

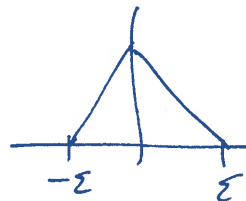
Thm: Suppose $\theta \in \mathbb{R}/\mathbb{Z}$. Then $\exists k \in \mathbb{N}$ such that $\|k^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq N^{-c}$.

Proof: Let $\varepsilon > 0$ and choose a cut-off function $\psi: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ 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 $k \leq \varepsilon^{-c_0}$ (c_0 to be spec.) with $\|k^2\theta\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$.

Then $\sum_{n=1}^N \psi(k^2 n^2 \theta) = 0$ - (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 $\frac{1}{N} \left| \sum_{n=1}^N e^{2\pi i n^2 \theta r} \right| \geq \frac{\varepsilon^c}{2}$.

$$\left(|a_r| \leq \int \psi = 1 \right)$$

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

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

Contradiction upon taking $h=qr$.

Remark: The basic idea, though ~~phrased~~ 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 θ spreads evenly mod 1.

We can use this to prove:

Lemma: 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 $O(L^c)$

sub-progressions 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

$$\|d\|_{R/Z} \leq \frac{1}{M}. \text{ If } Q \text{ is a progression of length } M' \text{ and}$$

~~the~~ common difference d , then the variation of q on Q

$$\text{is at most } \frac{M'}{M}. \text{ Take } M = L^{3/4} \\ M' = L^{1/4}.$$

The variation of q is $O(L^{-1/2})$ ~~is~~ desired. 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 $O(L^{2/4})$ of them.

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

Consider a progression $Q = \{x + ld : l = 0, \dots, L-1\}$. On Q , we

$$\text{have } q(x) = q(x_0 + ld) = \alpha d^2 l + \beta x_0 d l + \gamma x_0 d.$$

If $L^{1/2} \leq L^{1/3}$ (say) then the quadratic term $\|\alpha d^2 l\|_{R/Z}$ varies by at

most $L^{-c/3}$ on Q . Subdivide P into progressions Q of this form.

Then further subdivide those to make the variance of

the linear part small. II

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 $\psi_0, \dots, \psi_{N^c}$ and a progression $P \subseteq \mathbb{Z}/N\mathbb{Z}$, $|P| \geq \exp(-\frac{1}{\alpha^c}) N^{\alpha^c}$

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

To conclude, subdivide each $P+i$ into further subprogressions in which

ψ_i is roughly constant. In this way we get a subprogression Q

s.t. $\left| \mathbb{E}_{x \in Q} f(x) \right| \geq \alpha^c$. Some 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.

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

Next semester? Nil-manifolds, Nil-sequences?
Arithmetic progressions of primes?
Gromov's theorem on groups with poly. growth.