Dann

$$|I_2| = \left|\sum_{a\neq 0} \hat{1}_A(a)^2\, \hat{1}_A(-2a)\right|$$

$$\leq \sum_{a\neq 0} |\hat{1}_A(a)|^2 \cdot \delta^2/2$$

$$\underset{\text{Parseval-Plancherel}}{=} \left(\langle 1_A, 1_A\rangle - |\hat{1}_A(0)|^2\right) \cdot \delta^2/2$$

$$= (\delta - \delta^2)\, \delta^2/2$$

$$\leq \delta^3/2.$$

Also $E = I_1 + I_2 \geq \delta^3 - \delta^3/2 = \delta^3/2.$

<u>Fall 2</u>: Der „strukturierte" Fall

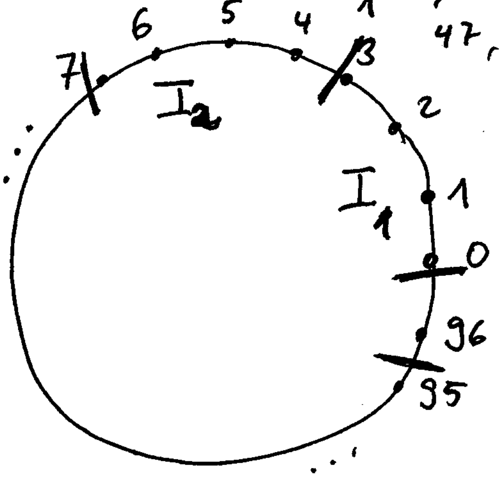
$$\exists\, a \neq 0 : \quad |\hat{1}_A(a)| > \delta^2/2.$$

Sei „o.B.d.A." n eine Primzahl (werden später sehen, warum das kein Problem ist). Partitioniere den Torus in M aufeinanderfolgende Intervalle $I_1, \dots, I_M$ mit Durchmesser so nah wie möglich bei $\delta^2/4$. Setze $P_j = \{x \in \mathbb{Z}/n\mathbb{Z} : e^{2\pi i (-a) x/n} \in I_j\}$.

Bsp. $n = 97$, $a = -2$, $\delta = 0{,}4$, $\delta^2/4 = 0{,}04$

$\lceil 97 \cdot 0{,}04 \rceil = 4$

$P_1 = \{47, 96, 48, 0\}$



P_j ist eine AP mit $r = 48$

Generell ist P_j eine AP mit Schrittweite $-\hat{a}$ (in $\mathbb{Z}/n\mathbb{Z}$)

Definiere f durch $f(x) = 1_A(x) - \delta$. Dann ist $\hat{f}(0) = 0$ und $\hat{f}(a) = \hat{1}_A(a)$ für alle $a \neq 0$.

Also

$$\begin{aligned}
\delta^2/2 < |\hat{f}(a)| &= |\langle f, \chi_{-a} \rangle| \\
&= \left| \frac{1}{n} \sum_x f(x)\, \chi_{-a}(x) \right| \\
&= \left| \frac{1}{n} \sum_{j=1}^{M} \sum_{x \in P_j} f(x)\, \chi_{-a}(x) \right| \\
&\leq \frac{1}{n} \sum_{j=1}^{M} \left| \sum_{x \in P_j} f(x)\, \chi_{-a}(x) \right| .
\end{aligned}$$

Für festes j wähle $x_j \in P_j$. Dann

$$\Big|\sum_{x\in P_j} f(x)\,\chi_{-a}(x)\Big| \le \Big|\sum_{x\in P_j} f(x)\,\chi_{-a}(x_j)\Big| + \Big|\sum_{x\in P_j} f(x)\,(\chi_{-a}(x)-\chi_{-a}(x_j))\Big|$$

$$\le \Big|\sum_{x\in P_j} f(x)\Big| + \underbrace{\sum_{x\in P_j}\frac{\delta^2}{4}}_{\frac{\delta^2}{4}|P_j|}.$$

Über j aufsummiert

$$\frac{\delta^2}{2} < \frac{1}{n}\sum_{j=1}^{M}\Big(\Big|\sum_{x\in P_j} f(x)\Big| + \frac{\delta^2}{4}|P_j|\Big)$$

$$= \frac{\delta^2}{4} + \frac{1}{n}\sum_{j=1}^{M}\Big|\sum_{x\in P_j} f(x)\Big|$$

$$\Longrightarrow \frac{\delta^2}{4} < \frac{1}{n}\sum_{j=1}^{M}\Big|\sum_{x\in P_j} f(x)\Big|.$$

Weil $\sum_x f(x) = 0$ ist, gilt auch

$$\frac{\delta^2}{4} < \frac{1}{n}\sum_{j=1}^{M}\Big(\Big|\sum_{x\in P_j} f(x)\Big| + \sum_{x\in P_j} f(x)\Big).$$

D.h. es gibt ein $j\in[M]$ mit $\sum_{x\in P_j} f(x) \ge \frac{\delta^2}{8}|P_j|$.

Damit

$$|A \cap P_j| = \sum_{x \in P_j} (\delta + f(x)) \geq \delta\left(1 + \frac{\delta}{8}\right) |P_j| .$$

D.h. die Menge A hat in der (langen) AP P_j eine größere Dichte als in $\mathbb{Z}/n\mathbb{Z}$. Jetzt kann man das Argument für die Menge $A \cap P_j$ in P_j wiederholen. In jedem Schritt wird die Dichte der betrachteten Menge um einen Faktor von $\frac{\delta}{8}$ vergrößert. Nach k Schritten, mit $\left(1+\frac{\delta}{8}\right)^k \geq 1$, hat man eine 3-AP sicher gestellt. $\boxtimes$

<u>Problem</u> des „o.B.d.A."s im Beweis: Wenn man induktiv von n auf $|P_j|$ schließt, ist $|P_j|$ i.A. keine Primzahl mehr.

<u>Lösung</u>: Konstruiere die AP mit Hilfe diophantischer Approximation.

<u>Lemma 5</u> (Dirichlet, 1842)
Sei $\alpha \in \mathbb{R}$ und $\varepsilon \in (0,1)$. Dann gibt es $p, q \in \mathbb{Z}$ mit $1 \leq q \leq \frac{1}{\varepsilon}$ und $\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q}$.

<u>Bew.:</u> Sei $M = \lfloor \frac{1}{\varepsilon} \rfloor$. Betrachte die Zahlen

$$\{0\alpha\}, \{1\alpha\}, \{2\alpha\}, \dots, \{M\alpha\},$$

wobei $\{\beta\} = \beta - \lfloor \beta \rfloor$ der fraktionale Teil einer Zahl β ist. Da $0 \le \{i\alpha\} < 1$ ist, gibt es zwei verschiedene Zahlen $i, j \in \mathbb{Z}$ mit $0 \le i, j \le M$ und $\{(i-j)\alpha\} \le \frac{1}{M+1}$.

Definiere $q = i - j$ und $p = \lfloor q\alpha \rfloor$. Dann ist

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{\alpha q}{q} - \frac{\lfloor q\alpha \rfloor}{q} \right| = \left| \frac{\{(i-j)\alpha\}}{q} \right| \le \frac{1}{(M+1)|q|} < \frac{\varepsilon}{|q|}$$

und $|q| \le M \le \frac{1}{\varepsilon}$, wie gewünscht. $\boxtimes$

Nochmal <u>Fall 2</u>: $\exists a \neq 0 : |\hat{1}_A(a)| > \frac{\delta^2}{2}$

Für ein später zu wählendes ε finde p, q mit

$$\left| \frac{a}{n} - \frac{p}{q} \right| < \frac{\varepsilon}{q}$$

nach Lemma 5. Partitioniere $[n]$ in AP mod q. Es gibt q solcher AP mit $\approx \frac{n}{q}$ Elementen. Für ein später zu wählendes M partitioniere jede der AP in M Intervalle. Jedes Intervall enthält $\approx \frac{n}{qM}$ Elemente. Sei I ein solches Intervall. Betrachte ein $x \in I$.

Dann ist

$$e^{\frac{2\pi i(-a)x}{n}} = e^{-2\pi i\left(\frac{p}{q}+\theta\right)x} \quad \text{mit } |\theta| < \frac{\varepsilon}{q}$$

$$= \underbrace{e^{-2\pi i \frac{p}{q}x}}_{\text{konstant auf } I} \cdot \underbrace{e^{-2\pi i \theta x}}_{\text{Variation auf } I:}$$

$$\approx |\theta| \frac{n}{M} \leq \frac{\varepsilon n}{qM}.$$

Wähle ε, M, so dass

$$\frac{\varepsilon n}{qM} = \frac{\delta^2}{4} \quad \text{und} \quad \frac{n}{qM} \approx \sqrt{n}.$$

z.B. $\quad \varepsilon = \frac{1}{\sqrt{n}}, \quad M = \frac{1}{q}\sqrt{n}\,\frac{4}{\delta^2}.$