Ungelöste Probleme der Zahlentheorie

Teil 9: Der Satz von Green/Tao/Ziegler (& PZLücken)

Dieser Satz ist das aktuell beste Resultat zur (ersten) Hardy-Littlewood-Vermutung (HL1) bzw. PZmustern, die ∞ oft auftreten können.

Formulierung des Satzes von Green/Tao/Ziegler (2010/11):

Die verallg. Hardy-Littlewood-Vermutung ist wahr für alle Systeme affin-linearen Formen Ψ von endlicher Komplexität. (Die "schwierigen binären" Fälle haben Komplexität $=\infty$).

Definition der Begriffe:

- Sei $d \in \mathbb{N}$. Eine Abb. $\psi: \mathbb{Z}^d \to \mathbb{Z}$ heißt affin-lineare Form, falls $\psi = \dot{\psi} + \psi(0)$ mit $\psi(0) \in \mathbb{Z}$ und $\dot{\psi}: \mathbb{Z}^d \to \mathbb{Z}$ lineare Form, d.h. $\dot{\psi}(x) = \sum_{i=1}^{d} a_i x_i$, die $a_i \in \mathbb{Z}$.
- System affin-linearer Formen: $\Psi = (\psi_1, \dots, \psi_t)$, $t \in \mathbb{N}$.
  Wir nehmen an, dass darin keine zwei Formen derart sind, dass die eine rationales Vielfaches der anderen ist, und alle nicht konstant.
- Sei $1 \le i \le t$, $s \ge 0$.

Gemeint sind: Partitionen! Ψ hat i-Komplexität $\le s$:$\iff$ die $t-1$ Formen $\{\psi_j;\ j \neq i\}$ können in $s+1$ Klassen eingeteilt werden, so dass ψ_i nicht im ($\mathbb{Z}$-) affin-linearen Span irgendeiner dieser Klassen liegt.

- Die Komplexität von Ψ ist dann das kleinste s, für das jedes ψ_i die i-Komplexität $\le s$ hat, sowie $=\infty$, falls kein solches s ex.

- Die verallgemeinerte HL-Vermutung besagt: Sei $N, d, t, L \in \mathbb{N}$, $\Psi = (\psi_1, \dots, \psi_t)$ affin-lineares System mit $\sum_i \sum_j |\dot{\psi}_i(e_j)| + \frac{1}{N} \sum_i |\psi_i(0)| \le L$, sei $K \subseteq [-N, N]^d \subseteq \mathbb{R}^d$ konvexe kompakte Menge. Dann gilt die asymptotische Formel:

$$\sum_{n \in K \cap \mathbb{Z}^d} \sum_{i=1}^{t} \underbrace{\Lambda}_{\substack{\uparrow \\ \text{von Mangold-Fkt.} \\ \leadsto \text{Primpotenzwerte der } \psi_i(n)}}(\psi_i(n)) = \underbrace{\beta_\infty \prod_p \beta_p}_{\text{Hauptterm mit singulärem Produkt, ist} \sim N^d} + o_{t,d,L}(N^d),$$

$\beta_\infty := \mathrm{vol}_d\left(K \cap \Psi^{-1}((\mathbb{R}^+)^t)\right) \approx N^d$,

$\beta_q := \frac{1}{q^d} \sum_{n \in \mathbb{Z}_q^d} \prod_{i=1}^{t} \Lambda_{\mathbb{Z}_q}(\psi_i(n))$, wo $\Lambda_{\mathbb{Z}_q}(b) := \begin{cases} \frac{q}{\varphi(q)}, & (b,q)=1 \\ 0, & \text{sonst.} \end{cases}$

Welche alten und neuen Spezialfälle sind damit bewiesen?

Beispiele:

(1) Prim-d-Tupel: $\Psi(n_1, \dots, n_d) := (n_1, \dots, n_d)$
zählt alle (unabhängigen) Prim-d-Tupel.
Die Komplexität von Ψ ist 0,
denn keine Form $\psi_j(n_j) = n_j$ liegt im Span der anderen Formen. | (1) herleitbar aus PZ-Satz

(2) Für $k \geq 2$ hat das System $\Psi(n_1, n_2) := (n_1, n_1+n_2, n_1+2n_2, \dots, n_1+(k-1)n_2)$,
das arithmetische Progressionen ("APs") aus k Primzahlen zählt,
die Komplexität $k-2$.
Denn keine Form liegt im Span einer einzelnen anderen Form,
aber im Span zweier anderen Formen. (Beweis erst 2004, "Satz von Green-Tao",
asymptotische Formel in GTZ neu)

(3) Für $N \in \mathbb{N}$ fest hat das System $\Psi(n_1, n_2) := (n_1, n_2, N - n_1 - n_2)$,
das die Lösungen zum ternären Goldbachproblem $N = p_1 + p_2 + p_3$ zählt,
die Komplexität 1.
Denn keine Form liegt im Span einer einzelnen anderen Form,
aber im Span der zwei anderen Formen. (Satz von Vinogradov, 1937)

(4) Das System $\Psi(n_1, n_2) := (n_1, n_2, n_1 + n_2 - 1, n_1 + 2n_2 - 2)$
zählt PZ-Progressionen, deren Abstand $n_2 - 1$ um eins kleiner als eine PZ ist.
Dieses hat Komplexität 2 (dieselbe Begründung wie in (3)). [Ist neu!]

(5) Würfel: Das System $\Psi(n_1, \dots, n_d) := \left(n_1 + \sum_{j \in A} n_j\right)_{A \in \{2, \dots, d\}}$
(d.h. $t = 2^{d-1}$, sei $d \geq 2$) zählt $(d-1)$-dimensionale Würfel in $\mathbb{Z}^{d-1}$, dessen
Ecken alle aus $\mathbb{P}^{d-1}$ sind. Hier ist t groß im Vergleich zu d,
aber die Komplexität von Ψ beträgt nur $d-2$. [neu! Asympt. Formel war
vorher nur im Mittel bekannt.]

Beweis der Komplexitätsgröße $d-2$ im Würfel-fall (nur "$\leq d-2$"):
Betr. man etwa die Form n_1, so lassen sich die anderen $t-1$ Formen in $d-1$ Klassen einteilen, wobei die i-te Klasse alle Formen mit n_{i+1} enthält. n_1 liegt dann nicht im Span einer dieser Klassen, denn in der i-ten Klasse haben n_1 und n_{i+1} denselben Koeffizienten.
Ebenso überlegt man sich dies mit den anderen Formen.

(6) Sei $d \geq 2$ und $t := \frac{1}{2}d(d+1)$, betr. $\Psi(n_1, \dots, n_d) := (n_i + n_j + 1)_{1 \leq i \leq j \leq d}$.
Dieses System zählt alle d-Tupel ungerader PZen $p_1, \dots, p_d$, deren Mittelpunkte $\frac{p_i + p_j}{2}$ auch wieder prim sind. (neu!)
Dieses hat Komplexität 1.
Denn: ist die Form $n_i + n_j + 1$ geg., wo $i<j$ ist, so fasse die anderen $t-1$ Formen in 2 Klassen zusammen: Diejenigen, die nicht n_i enthalten, und diejenigen, die n_i enthalten (und somit nicht n_j enthalten), und $n_i + n_j + 1$ kann in keinem Span einer anderen liegen. Für $2n_i + 1$ nimm die Klasse der Formen, die n_i enthalten (und damit ein n_j mit $j \neq i$), und die Klasse der Formen, die n_i nicht enthalten.
Auch hier liegt $2n_i + 1$ nicht im Span einer dieser beiden Klassen.

Beispiele für Systeme mit unendlicher Komplexität, für die der GTZ-Satz / die H-L-Vermutung unbewiesen bleibt:

(7) Das System $\Psi = (n_1, n_1 + 2)$ zählt PZ-Zwillinge.
Es hat unendliche Komplexität: Geg. die Form n_1, dann liegt $n_1 + 2$ im affin-linearen Span der Form n_1, und umgekehrt.
(8) Das System $\Psi = (n_1, N - n_1)$ zählt Lösungen des binären Goldbach-Problems $N = p_1 + p_2$ und hat ebenso unendl. Komplexität.
(9) Das System $\Psi = (n_1, 2n_1 + 1)$ zählt Sophie-Germain-PZen und hat unendl. Komplexität.

Offen bleiben also die "binären Fälle".

Die Hardy-Littlewoodsche Kreismethode kann übrigens nur Systeme mit Komplexität ≤ 1 behandeln! Insofern stellt der GTZ-Satz einen großen Fortschritt dar.
Welche Systeme nun endliche Komplexität haben, zeigt dieses Kriterium:

Lemma: Sei $\Psi = (\psi_1, \dots, \psi_t)$ ein System affin-linearer Formen.
Dieses hat endliche Komplexität genau dann, wenn keine zwei der ψ_i affin-abhängig sind.
In diesem Fall ist die Komplexität $\leq t - \dim(\overline{\Psi})$.

VR, der von den ψ_i aufgespannt wird

Beweis: Zum ersten Teil:
„$\Rightarrow$": Sind etwa ψ_i und ψ_j affin-abhängig, ist keine endl. Komplexität möglich, da ψ_i in jedem Span von Formen liegt, bei denen ψ_j dabei ist.
„$\Leftarrow$": Sind keine zwei der ψ_i affin-abhängig, so ist die i-Komplexität höchstens $t-2$, da man die $t-1$ anderen Formen in Klassen $\{\psi_j\}, i \neq j$ so zerlegen kann, daß ψ_i in keinem Span einer solchen Klasse liegt.
Zum zweiten Teil: seien keine zwei der ψ_i affin-abhängig, sei $r := \dim(\overline{\Psi})$.
OE sei $(\overline{\psi}_1, \dots, \overline{\psi}_r)$ eine Basis von $\overline{\Psi}$. Betr. die Klasseneinteilung
$\{\psi_2, \dots, \psi_r\}, \{\psi_{r+1}\}, \{\psi_{r+2}\}, \dots, \{\psi_t\}$ (#Klassen $= t-r+1$).
ψ_1 liegt dann nicht im Span einer dieser Klassen, also ist die 1-Komplexität $\leq t-r$. Analog gilt dies für jedes andere ψ_i. $\square$

Die PZ-Zwillingsvermutung ($\exists$ unendl. viele $p \in \mathbb{P}$ mit $p+2 \in \mathbb{P}$) bleibt mit dem GTZ-Satz also unbewiesen, ebenso die Vermutung zu PZ-Cousins $p, p+4 \in \mathbb{P}$ usw., und ebenso die de Polignac-Vermutung.
Die Vermutung von de Polignac besagt, daß jede gerade Zahl $2k$, $k \in \mathbb{N}$, unendlich oft als Differenz zweier aufeinanderfolgenden PZen schreibbar ist: $2k = p_{n+1} - p_n$ für ∞ viele n, wenn $p_1, p_2, \dots$ die aufsteigende Folge der PZen bezeichnet (d.h. die $p_n \in \mathbb{P}$ mit $2 = p_1 < p_2 < \dots$).
Über aufeinanderfolgende PZen sagt der GTZ-Satz nichts aus.

Wir besprechen deshalb noch damit verwandte Vermutungen über PZ Lücken, wo sich auch in letzter Zeit neue Ergebnisse aufgetan haben.

Aus dem PZsatz $\pi(x) \sim \frac{x}{\log x}$ folgt mit $x = p_n$, daß $p_n \sim n \log p_n$, so daß im Schnitt $p_{n+1} - p_n \approx \log p_n$ gilt.
Zur Untersuchung von PZ Lücken betrachtet man deswegen den Quotienten $\frac{p_{n+1} - p_n}{\log p_n}$. Man beachte dazu:

Zwischen zwei benachbarten PZen können beliebig große Lücken sein, wie die lange Folge $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$ zusammengesetzter, aufeinanderfolgender Zahlen zeigt.

Große PZ Lücken ("big gaps"):

Man betrachtet für "große Lücken", die ∞ oft auftauchen können, den Ausdruck

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n}.$$

Eulersche Konstante

Die unbewiesene "big gap"-Vermutung besagt, daß $\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 2e^{-\gamma}$ ist.
Bislang konnte gezeigt werden [Pintz 1997]:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n \log_{(2)} p_n \log_{(4)} p_n \left(\log_{(3)} p_n\right)^{-2}} \geq 2e^{\gamma}.$$

für den Beweis, daß hier ∞ stehen müsste, hatte Erdős einen Preis von 10.000 \$ ausgesetzt...

Kleine PZ Lücken ("small gaps"):

Hier betrachtet man $\Delta_1 := \liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n}$.
Das Ergebnis $\Delta_1 \leq 0.2484\ldots$ von W. Maier von 1988 war bis 2007 die schärfste obere Schranke, die bekannt war. Im Jahr 2007 lösten Goldston, Pintz und Yildirim die "small gap conjecture": sie zeigten, daß $\Delta_1 = 0$ ist.

Dabei konnten sie noch genauer zeigen, dass $\liminf\limits_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^{1/2}(\log_{(2)} p_n)^2} < \infty$ ist.

Unter Annahme der Elliott-Halberstam-Vermutung (dass die GRH im Mittel auch für alle „großen" Moduln gilt) konnten sie auch die schärfere bounded-gap-Vermutung zeigen, nämlich daß $\liminf\limits_{n\to\infty} (p_{n+1}-p_n)$ endlich ist, ja sogar ≤ 16.

Man beachte dazu: Stimmt die P-Zwillingsvermutung, so müßte
$\liminf\limits_{n\to\infty} (p_{n+1}-p_n) = 2$ sein.