Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a18: Das große Sieb

Stichworte: Das große Sieb (nach Montgomery), große-Sieb-Ungleichung

18.1. Einleitung: Wir zeigen den Satz vom großen Sieb, manchmal Montgomerys Sieb genannt. Alle Siebanwendungen dieser Vorlesung benutzen dieses Sieb, bzw. die große-Sieb-Ungleichung, die man zum Beweis des großen Siebes benötigt.

18.2. Satz vom großen Sieb: Sei $\mathcal{A} = (a_n)_{n \le N}$ eine Folge in $\mathbb{C}$, $w(p)$ die Anzahl der Streichungsresthklassen mod p, d.h. $w(p) := \#\{h(p);\ n \equiv h(p) \Rightarrow a_n = 0\}$, und sei $w(p) < p$ für alle $p \in \mathbb{P}$. Setze $g_w(q) := \mu^2(q) \prod_{\substack{p \mid q \\ p \in \mathbb{P}}} \frac{w(p)}{p - w(p)}$ und $L_w := \sum_{q \le Q} g_w(q)$ für $Q \ge 1$ beliebig. Dann ist

$$\Big|\sum_{n \le N} a_n\Big|^2 \le \frac{N + Q^2}{L_w} \sum_{n \le N} |a_n|^2.$$

Der Beweis des großen Siebs benötigt Exponentialsummen-Methoden.
Weiter zeigen wir den Satz nur mit "$\ll$" statt "$\le$" (ausreichend für alle hier vorgestellten Anwendungen).
Benötigt wird:

18.3. Die Große-Sieb-Ungleichung: Sei $(a_n)_{n \in \mathbb{N}} \subseteq \mathbb{C}$, $N, Q \ge 1$. Dann ist

$$\sum_{q \le Q} \sum_{\substack{a \bmod q \\ (a,q)=1}} \Big|\sum_{n \le N} a_n e\left(\frac{an}{q}\right)\Big|^2 \ll (N + Q^2) \sum_{n \le N} |a_n|^2.$$

Beweis:

Sei $F: [0,1] \to \mathbb{C}$ stetig diff'bar, auf $\mathbb{R}$ mit Periode 1 fortgesetzt.
(Bei uns: Setze $F(\alpha) := \left(\sum_{n \le x} a_n e(\alpha n)\right)^2$, wo $\alpha \in \mathbb{R}$.) Sei $z \in \mathbb{N}$.
Betr. $q \le z$, $q \in \mathbb{N}$, $1 \le a \le q$, $(a,q) = 1$, $\alpha \in [0,1]$. Dann:

$$\int_{a/q}^{\alpha} F'(t)\,dt = F(\alpha) - F\left(\frac{a}{q}\right) \Rightarrow \left|F\left(\frac{a}{q}\right)\right| \le |F(\alpha)| + \int_{a/q}^{\alpha} |F'(t)|\,dt. \quad (*)$$

Für $\delta > 0$ betr. $I(\frac{a}{q}) := [\frac{a}{q} - \delta, \frac{a}{q} + \delta] \subseteq [0,1]$.

$(*) \Rightarrow \quad 2\delta |F(\frac{a}{q})| \leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + \int_{I(\frac{a}{q})} \int_{a/q}^{\alpha} |F'(t)| dt \, d\alpha$

Mit $\alpha \in I(\frac{a}{q})$, $t \in [\frac{a}{q}, \alpha]$ folgt $t \in I(\frac{a}{q})$, also ist dies

$$\leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + \int_{I(\frac{a}{q})} \int_{I(\frac{a}{q})} |F'(t)| dt \, d\alpha,$$

also $\quad 2\delta |F(\frac{a}{q})| \leq \int_{I(\frac{a}{q})} |F(\alpha)| d\alpha + 2\delta \int_{I(\frac{a}{q})} |F'(\alpha)| d\alpha, \qquad \boxtimes$

wähle nun $\delta := \frac{1}{2z^2}$, so dass die Intervalle $I(a/q)$ für $q \leq z$ nicht überlappen (mod 1).

⌈Wäre sonst $x \in I(\frac{a}{q}) \cap I(\frac{a'}{q'})$ mit $\frac{a}{q} \neq \frac{a'}{q'}$, folgte $|\frac{a}{q} - \frac{a'}{q'}| \leq |\frac{a}{q} - x| + |x - \frac{a'}{q'}| < 2\delta = \frac{1}{z^2}$ $\oplus$

haben aber $|\frac{a}{q} - \frac{a'}{q'}| = \frac{|aq' - a'q|}{qq'} \neq 0$, also $\geq \frac{1}{qq'} \geq z^2$ im ↯ zu $\oplus$.⌋

Summation von $\boxtimes$ über alle IVe zeigt: $\frac{1}{z^2} \sum_{q \leq z} \sum_{\substack{a (q) \\ (a,q)=1}} |F(\frac{a}{q})| \leq \int_0^1 |F(\alpha)| d\alpha + \frac{1}{z^2} \int_0^1 |F'(\alpha)| d\alpha.$

Jetzt: $F(\alpha) = S(\alpha)^2$ mit $S(\alpha) = \sum_{n \leq x} a_n e(\alpha n)$, und $F'(\alpha) = 2 S(\alpha) S'(\alpha)$

zeigt $\sum_{q \leq z} \sum_{a(q), (a,q)=1} |S(\frac{a}{q})|^2 \leq z^2 \int_0^1 |S(\alpha)|^2 d\alpha + 2 \int_0^1 |S(\alpha) S'(\alpha)| d\alpha.$

Mit der Parsevalschen Gleichung $\int_0^1 |\sum_{n \leq x} a_n e(\alpha n)|^2 d\alpha = \sum_{n \leq x} |a_n|^2$

folgt nun $\int_0^1 |S(\alpha)|^2 d\alpha = \sum_{n \leq x} |a_n|^2$,

und haben $\int_0^1 |S(\alpha) S'(\alpha)| d\alpha \overset{C-S}{\leq} \left(\int_0^1 |S(\alpha)|^2 d\alpha\right)^{\frac{1}{2}} \left(\int_0^1 |S'(\alpha)|^2 d\alpha\right)^{\frac{1}{2}}$

$$\leq \left(\sum_{n \leq x} |a_n|^2\right)^{1/2} \cdot \left(\sum_{n \leq x} 4\pi^2 n^2 |a_n|^2\right)^{1/2} \leq 2\pi x \sum_{n \leq x} |a_n|^2.$$

Es folgt

$$\sum_{q \leq z} \sum_{a(q), (a,q)=1} |S(\frac{a}{q})|^2 \ll (z^2 + x) \sum_{n \leq x} |a_n|^2.$$ Jetzt: $Q = z$, $x = N$. $\square$

18.4. Bew. von Satz 18.2 (mit $\ll$ statt $\le$):

Sei $S(\alpha) = \sum_{n\le N} a_n e(\alpha n)$. Setze $Z(p,h) = \sum_{\substack{n\equiv h(p)\\ n\le N}} a_n$, $Z = \sum_{n\le N} a_n = S(0)$.

Dann ist für $p\in\mathcal{P}$:

$$\sum_{a=1}^{p} |S(\tfrac{a}{p})|^2 = \sum_{a=1}^{p}\sum_{n,m\le N} a_n\bar{a}_m e(\tfrac{a}{p}(n-m)) = p\sum_{\substack{n,m\le N\\ n\equiv m(p)}} a_n\bar{a}_m = p\sum_{h=1}^{p}|Z(p,h)|^2.$$

Die Subtraktion von $|S(0)|^2 = |Z|^2$ zeigt

$$\sum_{a=1}^{p-1}|S(\tfrac{a}{p})|^2 = p\sum_{h=1}^{p}|Z(p,h)|^2 - |Z|^2. \qquad (\times)$$

Für eine Streichungsrestklasse ist $Z(p,h)=0$, es folgt mit der Cauchy-Schwarz-Unglg.

$$|Z|^2 = \Big|\sum_{\substack{h\le p\\ Z(p,h)\neq 0}} Z(p,h)\Big| \underset{C\text{-}S}{\le} \Big(\sum_{\substack{h\le p\\ Z(p,h)\neq 0}} 1\Big)\cdot\Big(\sum_{h\le p}|Z(p,h)|^2\Big) = (p-w(p))\sum_{h\le p}|Z(p,h)|^2.$$

In $(\times)$ einsetzen: $\sum_{a=1}^{p-1}|S(\frac{a}{p})|^2 \ge \left(\frac{p}{p-w(p)}-1\right)|Z|^2 = \frac{w(p)}{p-w(p)}|S(0)|^2$.

Damit ist die Unglg. $\sum_{\substack{a\le p\\ (a,p)=1}} |S(\frac{a}{p})|^2 \ge \underbrace{\frac{w(p)}{p-w(p)}}_{=g_w(p)}\Big|\sum_{n\le N} a_n\Big|^2$ gezeigt.

Wegen dem Faktor $\mu^2(q)$ in $g_w(q)$ brauchen nur quadratfreie $q\le Q$ betrachtet werden.

Angenommen, für q und $\tilde{q}\le Q$, wo $(q,\tilde{q})=1$, sei $\sum_{\substack{a(q)\\ (a,q)=1}} |S(\frac{a}{q})|^2 \ge |S(0)|^2 g_w(q)$ $\oplus$ schon gezeigt.

Es folgt $\sum_{\substack{c\le q\tilde{q}\\ (c,q\tilde{q})=1}} |S(\frac{c}{q\tilde{q}})|^2 = \sum_{\substack{a\le q\\ (a,q)=1}}\sum_{\substack{b\le\tilde{q}\\ (b,\tilde{q})=1}} \underbrace{|S(\frac{a}{q}+\frac{b}{\tilde{q}})|^2}_{=\sum_n \underbrace{a_n e(n\frac{a}{q})}_{\text{neue } \tilde{a}_n}\cdot e(n\frac{b}{\tilde{q}}) = \tilde{S}(\frac{b}{\tilde{q}})} \ge g_w(\tilde{q})\sum_{\substack{a\le q\\ (a,q)=1}}|S(\frac{a}{q})|^2 \ge g_w(q\tilde{q})\cdot|S(0)|^2,$

$(q,\tilde{q})=1$ $\qquad$ g_w mult.

also folgt $\oplus$ für alle quadratfreien $q\le Q$.

Dies zeigt $\sum_{q\le Q}|S(0)|^2\cdot g_w(q) \le \sum_{q\le Q}\sum_{\substack{a(q)\\ (a,q)=1}}|S(\frac{a}{q})|^2$.

Mit der großen Sieb-Unglg. 18.3 für $q\le Q$ folgt nun die Beh. durch Auflösen nach $|S(0)|^2 = |\sum_{n\le N} a_n|^2$. $\square$