Ungelöste Probleme der Zahlentheorie

Teil 4: Das Goldbach-(und Zwillings-)problem

Aus dem Briefwechsel zwischen Goldbach und Euler, 1742, entnehmbar:

(a) Ist jede gerade Zahl ≥ 4 Summe zweier Primzahlen?
(binäres Problem, starke GB-Vermutung)

(b) Ist jede ungerade Zahl ≥ 7 Summe dreier Primzahlen?
(ternäres Problem, schwache GB-Vermutung)

1. Bem.: (a) $\Rightarrow$ (b), denn ist $n \geq 7$ ungerade, ist $n-3 \geq 4$ gerade, nach a) also $n-3 = p_1 + p_2 \Rightarrow n = 3 + p_1 + p_2$. ✓

Vermutung von Descartes 1650:

(c) Jede natürliche Zahl > 1 ist Summe von höchstens 3 Primzahlen.

2. Bem.: Klar gilt (a) $\Rightarrow$ (c),
aber auch (c) $\Rightarrow$ (b):
- falls $2n+1 = p_1 + p_2 + p_3$ nach (c), ok,
- falls $2n+1 = p_1 + p_2$ gilt, so ist $p_1 = 2$ oder $p_2 = 2$, etwa $2n+1 = 2 + q$, q unger. & prim, also $2n+1 = q + 2 = 5 + (q-3)$.
  - Ist $q-3 = \tilde{p}_1 + \tilde{p}_2$, folgt $2n+1 = 5 + \tilde{p}_1 + \tilde{p}_2$, ok,
  - Ist $\underbrace{q-3}_{\text{gerade}} = \hat{p}_1 + \hat{p}_2 + \hat{p}_3$, folgt, daß ein $\hat{p}_i = 2$, also $q = 5 + \hat{p}_2 + \hat{p}_3$ für $\hat{p}_1 = 2$, und $2n+1 = q+2 = 7 + \hat{p}_2 + \hat{p}_3$, ok,
  - Ist $q-3 = \tilde{p}_1$, ist $2n+1 = 5 + \tilde{p}_1 = 2 + 3 + \tilde{p}_1$, ok.
- falls $2n+1 = p$ prim, so kann analog durch Anwenden von c) auf $2n-2$ die Beh. b) gezeigt werden. $\square$

Heuristische Überlegungen zeigen, dass diese Vermutungen sehr plausibel sind: Es sollte $\approx \frac{n}{\log^2 n}$ viele Möglichkeiten geben, eine gerade Zahl als Summe zweier Pz zu schreiben.

Bekannt ist zum ternären GB-Problem folgendes:

Betr. die Darstellungsanzahl

$$r(n) := \#\{(p_1, p_2, p_3) \in \mathbb{P}^3 \mid p_1 + p_2 + p_3 = n\}, \quad n \in \mathbb{N}.$$

Dann gilt:

<u>Satz 1 (Vinogradov, 1937)</u>: Es gibt eine Funktion $\mathfrak{S}: \mathbb{N} \to \mathbb{R}$ und reelle Konstanten $c_1, c_2 > 0$ mit $c_1 < \mathfrak{S}(n) < c_2$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r(n) = \mathfrak{S}(n) \cdot \frac{n^2}{2(\log n)^3} \cdot \left(1 + O\left(\frac{\log\log n}{\log n}\right)\right).$$

Die Funktion $\mathfrak{S}$ heißt <u>Singuläre Reihe</u> und kann als $\mathfrak{S}(n) = \prod_{p \nmid n} \left(1 + \frac{1}{(p-1)^3}\right) \cdot \prod_{p \mid n} \left(1 - \frac{1}{(p-1)^2}\right)$ (0) geschrieben werden.

<u>Bem.</u>: Aus dem Satz folgt, dass $r(n) > 0$ ist für alle hinreichend großen ungeraden n. Für gerade n ist jedoch $\mathfrak{S}(n) = 0$, da dann $p = 2$ im zweiten Produkt als Index vorkommt und der entsprechende Faktor $1 - \frac{1}{(2-1)^2} = 0$ verschwindet.

Der Satz zeigt also (b) für alle hinreichend großen ungeraden n, besagt aber nichts für kleine ungerade n und gerade n ($\sim$ binäres GB-Problem).

Durch genaue Konstantenanalysen im Beweis konnte zunächst $n_0 = 3^{3^{15}}$ ermittelt werden (Borodzkin 1956), heute aktuell: $n_0 = 2 \cdot 10^{1346}$ (Liu Min-Chit & Wang Tian-Ze, 2002)

Verifiziert wurde die ternäre Vermutung bislang für $n \leq 1{,}6 \cdot 10^{18}$ (T. Oliveira e Silva, 2008)

Unter Ann. <u>der verallg. Riemannschen Vermutung</u> konnte inzwischen (unter Verwendung von numerischen Verifikationen) die ternäre Vermutung bewiesen werden (1997, J.-M. Deshouillers, G. Effinger, H. te Riele, D. Zinoviev).

- Die binäre Vermutung ist offen. Verifiziert wurde sie bislang für alle geraden $n \leq 4 \cdot 10^{18}$ (T. Oliveira e Silva).

- Dass alle ungeraden Zahlen Summe von ≤ 5 PZen ist, zeigte T. Tao kürzlich in einem eingereichten Paper.

- Chen Jingrun zeigte 1973, dass jede große gerade Zahl als $2n = p_1 + P_2$ schreibbar ist mit p_1 prim und wo P_2 eine Zahl mit höchstens 2 Primfaktoren ist.

- Vinogradov's Methoden zeigen, dass fast alle geraden Zahlen der binären Vermutung genügen: Ist $E(x) := \#\{n \leq x \mid 2 \text{ gerade } \& \ \underset{\text{unlösbar}}{n = p_1 + p_2}\}$ die Anzahl der Ausnahmen bis x, so gilt $E(x) = O(x^{1-\delta})$ für ein $\delta > 0$ (1975, Montgomery + Vaughan).

Eng verwandt mit dem GB-Problem ist das Zwillingsproblem
- Gibt es ∞ viele Primzahlen p, so dass auch $p+2$ prim ist?

$\rightsquigarrow$ de Polignac-Vermutung von 1849: Gibt es für jedes $k \geq 1$ zwei PZen p_1, p_2 mit $2k = p_1 - p_2$?

$\rightsquigarrow$ Satz von Brun: $\#\{p \leq x \mid p, p+2 \in \mathbb{P}\} = O\left(\frac{x}{\log^2 x}\right)$.

Sowie die Vermutung zu Sophie-Germain-Primzahlen:
- Gibt es ∞ viele Primzahlen p, so dass auch $2p+1$ prim ist?

Der Beweis des Satzes 1 von Vinogradov ist ein Paradebeispiel für die sogenannte Kreismethode bzw. Hardy-Littlewood-Methode, die heute zu den klassischen Methoden der additiven Zahlentheorie gehört. Wir werden den Beweisgang im folgenden kurz skizzieren. Sie liefert auch Teilergebnisse zu dem Zwillings- und S.-G.-PZ-Problem, auf die wir aber nicht näher eingehen werden.

Erläuterung der Kreismethode im ternären Problem:

Punkte auf komplexen Einheitskreis

Sei $n \in \mathbb{N}$ hinreichend groß, setze $e(x) := e^{2\pi i x}$ für $x \in \mathbb{R}$.

Für $\alpha \in \mathbb{R}$ sei $S(\alpha) := \sum_{p \in \mathbb{P}, p \leq n} \log p \; e(\alpha p)$ eine Exponentialsumme mit Primzahlen

Gewichtsfaktoren

und betr. $R(n) := \sum_{\substack{p_1, p_2, p_3 \in \mathbb{P}, \\ p_1 + p_2 + p_3 = n}} \log p_1 \log p_2 \log p_3$ die gewichtete Darstellungsanzahl im ternären Problem.

$S(\alpha)$ dient zur Berechnung von $R(n)$ mit der Formel

$$R(n) = \int_0^1 S(\alpha)^3 e(-n\alpha) \, d\alpha, \qquad (1)$$

denn r. S. $= \sum_{p_1, p_2, p_3 \leq n} \log p_1 \log p_2 \log p_3 \underbrace{\int_0^1 e(\alpha(p_1 + p_2 + p_3 - n)) \, d\alpha}_{\overset{\text{ONR}}{=} \begin{cases} 1, & p_1 + p_2 + p_3 = n \\ 0, & \text{sonst} \end{cases}} = R(n)$,

denn es gilt die Orthogonalitätsrelation (ONR):

$\int_0^1 e(\alpha m) \, d\alpha = 1$, falls $m = 0$,

und falls $m \in \mathbb{Z} \setminus \{0\}$, ist $\int_0^1 e(\alpha m) \, d\alpha = \left. \frac{e^{2\pi i \alpha m}}{2\pi i m} \right|_0^1 = \frac{1 - 1}{2\pi i m} = 0$.

Die Idee der Kreismethode beruht nun auf der Beobachtung, dass der Wert des Integrals maßgeblich durch den Wert auf Teilintervallen der Form $\mathfrak{M}(a,q) := \left[\frac{a}{q} - \frac{Q}{n}, \frac{a}{q} + \frac{Q}{n}\right] \cap [0,1]$, bestimmt wird.

wo $\underbrace{1 \leq q \leq Q}, 0 \leq a \leq q, (a,q) = 1$,

[d.h. der IV mittelpkt. $\frac{a}{q} \in \mathbb{Q}$ hat beschränkte Nennergröße

Diese heißen (aus historischen Gründen) die major arcs, wobei

$$\mathfrak{M} := \bigcup_{1 \leq q \leq Q} \bigcup_{(a,q) = 1} \mathfrak{M}(a,q).$$

Als Schranke Q für die Nenner der major arc-Mittelpunkte wählt man $Q := (\log n)^B$, $B > 0$, im GB-Problem.

Die Komplementmenge $\mathfrak{m} := [0,1] \setminus \mathfrak{M}$ nennt man minor arcs.

Die Aufspaltung $R(n) = \left(\int_{\mathfrak{M}} + \int_{\mathfrak{m}}\right) S^3(\alpha) e(-n\alpha)\, d\alpha$ (2) ist nun günstig.

Die Auswertung von $R(n)$ wird damit nun wie folgt durchgeführt:

1. Schritt: Für $\alpha \in \mathfrak{M}$ kann $S(\alpha)$ mit einer Formel der Art

$$S(\alpha) = \text{Hauptterm} + \text{Fehler kleinerer Größenordnung} \quad (3)$$

gezeigt werden; hier geht eine Formel zur Anzahl PZen in Restklassen ein (der sog. Satz von Siegel-Walfisz).

2. Schritt: Diese Formel (3) wird in (2) eingesetzt, man erhält

$$\int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha)\, d\alpha = \mathfrak{S}(n) \frac{n^2}{2} + O\left(\frac{n^2}{(\log n)^A}\right) \quad (4)$$

mit besagter singulärer Reihe $\mathfrak{S}(n)$ wie in (0) und ein $A > 0$ bel., wenn $B = B(A) > 0$ geeignet.

3. Schritt: Vinogradovs wesentlicher Beitrag war nun die Absch. von $\int_{\mathfrak{m}}$:
Es ist $\max_{\alpha \in \mathfrak{m}} |S(\alpha)| = O\left(\frac{n}{(\log n)^C}\right)$ für alle $C > 0$ groß genug, also ist

$$\int_{\mathfrak{m}} S^3(\alpha) e(-n\alpha)\, d\alpha \le \max_{\alpha \in \mathfrak{m}} |S(\alpha)| \cdot \underbrace{\int_0^1 |S(\alpha)|^2\, d\alpha}_{\overset{=}{\text{ONR}}\ O(n \log^2 n)} = O\left(\frac{n^2}{(\log n)^{C-2}}\right). \quad (5)$$

Aus (4) und (5) folgt dann eine Formel für $R(n)$, aus der die für $r(n)$ im Satz 1 nicht allzu schwer hergeleitet werden kann.
Ein Ansatz wie in (1) kann dann auch für andere additive Probleme hinzugezogen werden (Waring, PZ-Zwillinge etc.), was die Bezeichnung als "Methode" rechtfertigt.