Lemma 5.3. Wenn $|\alpha - \frac{a}{q}| \leq \frac{1}{q^2}$ wobei $a \in \mathbb{Z}$, $q \in \mathbb{N}$, $ggT(a,q) = 1$,

dann

$$\sum_{h=1}^{H} \min\left(n, \frac{1}{\|h\alpha\|}\right) \leq 3\left(\frac{H}{q}+1\right)(n + 4q\log 2q)$$

für alle $H, n \in \mathbb{N}$.

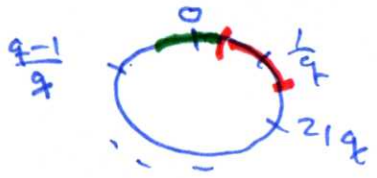
Beweis. Da man $[H]$ mit $\frac{H}{q}+1$ Intervallen der Form $[m, m+q-1]$ überdecken kann, genügt es

$$\sum_{h=m}^{m+q-1} \min\left(n, \frac{1}{\|h\alpha\|}\right) \leq 3(n + 4q\log 2q)$$

für alle $m \in \mathbb{N}$ zu beweisen. Für $u \in \mathbb{R}$ setzen wir

$$N(u) = \{ h \in [m, m+q-1] : \|h\alpha - u\| \leq \tfrac{1}{2q} \}.$$

Dann $[m, m+q-1] = N(0) \cup N(\frac{1}{q}) \cup \dots \cup N(\frac{q-1}{q})$.



Also

$$\sum_{h=m}^{m+q-1} \min\left(n, \frac{1}{\|h\alpha\|}\right) \le |N(0)|\, n + \sum_{j=1}^{q-1} \sum_{h \in N(\frac{j}{q})} \frac{1}{\|h\alpha\|}$$

Wir werden

$$|N(u)| \le 3 \quad \text{für alle } u \in \mathbb{R} \qquad \text{------ (5.2)}$$

$$\frac{1}{\|h\alpha\|} \le \frac{2}{\|\frac{j}{q}\|} \quad \text{für alle } j \in [q-1],\ h \in N(\tfrac{j}{q}) \text{ ... (5.3)}$$

zeigen. Dann folgt

$$\sum_{h=m}^{m+q-1} \min\left(n, \frac{1}{\|h\alpha\|}\right) \le 3n + \sum_{j=1}^{q-1} 3 \cdot \frac{2}{\|\frac{j}{q}\|}$$

$$\le 3n + 12 \sum_{j \le q/2} \frac{q}{j}$$

$$\overset{(5.1)}{\le} 3n + 12\, q \log 2q .$$

Beweis von (5.3) Sei $j \in [q-1]$, $h \in N(\frac{j}{q})$. Nun

$$\|h\alpha - \tfrac{j}{q}\| \le \tfrac{1}{2q} .$$

Wenn $j \leq \frac{q}{2}$ ist $\|h\alpha\| \geq (j - \frac{1}{2})/q \geq \frac{1}{2} j/q$,

also $\frac{1}{\|h\alpha\|} \leq \frac{2q}{j}$.

Wenn $j \geq \frac{q}{2}$ ist $\|h\alpha\| \geq (q-j-\frac{1}{2})/q \geq \frac{q-j}{2}/q$,

also $\frac{1}{\|h\alpha\|} \leq \frac{2q}{q-j} = \frac{2}{\|\frac{j}{q}\|}$.

Beweis von (5.2) Für h mit $0 \leq h \leq q-1$ ist

$$m+h \in N(u) \iff \|(m+h)\alpha - u\| \leq \frac{1}{2q}$$

$$\iff \left\| h \cdot \frac{a}{q} + h\left(\alpha - \frac{a}{q}\right) + (m\alpha - u) \right\| \leq \frac{1}{2q}$$

Wegen $\left|h\left(\alpha - \frac{a}{q}\right)\right| \leq \frac{h}{q^2} < \frac{1}{q}$ impliziert die Dreiecksungl.

$$m+h \in N(u) \implies \left\| h \cdot \frac{a}{q} + (m\alpha - u) \right\| < \frac{3}{2q}$$

$\Longrightarrow \quad h \cdot \frac{a}{q} + \mathbb{Z} \in \left((m\alpha - u) - \frac{3}{2q} , (m\alpha - u) + \frac{3}{2q} \right)$

In diesem Intervall liegen genau drei Zahlen aus $\frac{\mathbb{Z}}{q}$, sagen wir $\frac{r_1}{q}, \frac{r_2}{q}, \frac{r_3}{q}$.

Für $m+h \in N(u)$ gibt's also $z \in \mathbb{Z}$ und $i \in [3]$ mit

$$h \cdot \frac{a}{q} + z = \frac{r_i}{q} ,$$

d.h. $$ha + qz = r_i .$$

Da $h \cdot a \equiv r_i \pmod{q}$ sein muss und $ggT(a,q) = 1$ folgt $|N(u)| \leq 3$. □

Sei $P : \mathbb{R} \longrightarrow \mathbb{R}$ eine Funktion.

Für $h \in \mathbb{R}$ schreiben wir P_h für die Funktion

$$P_h(x) = P(x+h) - P(x) .$$

Dies setzen wir rekursiv fort durch

$$P_{h_1,h_2}(x) = P_{h_1}(x+h_2) - P_{h_1}(x)$$

$$= P(x+h_1+h_2) - P(x+h_1) - P(x+h_2) + P(x),$$

...

Ist $P = \alpha x^k + \dots$ ein Polynom vom Grad k, so ist

$$P_{h_1}(x) = \alpha\left((x+h_1)^k - x^k\right) + \dots$$

$$= k\alpha h_1 x^{k-1} + \dots,$$

also auch

$$P_{h_1h_2}(x) = k(k-1)\alpha h_1 h_2 x^{k-2} + \dots$$

$$\vdots$$

$$P_{h_1,\dots,h_{k-1}}(x) = k!\,\alpha h_1 \cdot \dots \cdot h_{k-1} x + \dots$$

Satz 5.14 (Weyl) Ist $P : \mathbb{R} \longrightarrow \mathbb{R}$ eine Funktion, $k \in \mathbb{N}$, $n \in \mathbb{N}$ und

$$S = \sum_{m=1}^{n} e(P(m)),$$

so gilt

$$|S|^{2^k} \leq (2n)^{2^k-1} + 2^k (2n)^{2^k-k-1} \sum_{h_1+\dots+h_k \leq n} \left| \sum_{m=1}^{n-(h_1+\dots+h_k)} e(P_{h_1\dots h_k}(m)) \right|$$

Beweis. Induktion nach k

$k=1$ Hier ist

$$|S|^2 = \sum_{m=1}^{n} e(P(m)) \cdot \sum_{m'=1}^{n} e(-P(m'))$$

$$\leq n + 2 \left| \sum_{1 \leq m < m' \leq n} e(P(m') - P(m)) \right| \qquad \boxed{m' = m+h}$$

$$\leq n + 2 \sum_{h=1}^{n-1} \left| \sum_{m=1}^{n-h} e(\underbrace{P(m+h) - P(h)}_{= P_h(m)}) \right|.$$

Induktionsschritt $k \to k+1$ | Wir wenden die Ungleichung

$$(y_0 + \dots + y_{n-1})^2 \le n\,(y_0^2 + \dots + y_{n-1}^2)$$

mit

$$y_0 = (2n)^{2^k} - 1$$

$$y_h = 2^k (2n)^{2^k - k - 1} \sum_{h_2 + \dots + h_k < n-h} \left| \sum_{m=1}^{n-h-(h_2+\dots+h_k)} e(P_{h h_2 \dots h_k}(m)) \right|$$

an. Dies liefert

$$|S|^{2^{k+1}} \le n\,(y_0^2 + \dots + y_{n-1}^2).$$

Dabei

$$n y_0^2 = n \cdot (2n)^{2^{k+1} - 2} = \frac{1}{2} (2n)^{2^{k+1}} - 1$$

und für $1 \le h_1 \le n-1$ ist

$$n y_{h_1}^2 = 2^{2k} (2n)^{2^{k+1} - 2k - 2} n \left(\sum_{h_2 + \dots + h_k < n - h_1} | \dots | \right)^2.$$

Da es nur $\leq n^{k-1}$ Möglichkeiten für $(h_2, \dots, h_{k-1})$ gibt folgt

$$n y_{h_1}^2 \leq 2^{2k} (2n)^{2^{k+1}-2k-2} n^{k-1} \cdot n \sum_{h_2+\dots+h_k<n-h_1} \left| \dots \right|^2$$

$$= 2^k (2n)^{2^{k+1}-k-2} \sum_{h_2+\dots+h_k<n-h_1} \left| \sum_{m=1}^{n-(h_1+\dots+h_k)} e(P_{h_1\dots h_k}(m)) \right|^2$$

$$\leq 2^k (2n)^{2^{k+1}-k-2} \sum_{h_2+\dots+h_k<n-h_1} \left(n + 2 \sum_{h_{k+1}=1}^{n-1-(h_1+\dots+h_k)} \left| \sum_{m=1} e(P_{h_1\dots h_{k+1}}(m)) \right| \right)$$

$$\leq 2^k (2n)^{2^{k+1}-k-2} \cdot n^k$$

$$+ 2^{k+1} (2n)^{2^{k+1}-k-2} \sum_{h_2+\dots+h_{k+1}<n} \left| \sum_{m=1}^{n-(h_1+\dots+h_{k+1})} e(P_{h_1\dots h_{k+1}}(m)) \right|$$

Insgesamt

$$|S|^{2^{k+1}} \leq \frac{1}{2}(2n)^{2^{k+1}-1} + \frac{1}{2}(2n)^{2^{k+1}-1} + 2^{k+1}(2n)^{2^{k+1}-k-2} \sum_{h_1+\dots+h_{k+1}<n} \left| \sum_{m=1}^{n-(h_1+\dots+h_{k+1})} e(P_{h_1\cdots h_{k+1}}(m)) \right|$$

□

Folgerung 5.5. Es sei $P = \alpha x^k + \dots$ ein Polynom vom Grad k, $n \in \mathbb{N}$ und

$$S = \sum_{m=1}^{n} e(P(m)).$$

Dann

$$|S|^{2^{k-1}} \leq (2n)^{2^{k-1}-1} + 2^{k-1}(2n)^{2^{k-1}-k} \sum_{h_1+\dots+h_{k-1}<n} \min\left(\frac{1}{\|k!\, h_1 \cdots h_{k-1} \alpha\|}, n\right)$$

□

Definition 5.6. Für $k \geq 1$ und $n \in \mathbb{N}$ setze

$$\tau_k(n) = \left| \{(d_1, \dots, d_k) \in \mathbb{N}^k : d_1 \cdot \dots \cdot d_k = n\} \right|.$$

Lemma 5.7. Für alle $k \geq 1$ und $\varepsilon > 0$ ist $\tau_k(n) = O(n^\varepsilon)$.

Beweis Ist $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ die Primfaktorzerlegung von n

so gilt

$$\tau_k(n) = \prod_{i=1}^{r} \binom{\alpha_i + k - 1}{k-1},$$

dann für jede Zahl $\alpha \in \mathbb{N}_0$ gibt's $\binom{\alpha+k-1}{k-1}$ additive Zerlegungen

$\alpha = m_1 + \ldots + m_k$ mit $m_1, \ldots, m_k \in \mathbb{N}_0$.

Für jede Primzahl p existiert

$$C_p = \sup \left\{ \binom{\alpha+k-1}{k-1} p^{-\alpha\varepsilon} : \alpha \in \mathbb{N}_0 \right\} \geq 1$$

Außerdem $\dfrac{\tau_k(n)}{n^\varepsilon} \leq C_{p_1} \cdot \ldots \cdot C_{p_r}$.

Es reicht daher zu zeigen, dass nur endlich viele Primzahlen p mit $C_p > 1$ existieren. Dies ist klar. □

Satz 5.8 (Weyl-Ungleichung) Es sei $P = \alpha x^k + \dots$

ein Polynom vom Grad k,

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2}, \quad \text{wobei} \quad ggT(a,q) = 1$$

und $\varepsilon > 0$. Dann

$$\left| \sum_{m=1}^{n} e(P(m)) \right| \leq O\left(n^{1+\varepsilon} \left(\frac{1}{n} + \frac{1}{q} + \frac{q}{n^k} \right)^{1/2^{k-1}} \right).$$

Beweis. Setze $S = \sum_{m=1}^{n} e(P(m))$, $K = 2^{k-1}$.

Wenn $q \geq n^k$ ist die Beh. schlechter als die triviale Schranke

$|S| \leq n$. Sei also $q < n^k$.

Nach Folg. 5.5 ist

$$|S|^K \leq O\left(n^{K-1} + n^{K-k} \sum_{h=1}^{k! n^{k-1}} \tau_k(h) \min\left(\frac{1}{\|h\alpha\|}, n \right) \right)$$

$$\leq O\left(n^{K-1} + n^{K-k+\varepsilon} \sum_{h=1}^{k! n^{k-1}} \min\left(\frac{1}{\|h\alpha\|}, n \right) \right)$$

Nach Lemma 5.3 ist dabei

$$\sum_{h=1}^{k!\,n^{k-1}} \min\left(\frac{1}{\|h\alpha\|}, n\right) \leq O\left(\left(\frac{n^{k-1}}{q}+1\right)(n+q\log 2q)\right)$$

$$= O\left(\frac{n^k}{q} + n^{k-1+\varepsilon} + n + q\cdot n^{\varepsilon}\right)$$

$$= n^{k+\varepsilon} O\left(\frac{1}{q} + \frac{1}{n} + \frac{q}{n^k}\right),$$

denn da $q \leq n^k$ ist $\log q \leq n^{\varepsilon}$.

Somit $|S|^k \leq O\left(n^{k-1} + n^{k+2\varepsilon}\left(\frac{1}{q}+\frac{1}{n}+\frac{q}{n^k}\right)\right)$

$$= O\left(n^{k+2\varepsilon}\left(\frac{1}{q}+\frac{1}{n}+\frac{q}{n^k}\right)\right),$$

d.h. $|S| \leq O\left(n^{1+\varepsilon}\left(\frac{1}{q}+\frac{1}{n}+\frac{q}{n^k}\right)^{1/k}\right)$.