$$\sum_{t} |\hat{c}(t)|^2 \cdot (p-\omega)$$

$$= p \cdot \sum_{\substack{x: \\ c(x)\neq 0}} |c(x)|^2 \cdot \sum_{\substack{x: \\ c(x)\neq 0}} 1^2$$

$$\underset{\uparrow}{\geq} \; p \cdot \Big| \sum_{\substack{x: \\ c(x)\neq 0}} c(x) \Big|^2 \qquad = p \cdot |\hat{c}(0)|^2 .$$

Cauchy-Schwarz

$$\Rightarrow \sum_{t} |\hat{c}(t)|^2 \geq \frac{p}{p-\omega} \cdot |\hat{c}(0)|^2$$

$$\Rightarrow \sum_{t\neq 0} |\hat{c}(t)| \geq \frac{\omega}{p-\omega} \cdot |\hat{c}(0)|^2 .$$

$\square$

<u>Cor 11.4.3</u> Let $d \geq 1$ be sqfree, $c : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$, and assume that for each $p \mid d$, there are $\omega(p)$ residue classes $a \bmod p$ s.t. $c(x) = 0$ whenever $x \equiv a \bmod p$.

Then,
$$\sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} |\hat{c}(t)|^2 \geq \Big(\prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}\Big) \cdot |\hat{c}(0)|^2 .$$

<u>Pf</u> HW (use the Chin. remainder thm). $\square$

Def The Fourier transform of a fct. $f \in L^1(\mathbb{Z})$ $(f : \mathbb{Z} \to \mathbb{C})$ is the function $\hat{f} : \mathbb{R}/\mathbb{Z} \longrightarrow \mathbb{C}$ given by $\hat{f}(t) = \sum_{n \in \mathbb{Z}} f(n) e(nt)$.

Rmk a) If $f \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$, then $\hat{f} \in L^2(\mathbb{R}/\mathbb{Z})$.

b) If $f, g \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$, then

$$\underset{\displaystyle \int_{\mathbb{R}/\mathbb{Z}} f(t)\overline{g(t)}\,dt}{\overset{\shortparallel}{\langle \hat{f}, \hat{g} \rangle}} = \underset{\displaystyle \sum_{n \in \mathbb{Z}} f(n)\overline{g(n)}}{\overset{\shortparallel}{\langle f, g \rangle}}$$

Lemma 11.4.4 (Analytic large sieve inequality)

Let $M \in \mathbb{R}$, $N \geq 1$, $\delta > 0$.

Let $f : \mathbb{Z} \to \mathbb{C}$ with $f(x) = 0$ unless $x \in [M-N, M+N]$.

Let $\alpha_1, \dots, \alpha_k \in \mathbb{R}/\mathbb{Z}$ be <u>δ-separated</u>:

$$\|\alpha_i - \alpha_j\|_{\mathbb{R}/\mathbb{Z}} \geq \delta \quad \forall i \neq j.$$

Then, $$\sum_i |\hat{f}(\alpha_i)|^2 \ll \left(N + \frac{1}{\delta}\right) \cdot \underbrace{\sum_{n \in \mathbb{Z}} |f(n)|^2}_{\left(= \int_{\mathbb{R}/\mathbb{Z}} |\hat{f}(t)|^2 dt\right)}.$$

<u>Note</u> $\frac{LHS}{k}$ looks like an approx. for the Riemann integral $\int_{\mathbb{R}/\mathbb{Z}} |\hat{f}(t)|^2 dt$.

<u>Idea</u> $\hat{f}(\alpha_i) = \langle f, g_i \rangle$ for $g_i : \mathbb{Z} \to \mathbb{C}$, $g_i(n) = e(-\alpha_i n)$.

$$= \langle f, \tilde{g}_i \rangle \text{ for } \tilde{g}_i = g_i \cdot 1_{[M, M+N]}.$$

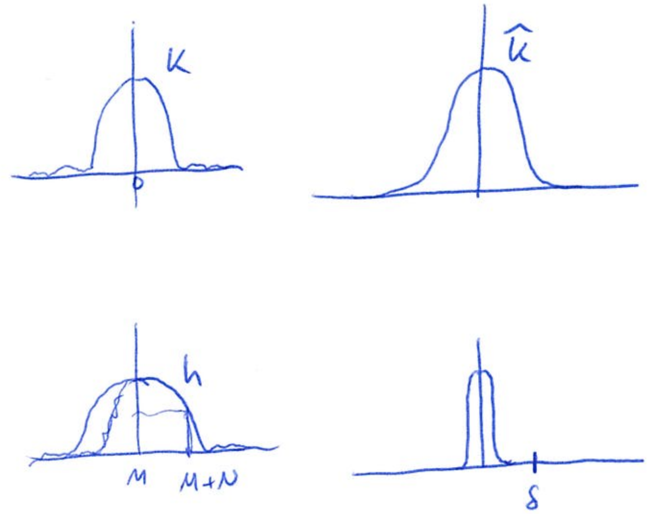
$$\left.\begin{aligned} \langle \tilde{g}_i, \tilde{g}_i \rangle &= \sum_{n \in [M, M+N]} 1 = N+1 \\ \langle \tilde{g}_i, \tilde{g}_j \rangle &= \sum_{n \in [M, N+N]} e((\alpha_i - \alpha_j)n) \approx 0 \text{ for } i \neq j \end{aligned}\right\} \Rightarrow \left(\frac{g_i}{\sqrt{N}}\right)_{i=1,\dots,k} \text{ almost orthonormal}$$

$$\underset{\text{Pythagoras}}{\overset{\approx}{\Rightarrow}} \sum_i |\langle f, \tilde{g}_i \rangle|^2 \lessapprox N \|f\|^2.$$

"$\underset{\sim}{\square}$"

Pf Let g_i as before.

Let $K \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ smooth with



a) $K(x) \geq 0 \quad \forall x \in \mathbb{R}$

b) $\hat{K}(t) \geq 0 \quad \forall t \in \mathbb{R}$

c) $\hat{K}(t) = 0$ if $|t| \geq \frac{1}{2}$.

d) $K(x) \geq 1 \quad \forall x \in (-A, A)$.

$\Rightarrow K(0) = \int \hat{K}(t)\,dt > 0$.

Let $K(x) > 0$ if $0 \leq x \leq A$.

$A > 0$ small enough so

Let $S = \max\left(1, \frac{1}{\delta}, \frac{N}{A}\right)$

and let $h(x) = K\left(\frac{x-M}{S}\right)$. $\Rightarrow$ $h(x) \geq 1 \quad \forall x \in [M-N, M+N]$.

$\Rightarrow \hat{h}(t) = S \cdot \hat{K}(Sx) \cdot e(Mt)$. $\left(\operatorname{supp}(\hat{h}) \subseteq \left(-\frac{1}{2S}, \frac{1}{2S}\right) \subseteq \left(-\frac{\delta}{2}, \frac{\delta}{2}\right)\right)$

Let $\widetilde{g_i} = g_i \cdot h \in L^1(\mathbb{Z}) \cap L^2(\mathbb{Z})$

$$\Rightarrow \langle g_i, g_j \rangle = \sum_{n \in \mathbb{Z}} h(n)^2 \, e((\alpha_i - \alpha_j)n)$$

$$= \sum_{t \in \mathbb{Z}} \widehat{h^2}(t + \alpha_i - \alpha_j)$$

Poisson summation

$$= \sum_{t \in \mathbb{Z}} \underbrace{(\hat{h} * \hat{h})}_{\operatorname{supp}(-) \subseteq \left(-\frac{1}{S}, \frac{1}{S}\right) \subseteq (-\delta, \delta)}(t + \alpha_i - \alpha_j) = \begin{cases} (\hat{h} * \hat{h})(0) = S \cdot (\text{const.}), & i = j, \\ 0, & i \neq j. \end{cases}$$

(because $\|\alpha_i - \alpha_j\|_{\mathbb{R}/\mathbb{Z}} \geq \delta$)

Let $\frac{f}{h}(x) = 0$ if $x \notin [M-N, M+N]$.

$$\Rightarrow \sum_i \left|\left\langle \frac{f}{h}, \tilde{g_i} \right\rangle\right|^2 \ll S \underbrace{\left\|\frac{f}{h}\right\|^2}_{\sum_{n\in\mathbb{Z}} \frac{|f(n)|^2}{|h(n)|^2}} \ll S \sum_{n\in\mathbb{Z}} |f(n)|^2$$

Pythagoras

$$\left\langle \frac{f}{h}, g_i h \right\rangle \underset{\text{h is real-valued}}{=} \langle f, g_i\rangle = \hat{f}(\alpha_i)$$

$$\underbrace{\sum_{n\in\mathbb{Z}} \frac{|f(n)|^2}{|h(n)|^2}}_{n\in[M,M+N]} \ll |f(n)|^2$$

h(x) bounded from below for $M \le x \le M+N$

$$\cancel{\left\langle \frac{f}{h}, \tilde{g_i}\right\rangle = \sum_{n\in\mathbb{Z}} f(n)\,\tilde{g_i}(n)}$$

$$\cancel{= \sum_{n\in[M,M+N]} f(n)\, g_i(n)\, h(n)}$$

$\square$

Thm 11.4.5 (Large sieve)

Let ~~$S \subseteq [M, M+N]$ be a subset,~~ $z \geq 1$, $M \in \mathbb{Z}$, $N \geq 1$.

For each $p \leq z$, ~~assume that there are $\omega(p)$ residue~~

let $E_p \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set of size $\omega(p)$.

Then, the set $S := \{M \leq n \leq M+N : \forall p \leq z : n \bmod p \notin E_p\}$

has size $\#S \ll \dfrac{N + z^2}{J}$,

where
$$J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}.$$

Pf Let $f := 1_S \in L^1(\mathbb{Z})$.

The numbers $\frac{t}{d} \in \mathbb{R}/\mathbb{Z}$

with $d \leq z$ are $\frac{1}{z^2}$-separated (as $\frac{t_1}{d_1} - \frac{t_2}{d_2} = \frac{\cdots}{d_1 d_2}$).

$$\Rightarrow \sum_{d \leq z} \sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} \left|\hat{f}\left(\frac{t}{d}\right)\right|^2 \ll (N + z^2) \cdot \underbrace{\sum_{n \in \mathbb{Z}} |f(n)|^2}_{\#S}. \qquad (\mathrm{I})$$

On the other hand, by Cor 11.4.3, If $g : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$, $x \mapsto \sum_{n \equiv x \bmod d} f(n)$, then $\hat{f}\left(\frac{t}{d}\right) = \hat{g}(t)$.

$$\sum_{t \in (\mathbb{Z}/d\mathbb{Z})^\times} \left|\hat{f}\left(\frac{t}{d}\right)\right|^2 \geq \left(\prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)}\right) \cdot |\underbrace{\hat{f}(0)}_{\sum_{n \in \mathbb{Z}} f(n) = \#S}|^2 \qquad (\mathrm{II})$$

$(\mathrm{I}), (\mathrm{II}) \Rightarrow \#S \ll \dfrac{N + z^2}{J}$.

$\square$

Cor 11.4.6 The number of $n \leq N$ which are a quadratic residue modulo each prime $p \leq z$ is $\ll \frac{N}{z} + z$.

Rmk For $z = N^{1/2}$, we get $\ll N^{1/2}$.

Note: Every square $n \leq N$ is a quadr. res. mod every prime p.

Pf of Cor Let $E_p = \{ x \in \mathbb{Z}/p\mathbb{Z} \text{ quadr. nonres.} \}$.

$$\Rightarrow \omega(p) = \# E_p = \begin{cases} \frac{p-1}{2}, & p > 2, \\ 0, & p = 2. \end{cases}$$

$$\Rightarrow \frac{\omega(p)}{p - \omega(p)} = \begin{cases} \frac{p-1}{p+1}, & p > 2 \\ 0, & p = 2 \end{cases}$$

$$J = \sum_{\substack{d \leq z \\ \text{sqfree}}} \prod_{p \mid d} \frac{\omega(p)}{p - \omega(p)} \asymp z \text{ for example by Wiener-Ikehara.}$$

$$\Rightarrow \# \{ n \leq z \text{ quadr. res. mod each } p \leq z \} \ll \frac{N + z^2}{J} \asymp \frac{N}{z} + z \qquad \square$$