Ungelöste Probleme der Zahlentheorie

Teil 8: Die Hardy-Littlewood-Vermutungen und deren Inkompatibilität

Wir besprechen in diesem Teil zwei bekannte Vermutungen von Hardy und Littlewood.
Zuerst behandeln wir die
erste Hardy-Littlewood-Vermutung ("HL1"),
auch "Prim-k-Tupel-Vermutung" genannt.

Es geht um die Verallgemeinerung der Primzahlzwillingsvermutung auf beliebige k-Tupel aus Primzahlen (Drillinge, Vierlinge, usw.).

Bsp. für Drillinge: $(n, n+2, n+6)$ hat Werte in $\mathbb{P}^3$ für $n = 5, 11, 17$, und vermutlich unendlich oft.
Bei dem Tripel $(n, n+2, n+4)$ können wir dies nicht erwarten: nur das PZ tripel $(3,5,7)$ erfüllt diese Konstellation.
$\left[\, n \equiv 1\,(3) \rightsquigarrow 3 \mid n+2,\ n \equiv 2\,(3) \rightsquigarrow 3 \mid n+4 \,\right]$
Und ebenso ist das Paar $(n, n+1)$ unzulässig für PZwerte: $n \equiv 1\,(2) \Rightarrow 2 \mid n+1$, d.h. nur $(2,3)$ möglich.
Wir möchten ein k-Tupel $(b_1, \dots, b_k) \in \mathbb{N}^k$ unzulässig nennen, wenn $(n+b_1, \dots, n+b_k) \in \mathbb{P}^k$ nicht unendlich oft möglich ist.
Dies ist der Fall, wenn es ein $p \in \mathbb{P}$ so gibt, dass alle Reste $a \bmod p$ zu einem b_i kongruent mod p sind, d.h. wenn die b_i alle Reste mod p abdecken (dann ist eine der Zahlen $n+b_1, \dots, n+b_k$ notwendigerweise durch p teilbar).
Wir definieren zulässige k-Tupel wie folgt:
Ein k-Tupel $(b_1, b_2, \dots, b_k) \in \mathbb{N}^k$ heißt zulässig, falls $b_1 < b_2 < \dots < b_k$
und $\neg\left(\exists p\ \forall a \bmod p\ \exists i \in \{1, \dots, k\} : b_i \equiv a\,(p)\right)$
$\Leftrightarrow\ \forall p\ \exists a \bmod p\ \forall i \in \{1, \dots, k\} : b_i \not\equiv a\,(p)$.
"Für alle $p \leq k$ ex. eine Restklasse $a \bmod p$, die $\{b_1, \dots, b_k\}$ nicht trifft"

Um Zulässigkeit zu überprüfen, genügt es, dafür nur die Primzahlen $p \leq k$ zu testen (wegen Schubfachprinzip).

<u>Bsp.:</u>
- $(b_1, b_2) = (0,2)$: PZ Zwillinge
- $(b_1, b_2) = (0,4)$: PZ Cousins
- Länge 5: $(0,2,6,8,12)$ ist zulässiges k-Tupel in $[0,13]$.
  Denn: kein b_i ungerade, kein $b_i \equiv 1\ (3)$, kein $b_i \equiv 4\ (5)$.
- Aber: Es gibt <u>kein</u> zulässiges 6-Tupel in $[0,13]$!
  (Beachten Sie diesen Zusatz! Sonst stimmt die Beh. nicht, wie wir bei der Vorlesung festgestellt haben...)

Damit formulieren wir nun die offene Prim-k-tupel-Vermutung wie folgt:

<u>(HL1):</u> Wenn $(b_1, \dots, b_k) \in \mathbb{N}^k$ zulässig ist, dann gibt es unendlich viele $n \in \mathbb{N}$ so, dass $n+b_1, n+b_2, \dots, n+b_k \in \mathbb{P}$.
(Inkl.: Formel für die asymptotische Dichte solcher n.)

Diese Vermutung umfasst also die PZ Zwillings-Vermutung, PZ-Drillinge usw.

<u>Bem.:</u> Die allgemeinere Vermutung, bei der die $X+b_i$ durch beliebige irreduzible Polynome ersetzt werden, heißt <u>"Schinzel's Hypothesis H"</u>.
Die quantitative Version heißt
<u>Bateman-Horn-Vermutung:</u> Seien $f_1, \dots, f_m \in \mathbb{Z}[X]$ verschiedene, irreduzible Polynome mit der <u>Bunyakovsky-Eigenschaft</u> ("zulässig"), d.h. $\nexists p \in \mathbb{P}\ \forall n \in \mathbb{N}: p \mid f_1(n) \cdots f_m(n)$, alle mit positiven Leitkoeff.
Sei $P(x) := \frac{1}{x} \cdot \# \{ n \leq x;\ f_1(n), \dots, f_m(n) \in \mathbb{P} \}$. Dann besagt die BH-Vermutung, dass

$$P(x) \sim \frac{C}{D} \cdot \int_2^x \frac{dt}{(\log t)^m}, \quad \text{wo } C := \deg f_1 \cdots \deg f_m$$

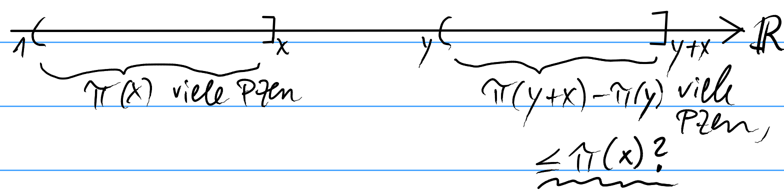
und $D := \prod_p \frac{1 - N(p)/p}{(1-1/p)^m}$, und $N(p) := \# \{ n \bmod p;\ f(n) \equiv 0\ (p) \}$.

2010/2011 wurde (HL1) "bis auf alle schwierigen Fälle" gelöst von <u>Green/Tao/Ziegler</u>, die eine mehrdimensionale Dirichlet-Version dieser Vermutung bewiesen haben. Die schwierigen Fälle sind die "binären" Fälle (PZ Zwillinge, PZ Cousins, binäres Goldbach-Problem, Sophie-Germain-Primzahlen...)
Bis auf die "Binär-Fälle" ist damit auch (HL1) bewiesen.

Nun zur <u>zweiten Hardy-Littlewood-Vermutung</u>.
Wir betrachen wieder die PZ Zählfkt. $\pi(x) := \#\{p \le x\}$, $x > 1$ reell.

Der PZSatz $\pi(x) \sim li(x) = \int_2^x \frac{dt}{\log t}$ legt nahe, dass Intervalle fester Länge weniger PZen enthalten, umso größer die IVgrenzen sind:

<u>(HL 2)</u>: $\forall x, y \geq 2: \ \pi(y+x) - \pi(y) \le \pi(x)$,
dabei sei ohne Einschränkung $x \le y$ wg. Symmetrie.



Wir definieren die Fkt. $\underline{S_1(x)} := \max_{y \ge x} \left(\pi(y+x) - \pi(y)\right)$.

Damit gilt: $(HL\,2) \iff \forall x \geq 2: \ S_1(x) \le \pi(x)$.
Klar gilt: $S_1(x) \geq \pi(2x) - \pi(x) \sim \pi(x)$,
nach Rosser/Schoenfeld [1962] gilt: $\forall x \geq 2: \ \pi(2x) - \pi(x) < \pi(x)$
$\iff \pi(2x) < 2\pi(x)$

Mit dem großen Sieb konnten Montgomery & Vaughan zeigen, dass
$\forall x \geq 2: \ S_1(x) \le 2\pi(x)$ gilt.
Bislang bestes Ergebnis zu (HL2):
[P. Dusart 2002] (HL2) gilt für $2 \le x \le y \le \frac{7}{5} x \log x \log\log x$.

Für einige Überraschung sorgte 1974 die Arbeit von Hensley & Richards, in der sie nachwiesen, dass (HL 1) und (HL 2) inkompatibel sind in folgenden Sinne. Sie zeigten:

Ist (HL 1) wahr, so ist (HL 2) falsch.

Die beiden Vermutungen können demnach nicht beide wahr sein. Man vermutet, dass (HL 1) wahr und (HL 2) falsch ist.

Wir umreißen im folgenden deren Beweisidee.

Sei $\underline{\varrho(x)} := \limsup_{y\to\infty} (\pi(y+x) - \pi(y))$ (Klar: $\varrho(x) \geq \pi(x) - 1$ ($y=2$).)

sowie $\underline{\varrho^*(x)} := \max_{y \leq x} \# \{ n \in]y, y+x] ;\ \forall m \leq x : (m,n) = 1 \}$.

<u>Vgl. $\varrho_1(x)$ mit $\varrho(x)$:</u> Die Zahl $\varrho(x)$ ist die größte Länge eines PZblocks (in einem IV der Länge x), die unendl. oft vorkommt.

Die Zahl $\varrho_1(x)$ ist die größtmögliche Länge eines PZblocks überhaupt, der vorkommt (u.U. auch nur ein einziges Mal) in einem IV der Länge x.

Dies zeigt $\underline{\varrho(x) \leq \varrho_1(x)}$ für alle $x \geq 2$. $\underline{(1)}$

<u>Vgl. $\varrho_1(x)$ mit $\varrho^*(x)$:</u> Es gilt $\underline{\varrho_1(x) \leq \varrho^*(x)}$ für alle $x \geq 2$, $\underline{(2)}$

denn die PZen in $]y, y+x]$ sind zu allen $m \leq x$ teilerfremd.

Die Fkt. $\varrho^*(x)$ lässt sich mit dem Chinesischen Restsatz nun umschreiben zu $\varrho^*(x) = \max \{ k;\ \exists$ zulässiges k-Tupel $(e_1, \dots, e_k)$ in einem IV $]y, y+x] \}$.

Dabei kann OE $y = 0$ gesetzt werden, denn Zulässigkeit ist translationsinvariant.

Ist nun (HL 1) wahr, so folgt also $\varrho^*(x) \leq \varrho(x)$ für alle $x \geq 2$, und dann sind die drei Funktionen alle gleich wegen $\underline{(1) \& (2)}$.

Haben also: $\underline{\varrho(x) \leq \varrho_1(x) \leq \varrho^*(x) \underset{(HL1)}{\leq} \varrho(x)}$, und: $\underline{(HL2) \Leftrightarrow \varrho_1(x) \leq \pi(x)}$.

Hensley & Richards zeigten nun folgendes:

(*) $\underline{\varrho^*(x) - \pi(x) \xrightarrow{x\to\infty} \infty}$, genau: $\varrho^*(x) - \pi(x) \geq (\log 2 - \varepsilon)\frac{x}{\log^2 x}$ für $x \geq x_0$.

Damit ist, wenn (HL1) wahr und $\boxed{\varrho_1(x) = \varrho(x) = \varrho^*(x) > \pi(x)}$ ist, dann $\pi(y+x) - \pi(y) > \pi(x)$, d.h. (HL2) $(\Leftrightarrow \varrho_1(x) \leq \pi(x))$ falsch und das sogar unendlich oft für so ein x (wegen $\varrho(x) = \limsup_{y\to\infty} \ldots$).

Um die Inkompatibilität von (HL1) und (HL2) zu zeigen, reicht schon ein x_0 aus mit $\varrho^*(x_0) > \pi(x_0)$.
Daher suchten H.&R. nach so einem x_0 numerisch per Computer.
Für kleine x fanden sie $\pi(x) < \varrho^*(x)$, die Funktionen treffen sich einige Male, und später übertrifft $\varrho^*(x)$ die Funktion $\pi(x)$ (ab $x = 20.000$)
(diese großen x fanden H.&R. allerdings erst <u>nach</u> ihrem Beweis von (*) ...).

<u>Bsp.:</u> $\pi(13) = 6$, $\varrho^*(13) = 5$.

H.& R. bewiesen (*) durch Konstruktion einer zulässigen Menge im Intervall $[-\frac{x}{2}, \frac{x}{2}]$, die fast $2\pi(\frac{x}{2})$ viele Elemente hat.
$[\rightsquigarrow \varrho^*(x) \gtrsim 2\pi(\frac{x}{2}) \underset{\text{Rosser/Schoenfeld}}{>} \pi(x)$, $]$

- Es sind sogar $\geq \pi(x) + (\log 2 - \varepsilon)\frac{x}{\log^2 x}$ viele, wenn genau gezählt wird $(x \geq x_0)$.
- Diese Menge ist die Restmenge, die nach Sieben aller Vielfachen von kleinen Pzen entsteht. Für große Pzen p überlegt man sich, dass es eine Restklasse a mod p geben muss, deren Elemente in $[-\frac{x}{2}, \frac{x}{2}]$ alle schon durch kleine Pzen teilbar sind und deswegen die Restmenge nicht trifft. Daher ist die Menge zulässig.