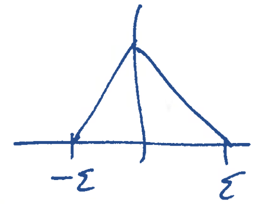
Thm: Suppose $\theta \in \mathbb{R}/\mathbb{Z}$. Then $\exists\ 1 \leq n \leq N$ such that $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq N^{-c}$.

Proof: Let $\varepsilon > 0$ and choose a cut-off function $\psi : \mathbb{R}/\mathbb{Z} \to \mathbb{R}_{\geq 0}$ with:

(i) $\psi(x) = 0$ if $\|x\|_{\mathbb{R}/\mathbb{Z}} > \varepsilon$



(ii) $\|\psi\|_1 = \int \psi = 1$

(iii) $\psi(x) = \sum_r a_r e^{2\pi i r x}$ where $\sum_{|r| > \varepsilon^{-C}} |a_r| < \frac{1}{2}$

Suppose that there is no $n \leq \varepsilon^{-C_0}$ (C_0 to be spec.) with $\|n^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$.

Then $\sum_{n=1}^{N} \psi(n^2\theta) = 0$. (by (i)).

$$\Rightarrow \sum_{n=1}^{N} \sum_r a_r e^{2\pi i n^2 \theta r} = 0 \Rightarrow \sum_r a_r \sum_{n=1}^{N} e^{2\pi i n^2 \theta r} = 0$$

Note that $a_0 = \int \psi = 1$. Thus $\left| \sum_{r \neq 0} a_r \sum_{n=1}^{N} e^{2\pi i n^2 \theta r} \right| \geq N$.

By triangle-ineq. and (iii), we have $\sum_{\substack{r \neq 0 \\ |r| < \varepsilon^{-C}}} |a_r| \cdot \left| \sum_{n=1}^{N} e^{2\pi i n^2 \theta r} \right| \geq \frac{N}{2}$.

By pigeonhole, $\exists r$, $1 \leq r \leq \varepsilon^{-C}$ such that $\frac{1}{N} \left| \sum_{n=1}^{N} e(r\theta n^2) \right| \gg \varepsilon^{C}$.

$$\left(|a_r| \leq \int \psi = 1 \quad \text{all } r \right)$$

By Weyl's ineq. $\exists q$, $1 \le q \le \varepsilon^{-c'}$ such that $\|qr\theta\|_{\mathbb{R}/\mathbb{Z}} \le \frac{\varepsilon^{-c'}}{N^2}$.

But then $\|q^2 r^2 \theta\|_{\mathbb{R}/\mathbb{Z}} < \frac{\varepsilon^{-c-2c'}}{N^2}$. Taking C_0 sufficiently large gives

Contradiction upon taking $h = qr$.

<u>Remarks</u>: The basic idea, though ~~phys~~ phrased strangely, is to split the set of θ into what Hardy and Littlewood call

- major arcs: $\theta \approx \frac{a}{q}$ with q small. In this case take $h = q^2$.
- minor arcs: $\theta \not\approx \frac{a}{q}$ with q small, show using Weyl that $n^2\theta$ spreads evenly mod 1.

We can use this to prove:

<u>Lemma</u>: Let $P \subseteq \mathbb{Z}$ be an arithmetic progression of length L.

(i) Let $\varphi(x) = \alpha x + \beta$ be a linear phase (i.e. $\alpha, \beta \in \mathbb{R}/\mathbb{Z}$).
Then I can partition P into $O(L^{3/4})$ sub-progressions on which φ varies by at most $O(L^{-1/2})$.

(ii) Let $\varphi(x) = \alpha x^2 + \beta x + \gamma$. Then can partition P into $O(L^{1-c})$ subprogressions on which φ varies by at most $O(L^{-c})$. ($c > 0$ absolute).

WLOG P has common diff 1.

Proof: (i) By pigeonhole principle there is d, $1 \leq d \leq M$ such that $\|\alpha d\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{M}$. If Q is a progression of length M' and ~~and~~ common difference d, then the variation of φ on Q is at most $\frac{M'}{M}$. Take $M = L^{3/4}$, $M' = L^{1/4}$.

The variation of φ is $O(L^{-1/2})$ as claimed. The progressions Q have common difference $d \leq L^{3/4}$ and length $\leq L^{1/4}$, and it is clear that P may be partitioned into $O(L^{3/4})$ of them.

(ii) (Sketch) By the theorem on $\|n^2\theta\|$ I can ~~partition~~ find d, $1 \leq d \leq L^{1/2}$, such that $\|d^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq L^{-c}$.

Consider a progression $Q = \{x + \ell d : \ell = 0, \dots, L'-1\}$. On Q, we have $\varphi(x) = \varphi(x_0 + \ell d) = \alpha d^2 \ell + \beta_{x_0,d} \cdot \ell + \gamma_{x_0,d}$.

If $L' < L^{c/3}$ (say) then the quadratic term $\|\alpha d^2 \ell\|_{\mathbb{R}/\mathbb{Z}}$ varies by at most $L^{-c/3}$ on Q. Subdivide P into progressions Q of this form. Then further subdivide those to make to make the variance of the linear part small. $\square$

Conclusion of the proof of Szemerédi for 4-term APs.

We've shown, if $A \subseteq [N]$, $|A| = \alpha N$, $N > \alpha^{-C}$, A contains no 4-term APs, then the balanced function, f, of A is such that there are quadratics $\psi_0 \cdots \psi_{N'-1}$ and a progression $P \subseteq \mathbb{Z}/N'\mathbb{Z}$, $|P| \geq \exp\left(-\frac{1}{\alpha^c}\right) N^{\alpha^c}$

s.t. $\mathbb{E}_i \left| \mathbb{E}_{x \in P+i} f(x) e(-\psi_i(x)) \right| \gg \alpha^c$; [Recall $N' \sim 10N$].

To conclude, subdivide each $P+i$ into further subprogressions on which ψ_i is roughly constant. In this way we get a subprogression Q s.t. $\left| \mathbb{E}_{x \in Q} f(x) \right| \geq \alpha^c$. Same trick used in Roth allows to remove modulus signs. Further technicality: Q is only a progression $(\text{mod } N')$

Exercise: A progression $(\text{mod } N')$ of length L can be partitioned into $O(\sqrt{L})$ genuine progressions in $[N']$.

After this is done, we have a genuine subprogression $\tilde{Q} \subseteq [N]$ such that $\mathbb{E}_{x \in \tilde{Q}} f(x) \geq \alpha^c \Rightarrow \frac{|A \cap \tilde{Q}|}{|\tilde{Q}|} \geq \alpha + \alpha^c$. $\square$

Next: Sum-product in $\mathbb{F}_p$ and exponential sums / Gauss sums.

$$A \subseteq \mathbb{F}_p, \ |A| \leq K^{-C} p \Rightarrow |A \cdot A| \text{ or } |A+A| \geq K|A|$$

$$|A| \geq K^C.$$

Next semester? Nil-manifolds, nil-sequences?

Arithmetic progressions of primes?

Gromov's theorem on groups with poly. growth.