Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a22: Kreismethode und Goldbachproblem

Stichworte: Goldbachsche Vermutung, Waring-Problem, Heuristik Kreismethode, major und minor arcs im ternären Goldbach Problem, Satz von Vinogradov, singuläre Reihe

---

22.1. Einleitung:

Additive Zahlentheorie-Probleme: Für Teilmengen $\mathcal{A}_1, \dots, \mathcal{A}_k \subseteq \mathbb{N}$ sei die Summenmenge $\mathcal{A}_1 + \dots + \mathcal{A}_k := \{ n \in \mathbb{N} ; \exists\, a_i \in \mathcal{A}_i, 1 \le i \le k : n = a_1 + \dots + a_k \}$.

- Von einem direkten additiven Problem spricht man, wenn man etwa $\mathcal{A} = \mathcal{A}_1 + \dots + \mathcal{A}_k$ beweisen möchte für eine bestimmte feste Teilmenge $\mathcal{A} \subseteq \mathbb{N}$.
- Von einem inversen additiven Problem spricht man, wenn man aus $\#\mathcal{A}$ und anderen Eigenschaften von $\mathcal{A}$ auf $\mathcal{A}_i$ mit $\mathcal{A} = \mathcal{A}_1 + \dots + \mathcal{A}_k$ schließen möchte.

Wir möchten in diesem Kapitel nur direkte additive Probleme besprechen. Darunter fällt insb. die Goldbach-Vermutung und das Waring-Problem.

22.2. Die Goldbach-Vermutung: Aus dem Briefwechsel von 1742 zwischen Euler und Goldbach:

(1) $n \in \mathbb{N}_{>1} \Rightarrow \exists\, p_1, p_2 \in \mathbb{P} : 2n = p_1 + p_2$? (binäres Problem, ungelöst)

(2) $n \in \mathbb{N}_{>2} \Rightarrow \exists\, p_1, p_2, p_3 \in \mathbb{P} : 2n + 1 = p_1 + p_2 + p_3$? (ternäres Problem, gelöst von [Vinogradov 1937] für alle $n > n_0$, arXiv-Beweis: [H. Helfgott, 2013].

Das Waring-Problem: E. Waring behauptete 1770 ohne Beweisangabe, dass jede nat. Zahl die Summe von 4 Quadraten, 9 Kuben, 19 4-ten Potenzen usw. sei.

Formal: $\forall k \ge 2\ \exists\, g(k) \in \mathbb{N}\ \forall n \in \mathbb{N} : \exists\, a_1, \dots, a_\ell \in \mathbb{N} : n = a_1^k + \dots + a_\ell^k,\ 1 \le \ell \le g(k)$.

- Für $k = 2$ liefert der Satz von Lagrange den Wert $g(2) = 4$.
- [Wieferich & Kempner 1910]: $g(3) = 9$, was optimal ist, da 23, 239 nicht als Summe von ≤ 8 Kuben geschrieben werden können.
- [Hilbert 1909]: $g(k) < \infty$ bewiesen

• Um 1919 entwickelten Hardy/Littlewood/Ramanujan die Kreismethode, die zunächst zur Lösung des Waring-Problems diente, aber tatsächlich auch das Goldbach-Problem und allgemeiner bel. direkte additive Probleme behandeln kann und bis heute verwendet wird.

Beispielsweise wird die quantitative Version der PZ-Zwillings-Vermutung in 17.9 mit der Kreismethode ermittelt. Das ternäre Goldbachproblem haben Hardy & Littlewood so bereits unter Ann. der (GRH) für alle $n \geq n_0$ (zur Behandlung der minor arcs) gelöst.

22.3. Heuristik Kreismethode: Betr. die Anzahl Darstellungen, n als Summe von El. aus $\mathcal{A}_1, \dots, \mathcal{A}_k$ zu schreiben:

$$R(n) := \sum_{\substack{a_i \in \mathcal{A}_i \\ n = a_1 + \dots + a_k}} 1 = \#\{(a_1, \dots, a_k) \in \mathcal{A}_1 \times \dots \times \mathcal{A}_k;\ n = a_1 + \dots + a_k\}.$$

Ziel: z.z. $R(n) \overset{!}{>} 0$ oder $R(n) \overset{!}{\gg} 1$ oder noch besser, wenigstens für alle hinr. großen $n \geq n_0$ oder ∞ viele n.

Die Grundidee ist, eine Fourieranalyse durchzuführen: man gehe über zur komplexen Exponentialsumme $T_i(\alpha) = \sum_{\substack{m \in \mathcal{A}_i \\ m \leq x}} e(\alpha m)$, wo $e(\alpha) = e^{2\pi i \alpha}$, $x \geq n$ oder $x = n$, dann schreibe $R(n)$ als komplexes $\int$, denn $R(n) = \int_0^1 T_1(\alpha) \cdots T_k(\alpha)\, e(-n\alpha)\, d\alpha$.

$$\text{r.S.} = \sum_{m_i \in \mathcal{A}_i} \underbrace{\int_0^1 e(\alpha(m_1 + m_2 + \dots + m_k - n))\, d\alpha}_{\overset{\text{Orthogonalitätsrelation}}{=} \begin{cases} 1, & m_1 + m_2 + \dots + m_k - n = 0, \\ 0, & \text{sonst} \end{cases}} = R(n). \quad \text{J}$$

Vgl. Ü Blatt 5 A3(a)

Die Kreismethode beruht nun auf der Beobachtung, dass der Wert des $\int_0^1$ vor allem durch den Wert auf bestimmten Teilintervallen von $[0,1]$ gegeben ist. Man nennt diese maßgeblichen Teilintervalle die "major arcs" und die Restintervalle die "minor arcs" (ursprünglich "arc" als Bogen (wegen $e(\alpha) = e^{2\pi i \alpha}$ auf Einheitskreis $|z| = 1$) interpretiert). Die genaue Wahl dieser arcs hängt aber vom konkreten Problem ab.

22.4. <u>Mehr quantitative Heuristik:</u>

Betr. nun mit $T_1(\alpha)\cdots T_n(\alpha) =: T(\alpha)$ eine einzige Exponentialsumme $T(\alpha) = \sum_{m\le x} c_m e(\alpha m)$.

Dann ist $c_N = \int_0^1 T(\alpha) e(-N\alpha)\,d\alpha \underset{\text{Riemann}\Sigma}{=} \lim_{q\to\infty} \frac{1}{q}\sum_{a\le q} T(\frac{a}{q}) e(-N\frac{a}{q})$. ⊛.

- Integrand bei $\alpha = \frac{a}{q} \in \mathbb{Q}$: $T(\frac{a}{q}) e(-N\frac{a}{q}) = \sum_m c_m e(\frac{a}{q}(m-N))$

$$= \sum_{m\equiv N(q)} c_m \cdot 1 + \sum_{m\equiv N+1(q)} c_m e(\tfrac{a}{q}) + \sum_{m\equiv N+2(q)} c_m e(2\tfrac{a}{q}) + \dots + \sum_{m\equiv N+q-1(q)} c_m e((q-1)\tfrac{a}{q})$$

alle q-ten Einheitswurzeln

Als Bsp., im einfachen Fall, wenn alle $c_m = 1$, sind alle $\sum_{m\equiv N+j(q)} c_m \approx \frac{x}{q}$ etwa gleich, und stellen "Ausschläge" bzw. "Peaks" des Integranden dar.
(Im Prinzip könnten sich diese aber auch wieder wegheben.)

- Integrand nahe $\frac{a}{q}$, d.h. bei $\alpha = \frac{a}{q} + \beta$ mit $|\beta| > 0$ klein:

$$T(\tfrac{a}{q}+\beta) e(-N(\tfrac{a}{q}+\beta)) = \sum_m c_m e(\tfrac{a}{q}(m-N)) \cdot \underbrace{e(\beta(m-N))}_{\approx 1 \text{ für } \beta\approx 0}$$ ← "Peaks" ungefähr wie bei a/q

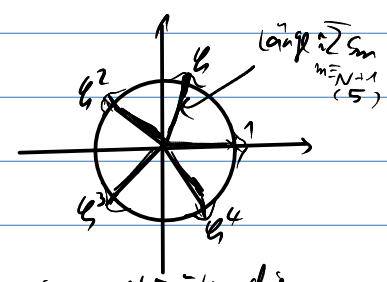
22.5. <u>Bsp.:</u> $\frac{a}{q} = \frac{1}{5}$: $T(\frac{1}{5}) e(-N\cdot\frac{1}{5}) = \sum_{m\equiv N(5)} c_m + \sum_{m\equiv N+1(5)} c_m \zeta + \dots + \sum_{m\equiv N+4(5)} c_m \zeta^4$

$\zeta = e(\frac{1}{5})$ die 5-te EW

Wir erhalten Frequenzbilder $f(\beta) = T(\frac{a}{q}+\beta) e(-N(\frac{a}{q}+\beta))$ für β klein, d.h. Ausschläge nahe $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ als "Zerlegung in Frequenzen":

Die Summe der Ausschläge bzw. Überlagerung liefert in etwa den Wert von $T(\alpha) e(-N\alpha)$.

⌈Aus ⊛ folgt: $\underbrace{\frac{1}{Q}\sum_{q\le Q}}_{\text{Mittelwert von ⊛}} \underbrace{\frac{1}{q}\sum_{a\le q} T(\frac{a}{q}) e(-N\frac{a}{q})}_{\text{Überlagerungen für alle } q\le Q,\ a\le q} \xrightarrow{Q\to\infty} c_N$. ⌋



(summiert über diese Vektoren)

↳ zusammen mit Überlagerung der Bilder bei $q=2$, $q=3$, $q=4$, ...

22.6. **Kreismethode im ternären Goldbach-Problem:**
Für $\alpha \in \mathbb{R}$ sei $S(\alpha) := \sum_{p \le n} \log(p)\, e(\alpha p)$ und $R(n) := \sum_{p_1+p_2+p_3=n} \log(p_1)\log(p_2)\log(p_3)$.

Die zusätzliche Gewichtung mit $\log(p)$ macht die Behandlung der PZsummen technisch einfacher; vergleichbar mit $\pi \to \vartheta$ beim PZS. Haben: $R(n) = \int_0^1 S^3(\alpha) e(-n\alpha)\, d\alpha$.

- Wahl der major arcs $\mathfrak{M} \subseteq [0,1]$: Sei $B > 0$, $Q := \log^B(n)$. Für $1 \le q \le Q$, $0 \le a \le q$ mit $(a,q) = 1$ def. den major arc $\mathfrak{M}(a,q) := [\frac{a}{q} - \frac{Q}{n}, \frac{a}{q} + \frac{Q}{n}] \cap [0,1]$.
und $\mathfrak{M} := \bigcup_{q \le Q} \bigcup_{\substack{0 \le a \le q \\ (a,q)=1}} \mathfrak{M}(a,q) \subseteq [0,1]$.

Bel.: Die major arcs sind p.w. disjunkt für große n. $\ulcorner \alpha \in \mathfrak{M}(a,q) \cap \mathfrak{M}(a',q')$, wo $\frac{a}{q} \ne \frac{a'}{q'}$
$\Rightarrow \frac{1}{Q^2} \le \frac{1}{qq'} \le \frac{|aq'-a'q|}{qq'} = |\frac{a}{q} - \frac{a'}{q'}| \le |\frac{a}{q} - \alpha| + |\alpha - \frac{a'}{q'}| \le 2\frac{Q}{n} \Rightarrow n \le 2Q^3 = 2(\log(n))^{3B}$,
was für alle hinr. großen n nicht stimmt.)

- Wahl der minor arcs als $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.
- Aufspaltung: $R(n) = \int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} S^3(\alpha) e(-n\alpha)\, d\alpha$.

$\rightsquigarrow$ ergibt Asymptotik, erwarten Hauptterm in $\int_{\mathfrak{M}}$, $\int_{\mathfrak{m}}$ trägt zum Fehlerterm bei (obwohl Maß von $\mathfrak{M}$ gegen 0 geht bei $n \to \infty$)

22.7. **Major arcs im ternären Goldbachproblem:** Hier (wie meist) ist die Auswertung von $\int_{\mathfrak{M}}$ eine direkte Rechnung. Im wesentlichen muss $S(\frac{a}{q})$ berechnet werden:

$$S(\tfrac{a}{q}) = \sum_{\substack{r \le q \\ (r,q)=1}} \sum_{\substack{p \le n \\ p \equiv r (q)}} \log(p)\, \underbrace{e(\tfrac{a}{q}p)}_{= e(\frac{a}{q}r)} + \underbrace{O(\log(q))}_{\text{für die } r \text{ mit } (r,q)>1} = \sum_{\substack{r \le q \\ (r,q)=1}} e(\tfrac{ar}{q}) \cdot \sum_{\substack{p \le n \\ p \equiv r (q)}} \log(p) + O(\log(q))$$

Für die PZsumme wird jetzt der Satz von Siegel-Walfisz 11.6 eingesetzt. Nach diesem ist die PZsumme $\approx \frac{n}{\varphi(q)}$.
Die zahlentheoretische Funktion $c_q(a) := \sum_{\substack{r \le q \\ (r,q)=1}} e(\frac{ar}{q})$ heißt Ramanujan-Summe.
Für sie ist $c_q(a) = \mu(q)$ für $(a,q)=1$

Also ist $S(\frac{a}{q}) = \frac{\mu(q)}{\varphi(q)} n + \text{Fehlerterm}$.

Um $S(\frac{a}{q}+\beta)$ auszuwerten, ist jetzt noch eine partielle Summation erforderlich; sie zeigt, dass $S(\frac{a}{q}+\beta) = \frac{\mu(q)}{\varphi(q)} \sum_{m\le n} e(\beta m)$ + Fehlerterm ist.

Insg. folgt so:

Satz: Für $A>0$ ex. $B(A)>0$, so dass für $Q := \log^B n$ (in der Def. von $\mathfrak{M}$) gilt:

$$\int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha)\, d\alpha = \mathfrak{S}(n)\cdot\frac{n^2}{2} + O\left(\frac{n^2}{\log^A n}\right),$$

wobei die O-Konstante nur von A abhängt. Dabei heißt $\mathfrak{S}(n) := \sum_{q=1}^{\infty} \frac{\mu(q)\, c_q(-n)}{\varphi(q)^3}$ die singuläre Reihe des ternären Goldbachproblems. ← absolut kgt.! $\left[|c_q(-n)| \le \varphi(q)\right]$

22.8. **Minor arcs im ternären Goldbachproblem**: Sei nun $\alpha \in \mathfrak{m}$. Nach dem Dirichletschen Approximationssatz 222.8 (ZTI) gibt es einen Bruch $\frac{a}{q}$, $(a,q)=1$, mit $q \le \frac{n}{Q}$ und $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q\cdot\frac{n}{Q}} = \frac{Q}{nq} \left(\le \frac{1}{q^2}\right)$. Da $\alpha \in \mathfrak{m}$, gilt für dieses q dann $q > Q = \log^B(n)$, denn sonst wäre ja $\alpha \in \mathfrak{M}(a,q) \subseteq \mathfrak{M}$ ↯.

Demnach sind die Punkte α der minor arcs nur mit gekürzten Brüchen von großem Nenner q approximierbar. Ist q groß, kann mit folgendem Satz eine nichttriviale obere Schranke für $|S(\alpha)|$ gezeigt werden; dies zeigt, dass $\int_{\mathfrak{m}}$ ein Fehlerterm ist.

22.9. **Satz von (Vinogradov/Vaughan)**: Gilt $\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}$, $1 \le q \le n$, $(a,q)=1$, so ist

$$S(\alpha) \ll \left(\frac{n}{q^{1/2}} + n^{4/5} + n^{1/2} q^{1/2}\right)(\log(n))^4.$$

[Beweis: z.B. [Nathanson, Lemma 8.8]; benutzt + (im Prinzip) Vaughans Identität 21.7.]

Mit diesem Satz kann die (GRH) aus dem Beweis von Hardy & Littlewood eliminiert werden.

Zusammenfassung des Ergebnisses:

22.10. **Satz von Vinogradov**: Es gibt eine zahlentheoretische Fkt. $\mathfrak{S}(n)$ und $c_1, c_2 > 0$ mit $c_1 < \mathfrak{S}(n) < c_2$ für alle ungeraden n, so dass für alle $n \ge n_0$ gilt:

$$R(n) = \mathfrak{S}(n)\frac{n^2}{2} + O\left(\frac{n^2}{\log^A n}\right).$$

[Für $r(n) = \sum_{p_1+p_2+p_3=n} 1$ kann mit partieller Σ daraus $r(n) = \mathfrak{S}(n)\frac{n^2}{2\log^2 n}\left(1 + O\left(\frac{\log\log n}{\log n}\right)\right)$ hergeleitet werden.]

Damit ist für alle ungeraden $n \ge n_0$ also $R(n) > 0$ gezeigt [weil dann Fehlerterm < Hauptterm].

Dazu bleibt noch die (untere) Abschätzung von $\mathfrak{S}(n)$ zu zeigen.

22.11. **Satz (Eulerproduktdarstellung der singulären Reihe):** Es gilt

$$\mathfrak{S}(n) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

Insb. ist also $\mathfrak{S}(n)=0$ für gerade n und $1 \ll \mathfrak{S}(n) \ll 1$ für ungerade n.

Bew.: Die zahlentheoretische Fkt. $\frac{\mu(q)c_q(-n)}{\varphi(q)^3}$ ist multiplikativ in q, da $c_q(-n)$ multiplikativ in q ist. Der Euler-Produktsatz liefert also

$$\mathfrak{S}(n) = \prod_p\Big(1+\underbrace{\sum_{k=1}^{\infty}\frac{\mu(p^k)c_{p^k}(-n)}{\varphi(p^k)^3}}_{=0 \text{ für } k\geq 2}\Big) = \prod_p\left(1-\frac{c_p(-n)}{\varphi(p)^3}\right) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

$$c_p(-n) = \begin{cases} p-1, & p\mid n \\ -1, & \text{sonst}\end{cases}$$

$\square$

22.12. **Bem.:** Die singuläre Reihe ist $=0$ für gerade n. Wäre dies nicht so, würde der Satz 22.10 von Vinogradov bereits das binäre Goldbachproblem positiv entscheiden; für $n>6$ gerade ist in $n=p_1+p_2+p_3$ notwendig ein $p_i=2$, etwa $p_1=2$ und (jedes) $n-p_1=p_2+p_3$ wäre Summe zweier PZen. Stattdessen zeigt 22.10 nur eine obere Absch. für $R(n)$ in diesem Fall, so dass die Methode dann "zusammenbricht" bzw. ein "singulärer Fall" vorliegt; daher der Begriff "singuläre Reihe".

ENDE der Vorlesung ZT II