all the vertices of degree 0, but we only proved the lemma on paths of length 2 for vertex sets of equal size): it is conceivable that there are vertices in V' of degree 0. If $\eta < \frac{1}{4}$ then there are certainly no more than $\frac{1}{2}|V'|$ such vertices, so deleting them we get a further set $V'' \subset V', |V'' \geq \frac{\alpha n}{8}$ such that $\forall_\eta$ pairs $(v_1, v_2) \in V'' \times V''$ there are $\geq \frac{\eta\alpha^2}{8}n$ common neighbours in W and such that $\deg(v) \geq \frac{\alpha n}{2} \forall v \in V''$.

Now we look at W. There are $\geq \frac{\alpha^2 n^2}{16}$ edges from V'' to W; it follows that there are $\geq \frac{\alpha^2 n}{32}$ vertices in W having at least $\frac{\alpha^2 n}{32}$ neighbours in V''. Let W' be the set of such. We now make further refinement of V'': by another simple averaging argument, we can pass to $V''' \subset V'', |V'''| \geq \frac{1}{2}|V''| \geq \frac{\alpha n}{16}$ such taht if $x \in V''', \forall_{2\eta} y \in V''$, x and y share $\frac{\eta\alpha^2}{8}n$ common neighbours in W.

We claim that for suitably chosen η, V''' and W' have the desired property, namely many paths of length 3 between each pair of vertices. Suppose we fix $x \in V''', y \in W'$. By construction, $N(y)$ [in V'' is of size] $\geq \frac{\alpha^2 n}{32}$. Also, $(1-2\eta)|V''|$ vertices share $\geq \frac{\eta\alpha^2}{8}n$ common neighbours with x. Set $\eta = \frac{\alpha^2}{96}$, then these two sets intersect in a set of size $\geq \eta|V''|$. This gives us at least $\eta|V''|\frac{\eta\alpha^2}{8}n \geq \frac{\eta^2\alpha^3}{64}n^2$ paths of length 3 between x and y, as required.

Proof of Balog-Szeverédi-Gowers: Recall we had sets $A, B \subset$ some abelian group with $\omega_+(A,B) \geq \frac{11}{K}$ This implies the number of solutions to $a_1 - b_1 = a_2 - b_2$ (or equivalently $a_1 + b_2 = a_2 + b_1$) is at least $\frac{1}{K}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$. This implies, by an easy averaging argument, that there are many $\underline{\text{popular differences}}$ between A and B: writing $s(x) = \#\{(a,b) \in A \times B : a - b = x\}$, there are at least $\frac{1}{2K}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$ values of x such that $s(x) \geq \frac{1}{2K}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$ (cf the proof of Ruzsa 3).

Form a bipartite graph G on $A \cup B$ by joining a to b iff $a - b$ is a popular difference. Note that $\omega_+(A,B) \geq \frac{1}{K} \Rightarrow K^{-2}|A| \leq |B| \leq K^2|A|$ (this drops out of our proof that $\omega_+(A,B) \leq 1$). Pad out the smaller of the two vertex classes so that each has $n = \max(|A|, |B|)$ vertices.

It follows from the paths of length 3 lemma that there are $A' \subset A, B' \subset B, \frac{|A|'}{|A|}, \frac{|B'|}{|B|} \geq cK^{-C}$ with $\geq cK^{-C}n^2$ paths of length 3 between [each pair of vertices from] them. This means that $\forall a' \in A', b' \in B'$ there are $\geq cK^{-C}$ choices of $b'' \in B, a'' \in A$ (note these are in B, A, not generally B', A') such that all three of $a' - b'', a'' - b'', a'' - b'$ are popular. But note that $a' - b' = (a' - b'') - (a'' - b'') + (a'' - b') = x + y + z$ where x, y, z are populare differences. Notice that given $x, y, z, a' - b'$ we can easily recover a'', b''. Thus we have $\geq cK^{-C}n^2$ representations of $a' - b'$ as $x - y + z$ with x, y, z popular. However, there are certainly no more than $2K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$ popular differences (by double-counting pairs (a,b) with $a - b$ popular), $\leq CK^C n$. Thus $|A'| - |B'|cK^{-C}n^2 \leq (CK^C n)^3$ which implies $|A' - B'| \leq CK^C n$. Note that $|A'|, |B'| \geq cK^C n$; thus we have the result.

Chapter 5: Longer progressions and higher Gowers norms

Recall Roth's theorem: in qualitative terms, every subset of $\{1, \ldots, N\}$ of positive density contains a non-trivial 3AP. The same is true for progressions of length $k > 3$ - a famous theorem of Szeverédi. The first quantitative bounds for Szeverédi's theorem were obtained by Gowers in 1998:

Theorem (Gowers): Let $k \geq 3$ be an integer. Suppose $A \subset \{1, \ldots, N\}$ is a set of size at least $N(\log\log N)^{-c_k}$ (for fixed $c_k > 0$). Then A contains a nontrivial k-term AP. We shall prove this only for the case $k = 4$; it is fair to say that the mathematical establishment "does not know the correct proof" for $k \geq 5$ (and possibly even for $k = 4$). That said, we shall do much of the proof in full generality; the main "hole" is that we will not be able to proove an inverse theorem for a general Gowers u_k-norm.

Recall that in the proof of Roth's theorem we introduced $G = \frac{\mathbb{Z}}{N'\mathbb{Z}}$ where $N' = 2N+1$; here we'll need $N' = (k-1)N+1$. Recall we looked at the Gowers u^2-norm: if $f : G \to \mathbb{C}$ we define $\|f\|_{u^2} = (\mathbb{E}_{x,h_1,h_2 \in G} f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2))^{\frac{1}{4}}$. This and much of what we say is valid in any abelian G (and probably even for G nonabelian).

Definition (Gowers u^k-norms): Let $k \geq 2$ be an integer. Write [here the lecturer paused for several moments in aparrent disgust] $C : \mathbb{C} \to \mathbb{C}$ for complex conjugation. Let G be a finite abelian group, $f : G \to \mathbb{C}$ a function. Then we define $\|f\|_{u_k} = (\mathbb{E}_{x,h_1,\ldots,h_k \in G} \prod_{\omega \in \{0,1\}^k} C^{|\omega|} f(x + \omega \cdot \boldsymbol{h}))^{\frac{1}{2^k}}$ where $\boldsymbol{h} = (h_1, \ldots, h_k), \omega \cdot \boldsymbol{h} = \omega_1 h_1 + \cdots + \omega_k h_k, |\omega| = |\omega_1| + \cdots + |\omega_k|$. We also introduce the Gowers inner product, defined for a collection $(f_\omega)_{\omega \in \{0,1\}^k}$ of complex-valued functions, $\langle (f_\omega) \rangle_{u^k} = \mathbb{E}_{x,h_1,\ldots,h_k} \prod_{\omega \in \{0,1\}^k} C^{|\omega|} f_\omega(x + \omega \cdot h)$. For example, $\langle f_{00}, f_{10}, f_{01}, f_{11} \rangle_{u^2} = \mathbb{E}_{x,h_1,h_2} f_{00}(x)\overline{f_{10}(x+h_1)f_{01}(x+h_2)}f_{11}(x+h_1+h_2)$.

Proposition: Let $k \geq 2$ be an integer. Let $(f_\omega)_{\omega \in \{0,1\}^k}, f, g$ be complex-valued functions. Then i) (Gowers Cauchy-Schwartz) $\langle f_\omega \rangle_{u^k} \leq \prod_{\omega \in \{0,1\}^k} \|f_\omega\|_{u_k}$ ii) The Gowers norms are nested: $\|f\|_{u^2} \leq \|f\|_{u^3} \leq \ldots$ iii) The Gowers norms are genuine norms (this is nice to know, though we shall never actually need it in this course); the nontrivial parts of this are $\|f + g\|_{u^k} \leq \|f\|_{u^k} + \|g\|_{u^k}$ and $\|f\|_{u^k} = 0 \Rightarrow f = 0$. Proof: i) is facilitated by a clever rewriting of $\langle (f_\omega) \rangle_{u^k}$ followed by k applications of Cauchy-Schwartz; for example, $\langle (f_\omega) \rangle_{u^2} = \mathbb{E}_{x,x',y,y' \in G} f_{00}(x+y)\overline{f_{10}(x'+y)f_{01}(x+y')}f_{11}(x'+y')$; the more general form is obvious but horrible to notate. Doing Cauchy-Schwartz "in" the variables x, x' gives $|\langle (f_\omega) \rangle_{u^2}| \leq (\mathbb{E}_{x,x'}(\mathbb{E}_y f_{00}(x+y)\overline{f_{10}(x'+y)})^2)^{\frac{1}{2}} (\mathbb{E}_{x,x'}(\mathbb{E}_{y'} \overline{f_{01}(x+y')}f_{11}(x'+y'))^2)^{\frac{1}{2}} = \langle f_{00}, f_{10}, f_{00}, f_{10} \rangle_{u^2}^{\frac{1}{2}} \langle f_{01}, f_{11}, f_{01}, f_{11} \rangle_{u^2}^{\frac{1}{2}}$ (i.e. the product of the square roots of those norms). Applying Cauchy-Schwartz "in the ys" gives e.g. $\langle f_{00}, f_{10}, f_{00}, f_{10} \rangle_{u^2} \leq \langle f_{00}, f_{00}, f_{00}, f_{00} \rangle_{u^2}^{\frac{1}{2}} \langle f_{10}, f_{10}, f_{10}, f_{10} \rangle_{u^2}^{\frac{1}{2}} = \|f_{00}\|_{u^2}^2 \|f_{10}\|_{u^2}^2$, and similarly for the other factor, whence the result. ii) follows from i): $\|f\|_{u^k}^{2^k} = \langle f, \ldots, f, 1, \ldots, 1 \rangle_{u^{k+1}}$ where there are 2^k fs and 2^k 1s; this is at most $\|f\|_{u^{k+1}}^{2^k} \|1\|_{u^{k+1}}^{2^k} = \|f\|_{u^{k+1}}^{2^k}$ by Gowers-Cauchy-Schwartz. To prove iii) write $\|(f+2)\|_{u^k}^{2^k} = \langle f+g, \ldots, f+g \rangle_{u^k}$ whgich may be expanded using multilinearity as a sum of 2^{2^k} terms each of the form $\langle f, g, f, f, g, \ldots \rangle_{u^k}$, where the number of terms with i fs and $2^k - i$ gs is $\binom{2^k}{i}$. By Gowers-Cauchy-Schwartz each such term is $\leq \|f\|_{u^k}^i \|g\|_{u^k}^{2^k-i}$; hence $\|f+g\|_{u^k}^{2^k} \leq \sum_i \binom{2^k}{i} \|f\|_{u^k}^i \|g\|_{u^k}^{2^k-i} = (\|f\|_{u^k} + \|g\|_{u^k})^{2^k}$. To see that $\|f\|_{u^k} = 0 \Rightarrow f = 0$ it suffices to deal with $k = 2$ (because the norms are nested); the easiest way to do this is to use $\|f\|_{u^2} = \|\widehat{f}\|_4$, hence $\|f\|_{u^2} = 0 \Rightarrow \|\widehat{f}\|_4 = 0 \Rightarrow \widehat{f} = 0 \Rightarrow f = 0$ by the inversion formula (as an exercise the reader may prove the result directly).

We shall start looking at Gowers' proof for progressions of length 4. The proof is by the density increment strategy, as in chapter 1 (of course, our proof there was deliberately chosen to be as easy as possible to generalize).

Proposition (density increment): Let $0 < \alpha < 1, N > C\alpha^{-C}$. Let P be a progression of length N, and $A \subset P$ a set of size αN. Then at least one of the following holds: i) A contains $\geq \frac{1}{20}\alpha^4 N^2$ 4APs (this value should be modified slightly, see below), and in particular at least one ii) There is a progression $P', |P'| \geq N^{\alpha^c}$ such that $\frac{|\alpha \cap P'|}{|P'|} \geq \alpha + c\alpha^c$. With reference to section 1.1, the reader should convince theirself that this implies Gowers' result.

Turning now to the proof of the proposition, take $N' = 6N + 1$ and consider $G = \frac{\mathbb{Z}}{N'\mathbb{Z}}$. wlog take $P = \{1, \ldots, N\}$ and consider A as a subset of G. Introduce $f := 1_A - \alpha 1_{[N]}$, the balanced function of A. For $f_1, f_2, f_3, f_4 : G \to \mathbb{C}$ define $AP_4(f_1, f_2, f_3, f_4) = \mathbb{E}_{x,d} f_1(x) f_2(x + d) f_3(x + 2d) f_4(x + 3d)$.

Lemma: Suppose $0 < \alpha < 1$, $N > C\alpha^{-C}$ and A has fewer than $\frac{1}{20}\alpha^4 N^2$ 4APs. Then there are 1-bounded functions $g_1, \ldots, g_4$ at least one of which is the balanced function f, such that $|AP_4(g_1, g_2, g_3, g_4)| \geq c\alpha^4$. The proof is identical to that of the corresponding lemma in chapter 1.

Lemma (Generalised von Neumann Theorem): Let $f_1, f_2, f_3, f_4 : G \to \mathbb{C}$ be 1-bounded. Then $|AP_4(f_1, f_2, f_3, f_4)| \leq \|f_i\|_{u^3}$ for $i = 1, 2, 3, 4$; we'll sketch the proof for $i = 1$ (the other cases are similar): $AP_4(f_1, f_2, f_3, f_4) = \mathbb{E}_{x,y,z} f_1(x + y + z) f_2(\frac{1}{2}y + \frac{2}{3}z) f_3(-x + \frac{1}{3}z) f_4(-2x - \frac{1}{2}y)$ (this paramaterization has been chosen such that only the f_1 term contains all three parameters; we have used that $(6, N') = 1$). Now apply Cauchy-Schwartz to eliminate f_2, f_3, f_4 in turn, much as in the first chapter; one ends up with $|AP_4(f_1, f_2, f_3, f_4)|^8 \leq \mathbb{E}_{x,x',y,y',z,z'} f_1(x + y + z)\overline{f_1(x' + y + z) f_1(x + y' + z) f_1(x + y + z')} \ldots \overline{f_1(x' + y' + z')} = \|f_1\|_{u^3}^8$. Much the same result holds for general k, but the notation becomes very unwieldy.

Combining the last two lemmas, we have: Corollary: Suppose $0 < \alpha < 1, N > C\alpha^{-C}$, and A has fewer than $\frac{1}{20}\alpha^4 N^2$ 4APs. Then $\|f\|_{u^3} \geq c\alpha^4$, where f is the balanced function of A. Our task now is to prove the following result of Gowers, a (consequence of a) "local inverse theorem" for the u^3 norm: (At this point the lecturer became too lazy to write N's; thus, we freely write N where we mean N')

Proposition: Suppose $f : \{1, \ldots, N\} \subset \frac{\mathbb{Z}}{N'\mathbb{Z}} \to \mathbb{C}$ is 1-bounded and $\mathbb{E}_x f(x) = 0, \|f\|_{u^3} \geq \delta$. Then there is a progression P of length at least $\exp(\frac{1}{\delta^2})N^{\delta^C}$ such that $\mathbb{E}_{x \in P} f(x) \geq c\delta^C$ (the factor of $\exp(\frac{1}{\delta^2})$ was forgotten above, but the lecturer assures us the density incremend argument remains valid).

Proof of the local inverse theorem, I: First, a preliminary observation, in fact the motivating observation for the whole subject: set $f(x) = e(\frac{x^2}{N})$, then f is 1-bounded and $\|f\|_{u^3} = \mathbb{E}_{x,h_1,h_2,h_3} e(\frac{1}{N}(x^2 - (x + h_1)^2 - \cdots - (x + h_1 + h_2 + h_3)^2)) = 1$ (as the sum in the $e(\ldots)$ is a "3rd difference" (3rd discrete derivative) of squares, so always 0 (or we can see this directly by expanding out)). It's possible to verify that this f does not correlate with any linear phase $e(\frac{rx}{N})$.

This example is, with the benefit of hindsight, extremely natural: if $f(x) = e(\psi(x))$ then $\|f\|_{u^3}$ is telling us that the third discrete derivative $\Delta^3\psi(x) = \psi(x) - \psi(x + h_1) - \cdots - \psi(x + h_1 + h_2 + h_3)$ is "biased". This at least suggests that f itself has "quadratic bias". The true result is not as nice as it might be; it is not the case that such an f is always correlated with a quadratic phase function $e(\frac{rx^2}{N})$ - but something almost as good is true; see later.

The key idea is to study the "derivatives" of f. Define $\Delta(f, h)(x) := f(x)\overline{f(x + h)}$. Suppose that $\|f\|_{u^3} \geq \delta$. We have $\|f\|_{u^2}^8 = \mathbb{E}_h \|\Delta(fh)\|_2^4$ (this is easy to check; informally it is because "both sides count parallelepipeds"). It follows that there are $\geq \frac{\delta^8 N}{2}$ values of h for which $\|\Delta(f, h)\|_{u^2} \geq \frac{\delta^2}{2}$ (a simple averaging argument). For each such h we apply the inverse theorem for u^2 to calculate that there is some $\varphi(h)$ such that $|\widehat{\Delta(f, h)}(\varphi(h))| \geq \frac{\delta^4}{4}$. Observe that if $f(x) = e(\frac{x^2}{N})$ then $\Delta(f, h)(x) = e(\frac{-2hx}{N})e(-\frac{h^2}{N})$, so we can take $\varphi(h) = -2h$. In the more general setting we'll look for some linearity in φ.

Lemma (Gowers): this was described by Gowers as "the lemma that changed my life", and formed the core of his Fields medal. Suppose that $f : G = \frac{\mathbb{Z}}{N\mathbb{Z}} \to \mathbb{C}$ is a 1-bounded function and $S \subset G, |S| = \sigma|G|$ is a set such that $\widehat{\Delta(f,h)}(\varphi(h))| \geq \eta \forall h \in S$ for some $\varphi : S \to \frac{\mathbb{Z}}{N\mathbb{Z}}$ (for some fixed $0 < \eta < 1$). Let $\Gamma := \{(x, \varphi(x)) : x \in S\} \subset (\frac{\mathbb{Z}}{N\mathbb{Z}})^2$ be the graph of φ. Then the additive energy $\omega_+(\Gamma)$ is at least $\sigma\eta^8$: the hypotheses imply that $\mathbb{E}_h 1_S(h)|\widehat{\Delta(f,h)}(\varphi(h))^2)|^2 \geq \sigma\eta^2$. Expanding out, we obtain $\mathbb{E}_h 1_S(h)\mathbb{E}_{x,y} f(x)\overline{f(x+h)f(y)}f(y+h)e(\frac{-\varphi(h)(x-y)}{N}) \geq \sigma\eta^2$. Substituting $y = x + k$ this yields $\mathbb{E}_{h,x,k} 1_S(h)f(x)\overline{f(x+h)f(x+k)}f(x+h+k)e(\frac{-\varphi(h)k}{N}) \geq \sigma\eta^2 \Rightarrow \mathbb{E}_{x,k}|\mathbb{E}_h 1_S(h)\overline{f(x+h)}f(x+h+k)e(\frac{-\varphi(h)k}{N})| \geq \sigma\eta^2$ (by the triangle inequality and the fact that f is 1-bounded), which in turn implies $\mathbb{E}_{x,k}|\mathbb{E}_h 1_S(h)\overline{f(x+h)}f(x+h+k)e(\frac{-\varphi(h)k}{N})|^2 \geq \sigma^2\eta^4$ ($\star$) (by Cauchy-Schwartz).

Write $F_k(t) := 1_S(t)e(\frac{-\varphi(t)k}{N})$ and $G_k(t) := \Delta(f,k)(t)$. Then ($\star$) can be rewritten as $\mathbb{E}_k||F_k^0 \star G_k||_2^2 \geq \sigma^2\eta^4$, wree $F_k^0(t) = F_k(-t)$. Writing this in Fourier [space] and using Parseval we obtain $\mathbb{E}_k \sum_r |\widehat{F_k}(-r)|^2|\widehat{G_k}(r)|^2 \geq \sigma^2\eta^4$.

Since G_k is 1-bounded, so is $G_k \star G_k$ and hence by Parseval $\sum_r |\widehat{G_k}(r)|^4 = ||G_k \star G_k||_2^2 \leq 1$. Applying Cauchy-Schwartz to the preceding inequality therefore yields $\mathbb{E}_k(\sum_r |\widehat{F_k}(r)|^4)^{\frac{1}{2}} \geq \sigma^4\eta^8$. Expanding this out using the definition of F_k we get $\mathbb{E}_{t_1,t_2,t_3,t_4} 1_S(t_1)1_S(t_2)1_S(t_3)1_S(t_4)\mathbb{E}_k e(-\frac{k}{N}(\varphi(t_1)+\varphi(t_2)-\varphi(t_3)-\varphi(t_4)))\sum_r e(-\frac{r}{N}(t_1+t_2-t_3-t_4))$. But this is simply $\frac{1}{N^3}$ times a count of the number of quadruples $t_1, t_2, t_3, t_4 \in S$ with $t_1+t_2 = t_3+t_4$ and $\varphi(t_1)+\varphi(t_2) = \varphi(t_3)+\varphi(t_4)$, thus completing the proof.

What do we do with φ^2?

Proposition: Suppose $K \geq 1$ and $S \subset \frac{\mathbb{Z}}{N\mathbb{Z}}$ (N prime) is a set of size at least $\exp(K^C)$. Let $\varphi : S \to \frac{\mathbb{Z}}{N\mathbb{Z}}$ be a function and write $\Gamma = \{(x, \varphi(x)) : x \in S\}$ for its graph. Suppose that $\sigma[\Gamma] \leq K$. Then there is a progression $P, |P| \geq \exp(-K^C)N^{\frac{1}{K^C}}$ and a linear map $\psi(x) = ax+b$ such that $\varphi(x) = \psi(x)$ for at least a K^{-C} proportion of $x \in P$. (This lecture will be technical and unpleasant; as such it is least likely to be examined).

Proof: Suppose to begin with we have a set $A \subset \mathbb{Z}$ with $\sigma(A) \leq K$. During the proof of Freiman-Ruzsa (follow that proof but omit Chang's covering lemma) we obtained a GAP Q with dimension $\leq K^C$ and size $\geq \exp(-K^C)|A|$ with $Q \subset 2A-2A$. We have (by the usual double counting argument) $\sum_x |A \cap (Q+x)| = |A||Q|$. But this sum has support $A - Q = 3A - 2A$, which by Ruzsa calculus is a set of size $\leq K^C|A|$. Hence there is some x such that $|A \cap (Q+x)| \geq K^{-C}|Q|$. (This manouver was srs; if we'd just stuck A in a progression as in Freiman-Ruzsa, we'd lose a whole log in our final bound (getting a result with a log log log in place of a log log)).

$x+Q$ is a generalized progression; suppose it is $\{x_0+l_1x_1+\cdots+l_dx_d : 0 \leq l_i < L_i\}$ with $L_1 \leq \cdots \leq L_d$. By fixing $l_1, \ldots, l_{d-1}$ and letting l_d vary, we may partition Q into translates of some (one-dimensional, genuine) progression of length at least $|Q|^{\frac{1}{d}} \geq \exp(-K^C)N^{\frac{1}{K^C}}$ (and note that this is a genuine partition, not merely a covering, since recall Q may be taken proper). By the pigeonhole principle there is some progression $P, |P| \geq \exp(-K^C)N^{\frac{1}{K^C}}$ with $|A \cap P| \geq K^{-C}|P|$ (Aside: we could have obtained this result a bit more quickly, but the "geometry of numbers" section is to a centain extent worthwhile in its own right).

We can make all this work for $A \subset \mathbb{Z}^2$: any finite subset of $\mathbb{Z}^2$ is Freiman

8-isomorphic to a subset of $\mathbb{Z}$ by some $\pi : A \to \mathbb{Z}$. Once we have this, a proper GAP $Q \subset 2\pi(A) - 2\pi(A)$ may be pulled bay to one in $2A - 2A$ (the definition of GAP in $\mathbb{Z}^2$ is obvious); the rest of the argument works as before. To see that $A \subset \mathbb{Z}^2$ is Freiman 8-isomorphic to a subset of $\mathbb{Z}$, translate A to lie in $[0, \dots, m-1]^2$ for some m and then define $\pi(x, y) = x + 8my$; it is an easy check that this $\pi\mid_A$ really is a Freiman 8-isomorphism.

Finally, we turn to $\Gamma \subset (\frac{\mathbb{Z}}{N\mathbb{Z}})^2$. Let $\overline{\Gamma}$ be the image of Γ under the unfolding map $\psi : (\frac{\mathbb{Z}}{N\mathbb{Z}})^2 \hookrightarrow \{0, \dots, N-1\}^2 \subset \mathbb{Z}^2$. Clearly $|\overline{\Gamma}| = |\Gamma|$; $\overline{\Gamma} + \overline{\Gamma}$ may well be larger than $\Gamma + \Gamma$, but not by too much: each sum in $\Gamma + \Gamma$ gives rise to no more than four sums in $\overline{\Gamma} + \overline{\Gamma}$, whence $\sigma[\overline{\Gamma}] \leq 4K$. Applying our earlier remarks, there is a progression $P \subset \mathbb{Z}^2, |P| \geq \exp(-K^{-C})N^{\frac{1}{K^C}}$, such that $|\overline{\Gamma} \cap P| \geq K^{-C}|P|$. The lower bound $|\Gamma| \geq \exp(K^C)$ tells us that $|\overline{\Gamma} \cap P| > 1$; this implies, since $\overline{\Gamma}$ is a graph (and so has at most one point with any given "x coordinate") that the common difference $d = (d_1, d_2)$ of P has $d_1 \not\equiv 0 \mod N$. It follows that the image of P in $(\frac{\mathbb{Z}}{N\mathbb{Z}})^2$ has the same size as P; calling it R, we therefore have $|R| \geq \exp(-K^C)N^{\frac{1}{K^c}}$ and $|\Gamma \cap R| \geq K^{-C}|R|$. But R is itself the graph of a linear function $x \mapsto ax + b$, so we have the result.

Summarizing the results of this section, we have: Corollary: Suppose N is prime and $f : \frac{\mathbb{Z}}{N\mathbb{Z}} \to \mathbb{C}$ is a 1-bounded function with $\|f\|_{u^3} > \delta$. Then there is a progression $P \subset \frac{\mathbb{Z}}{N\mathbb{Z}}, |P| \geq \exp(-\frac{1}{\delta^c})N^{\delta^c}$ together with $a, b \in \frac{\mathbb{Z}}{N\mathbb{Z}}$ such that $\mathbb{E}_{h\in P}|\widehat{\Delta(f,h)}(ah+b)|^2 \geq \delta^c$: $\|f\|_{u^3}$ large implies many $|\widehat{\Delta(f,h)}(\varphi(h))|$ are large. Gowers' magic lemma implies the graph Γ of φ has large additive energy; Balog-Szeverédi-Gowers implies a large subgraph Γ' has small doubling, now apply the previous lemma.

Gowers' Local Inverse Theorem for the U^3 norm, part II

Our task now is to "find some weak quadratic behaviour for f". We'll illustrate first of all with the model case $P = \frac{\mathbb{Z}}{N\mathbb{Z}}, a = 2, b = 0$. Suppose then that $\mathbb{E}_{h\in\frac{\mathbb{Z}}{N\mathbb{Z}}}|\widehat{\Delta(f,h)}(2h)|^2 \geq \eta$. Expanding out, $\mathbb{E}_{h,x,y}f(x)\overline{f(x+h)f(y)}f(y+h)e(\frac{-2h(x-y)}{N}) \geq \eta$. Substituting $y = x+k$ we get $\mathbb{E}_{x,h,k}f(x)\overline{f(x+h)f(x+k)}f(x+h+k)e(\frac{2hk}{N}) \geq \eta$. The LHS is $\|g\|_{u^2}^4$ where $g(x) = f(x)e(\frac{x^2}{N})$ (note $x^2 - (x+h)^2 - (x+k)^2 + (x+h+k)^2 = 2hk$). By the u^2 inverse theorem, there is some θ such that $|\mathbb{E}_x g(x)e(-\theta x)| \geq \eta^{\frac{1}{2}}$, hence $|\mathbb{E}_x f(x)e(\frac{x^2}{N} - \theta x)| \geq \eta^{\frac{1}{2}}$ - f correlates with a genuine quadratic.

What if we only have the <u>local</u> information $\mathbb{E}_{h\in P}\mathbb{E}_{x,k\in G}f(x)\overline{f(x+h)f(x+k)}f(x+h+k)e(\frac{(ah+b)k}{N}) \geq \eta$. This equals $\mathbb{E}_{h\in P}\mathbb{E}_{x,k\in G}f_1(x)\overline{f_2(x+h)f_3(x+k)}f_4(x+h+k)$ where $f_1(x) = f_3(x) = f(x)e(\frac{ax^2}{2N})$, $f_2(x) = f_3(x) = f(x)e(\frac{ax^2}{2N} \pm \frac{bx}{N})$ (the sign on both is the same, the lecturer simply fails to remember whether it is plus or minus). Introducing two additional averagings, this may be written as $\mathbb{E}_{i,j\in G}\mathbb{E}_{x,h,k\in P}f_{1,i}(x)\overline{f_{2,i}(x+h)f_{3,i,j}(x+k)}f_{4,i,j}(x+h+k)$ where $f_{1,i}(x) = f_1(x+i), f_{2,i}(x) = f_2(x+i), f_{3,i,j}(x) = f_3(x+i+j), f_{4,i,j}(x) = f_4(x+i+j)$; note these are all 1-bounded functions.

For the moment, suppose $P = \{0, \dots, L-1\}$.

Lemma: Suppose $g_1, \dots, g_4 : \frac{\mathbb{Z}}{N\mathbb{Z}} \to \mathbb{C}$ are 1-bounded functions and that $\mathbb{E}_{x,h,k\in P}g_1(x)\overline{g_2(x+h)g_3(x+k)}g_4(x+h+k) \geq \eta$, where $P = \{0, \dots, L-1\}$. Then there is some $\theta \in \mathbb{R}$ such that $|\mathbb{E}_{x\in P}g_1(x)e(\theta x)| \geq c\eta^C$. The proof illustrates an important technique in harmonic analysis for dealing with "sharp cutoffs", but is quite technical and hence probably nonexaminable. Write $G' := \frac{\mathbb{Z}}{3L\mathbb{Z}}$; we may write the assumption as $\mathbb{E}_{x,h,k\in G'} g_1(x)\overline{g_2(x+h)g_3(x+k)}g_4(x+h+k)1_P(x)1_P(h)1_P(k) \geq \frac{\eta}{27}$ ($\star$). We want to expand the $1_P(h), 1_P(k)$ using Fourier inversion, but were we to do this immediately it wouldn't work, because these "cutoff" functions are "too sharp"; to make it work, we will replace the 1_Ps by smoothed variants of them, $\tilde{1}_P$. If we draw a graph, 1_P is a "bar" stretching from 0 to L and then immediately falling to 0; we replace this immediate drop with a linear slope of "width" $2\epsilon L$. In a paper, merely drawing the graph would suffice, but as this is a part III course and the technique will be new to many readers, we shall go into more detail: $\tilde{1}_P$ is the convolution of 1_P with $\frac{1}{2\epsilon L}1_{\{-\epsilon L,\dots,\epsilon L\}}$ (strictly speaking there should be integer parts here, but to include them would be incredibly tedious), where ϵ is say $\frac{\eta}{1000}$.

It is easy to see that $\mathbb{E}_x|1_P(x) - \tilde{1}_P(x)| \leq 2\epsilon$. Hence, in ($\star$), we can replace $1_P(h), 1_P(k)$ by their smoothed variants, obtaining $\mathbb{E}_{x,h,k\in G'} g_1(x)1_P(x)\overline{g_2(x+h)g_3(x+k)}g_4(x+h+k)\tilde{1}_P(h)\tilde{1}_P(k) \geq \frac{\eta}{54}$ (†). Note that if $I \subset G'$ is an interval and $r \in \frac{\mathbb{Z}}{3L\mathbb{Z}}$ a frequency, taken with $|r| \leq \frac{3L}{2}$, $|\widehat{1_I}(r)| \leq C\min(1, \frac{1}{|r|})$ (by the geometric series formula: $|\widehat{1_I}(r)| = |\mathbb{E}_{x\in G'}1_I(x)e(\frac{-rx}{3L})| \leq \frac{1}{3L}\frac{2}{|1-e(\frac{2\pi r}{3L})|} \leq \frac{C}{|r|}$ by the double angle formulae and the fact that $|\sin t| \geq \frac{2}{\pi}|t|$ for $|t| \leq \frac{\pi}{2}$). It follows from this estimate and the fact that the FT of a convolution is the product of the FTs that $|\widehat{\tilde{1}_P}(r)| \leq \frac{C}{\eta} \mid (1, \frac{1}{|r|^2})$; it follows from Fourier inversion and the fact that $\sum n^{-2} < \infty$ that $\tilde{1}_P(x) = \sum_r a_r e(\frac{rx}{3L})$, where $\sum_r |a_r| < \frac{C}{\eta}$ (of course $a_r = \widehat{\tilde{1}_P}(r)$).

Substituting into (†) gives $\sum_{r,s} a_r a_r \mathbb{E}_{x,h,k\in G'} g_1(x)1_P(x)\overline{g_2(x+h)g_3(x+k)}g_4(x+h+k)e(\frac{rh}{3L})e(\frac{sk}{3L}) \geq \frac{\eta}{54} \Rightarrow \sum_{r,s} a_r a_s \sum_{x,h,k\in G'} g_1(x)1_P(x)\overline{g'_{2,r}(x+h)g'_{3,s}(x+k)}g'_{4,r,s}(x+h+k) \geq \frac{\eta}{54}$ where $g'_{2,r}(x) = g_2(x)e(\frac{-rx}{3L}), g'_{3,s}(x) = g_3(x)e(\frac{-sx}{3L}), g'_{4,r,s}(x) = g_4(x)e(\frac{(r+s)x}{3L})$. Hence there are r, s such that $\mathbb{E}_{x,h,k\in G'} g_1(x)1_P(x)\overline{g'_{2,r}(x+h)g'_{3,s}(x+k)}g'_{4,r,s}(x+h+k) \geq c\eta^3$.

By Gowers-Cauchy-Schwartz, $\|g1_P\|_{u^2} \geq c\eta 3$. Finally, apply the inverse theorem for the u^2-norm to get the result.

Let us return to $\mathbb{E}_{i,j\in G}\mathbb{E}_{x,h,k\in P} f_{1,i}(x)\overline{f_{2,i}(x+h)f_{3,i,j}(x+k)}f_{4,i,j}(x+h+k) \geq c\delta^C$. There exists a j such that the same is true without the expectation over j. For at least $c\delta^C N$ values of i we have $\mathbb{E}_{x,h,k} f_{1,i}(x)\dots f_{4,i,j}(x+h+k) \geq c\delta^C$. By the preceding lemma, for each such i, $|\mathbb{E}_{x\in P} f_{1,i}(x)e(-\theta_i x)| \geq c\delta^C$ for some $\theta_i \in \mathbb{R}$. Thus $\mathbb{E}_i|\mathbb{E}_{x\in P} f_{1,i}(x)e(-\theta_i x)| \geq c\theta^C$ (defining θ_i arbitrarily for other i). Recall $f_{1,i}(x) = f_1(x+i)$ and $f_1(x) = f(x)e(\frac{-\alpha x^2}{2N})$ (or possibly $f(x)e(\frac{-\alpha x^2}{2N} \pm \frac{bx}{N})$, the lecturer forgets). So this implies the following:

Proposition: Suppose $f : \frac{\mathbb{Z}}{N\mathbb{Z}} \to \mathbb{C}$ is a 1-bounded function with $\|f\|_{u^3} \geq \delta$. Then there is a progression P of length $\geq \exp(-\frac{1}{\delta^C})N^{\delta^C}$ together with quadratic polynomials $\psi_1, \dots, \psi_N : \frac{\mathbb{Z}}{N\mathbb{Z}} \to \mathbb{R}$ such that $\mathbb{E}_i|\mathbb{E}_{x\in P+i} f(x)e(-\psi_i(x))| \geq c\delta^C$ (Note: we only did this for $P = \{0, \dots, L-1\}$, but the general case reduces to this by an affine linear substitution.

Some diophantime approximation

Proposition: There is an absolute constant $c > 0$ such that: for any $\theta \in \mathbb{R}, N \geq 2$ there is an $n \leq N$ such that $\|n^2\theta\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq N^{-c}$.

Lemma (Weyl's inequality for quadratics (non-standard form)): Suppose $\alpha, \beta\gamma \in \mathbb{R}, N > \delta^{-C}$ and that $\frac{1}{N}|\sum_{n \leq N} e(\alpha n^2 + \beta n + \gamma)| \geq \delta$. Then there is $1 \leq q \leq \delta^{-C}$ such that $\|q\alpha\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \frac{\delta^{-C}}{N^2}$: Squaring gives $\frac{1}{N^2}\sum_{n,m \leq N} e(\alpha(m^2 - n^2) + \beta(m-n))| \geq \delta^2$. Substituting $m = n + h$ tells us $\frac{1}{N^2}\sum_{|h| \leq N}|\sum_{n \in I_h} e(2\alpha nh)| \geq \delta^2$, where the I_h are subintervals of $\{1, \ldots, N\}$.

$\sum_{|h| \leq N}|\sum_{n \in I_n} e(2\alpha hn)| \geq \delta^2 N^2$. The inner sum is bounded by $\min(N, \frac{2}{|1 - e(2\alpha h)|})$ by summing the GP; since $|\sin t| \geq \frac{2}{\pi}|t|$ for $|t| \leq \frac{\pi}{2}$, this easily implies there are $\geq \delta^{C_0}N$ values of $h \in \{1, \ldots, N\}$ such that $\|2\alpha h\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \frac{\delta^{-C_0}}{N}$ (Unlike C, C_0 will take some fixed value throughout this proof. We are being very lazy by including it at all; it could undoubtably be calculated and shownto be about 3).

Let $Q := \delta^{C_1}N^2$, where C_1 is to be specified later. Applying Dirichlet's argument, there is a $q \leq Q$ such that $|\alpha - \frac{a}{q}| \leq \frac{1}{qQ}$. If $q \leq \delta^{-C_1}$ this already implies the result; suppose, then, that $q > \delta^{-C_1}$. Wlog a, q are coprime; suppose that h, h' are [distinct] integers in some interval of length $\frac{q}{2}$. Then $ah \not\equiv ah' \mod q$ and therefore $\|\alpha(h - h')\|_{\frac{\mathbb{R}}{\mathbb{R}}} \geq \frac{1}{q} - \frac{1}{2Q} \geq \frac{1}{2q}$. In other words, the fractional parts $\|\alpha h\|_{\frac{\mathbb{R}}{\mathbb{Z}}}$ are $\frac{1}{2q}$-spaced as h ranges over any interval of length $\frac{q}{2}$.

In particular, the number of $\tilde{h}$ in such an interwal with $\|\alpha\tilde{h}\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \frac{\delta^{-C_0}}{N}$ is $O(1 + \frac{\delta^{-C_0}q}{N})$. The interval $\{1, \ldots, 2N\}$ may be subdivided into $O(1 + \frac{N}{q})$ subintervals of length $\frac{q}{2}$. Hence the number of $h \in \{1, \ldots, N\}$ satisfying $\|2\alpha h\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \frac{\delta^{-C_0}}{N}$ is $O((1 + \frac{\delta^{-C_0}q}{N})(1 + \frac{N}{q})) = O(1 + \frac{\delta^{-C_0}q}{N} + \delta^{-C_0} + \frac{N}{q})$ which is less than $\delta^{C_0}N$ provided C_1 is chosen sufficiently large and also provided $N > \delta^{-C}$.

Proposition: Let $\theta \in \mathbb{R}, N \geq 2$. Then there is $n \leq N$ such that $\|n^2\theta\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq N^{-C}$: suppose not. Then there is some C_0 and [small] ϵ such that $\|n^2\theta\|_{\frac{\mathbb{R}}{\mathbb{Z}}} > \epsilon$ whenever $n \leq \epsilon^{-C_0}$. Take a nonnegative function $\psi : \frac{\mathbb{R}}{\mathbb{Z}} \to \mathbb{R}_{\geq 0}$ with $\|\psi\|_1 = 1, \psi(x) = 0$ if $\|x\|_{\frac{\mathbb{R}}{\mathbb{Z}}} > \epsilon$ and $\psi(x) = \sum_{r \in \mathbb{Z}} a_r e(rx)$ where $\sum_{|r| > \epsilon^{-C}} |a_r| \leq \frac{1}{2}$ (the reader may verify that the function $\psi(x) = 0$ for $x \leq -\epsilon$, then slopes linearly up to $\psi(0) = \frac{1}{\epsilon}$, then linearly down to $\psi(\epsilon) = 0$ and 0 therafter, works; this is similar to our previous "smoothed" functions (we want a cutoff for $[-\epsilon, \epsilon]$, but a simple $\psi(x) = \frac{1}{2\epsilon}I_{[-\epsilon,\epsilon]}$ would not have the Fourier behaviour we want). This function does have the Fourier behaviour we want; $\widehat{\psi}(r)$ is a Fejér kernel, which decays like $\frac{1}{|r|^2}$).

We have $\sum_{n \leq \epsilon^{-C_0}} \psi(n^2\theta) = 0$. Expanding ψ in Fourier gives $\sum_r a_r \sum_{n \leq \epsilon^{-C_0}} e(rn^2\theta) = 0$. But $a_0 = \int \psi(x)dx = 1$, so the contribution from that is ϵ^{-C_0}; hence $|\sum_{r \neq 0} a_r \sum_{n \leq \epsilon^{-C_0}} e(rn^2\theta)| \geq \epsilon^{-C_0}$. Hence $\sum_{r \neq 0, |r| < \epsilon^{-C}} \sum_{n \leq \epsilon^{-C_0}} e(rn^2\theta)| \geq \frac{1}{2}\epsilon^{-C_0}$. Hence there is a particular value of r such that $|\sum_{n \leq \epsilon^{-C_0}} e(rn^2\theta)| \geq \frac{1}{2}\epsilon^{C - C_0}$. Applying Weyl's inequality, there is a $q \leq \epsilon^{-C'}$ such that $\|qr\theta\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \epsilon^{2C_0 - C'}$. Multiplying by qr we get $\|q^2r^2\theta\|_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \epsilon^{2C_0 - 2C' - C}$, which is $< \epsilon$ if C_0 is chosen large enough, so we have a contradiction.

Proposition: Suppose $P \subset \mathbb{Z}$ is a progression of length L. i) Suppose $\varphi(x) = \alpha x + \beta$ is linear. Then we can partition P into $O(L^{\frac{3}{4}})$ subprogressions on which φ varies by no more than $O(L^{-\frac{1}{2}})(\mod 1)$ ii) Suppose $\psi(x) = \alpha x^2 + \beta x + \gamma$.

Then we can partition P into $O(L^{1-c})$ subprogressions on which ψ varies by no more than $O(L^{-C})(\mod 1)$: Wlog $P = \{1, \dots, L\}$. For i), by Dirichlet's theorem there is $d \leq L^{\frac{1}{2}}$ such that $||\alpha d||_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq L^{-\frac{1}{2}}$. On any progression with common difference d and length $\leq L^{\frac{1}{4}}$ the variation of φ is $\leq L^{-\frac{1}{4}}$); clearly $\{1, \dots, L\}$ can be partitioned into $O(L^{\frac{3}{4}})$ such progressions. For ii), by the preceding proposition there is $d \leq L^{\frac{1}{2}}$ such that $||d^2\alpha||_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq L^{-c}$. Let $L' := L^{\frac{c}{3}}$ (for the same c) and consider a progression $Q = \{a, a+d, \dots, a+(L'-1)d\}$ [we can partition P into such]. We have $\psi(a+td) = t^2(\alpha d^2) + d(2\alpha ad + bd) + \alpha a^2 + \beta a + \gamma$. Note that the total variation of $t^2(\alpha d^2)(\mod 1)$ is $\leq L^{-\frac{c}{3}}$. Now use i) to further subpartition Q into progressions on which the variation of $t(2\alpha ad + \beta d)$ is small. (The same argument works inductively for polynomials of degree k, provided we have Weyl's inequality for this degree).

Recall: (1) If $A \subset \{1, \dots, N\}$ has few 4APs then $||f||_{u^3} \geq \alpha^C$ (2) If $||f||_{u^3} \geq \delta$ then there is $P \subset \frac{\mathbb{Z}}{N'\mathbb{Z}}, |P| \geq \exp(-\frac{1}{\delta^c})N^{\delta^c}$ and quadratic phases $\psi_1, \dots, \psi_N$ such that $\mathbb{E}_{i \in \frac{\mathbb{Z}}{N'\mathbb{Z}}}|\mathbb{E}_{x \in i+P} f(x)e(-\psi_i(x))| \geq \delta^c$. Next we shall perform (3): remove the ψ_i and find a progression $\tilde{P}$ such that $|\sum_{x \in \tilde{P}} f(x)| \geq \delta^c$.

Our result so far can be summed up as: Suppose that $f : \frac{\mathbb{Z}}{N'\mathbb{Z}} \to \mathbb{C}$ is 1-bounded and $||f||_{u^3} \geq \delta$. Then there is a progression $Q \subset \frac{\mathbb{Z}}{N'\mathbb{Z}}$ with length $L \geq \exp(-\frac{1}{\delta^c})N^{\delta^c}$ together with quadratics $\psi_1, \dots, \psi_{N'}$, for which $\sum_{i \in \frac{\mathbb{Z}}{N'\mathbb{Z}}} |\sum_{x \in i+Q} f(x)e(-\psi_i(x))| \geq \delta^C N'L$ $(\star)$.

Lemma (Genuine progressions from $\mod N'$ progressions): Suppose $P \subset \frac{\mathbb{Z}}{N'\mathbb{Z}}$ is a progression of length L. Then we can partition $P \cap \{1, \dots, N\}$ into $\leq 2\sqrt{L}$ genuine progressions [i.e. arithmetic progressions in $\mathbb{Z}$]: let the common difference of P be d and $\delta > 0$ a parameter (in fact $\delta = \frac{1}{\sqrt{L}}$). Applying Dirichlet's lemma, there is $r \leq \frac{1}{\delta}$ such that $||\frac{rd}{N'}||_{\frac{\mathbb{R}}{\mathbb{Z}}} \leq \delta$. Any progression with common difference rd and length $\leq \frac{1}{\delta}$ will then intersect $\{1, \dots, N\}$ in a genuine progression - and we can partition P into $\leq r(\frac{L\delta}{r} + 1) \leq 2\sqrt{L}$ such progressions.

Applying the lemma to each progression $i+Q$ in $(\star)$ we get genuine progressions $P_1, \dots, P_M \subset \{1, \dots, N\}, M \leq 2\sqrt{L}N'$ such that $\sum_{i=1}^{M} |\sum_{x \in P_i} f(x)e(-\psi_i(x))| \geq \delta^C \sum_{i=1}^{M} |P_i| = \delta^C LN$ (relabelling the ψs so that ψ_i corresponds to P_i); this holds because $\bigcup_{i=1}^{M} P_i$ covers each point of $\{1, \dots, N\}$ precisely L times.

The contribution to this from those P_i with $|P_i| \leq \frac{\delta^C LN}{10M}$ is manifestly $\leq \frac{\delta^C LN}{10}$. The remaining progressions have size $\geq c\delta^C\sqrt{L}$. Applying the result from the previous lecture, we partition each of them into subprogressions P'_i, at most $O(|P_i|^{1-c})$ in number, such that the variation of ψ_i is $\leq \frac{\delta^c}{1000}$ [on any P'_i]; the reader may check this is valid provided L is big enough, which it will be for N sufficiently large.

It is then easy to see that $\sum_{i=1}^{M'} |\sum_{x \in P'_i} f(x)| \geq \frac{\delta^C LN}{2}$. Furthermore, $M' << \sum_{i=1}^{M} |P_i|^{1-c} \leq M^c(LN)^{1-c}$ (by Hölder's inequality, using $\sum |P_i| = LN$), $\leq L^{1-\frac{c}{2}}N$. Critically, this is appreciably smaller than LN, giving us that the P'_i are longish on average.

Lemma: Suppose $P_1, \dots, P_{M'}$ are progressions in $\{1, \dots, N\}$ such that $\bigcup P'_i$ covers each point L times. Suppose $f : \{1, \dots, N\} \to \mathbb{R}$ is 1-bounded and that [replacing some of what were Ms in the lecture with M's, since I believe this was a matter of mistakes or laziness rather than intent] $\sum_{i=1}^{M'} |\sum_{x \in P_i} f(x)| \geq$

$\eta \sum_{i=1}^{M'} |P_i| = \eta LN$. Suppose also $\sum f(x) = 0$ (i.e., precisely the situation we have). Then there is a progression P of length at least $\frac{\eta LN}{4M'}$ such that $\sum_{x \in P} f(x) \geq \frac{\eta}{2}|P|$: adding $\sum_{i=1}^{M'} \sum_{x \in P_i} f(x) = 0$ to both sides gives $\sum_{i=1}^{M'} (\sum_{x \in P_i} f(x))_+ \geq \frac{\eta}{2} LN$, where $(z)_+$ takes the value z if $z > 0$, 0 otherwise. The contribution to this from those P_i with $|P_i| \leq \frac{\eta LN}{4M'}$ is manifestly $\leq \frac{\eta LN}{4}$, whence the $\sum_{i:|P_i| \geq \frac{\eta LN}{4M'}} (\sum_{x \in P_i} f(x))_+ \geq \frac{et\ LN}{4} \geq \frac{\eta}{4} \sum_{i:|P_i| \geq \frac{\eta LN}{4M'}} |P_i|$. The reader may check that the density increment proposition, and hence Gowers' theorem, is now proven.

Sum-product phenomena

The lecturer would assert that almost all interesting problems in number theory deal with the relation between additive and multiplicative phenomena. A motivating conjecture in this field is that of Erdős-Szeverédi: Suppose $A \subset \mathbb{Z}$ is a finite set; as usual we define $A + A := \{a + a' : a, a' \in A\}$, $A \cdot A := \{aa' : a, a' \in A\}$. (Note that since $\mathbb{Z}$ embeds into a field, we may (to a certain extent) treat it as a group under multiplication; we can show that all our sumset results (Ruzsa calculus etc.) also hold for product sets). Suppose $|A| = n$. The conjecture is that $|A + A| + |A \cdot A| \geq c_\epsilon n^{2-\epsilon} \forall \epsilon > 0$; the best known result to date is a theorem of Solymoshin which states it is $\geq c_\epsilon n^{\frac{4}{3}-\epsilon}$. This theorem essentially claims that it is impossible for a set to be "special" (having small doubling) in both additive and multiplicative ways.

We shall concentrate on two theorems in this section: Theorem (Bourgain, Katz, Tao): Suppose p is a (large) prime and $\delta > 0$ a parameter. Suppose $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ has $p^\delta \leq |A| \leq p^{1-\delta}$. Then there is $\delta' = \delta'(\delta) > 0$ such that $|A + A| + |A \cdot A| \geq |A|^{1+\delta'}$ (in fact, the lower bound on $|A|$ was shown to be unnecessary in later work of Bourgain, Glibichuk and Konygin. We shall in historically unsound fashion follow their method for most of the proof, but only achieve the earlier result).

Our second theorem is usually given as a consequence of the above, but we shall proove it independently, first: Theorem (Bourgain et al): Suppose $H \leq (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ is a subgroup of size at least p^δ. Then, uniformly in r, we have $\frac{1}{|H|} |\sum_{x \in H} e(\frac{rx}{p})| << p^{-\delta'}$ for some $\delta' = \delta'(\delta) > 0$ [this says informally that multiplicative progressions are extraordinarily average in terms of their additive behaviour (they do not correlate with any additive phase)].

Theorem: Suppose $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$. Then there is some $\xi \neq 0$ such that $|A + \xi \cdot A| \geq \frac{1}{2} \min(|A|^2, p)$ (here $A + \xi \cdot A = \{a + \xi a' : a, a' \in A\}$): we use additive energy. $\sum_{\xi \neq 0} \omega_+(A, \xi \cdot A)$ counts $\frac{1}{|A|^3}$ times the number of solutions to $a_1 - a_2 = \xi(a_3 = a_4)$ with $a_1, \ldots, a_4 \in A, \xi \neq 0$. Clearly if $a_1 - a_2, a_3 - a_4 \neq 0$ there is a unique ξ solving this; if they are both zero, any ξ will do. So the total number of solutions is $\leq |A|^2(|A| - 1)^2 + (p - 1)|A|^2$. Hence there is at least one ξ such that $\omega_+(A, \xi \cdot A) \leq \frac{1}{|A|} + \frac{(|A|-1)^2}{(p-1)|A|} \leq 2 \max(\frac{1}{|A|}, \frac{|A|}{p})$. But recall that if $\omega_+(U, V) \leq \delta$ then $\sigma[U, V] \geq \frac{1}{\delta}$. This completes the proof.

Lemma: Let $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$. Then $|3A^2 - 3A^2| \geq \frac{1}{2} \min(|A|^2, p)$ (writing $A^2 = a \cdot a = \{aa' : a, a' \in A\}$): Let $\xi \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$. Observe that $|A + \xi \cdot A| = |A|^2$ unless there are $a_1, a_2, a_3, a_4 \in A$ with $a_1 + \xi a_2 = a_3 + \xi a_4$, i.e. $\xi \in \frac{A-A}{A-A}$ (obviously defined as $\{\frac{a_1-a_2}{a_3-a_4} : a_i \in A \forall i\}$). We consider two possibilities: either $\frac{A-A}{A-A} = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (we always have $0 \in \frac{A-A}{A-A}$, so do not need to worry about the difference between $\frac{\mathbb{Z}}{p\mathbb{Z}}$ and $(\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$), or it does not.

First consider the case $\frac{A-A}{A-A} \neq \frac{\mathbb{Z}}{p\mathbb{Z}}$. Then there is some $\xi \in \frac{A-A}{A-A}$ such that $\xi + 1 \notin \frac{A-A}{A-A}$. By the earlier observation, $|A + (\xi+1)\cdot A| = |A|^2$. Suppose $\xi = \frac{a_1 - a_2}{a_3 - a_4}$. Then $3A^2 - 3A^2 \supset (a_3 - a_4)\cdot A + (a_1 - a_2 + a_3 - a_4)\cdot A = (a_3 - a_4)(A + (\xi + 1)\cdot A)$, which means $|3A^2 - 3A^2| \geq |A|^2$. For the case $\frac{A-A}{A-A} = \frac{\mathbb{Z}}{p\mathbb{Z}}$, by the lemma there is some $\xi \in (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ such that $|A + \xi \cdot A| \geq \frac{1}{2}\min(|A|^2, p)$. Suppose $\xi = \frac{a_1 - a_2}{a_3 - a_4}$. Then $3A^2 - 3A^2 \supset 2A^2 - 2A^2 \supset (a_3 - a_4)\cdot A + (a_2 - a_2)\cdot A = (a_3 - a_4)\cdot(A + \xi \cdot A)$. Hence $|3A^2 - 3A^2| \geq \frac{1}{2}\min(|A|^2, p)$, as claimed.

Remark: The Katz-Tao lemma is: Suppose $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ has $|A + A|, |A \cdot A| \leq K|A|$. Then there is $A' \subset A, |A'| \geq K^{-C}|A|$ such that $|3A'^2 - 3A'^2| \leq K^C|A'|$. Together with the lemma just proved, this implies the Bourgain-Katz-Tao sum product theorem, and in fact without needing the assumption that $|A| \geq p^{\delta}$. The proof is by clever use of B-S-G (The original proof of Bourgain-Katz-Tao used the Katz-Tao lemma and a weaker result similar to our lemma above).

Corollary: Let $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ be a set of size $\geq p^{\delta}$. Then there is a $k = k(\delta)$ such that $kA^k - kA^k = \frac{\mathbb{Z}}{p\mathbb{Z}}$; if our A is a multiplicative subgroup then $A^k = A$ and so the result is $kA - kA = \frac{\mathbb{Z}}{p\mathbb{Z}}$: iterating the lemma C_{δ} times gives a $k_0 = k_0(\delta)$ such that $|k_0 A^{k_0} - k_0 A^{k_0}| > \frac{1}{2}p$ ($\geq$, and hence ¿ since p is assumed odd). But if $X \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ has cardinality $> \frac{1}{2}p$ then $X + X = \frac{\mathbb{Z}}{p\mathbb{Z}}$, since for any $t \in \frac{\mathbb{Z}}{p\mathbb{Z}}$, the sets X and $t - X$ must overlap. Thus setting $k = 2k_0$ we have the result.

Let $K \geq 1$ be a parameter and let $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$. Define $\mathrm{Alg}_K(A) := \{\xi : |A + \xi \cdot A| \leq K|A|\}$ (equivalently we could require $d(A, \xi \cdot A) \leq \log K$).

Lemma (Basic properties of Alg): (i) $0 \in \mathrm{Alg}_K(A)$ (ii) If $\xi \in \mathrm{Alg}_K(A)$ then $-\xi \in \mathrm{Alg}_{K^C}(A)$ (iii) If $\xi_1, \xi_2 \in \mathrm{Alg}_K(A)$ then $\xi_1 + \xi_2 \in \mathrm{Alg}_{K^C}(A)$ (iv) If $\xi_1, \xi_2 \in \mathrm{Alg}_K(A)$ then $\xi_1\xi_2 \in \mathrm{Alg}_{K^C}(A)$: the proof is mostly immediate from Ruzsa calculus (and if worked out explicitly, most of the Cs are quite small - 2 or 3). For (iv), note that $d(\xi_1 \cdot A, \xi_1\xi_2 \cdot A) = d(A, \xi_2 \cdot A)$ and so the result is immediate from the Ruzsa triangle inequality.

Proposition: Let $A, B \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ be such that $p^{\alpha} \leq |A| \leq p^{1-\alpha}, |B| \geq p^{\beta}$. Then there is some $b \in B$ such that $|A + b \cdot A| \geq |A|^{1+c_{\alpha,\beta}}$: By the corollary there is $k = k(\beta)$ such that $kB^k - kB^k = \frac{\mathbb{Z}}{p\mathbb{Z}}$. Suppose $|A + b \cdot A| \leq K|A|$ for some K and for all $b \in B$. By many applications of the preceding lemma, $|A + \xi \cdot A| \leq K^{C_{\beta}}|A|$ for all $\xi \in \frac{\mathbb{Z}}{p\mathbb{Z}}$. But on the other hand there is some ξ for which $|A + \xi \cdot A| \geq \frac{1}{2}\min(|A|^2, p)$. By the assumptions on $|A|$ this is a contradiction if $K \leq |A|^{c_{\alpha,\beta}}$ for sufficiently small $c_{\alpha,\beta} > 0$ (Note we have been rather lazy here; c is in fact "not very" dependent on α. It is "mostly" a function of β).

Bourgain's Exponential Sum Estimate

Let $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$, and let $\delta > 0$ be a parameters. Then we write $\mathrm{Spec}_{\delta}(A) := \{\xi : \frac{1}{|A|}|\sum_{x \in A} e(\frac{\xi x}{p})| \geq \delta\}$ for "the set of δ-large Fourier coefficients of A".

A rephrasing of Bourgain's exponential sum estimate is: if $H \leq (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ is a multiplicative subgroup with $|H| \geq p^{\delta}$ then $\mathrm{Spec}_{\eta}(H) = \{0\}$ for some $\eta =$

$p^{-\delta'}, \delta' = \delta'(\delta) > 0$. It should be clear that $\mathrm{Spec}_\eta(H)$ is H-invariant for any η, i.e. if $x \in \mathrm{Spec}_\eta(H)$ then so is hx for any $h \in H$. It turns out that $\mathrm{Spec}(H)$ also has a certain amount of additive structure (in fact this is true for any set H, not necessarily a multiplicative subgroup):

Lemma (Additive Structure of Spec): Let $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$, $0 < \delta < 1$. Then for a proportion at least $\frac{\delta^2}{2}$ of the pairs $x, y \in \mathrm{Spec}_\delta(A)$ we have $x - y \in \mathrm{Spec}_{\frac{\delta^2}{2}}(A)$: Suppose that $\mathrm{Spec}_\delta(A) = \{\xi_1, \dots, \xi_k\}$. For each j we may find a complex number c_j, $|c_j| = 1$ such that $c_j \sum_{x \in A} e(\frac{\xi_j x}{p})$ is real and $\geq \delta|A|$ (i.e. c_j is just a phase factor). Summing over j gives $\sum_{j=1}^k c_j \sum_{x \in A} e(\frac{\xi_j x}{p}) \geq deltak|A|$. Swapping the summations and applying Cauchy-Schwartz, $\sum_{x \in A} |\sum_{j=1}^k c_j e(\frac{\xi_j x}{p})|^2 \geq \delta^2 k^2 |A|$. Expanding the sum and exchanging the order once more yields $\sum_{1 \leq i,j \leq k} c_j \overline{c_j} \sum_{x \in A} e(\frac{(\xi_i - \xi_j)x}{p}) \geq \delta^2 k^2 |A|$ and hence by the triangle inequality $\sum_{1 \leq i,j \leq k} |\sum_{x \in A} e(\frac{(\xi_i - \xi_j)x}{p})| \geq \delta^2 k^2 |A|$. If the inner sum were $< \frac{\delta^2 |A|}{2}$ for $\geq 1 - \frac{\delta^2 k^2}{2}$ pairs i, j, we have an easy contradiction. (In his original paper, the famously terse Bourgain neglected to prove this lemma at all, merely writing "linearisation gives").

Corollary: Suppose $H \leq (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ is a multiplicative subgroup. Let $0 < \delta < 1$. Write $A := \mathrm{Spec}_\delta(H), A' = \mathrm{Spec}_{\frac{\delta^2}{2}}(H)$. Write $L := \frac{|A'|}{|A|}$. Then for every $h \in H$ we have $\omega_+(A, h \cdot A) \geq \frac{\delta^4}{L}$: apply the preceding lemma. For each $x \in A'$ write $r(x) = \#\{(a, a') \in A \times A : a - a' = x\}$. We showed that $\sum_{x \in A'} r(x) \geq \frac{\delta^2}{2}|A|^2$. Applying Cauchy-Schwartz we get $\sum_{x \in A'} r(x)^2 \geq \frac{1}{|A'|}(\sum_{x \in A'} r(x))^2 = \frac{\delta^4 |A|^4}{4|A|'} = \frac{\delta^4}{4L}|A|^3$. This means that the number of solutions to $a_1 + a_2 = a_3 + a_4$ is $\geq \frac{\delta^4}{4L}|A|^3$. The same is true of the number of solutions to $a_1 + ha_2 = a_3 + ha_4$ for each fixed $h \in H$, since A is H-invariant. This implies the result.

Additive-Multiplicative Balog-Szeverédi-Gowers

We use rough notation at some scale K (recall e.g. $X \gtrsim Y$ means $X \geq cK^{-C}Y$).

Lemma 25: Suppose $X \subset \frac{\mathbb{Z}}{p\mathbb{Z}}$ (in fact any ring will do) and suppose $H \subset (\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ is a set such that $\omega_+(X, h \cdot X) \gtrsim 1 \forall h \in H$. Then for each $h \in H$ there are sets $X_h, Y_h \subset X, |X_h|, |Y_h| \gtrsim |X|$ such that $|X_h + h \cdot Y_h| \lesssim |X|$: apply B-S-G for each h.

Our goal is to in some sense "remove the h-dependence of X_h, Y_h".

Proposition: With the same hypotheses, there is a set $X' \subset X, |X'| \gtrsim |X|$ and a set $H', |H'| \gtrsim |H|$ (note not $H' \subset H$; in fact we'll have $H' \subset aH - aH$ for some a, but this is irrelevant) such that $|X' + h \cdot X'| \lesssim |X| \forall h \in H'$.

We begin with yet another consequence/variant of Cauchy-Schwartz:

Lemma: Suppose S is a set. Suppose $S_1, \dots, S_k \subset S$ are sets with $|S_i| \geq \delta|S|$ for some $0 < \delta < 1$. Then there is an i such that $|S_i \cap S_j| \geq \frac{\delta^2}{2}|S|$ for at least $\frac{\delta^2 k}{2}$ values of j: we have $\sum_{i=1}^k \sum_x 1_{S_i}(x) \geq \delta k|S|$. Swapping the order and applying C-S, $\sum_x \sum_i \sum_j 1_{S_i}(x) 1_{S_j}(x) \geq \delta^2 k^2 |S|$, i.e. $\sum_{i,j} |S_i \cap S_j| \geq \delta^2 k^2 |S|$, and the result follows by a simple averaging argument.

Proof of the proposition: by Lemma 25 there are $X_h, Y_h, |X_h|, |Y_h| \gtrsim |X|$ such that $|X_h + h \cdot Y_h| \lesssim |X|$. Applying the preceding lemma to the sets $X_h \times Y_h \in X \times X$, we obtain an h_0 such that $|X_{h_0} \cap X_h|, |Y_{h_0} \cap Y_h| \gtrsim |X| \forall h \in H'$, and $|H'| \gtrsim |H|$ ($\star$).

Now $|X_{h_0} + h_0 \cdot Y_{h_0}|, |X_h + h \cdot Y_h| \lesssim |X|$; by Ruzsa calculus we have $\sigma[X_{h_0}], \sigma[X_h], \sigma[Y_{h_0}], \sigma[Y_h] \lesssim$

1 and of course $X_{h_0} \sim h_0 \cdot Y_{h_0}, X_h \sim h \cdot Y_h$. By one of the rules of Ruzsa calculus together with $(\star)$ we obtain $X_h \sim X_{h_0}, Y_h \sim Y_{h_0}$. It therefore follows that $h_0 \cdot Y_{h_0} \sim X_{h_0} \sim X_h \sim h \cdot Y_h \sim h \cdot Y_{h_0}$ (this took two pages of the Ruzsa triangle inequality in Bourgain's original paper - see the power of Ruzsa calculus and rough notatin). Therefore $Y_{h_0} \sim \frac{h}{h_0} \cdot Y_{h_0} \forall h \in H'$; this proves the proposition: take $X' := Y_{h_0}$ and redefine $H' := \frac{1}{h_0}H'$.

Combining this with the earlier corollary gives:

Corollary: Suppose $H \leq (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ is a multiplicative subgroup. Let $0 < \delta < 1$ and let $A = \mathrm{Spec}_{\delta}(H), A' = \mathrm{Spec}_{\frac{\delta^2}{2}}(H)$. Let $L := \frac{|A'|}{|A|}$. Using rough notation at scale $\frac{L}{\delta}$, there is a set $X \subset A, |X| \gtrsim |A|$ and a set $H' \subset (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}, |H'| \gtrsim |H|$ such that $|X + h \cdot X| \lesssim |X|$ for all $h \in H'$.

Proof of Bourgain's exponential sum estimate: Let $H \leq (\frac{\mathbb{Z}}{p\mathbb{Z}})^{\times}$ be a subgroup, $|H| \geq p^{\delta}$. Suppose for contradiction that $\mathrm{Spec}_{\eta}(H) \neq \{0\}$ for some $\eta = p^{-o(1)}$. Let $J = J(\delta)$ be an integer to be specified; set $\alpha_0 = \eta$ and $\alpha_{i+1} := \frac{\alpha_i^2}{2}$ for $i \geq 0$. Note $\mathrm{Spec}_{\alpha_0}(H) \subset \mathrm{Spec}_{\alpha_1}(H) \subset \cdots \subset \mathrm{Spec}_{\alpha_j}(H)$. Hence by pigeonhole there is an $\alpha = \alpha_i$ such that $|\mathrm{Spec}_{\alpha_{i+1}}(H)| \leq p^{\frac{1}{J}}|\mathrm{Spec}_{\alpha}(H)|$ (this is called a Diadic pigeonhole argument). Write $A = \mathrm{Spec}_{\alpha_i}(H), A' = \mathrm{Spec}_{\alpha_{i+1}}(H)$, $\alpha' = \alpha_{i+1}$; note $\alpha \geq (\frac{\eta}{2})^{2^J} = p^{-o_J(1)}$. Notice also that $|A| \geq p^{\delta}$ since A is H-invariant.

By previous lemmas we have $\omega_+(A, h \cdot A) \gtrsim 1 \forall h \in H$ where the rough notation is at scale $\frac{L}{\alpha}$, where $L = \frac{|A|}{|A'|} \leq p^{\frac{1}{J}}$. Applying the additive-multiplicative B-S-G theorem, there is a set $X \subset A, |X| \geq (\frac{\alpha}{p^{\frac{1}{J}}})^C|A|$ and set H', $|H'| \geq (\frac{\alpha}{p^{\frac{1}{J}}})^C|H|$ such that $|X + h \cdot X| \leq (\frac{p^{\frac{1}{J}}}{\alpha})^C|X| \forall h \in H'$. If we choose δ sufficiently large then $|X|, |H'| \geq p^{\frac{\delta}{2}}$ and this will contradict our earlier lemma (the one giving a lower bound on $\sup_b|A + b \cdot A|$).

Bourgain-Katz-Tao: For $A \subset \frac{\mathbb{Z}}{p\mathbb{Z}}, p^{\alpha} \leq |A| \leq p^{1-\alpha}$, we have $|A + A| + |A \cdot A| \geq |A|^{1+c_{\alpha}}$: suppose $|A + A|, |A \cdot A| \leq K|A|$; our task is to prove $K \geq |A|^{c_{|}alpha}$. We use rough notation at scale K. Look at the sets aA for $a \in A$. These all lie in $A \cdot A$, so by our variant of Cauchy-Schwartz there is some $a_0 \in A$ such that $|A \cap \frac{a_0}{a}A| = |aA \cap a_0A| \gtrsim |A|$ for $\gtrsim |A|$ choices of a; call the set of these S.

Fix some a and set $A' = A \cap \frac{a_0}{a}A$. Since A' is so large, and since $\sigma_+[A] \leq K$, we have $\sigma_+[A'] \lesssim 1$. Hence the additive energy $\omega_+(A') \gtrsim 1$, which means that $\omega_+(A, \frac{a_0}{a}A) \gtrsim 1$. Set $B := \{\frac{a_0}{a} : a \in S\}$. Applying additive-multiplicative B-S-G gives a set $X \subset A, |X| \gtrsim |A|$ and a set $B' \subset B, |B'| \gtrsim |B|$ such that $X + b \cdot X| \lesssim |X| \forall b \in B'$. If K is a sufficiently small power of p this contradicts our earlier lemma.

Sum-product in $\mathbb{C}$

Theorem (Solymoshin, with a very Hungarian argument): Let $A \subset \mathbb{C}$ be finite. Then $|A+A|+|A \cdot A| \geq c|A|^{\frac{5}{4}}$. The lecturer believes this is the best known result of this form for complex numbers; for the reals there is an argument which gives $|A|^{\frac{4}{3}}$. We believe the "correct" exponent is likely to be 2. The only property of the complex numbers we'll use is the "Bersicoritch covering property".

Definition: Let (X, d) be a metric space. The Besicovitch constant of (X, d), if it exists, is the largest k for which there are balls $B_i = B(x_i, r_i), i = 1, \ldots, k$ such taht $x_i \notin B_j^0$ if $i \neq j$, but $\bigcap_{i=1}^k B_i \neq \emptyset$.

Lemma: The Besicovitch constant of $\mathbb{C}$ is 6: Suppose not. Then there are balls $B_i = B(x_i, r_i)$, $i = 1, \dots, 7$ with $x_j \notin B_i^0$ and some point $z \in \bigcap_{i=1}^7 B_i$. Wlog consider $x_1, x_2, \dots$ to be in clockwise order around z (the degenerate cases which actually take up most of the time in a proof are left as an exercise to the reader). Then $x_i x_{i+1}$ is the largest side of the triangle zx_ix_{i+1}, hence x_ix_{i+1} subtends an angle $\geq \frac{\pi}{3}$ at z $[\forall i]$, a contradiction.

Proof of Solymoshin: To each point $a \in A$ associate a nearest neighbour $a^\star \in A \setminus \{a\}$ (breaking ties by making an arbitrary choice).

The idea behing this proof is: Take $a_1, a_2, a_3 \in A$. If the nearest neighbour of $a_1 + a_2$ was always $a_1^\star + a_2$ and the nearest neighbour of a_1a_3 was always $a_1^\star a_3$ then we could argue as follows: may $\varphi : (a_1, a_2, a_3) \mapsto (a_1 + a_2, a_1^\star + a_2, a_1a_3, a_1^\star a_3) \in (A + A) \times (A + A) \times (A \cdot A) \times (A \cdot A)$. Then we'd have (if what we said held) $\mathrm{Im}\varphi \leq |A + A||A \cdot A|$. But by straightforward algebra φ is injective. Hence we'd have $|A|^3 \leq |A + A||A \cdot A|$, a stronger result than we need.

This idea is too simplistic, e.g. $a_1^\star + a_2$ need not be the nearest neighbour of $a_1 + a_2$ in $A + A$. Suppose $|A + A|, |A \cdot A| \leq K|A|$. We aim to prove $K \geq c|A|^{\frac{1}{4}}$. We say that a triple $(a_1, a_2, a_3) \in A \times A \times A$ is well-behaved if $U_{a_1,a_2} := |\{u \in A + A : |u - (a_1 + a_2)| \leq |(a_1^\star + a_2) - (a_1 + a_2)|\}| \leq 100K$ $(\star)$ and $V_{a_1,a_3} := |\{v \in A \cdot A : |v - a_1a_3| \leq |a_1^\star a_3 - a_1a_3|\}| \leq 100K$ $(\star\star)$. It is not obvious that there are any well-behaved triples; however, it turns out that at least 50% of all triples (a_1, a_2, a_3) are well behaved. To prove this calim, first fix a_2. Then if $u \in U_{a_1,a_2}$ then it lies in the ball $B_{|a_1^\star - a_1|}(a_1 + a_2$. But by Besicovitch's property, no u lies in more than 6 of these balls. Hence $\sum_{a_1} U_{a_1,a_2} \leq 6|A + A| \leq 6K|A|$; similarly $\sum_{a_1} V_{a_1,a_3} \leq 6K|A|$ [for any a_3]. It's very easy to see from this that more than 50% of triplets (a_1, a_2, a_3) are well-behaved.

Consider the map $\varphi : (a_1, a_2, a_3) \mapsto (a_1 + a_2, a_1^\star + a_2, a_1a_3, a_1^\star a_3)$, restricted to well-behaved triples. A simple algebraic computation confirms that φ is injective. Therefore $|\mathrm{Im}\varphi| \geq \frac{|A|^3}{2}$. OTOH suppose $(x, y, z, w) \in \mathrm{Im}\varphi$. There are at most $A + A$ choices for x. Amongst all possible choices for y (given x), choose one, $\overline{y}$, such that $|x - \overline{y}|$ is as big as possible. Write $(\overline{a_1}, \overline{a_2}, \overline{a_3})$ for the corresponding well-behaved triple. Then for all other permissible y we have $|\overline{a_1} + \overline{a_2} - y| = |x - y| \leq |x - \overline{y}| = |\overline{a_1} - \overline{a_1}^\star|$. Since $(\overline{a_1}, \overline{a_2}, \overline{a_3})$ is well-behaved, there are $\leq 100K$ choices for w. Hence $|\mathrm{Im}\varphi| \leq |A + A||A \cdot A|(100K)^2 \leq 10^4K^4|A|^2$. Comparing with $|\mathrm{Im}\varphi| \geq \frac{|A|^3}{2}$ gives the result.

This concludes the examinable section of the course; there was also a brief section on "Nilmanifolds and higher Gowers norms", which the lecturer claims make everything make a lot more sense.