Über Mittelwertsätze, Siebmethoden und die Riemannsche Vermutung in der additiven Zahlentheorie

Antrittsvorlesung zur Umhabilitierung nach Münster

PD Dr. Karin Halupczok

1. Dezember 2010

Primzahlen

Teilbarkeit in $\mathbb{N}$: $\quad a \mid b \quad :\Leftrightarrow \quad \exists c : b = ac$

Primzahlen

Teilbarkeit in $\mathbb{N}$: $\quad a \mid b \quad :\Leftrightarrow \; \exists c : b = ac$

$p \in \mathbb{N}$ heißt *prim*, falls $p > 1$ und $(t \mid p \Rightarrow t = 1 \text{ oder } t = p)$

Primzahlen

Teilbarkeit in $\mathbb{N}$: $a \mid b \quad :\Leftrightarrow \quad \exists c : b = ac$

$p \in \mathbb{N}$ heißt *prim*, falls $p > 1$ und $(t \mid p \Rightarrow t = 1 \text{ oder } t = p)$

Jedes $n > 1$ hat mindestens einen Primteiler, etwa den kleinsten Teiler d von n mit $1 < d \leq n$.

Primzahlen

Teilbarkeit in $\mathbb{N}$: $a \mid b \quad :\Leftrightarrow \quad \exists c : b = ac$

$p \in \mathbb{N}$ heißt *prim*, falls $p > 1$ und $(t \mid p \Rightarrow t = 1 \text{ oder } t = p)$

Jedes $n > 1$ hat mindestens einen Primteiler, etwa den kleinsten Teiler d von n mit $1 < d \leq n$.

Satz von Euklid

Es existieren unendlich viele Primzahlen.

Primzahlen

Teilbarkeit in $\mathbb{N}$: $\quad a \mid b \quad :\Leftrightarrow \quad \exists c : b = ac$

$p \in \mathbb{N}$ heißt *prim*, falls $p > 1$ und $(t \mid p \Rightarrow t = 1 \text{ oder } t = p)$

Jedes $n > 1$ hat mindestens einen Primteiler, etwa den kleinsten Teiler d von n mit $1 < d \leq n$.

Satz von Euklid

Es existieren unendlich viele Primzahlen.

Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen. Dann ist jeder Primteiler von $n := p_1 \cdots p_k + 1$ von $p_1, \ldots, p_k$ verschieden. (Denn aus $p_j \mid n$ folgt sonst $p_j \mid n - p_1 \cdots p_k = 1$, $\lightning$.)

Primzahlen

Teilbarkeit in $\mathbb{N}$: $a \mid b \quad :\Leftrightarrow \quad \exists c : b = ac$

$p \in \mathbb{N}$ heißt *prim*, falls $p > 1$ und ($t \mid p \Rightarrow t = 1$ oder $t = p$)

Jedes $n > 1$ hat mindestens einen Primteiler, etwa den kleinsten Teiler d von n mit $1 < d \leq n$.

Satz von Euklid

Es existieren unendlich viele Primzahlen.

Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen. Dann ist jeder Primteiler von $n := p_1 \cdots p_k + 1$ von $p_1, \ldots, p_k$ verschieden.
(Denn aus $p_j \mid n$ folgt sonst $p_j \mid n - p_1 \cdots p_k = 1$, ↯.)
So können unendlich viele Primzahlen gewonnen werden. $\square$

Primzahlzählfunktion

$$\pi(x) := \#\{p \leq x : p \text{ prim}\}$$

Primzahlzählfunktion

$$\pi(x) := \#\{p \leq x : p \text{ prim}\}$$

Der Euklid-Beweis zeigt: $\pi(x) \geq \log_2 \log_2 x$
(Aus $p_{k+1} \leq 1 + p_1 \cdots p_k$ folgt induktiv $p_k \leq 2^{2^{k-1}}$.)

Primzahlzählfunktion

$$\pi(x) := \#\{p \leq x : p \text{ prim}\}$$

Der Euklid-Beweis zeigt: $\pi(x) \geq \log_2 \log_2 x$
(Aus $p_{k+1} \leq 1 + p_1 \cdots p_k$ folgt induktiv $p_k \leq 2^{2^{k-1}}$.)

Elementare obere Abschätzung: $\pi(x) \leq \frac{x}{3}$ für $x \geq 33$.

Primzahlzählfunktion

$$\pi(x) := \#\{p \leq x : p \text{ prim}\}$$

Der Euklid-Beweis zeigt: $\pi(x) \geq \log_2 \log_2 x$
(Aus $p_{k+1} \leq 1 + p_1 \cdots p_k$ folgt induktiv $p_k \leq 2^{2^{k-1}}$.)

Elementare obere Abschätzung: $\pi(x) \leq \frac{x}{3}$ für $x \geq 33$.

Vermutung von Gauß (1849): Das logarithmische Integral

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right)$$

ist eine Approximation an $\pi(x)$, d. h. $\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1$.

Werte der Primzahlzählfunktion $\pi(x)$

x	$\pi(x) := \#\{p \leq x\}$	$\mathrm{li}(x) - \pi(x)$	$\pi(x) - \frac{x}{\log x}$
10^8	5761455	753	332774
10^9	50847534	1700	2592592
10^{10}	455052511	3103	20758029
10^{11}	4118054813	11587	169923159
10^{12}	37607912018	38262	1416705193
10^{13}	346065536839	108970	11992858452
10^{14}	3204941750802	314889	102838308636
10^{15}	29844570422669	1052618	891604962452
10^{16}	279238341033925	3214631	7804289844393
10^{17}	2623557157654233	7956588	68883734693928
10^{18}	24739954287740860	21949554	612483070893536
10^{19}	234057667276344607	99877774	5481624169369960
10^{20}	2220819602560918840	222744643	49347193044659702
10^{21}	21127269486018731928	597394253	446579871578168707
10^{22}	201467286689315906290	1932355207	4060704006019620994
10^{23}	1925320391606803968923	7250186214	37083513766578631310

Primzahlsatz

Tschebytschev (1850): Es gibt Konstanten $c_2 > c_1 > 0$ mit

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x},$$

der Beweis ist elementar.

Primzahlsatz

Tschebytschev (1850): Es gibt Konstanten $c_2 > c_1 > 0$ mit

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x},$$

der Beweis ist elementar.

Hadamard und de la Vallée–Poussin (1896):

Primzahlsatz: $\lim\limits_{x \to \infty} \dfrac{\pi(x)}{\mathrm{li}(x)} = 1.$

Primzahlsatz

Tschebytschev (1850): Es gibt Konstanten $c_2 > c_1 > 0$ mit

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x},$$

der Beweis ist elementar.

Hadamard und de la Vallée–Poussin (1896):

Primzahlsatz: $\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$

(Der Beweis ist analytisch: $\zeta(1 + it) \neq 0$ für alle $t \in \mathbb{R}$)

Primzahlsatz

Tschebytschev (1850): Es gibt Konstanten $c_2 > c_1 > 0$ mit

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x},$$

der Beweis ist elementar.

Hadamard und de la Vallée–Poussin (1896):
Primzahlsatz: $\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$
(Der Beweis ist analytisch: $\zeta(1+it) \neq 0$ für alle $t \in \mathbb{R}$)

Elementarer Beweis des Primzahlsatzes:
Selberg und Erdős (1948)

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Obige Tabelle zeigt: Der Fehlerterm ist vermutlich $\approx x^{1/2}$.

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Obige Tabelle zeigt: Der Fehlerterm ist vermutlich $\approx x^{1/2}$.

Das bislang beste bewiesene Ergebnis ist

$$\pi(x) = \mathrm{li}(x) + \mathrm{O}\big(x \exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})\big)$$

von Vinogradov und Korobov (1958).

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Obige Tabelle zeigt: Der Fehlerterm ist vermutlich $\approx x^{1/2}$.

Das bislang beste bewiesene Ergebnis ist

$$\pi(x) = \mathrm{li}(x) + \mathrm{O}\big(x \exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})\big)$$

von Vinogradov und Korobov (1958).

Bekannt ist: Ist der Fehlerterm $\mathrm{O}(x^{1/2}\log x)$, so gilt die Riemannsche Vermutung, und umgekehrt!

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?

Obige Tabelle zeigt: Der Fehlerterm ist vermutlich $\approx x^{1/2}$.

Das bislang beste bewiesene Ergebnis ist

$$\pi(x) = \mathrm{li}(x) + \mathrm{O}\big(x \exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})\big)$$

von Vinogradov und Korobov (1958).

Bekannt ist: Ist der Fehlerterm $\mathrm{O}(x^{1/2}\log x)$, so gilt die Riemannsche Vermutung, und umgekehrt!
(Beweis mit der “expliziten Formel”)

Die Riemannsche Vermutung (RH):

Alle Nullstellen von $\zeta(s)$ im Streifen $0 \le \operatorname{Re} s \le 1$ liegen auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Die Riemannsche Vermutung (RH):

Alle Nullstellen von $\zeta(s)$ im Streifen $0 \leq \operatorname{Re} s \leq 1$ liegen auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Es gibt mehrere Möglichkeiten, die Riemannsche Vermutung zu formulieren!

Die Riemannsche Vermutung (RH):

Alle Nullstellen von $\zeta(s)$ im Streifen $0 \leq \operatorname{Re} s \leq 1$ liegen auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Es gibt mehrere Möglichkeiten, die Riemannsche Vermutung zu formulieren!

Möbius-Funktion $\mu(n) := \begin{cases} (-1)^r, & n = p_1 \cdots p_r, \text{ die } p_i \text{ pwv} \\ 0 & \text{sonst.} \end{cases}$

Die Riemannsche Vermutung (RH):

Alle Nullstellen von $\zeta(s)$ im Streifen $0 \leq \operatorname{Re} s \leq 1$ liegen auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Es gibt mehrere Möglichkeiten, die Riemannsche Vermutung zu formulieren!

Möbius-Funktion $\mu(n) := \begin{cases} (-1)^r, & n = p_1 \cdots p_r, \text{ die } p_i \text{ pwv} \\ 0 & \text{sonst.} \end{cases}$

RH $\Leftrightarrow \forall \varepsilon > 0 : \sum_{n \leq x} \mu(n) = \mathrm{O}(x^{1/2+\varepsilon})$

Die Riemannsche Vermutung (RH):

Alle Nullstellen von $\zeta(s)$ im Streifen $0 \le \operatorname{Re} s \le 1$ liegen auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Es gibt mehrere Möglichkeiten, die Riemannsche Vermutung zu formulieren!

Möbius-Funktion $\mu(n) := \begin{cases} (-1)^r, & n = p_1 \cdots p_r, \text{ die } p_i \text{ pwv} \\ 0 & \text{sonst.} \end{cases}$

RH $\Leftrightarrow \forall \varepsilon > 0 : \sum_{n \le x} \mu(n) = \mathrm{O}(x^{1/2+\varepsilon})$

Soundararajan (2008):

$$\text{RH} \Rightarrow \sum_{n \le x} \mu(n) = \mathrm{O}(x^{1/2} \exp(\log(x)^{1/2} (\log\log x)^{14}))$$

Primzahlen zählen

Primzahlen in Progressionen zählen

Die Goldbachsche Vermutung und Primzahlzwillinge

Primzahlmuster

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \ : \ n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \;:\; n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Dirichlet (1837): Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $\equiv a \bmod q$.

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \ : \ n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Dirichlet (1837): Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $\equiv a \bmod q$.

Zählfunktion für Primzahlen in APs:
$\pi(x; q, a) := \#\{p \leq x : \ p \equiv a \bmod q\}$

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \;:\; n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Dirichlet (1837): Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $\equiv a \bmod q$.

Zählfunktion für Primzahlen in APs:
$\pi(x; q, a) := \#\{p \leq x : \; p \equiv a \bmod q\}$

Primzahlsatz in Progressionen:

Für $(a, q) = 1$ gilt

$$\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} \, \big(1 + \mathrm{o}(1)\big).$$

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \ : \ n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Dirichlet (1837): Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $\equiv a \bmod q$.

Zählfunktion für Primzahlen in APs:
$\pi(x; q, a) := \#\{p \leq x : \ p \equiv a \bmod q\}$

Primzahlsatz in Progressionen:

Für $(a, q) = 1$ gilt

$$\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} \left(1 + \mathrm{o}(1)\right).$$

Die Primzahlen verteilen sich demnach asymptotisch gleichmäßig auf die $\varphi(q)$ vielen reduzierten Restklassen $a \bmod q$.

Primzahlen in arithmetischen Progressionen

Arithmetische Progression (AP): $\{a + nq \ : \ n \in \mathbb{N}_0\}$ für $a, q \in \mathbb{N}$

Dirichlet (1837): Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $\equiv a \bmod q$.

Zählfunktion für Primzahlen in APs:
$\pi(x; q, a) := \#\{p \leq x : \ p \equiv a \bmod q\}$

Primzahlsatz in Progressionen:

Für $(a, q) = 1$ gilt

$$\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} \left(1 + \mathrm{o}(1)\right).$$

Die Primzahlen verteilen sich demnach asymptotisch gleichmäßig auf die $\varphi(q)$ vielen reduzierten Restklassen $a \bmod q$.

Aber: Die von $\mathrm{o}(1)$ induzierte Funktion hängt von q und a ab!

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a, q) = 1$ gilt die Abschätzung $\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a, q) = 1$ gilt die Abschätzung $\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Problem: Die Konstante C kann nicht effektiv berechnet werden!

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a, q) = 1$ gilt die Abschätzung $\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Problem: Die Konstante C kann nicht effektiv berechnet werden! Denn: Die Existenz von Siegel-Nullstellen (i. e. L-Nullstellen, die sehr nahe an $s = 1$ liegen) kann nicht ausgeschlossen werden.

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a,q) = 1$ gilt die Abschätzung $\pi(x;q,a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Problem: Die Konstante C kann nicht effektiv berechnet werden! Denn: Die Existenz von Siegel-Nullstellen (i. e. L-Nullstellen, die sehr nahe an $s = 1$ liegen) kann nicht ausgeschlossen werden.

Heath-Brown (1983): aus deren Existenz folgt die Zwillingsvermutung

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a, q) = 1$ gilt die Abschätzung $\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Problem: Die Konstante C kann nicht effektiv berechnet werden!
Denn: Die Existenz von Siegel-Nullstellen (i. e. L-Nullstellen, die sehr nahe an $s = 1$ liegen) kann nicht ausgeschlossen werden.

Heath-Brown (1983): aus deren Existenz folgt die Zwillingsvermutung

Anwendung: Ford, Luca, Pomerance (2010): Die Gleichung $\varphi(a) = \sigma(b)$ hat unendlich viele Lösungen
(Erdős-Vermutung von 1959)

Siegel-Walfisz (1936): Gleichmäßig in $q \leq (\log x)^A$, $(a, q) = 1$ gilt die Abschätzung $\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(xe^{-C\sqrt{\log x}})$, $C = C(A) > 0$

Problem: Die Konstante C kann nicht effektiv berechnet werden!
Denn: Die Existenz von Siegel-Nullstellen (i. e. L-Nullstellen, die sehr nahe an $s = 1$ liegen) kann nicht ausgeschlossen werden.

Heath-Brown (1983): aus deren Existenz folgt die Zwillingsvermutung

Anwendung: Ford, Luca, Pomerance (2010): Die Gleichung $\varphi(a) = \sigma(b)$ hat unendlich viele Lösungen
(Erdős-Vermutung von 1959)

Beweisidee: Fallunterscheidung nach der Existenz von Siegel-Nullstellen

Verallgemeinerte Riemannsche Vermutung (GRH):

Sei $L(s,\chi)$ eine Dirichletsche L-Funktion. Dann liegen alle Nullstellen von $L(s,\chi)$ mit $0 \leq \operatorname{Re} s \leq 1$ auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Verallgemeinerte Riemannsche Vermutung (GRH):

Sei $L(s,\chi)$ eine Dirichletsche L-Funktion. Dann liegen alle Nullstellen von $L(s,\chi)$ mit $0 \leq \operatorname{Re} s \leq 1$ auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

GRH für L-Funktionen mod $q \leq x \Leftrightarrow \pi(x;q,a) = \dfrac{\operatorname{li}(x)}{\varphi(q)} + \mathrm{O}(x^{1/2}\log x)$

Verallgemeinerte Riemannsche Vermutung (GRH):

Sei $L(s,\chi)$ eine Dirichletsche L-Funktion. Dann liegen alle Nullstellen von $L(s,\chi)$ mit $0 \le \operatorname{Re} s \le 1$ auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

GRH für L-Funktionen mod $q \le x \Leftrightarrow \pi(x; q, a) = \dfrac{\operatorname{li}(x)}{\varphi(q)} + \mathrm{O}(x^{1/2} \log x)$

Diese Abschätzung ist nichttrivial für $q \le x^{1/2-\varepsilon}$ bzw. $x \ge q^{2+\varepsilon}$.

Verallgemeinerte Riemannsche Vermutung (GRH):

Sei $L(s,\chi)$ eine Dirichletsche L-Funktion. Dann liegen alle Nullstellen von $L(s,\chi)$ mit $0 \le \operatorname{Re} s \le 1$ auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

GRH für L-Funktionen mod $q \le x \Leftrightarrow \pi(x;q,a) = \dfrac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}(x^{1/2}\log x)$

Diese Abschätzung ist nichttrivial für $q \le x^{1/2-\varepsilon}$ bzw. $x \ge q^{2+\varepsilon}$.

Diplomarbeit B. Suger (2010): GRH für L-Reihen mod
$q \le \exp(\frac{\log 2}{2}\lfloor(\log x)^{3/5}(\log\log x)^{29/15}\rfloor)$, $(a,q)=1$
Dann: $\sum_{\substack{n \le x \\ n \equiv a \bmod q}} \mu(n) = \mathrm{O}(x^{1/2}\exp((\log x)^{3/5}(\log\log x)^{16/5+\varepsilon}))$

Fehler–Abschätzung „im Mittel“ über alle Moduln q:

Fehler–Abschätzung „im Mittel" über alle Moduln q:

Satz von Bombieri–Vinogradov (1966):

Für $A > 0$ und $Q \le x^{1/2}(\log x)^{-A-5/2}$ gilt:

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| = \mathrm{O}(x(\log x)^{-A}).$$

Fehler–Abschätzung „im Mittel“ über alle Moduln q:

Satz von Bombieri–Vinogradov (1966):

Für $A > 0$ und $Q \leq x^{1/2}(\log x)^{-A-5/2}$ gilt:

$$\sum_{q \leq Q} \max_{(a,q)=1} \max_{y \leq x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| = \mathrm{O}(x(\log x)^{-A}).$$

Korollar:

- Der PZS in Progressionen gilt für “fast alle” Moduln $q \leq Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$,

Fehler–Abschätzung „im Mittel“ über alle Moduln q:

Satz von Bombieri–Vinogradov (1966):

Für $A > 0$ und $Q \leq x^{1/2}(\log x)^{-A-5/2}$ gilt:

$$\sum_{q \leq Q} \max_{(a,q)=1} \max_{y \leq x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| = \mathrm{O}(x(\log x)^{-A}).$$

Korollar:

- Der PZS in Progressionen gilt für “fast alle” Moduln $q \leq Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$,
- Die GRH ist für “fast alle” Moduln $q \leq Q$ mit $x^{1/2-\delta} \leq Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$ erfüllt,

Fehler–Abschätzung „im Mittel“ über alle Moduln q:

Satz von Bombieri–Vinogradov (1966):

Für $A > 0$ und $Q \le x^{1/2}(\log x)^{-A-5/2}$ gilt:

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| = \mathrm{O}(x(\log x)^{-A}).$$

Korollar:

- Der PZS in Progressionen gilt für “fast alle” Moduln $q \le Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$,
- Die GRH ist für “fast alle” Moduln $q \le Q$ mit $x^{1/2-\delta} \le Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$ erfüllt,

die Anzahl der Ausnahmen beträgt $\mathrm{o}(Q)$.

Fehler–Abschätzung „im Mittel“ über alle Moduln q:

Satz von Bombieri–Vinogradov (1966):

Für $A > 0$ und $Q \leq x^{1/2}(\log x)^{-A-5/2}$ gilt:

$$\sum_{q \leq Q} \max_{(a,q)=1} \max_{y \leq x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\varphi(q)} \right| = \mathrm{O}(x(\log x)^{-A}).$$

Korollar:

- Der PZS in Progressionen gilt für “fast alle” Moduln $q \leq Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$,
- Die GRH ist für “fast alle” Moduln $q \leq Q$ mit $x^{1/2-\delta} \leq Q = \mathrm{O}(x^{1/2}(\log x)^{-A-5/2})$ erfüllt,

die Anzahl der Ausnahmen beträgt $\mathrm{o}(Q)$.

Elliott-Halberstam-Vermutung: Die BV-Abschätzung gilt sogar für $Q \leq x(\log x)^{-B}$

Aktuelle Anwendung:
Goldston, Pintz, Yıldırım (2007): Nachweis der "small gap conjecture"

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0,$$

sogar:

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty$$

Aktuelle Anwendung:
Goldston, Pintz, Yıldırım (2007): Nachweis der "small gap conjecture"

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0,$$

sogar:

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty$$

Unter Annahme der EH-Vermutung folgt die "bounded gap conjecture"

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 16.$$

Aktuelle Anwendung:
Goldston, Pintz, Yıldırım (2007): Nachweis der "small gap conjecture"

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0,$$

sogar:

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty$$

Unter Annahme der EH-Vermutung folgt die "bounded gap conjecture"

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \leq 16.$$

Methode: Neue Variante des Selberg-Siebes, Bombieri-Vinogradov

Verbesserungen des Satzes von Bombieri-Vinogradov:

- Nur marginale Verbesserung für festes a: Bombieri, Friedlander und Iwaniec (1987): Q-Bereich vergrößerbar, allerdings konnte der Exponent $1/2$ nicht vergrößert werden,

Verbesserungen des Satzes von Bombieri-Vinogradov:

- Nur marginale Verbesserung für festes a: Bombieri, Friedlander und Iwaniec (1987): Q-Bereich vergrößerbar, allerdings konnte der Exponent $1/2$ nicht vergrößert werden, es sei denn, man betrachtet nicht die Beträge der Differenzen, sondern bewichtet diese mit sehr speziellen Funktionen

Verbesserungen des Satzes von Bombieri-Vinogradov:

- Nur marginale Verbesserung für festes a: Bombieri, Friedlander und Iwaniec (1987): Q-Bereich vergrößerbar, allerdings konnte der Exponent $1/2$ nicht vergrößert werden, es sei denn, man betrachtet nicht die Beträge der Differenzen, sondern bewichtet diese mit sehr speziellen Funktionen
- Erweiterung auf kurze Intervalle: Perelli, Pintz, Salerno (1984)

Verbesserungen des Satzes von Bombieri-Vinogradov:

- Nur marginale Verbesserung für festes a: Bombieri, Friedlander und Iwaniec (1987): Q-Bereich vergrößerbar, allerdings konnte der Exponent $1/2$ nicht vergrößert werden, es sei denn, man betrachtet nicht die Beträge der Differenzen, sondern bewichtet diese mit sehr speziellen Funktionen
- Erweiterung auf kurze Intervalle: Perelli, Pintz, Salerno (1984)
- Ergebnis von Fiorilli (2010): Unter Berücksichtigung des Vorzeichens spielt die Arithmetik von $a \neq 0$ eine Rolle: Der Wert von

$$\frac{1}{\frac{\varphi(a)}{a} \frac{x}{M}} \sum_{\substack{q \leq \frac{x}{M} \\ (q,a)=1}} \left(\psi(x; q, a) - \frac{\psi(x)}{\varphi(q)} - \Lambda(a) \right)$$

  für $M = M(x) \leq \log^B x$ für $B > 0$ fest, ist klein, wenn a mindestens zwei Primfaktoren hat, und ansonsten von a und M abhängig.

Vermutungen aus dem Briefwechsel zwischen Euler und Goldbach (1742, Goldbachsche Vermutungen):

(a) Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen. (*binäres Problem*)

(b) Jede ungerade Zahl ≥ 7 ist Summe dreier Primzahlen. (*ternäres Problem*)

Vermutungen aus dem Briefwechsel zwischen Euler und Goldbach (1742, Goldbachsche Vermutungen):

(a) Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen. (*binäres Problem*)

(b) Jede ungerade Zahl ≥ 7 ist Summe dreier Primzahlen. (*ternäres Problem*)

Vermutung von Descartes (vor 1650):

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

Vermutungen aus dem Briefwechsel zwischen Euler und Goldbach (1742, Goldbachsche Vermutungen):

(a) Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen. (*binäres Problem*)

(b) Jede ungerade Zahl ≥ 7 ist Summe dreier Primzahlen. (*ternäres Problem*)

Vermutung von Descartes (vor 1650):

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

Es gilt: $a \Rightarrow b$, $a \Rightarrow c$, $c \Rightarrow b$,
die Umkehrungen können nicht gezeigt werden

Vermutungen aus dem Briefwechsel zwischen Euler und Goldbach (1742, Goldbachsche Vermutungen):

(a) Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen. (*binäres Problem*)

(b) Jede ungerade Zahl ≥ 7 ist Summe dreier Primzahlen. (*ternäres Problem*)

Vermutung von Descartes (vor 1650):

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

Es gilt: $a \Rightarrow b$, $a \Rightarrow c$, $c \Rightarrow b$,
die Umkehrungen können nicht gezeigt werden

Zwillingsvermutung von de Polignac (1849): Es gibt unendlich viele Primzahlpaare $p, p + 2k$

Vermutungen aus dem Briefwechsel zwischen Euler und Goldbach (1742, Goldbachsche Vermutungen):

(a) Jede gerade Zahl ≥ 4 ist Summe zweier Primzahlen. (*binäres Problem*)

(b) Jede ungerade Zahl ≥ 7 ist Summe dreier Primzahlen. (*ternäres Problem*)

Vermutung von Descartes (vor 1650):

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

Es gilt: $a \Rightarrow b$, $a \Rightarrow c$, $c \Rightarrow b$,
die Umkehrungen können nicht gezeigt werden

Zwillingsvermutung von de Polignac (1849): Es gibt unendlich viele Primzahlpaare $p, p + 2k$

Gibt es unendlich viele Sophie-Germain-Primzahlpaare $p, 2p + 1$?

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Satz von Vinogradov (1937):

Es gibt ein $n_0 \in \mathbb{N}$, eine Funktion $\mathcal{S}_3 : \mathbb{N} \to \mathbb{R}$ und reelle $c, C > 0$ mit $c < \mathcal{S}_3(n) < C$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r_3(n) = \mathcal{S}_3(n) \frac{n^2}{2(\log n)^3} + \mathrm{O}\left(\frac{n^2 \log \log n}{\log^4 n}\right),$$

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Satz von Vinogradov (1937):

Es gibt ein $n_0 \in \mathbb{N}$, eine Funktion $\mathcal{S}_3 : \mathbb{N} \to \mathbb{R}$ und reelle $c, C > 0$ mit $c < \mathcal{S}_3(n) < C$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r_3(n) = \mathcal{S}_3(n) \frac{n^2}{2(\log n)^3} + \mathrm{O}\Big(\frac{n^2 \log \log n}{\log^4 n}\Big),$$

$$\mathcal{S}_3(n) = \prod_{p \nmid n} \Big(1 + \frac{1}{(p-1)^3}\Big) \cdot \prod_{p \mid n} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Satz von Vinogradov (1937):

Es gibt ein $n_0 \in \mathbb{N}$, eine Funktion $\mathcal{S}_3 : \mathbb{N} \to \mathbb{R}$ und reelle $c, C > 0$ mit $c < \mathcal{S}_3(n) < C$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r_3(n) = \mathcal{S}_3(n) \frac{n^2}{2(\log n)^3} + \mathrm{O}\Big(\frac{n^2 \log\log n}{\log^4 n}\Big),$$

$$\mathcal{S}_3(n) = \prod_{p \nmid n} \Big(1 + \frac{1}{(p-1)^3}\Big) \cdot \prod_{p \mid n} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

Es ist $\mathcal{S}_3(n) = 0$ für gerades n.

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Satz von Vinogradov (1937):

Es gibt ein $n_0 \in \mathbb{N}$, eine Funktion $\mathcal{S}_3 : \mathbb{N} \to \mathbb{R}$ und reelle $c, C > 0$ mit $c < \mathcal{S}_3(n) < C$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r_3(n) = \mathcal{S}_3(n) \frac{n^2}{2(\log n)^3} + \mathrm{O}\Big(\frac{n^2 \log \log n}{\log^4 n}\Big),$$

$$\mathcal{S}_3(n) = \prod_{p \nmid n} \Big(1 + \frac{1}{(p-1)^3}\Big) \cdot \prod_{p \mid n} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

Es ist $\mathcal{S}_3(n) = 0$ für gerades n.

Chen, Wang (1989): $n_0 \geq 10^{43000}$

Sei $r_3(n)$ die Anzahl der Darstellungen, n als Summe dreier Primzahlen zu schreiben.

Satz von Vinogradov (1937):

Es gibt ein $n_0 \in \mathbb{N}$, eine Funktion $\mathcal{S}_3 : \mathbb{N} \to \mathbb{R}$ und reelle $c, C > 0$ mit $c < \mathcal{S}_3(n) < C$ für alle ungeraden n, so dass für alle $n \geq n_0$ gilt:

$$r_3(n) = \mathcal{S}_3(n) \frac{n^2}{2(\log n)^3} + \mathrm{O}\Big(\frac{n^2 \log\log n}{\log^4 n} \Big),$$

$$\mathcal{S}_3(n) = \prod_{p \nmid n} \Big(1 + \frac{1}{(p-1)^3} \Big) \cdot \prod_{p \mid n} \Big(1 - \frac{1}{(p-1)^2} \Big).$$

Es ist $\mathcal{S}_3(n) = 0$ für gerades n.

Chen, Wang (1989): $n_0 \geq 10^{43000}$

Deshouillers, Effinger, te Riele, Zinoviev (1997), Saouter (1998):

Unter Annahme der GRH: $n_0 \geq 7$

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n\leq x}\left|r_2(n)-\mathcal{S}_2(n)\frac{n}{\log^2 n}\right|^2=\mathrm{O}\Big(\frac{x^3}{\log^A x}\Big)$$

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n\leq x}\left|r_2(n)-\mathcal{S}_2(n)\frac{n}{\log^2 n}\right|^2=\mathrm{O}\Big(\frac{x^3}{\log^A x}\Big)$$

Es ist

$$\mathcal{S}_2(n)=\prod_{p|n}\Big(1+\frac{1}{p-1}\Big)\prod_{p\nmid n}\Big(1-\frac{1}{(p-1)^2}\Big)$$

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n \leq x} \left| r_2(n) - \mathcal{S}_2(n) \frac{n}{\log^2 n} \right|^2 = \mathrm{O}\Big(\frac{x^3}{\log^A x} \Big)$$

Es ist

$$\mathcal{S}_2(n) = \prod_{p|n} \Big(1 + \frac{1}{p-1} \Big) \prod_{p \nmid n} \Big(1 - \frac{1}{(p-1)^2} \Big)$$

Korollar: Die Anzahl der Ausnahmen $\leq x$ im binären Problem ist $O(x/\log^A x)$.

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n \le x} \left| r_2(n) - \mathcal{S}_2(n) \frac{n}{\log^2 n} \right|^2 = \mathrm{O}\Big(\frac{x^3}{\log^A x} \Big)$$

Es ist

$$\mathcal{S}_2(n) = \prod_{p|n} \Big(1 + \frac{1}{p-1} \Big) \prod_{p \nmid n} \Big(1 - \frac{1}{(p-1)^2} \Big)$$

Korollar: Die Anzahl der Ausnahmen $\le x$ im binären Problem ist $O(x/\log^A x)$.

Pintz (2010+): Die Anzahl dieser Ausnahmen ist $\mathrm{O}(x^{2/3})$.

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n \le x} \left| r_2(n) - \mathcal{S}_2(n) \frac{n}{\log^2 n} \right|^2 = \mathrm{O}\Big(\frac{x^3}{\log^A x} \Big)$$

Es ist

$$\mathcal{S}_2(n) = \prod_{p|n} \Big(1 + \frac{1}{p-1} \Big) \prod_{p \nmid n} \Big(1 - \frac{1}{(p-1)^2} \Big)$$

Korollar: Die Anzahl der Ausnahmen $\le x$ im binären Problem ist $O(x/\log^A x)$.

Pintz (2010+): Die Anzahl dieser Ausnahmen ist $\mathrm{O}(x^{2/3})$.

Chen (1966/1973): Jede hinreichend große gerade Zahl n kann als $n = p + P_2$ geschrieben werden, wobei p prim und P_2 aus höchstens zwei Primfaktoren zusammengesetzt ist.

Der Vinogradov-Beweis liefert folgendes Mittelwertergebnis für das binäre Problem:

$$\sum_{n\le x}\left|r_2(n)-\mathcal{S}_2(n)\frac{n}{\log^2 n}\right|^2=\mathrm{O}\Big(\frac{x^3}{\log^A x}\Big)$$

Es ist

$$\mathcal{S}_2(n)=\prod_{p|n}\Big(1+\frac{1}{p-1}\Big)\prod_{p\nmid n}\Big(1-\frac{1}{(p-1)^2}\Big)$$

Korollar: Die Anzahl der Ausnahmen $\le x$ im binären Problem ist $O(x/\log^A x)$.

Pintz (2010+): Die Anzahl dieser Ausnahmen ist $\mathrm{O}(x^{2/3})$.

Chen (1966/1973): Jede hinreichend große gerade Zahl n kann als $n=p+P_2$ geschrieben werden, wobei p prim und P_2 aus höchstens zwei Primfaktoren zusammengesetzt ist.
Es gibt unendlich viele Primzahlen p mit $p+2=P_2$.

Mittelwertergebnis zum ternären Goldbachproblem mit einer Primzahl in Progressionen (Tolev 1997/H. 2006):

$$\sum_{q \le \frac{n^{1/2}}{\log^B n}} \max_{a,(a,q)=1} \Big| \sum_{\substack{p_1+p_2+p_3=n \\ p_1 \equiv a\,(q)}} 1 - \frac{n^2 \mathcal{S}_{3,a,q}(n)}{2\varphi(q) \log^3 n} \Big| = \mathrm{O}\Big(\frac{n^2}{\log^A n} \Big)$$

Mittelwertergebnis zum ternären Goldbachproblem mit einer Primzahl in Progressionen (Tolev 1997/H. 2006):

$$\sum_{q \leq \frac{n^{1/2}}{\log^B n}} \max_{a,(a,q)=1} \Bigg| \sum_{\substack{p_1+p_2+p_3=n \\ p_1 \equiv a\,(q)}} 1 - \frac{n^2 \mathcal{S}_{3,a,q}(n)}{2\varphi(q)\log^3 n} \Bigg| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Auch zwei Primzahlen möglich (H. 2008):

$$\sum_{\substack{q_1,q_2 \\ \leq \frac{n^{1/2}}{\log^B n}}} \max_{\substack{a_1,a_2 \\ (a_i,q_i)=1 \\ i=1,2}} \Bigg| \sum_{\substack{p_1+p_2+p_3=n \\ p_i \equiv a_i\,(q_i), \\ i=1,2}} 1 - \frac{n^2 \mathcal{S}_{3,a_1,q_1,a_2,q_2}(n)}{2\varphi(q_1)\varphi(q_2)\log^3 n} \Bigg| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Mittelwertergebnis zum ternären Goldbachproblem mit einer Primzahl in Progressionen (Tolev 1997/H. 2006):

$$\sum_{q \leq \frac{n^{1/2}}{\log^B n}} \max_{a,(a,q)=1} \Bigg| \sum_{\substack{p_1+p_2+p_3=n \\ p_1 \equiv a\,(q)}} 1 - \frac{n^2 \mathcal{S}_{3,a,q}(n)}{2\varphi(q)\log^3 n} \Bigg| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Auch zwei Primzahlen möglich (H. 2008):

$$\sum_{\substack{q_1,q_2 \\ \leq \frac{n^{1/2}}{\log^B n}}} \max_{\substack{a_1,a_2 \\ (a_i,q_i)=1 \\ i=1,2}} \Bigg| \sum_{\substack{p_1+p_2+p_3=n \\ p_i \equiv a_i\,(q_i), \\ i=1,2}} 1 - \frac{n^2 \mathcal{S}_{3,a_1,q_1,a_2,q_2}(n)}{2\varphi(q_1)\varphi(q_2)\log^3 n} \Bigg| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Methoden hier: Siebmethoden, Bombieri-Vinogradov

Mittelwertergebnis zum ternären Goldbachproblem mit einer Primzahl in Progressionen (Tolev 1997/H. 2006):

$$\sum_{q\le \frac{n^{1/2}}{\log^B n}} \max_{a,(a,q)=1} \Big| \sum_{\substack{p_1+p_2+p_3=n\\ p_1\equiv a\,(q)}} 1 - \frac{n^2\mathcal{S}_{3,a,q}(n)}{2\varphi(q)\log^3 n}\Big| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Auch zwei Primzahlen möglich (H. 2008):

$$\sum_{\substack{q_1,q_2\\ \le \frac{n^{1/2}}{\log^B n}}} \max_{\substack{a_1,a_2\\ (a_i,q_i)=1\\ i=1,2}} \Big| \sum_{\substack{p_1+p_2+p_3=n\\ p_i\equiv a_i\,(q_i),\\ i=1,2}} 1 - \frac{n^2\mathcal{S}_{3,a_1,q_1,a_2,q_2}(n)}{2\varphi(q_1)\varphi(q_2)\log^3 n}\Big| = \mathrm{O}\Big(\frac{n^2}{\log^A n}\Big)$$

Methoden hier: Siebmethoden, Bombieri-Vinogradov
Korollar (Meng 2007/2009): Fast alle geraden $n \not\equiv 2\,(6)$ lassen sich schreiben als $n = p_1 + p_2$, wobei $p_1 + 2 = P_2$ ist.

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen “in kurzen Intervallen”,

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen "in kurzen Intervallen", Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen "in kurzen Intervallen", Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Damit sind die Meng-Korollare verallgemeinerbar:

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen "in kurzen Intervallen", Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Damit sind die Meng-Korollare verallgemeinerbar:

Korollar 1: Fast alle geraden $n \not\equiv 2\,(6)$ sind schreibbar als $n = p_1 + p_2$ mit Primzahlen p_1, p_2, so dass $p_1 + 2 = P_3$ wobei p_1 in einem kurzen Intervall liegt.

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen "in kurzen Intervallen", Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Damit sind die Meng-Korollare verallgemeinerbar:

Korollar 1: Fast alle geraden $n \not\equiv 2\,(6)$ sind schreibbar als $n = p_1 + p_2$ mit Primzahlen p_1, p_2, so dass $p_1 + 2 = P_3$ wobei p_1 in einem kurzen Intervall liegt.

Korollar 2: Große ungerade n mit $n \not\equiv 1\,(6)$ sind schreibbar als $n = p_1 + p_2 + p_3$ mit Primzahlen p_1, p_2, p_3, so dass $(p_1 + 2)(p_2 + 2) = P_5$, wobei p_1, p_2 beide in kurzen Intervallen.

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen “in kurzen Intervallen”, Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Damit sind die Meng-Korollare verallgemeinerbar:

Korollar 1: Fast alle geraden $n \not\equiv 2\,(6)$ sind schreibbar als $n = p_1 + p_2$ mit Primzahlen p_1, p_2, so dass $p_1 + 2 = P_3$ wobei p_1 in einem kurzen Intervall liegt.

Korollar 2: Große ungerade n mit $n \not\equiv 1\,(6)$ sind schreibbar als $n = p_1 + p_2 + p_3$ mit Primzahlen p_1, p_2, p_3, so dass $(p_1 + 2)(p_2 + 2) = P_5$, wobei p_1, p_2 beide in kurzen Intervallen.

Korollar 3: Ist $X^\theta = Y$ mit $\theta \geq 0.922$, so gibt es $\geq cY(\log Y)^{-3}$ viele Primzahlen p mit $p + 2 = P_2$ und $X < p \leq X + Y$.

Neu (H., eingereicht): derartige Mittelwertsätze für das binäre Problem/Primzahlzwillinge gelten auch mit Primzahlen "in kurzen Intervallen", Methode: Verallgemeinerung von BV in kurzen Intervallen nach Perelli, Pintz, Salerno (1984)

Damit sind die Meng-Korollare verallgemeinerbar:

Korollar 1: Fast alle geraden $n \not\equiv 2\,(6)$ sind schreibbar als $n = p_1 + p_2$ mit Primzahlen p_1, p_2, so dass $p_1 + 2 = P_3$ wobei p_1 in einem kurzen Intervall liegt.

Korollar 2: Große ungerade n mit $n \not\equiv 1\,(6)$ sind schreibbar als $n = p_1 + p_2 + p_3$ mit Primzahlen p_1, p_2, p_3, so dass $(p_1 + 2)(p_2 + 2) = P_5$, wobei p_1, p_2 beide in kurzen Intervallen.

Korollar 3: Ist $X^\theta = Y$ mit $\theta \geq 0.922$, so gibt es $\geq cY(\log Y)^{-3}$ viele Primzahlen p mit $p + 2 = P_2$ und $X < p \leq X + Y$.

Rekord bisher: $\theta \geq 0.971$ von Wu (2004)

Anwendung eines derartigen, aber schwächeren Primzahlzwillings-Mittelwertsatzes bisher:

Anwendung eines derartigen, aber schwächeren Primzahlzwillings-Mittelwertsatzes bisher:

Balog, Cojocaru, David (2010+):
Die Koblitzsche Vermutung gilt im Mittel, d. h. bezeichnet $\mathcal{C}$ die Menge der elliptischen Kurven $E(a,b) : Y^2 = X^3 + aX + b$, $a, b \in \mathbb{Z}$, mit $|a| \leq A$, $|b| \leq B$, $A, B > x^{1/2+\varepsilon}$, $AB > x^{3/2+\varepsilon}$, so gilt

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) \sim \mathfrak{C} \frac{x}{\log^2 x}$$

für die "Zwillingszählfunktion"

$$\pi_E^{\text{twin}}(x) := \#\{p \leq x \; ; \; |E(\mathbb{F}_p)| \text{ ist prim}\}.$$

Anwendung eines derartigen, aber schwächeren Primzahlzwillings-Mittelwertsatzes bisher:

Balog, Cojocaru, David (2010+):
Die Koblitzsche Vermutung gilt im Mittel, d. h. bezeichnet $\mathcal{C}$ die Menge der elliptischen Kurven $E(a,b) : Y^2 = X^3 + aX + b$, $a, b \in \mathbb{Z}$, mit $|a| \leq A$, $|b| \leq B$, $A, B > x^{1/2+\varepsilon}$, $AB > x^{3/2+\varepsilon}$, so gilt

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) \sim \mathfrak{C} \frac{x}{\log^2 x}$$

für die "Zwillingszählfunktion"

$$\pi_E^{\text{twin}}(x) := \#\{p \leq x \; ; \; |E(\mathbb{F}_p)| \text{ ist prim}\}.$$

Primzahlen zählen

Primzahlen in Progressionen zählen

Die Goldbachsche Vermutung und Primzahlzwillinge

Primzahlmuster

Verallgemeinerung des Zwillings-, Goldbach- und
Sophie-Germain-Zwillingsproblems:

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems:

Prim-k-tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1x + b_1, a_2x + b_2, \ldots, a_kx + b_k \in \mathbb{Z}[x]$, die $a_i > 0$, zulässig, d. h. keine Primzahl teilt alle $\prod_{i=1}^{k}(a_in + b_i)$, $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1n + b_1, a_2n + b_2, \ldots, a_kn + b_k$ prim.

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems:

Prim-k-tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1x + b_1, a_2x + b_2, \ldots, a_kx + b_k \in \mathbb{Z}[x]$, die $a_i > 0$, zulässig, d. h. keine Primzahl teilt alle $\prod_{i=1}^{k}(a_in + b_i)$, $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1n + b_1, a_2n + b_2, \ldots, a_kn + b_k$ prim.

Bisher erst $k = 1$ bewiesen. ($=$ Satz von Dirichlet)

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems:

Prim-k-tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1x + b_1, a_2x + b_2, \ldots, a_kx + b_k \in \mathbb{Z}[x]$, die $a_i > 0$, zulässig, d. h. keine Primzahl teilt alle $\prod_{i=1}^{k}(a_in + b_i)$, $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1n + b_1, a_2n + b_2, \ldots, a_kn + b_k$ prim.

Bisher erst $k = 1$ bewiesen. (= Satz von Dirichlet)

Balog (1990): Prim-k-tupel-Vermutung gilt im Mittel, u.a.: Es gibt unendlich viele $3 \times 3 \times 3$-Würfel aus verschiedenen Primzahlen, bei der jede Zeile und Spalte und "Säule" aus Primzahlen einer arithmetischen Progression besteht. ("Balog-Würfel")

Beispiel für einen Balog-Würfel (nach Granville 2007):

47	383	719
179	431	683
311	479	647

149	401	653
173	347	521
197	293	389

251	419	587
167	263	359
83	107	131

Satz von Green-Tao (2007):
Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

Satz von Green-Tao (2007):
Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \ldots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Satz von Green-Tao (2007):
Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \ldots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Beispiel: $5, 11, 17, 23, 29,$ Länge 5

Satz von Green-Tao (2007):
Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \ldots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Beispiel: $5, 11, 17, 23, 29$, Länge 5

$\{199 + 210n\,;\ 0 \leq n \leq 9\}$, Länge 10

Satz von Green-Tao (2007):
Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \ldots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Beispiel: $5, 11, 17, 23, 29$, Länge 5

$\{199 + 210n\ ;\ 0 \leq n \leq 9\}$, Länge 10

Rekord (Frind, Jobling, Underwood): Länge $k = 23$:
$\{56211383760397 + n \cdot 44546738095860; 0 \leq n \leq 22\}$

Satz von Green-Tao (2007):

Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \ldots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Beispiel: $5, 11, 17, 23, 29$, Länge 5

$\{199 + 210n \,;\ 0 \leq n \leq 9\}$, Länge 10

Rekord (Frind, Jobling, Underwood): Länge $k = 23$:
$\{56211383760397 + n \cdot 44546738095860; 0 \leq n \leq 22\}$

Der Satz von Green-Tao zeigt: Es gibt eine Primzahl-AP der Länge k mit Einträgen unterhalb von $2^{2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}}$

Satz von Green-Tao (2007):

Es gibt unendlich viele lineare Polynome $f(x) = ax + b \in \mathbb{N}[x]$, für die $f(0), f(1), \dots, f(k-1)$ alle prim sind.
(D. h. es gibt unendlich viele arithmetische Progressionen $b, b+a, b+2a, \dots, b+(k-1)a$ der Länge k, die nur aus Primzahlen bestehen.)

Beispiel: $5, 11, 17, 23, 29$, Länge 5

$\{199 + 210n\ ;\ 0 \leq n \leq 9\}$, Länge 10

Rekord (Frind, Jobling, Underwood): Länge $k = 23$:
$\{56211383760397 + n \cdot 44546738095860; 0 \leq n \leq 22\}$

Der Satz von Green-Tao zeigt: Es gibt eine Primzahl-AP der Länge k mit Einträgen unterhalb von $2^{2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}}$

Diese Schranke müsste eher etwa $k!$ sein.

Korollare aus dem Satz von Green-Tao:

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

(Erinnerung: $x^2 + x + 41$ ist prim für $x = 0, 1, 2, \ldots, 39$.)

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

(Erinnerung: $x^2 + x + 41$ ist prim für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren $a, b \in \mathbb{Z}$, für die $aj + b$ prim ist für $0 \leq j \leq k^2 + k$, also ist $a(i^2 + i) + b$ prim für $0 \leq i \leq k$, setze $f(x) = ax^2 + ax + b$. $\square$

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

(Erinnerung: $x^2 + x + 41$ ist prim für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren $a, b \in \mathbb{Z}$, für die $aj + b$ prim ist für $0 \leq j \leq k^2 + k$, also ist $a(i^2 + i) + b$ prim für $0 \leq i \leq k$, setze $f(x) = ax^2 + ax + b$. $\square$

Ungelöst: Quadratische *normierte* Polynome?

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

(Erinnerung: $x^2 + x + 41$ ist prim für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren $a, b \in \mathbb{Z}$, für die $aj + b$ prim ist für $0 \leq j \leq k^2 + k$, also ist $a(i^2 + i) + b$ prim für $0 \leq i \leq k$, setze $f(x) = ax^2 + ax + b$. $\square$

Ungelöst: Quadratische *normierte* Polynome?

Korollar 2: Es gibt unendlich viele k^d-Balog-Würfel.

Korollare aus dem Satz von Green-Tao:

Korollar 1: Für $k \geq 3$ gibt es unendlich viele quadratische Polynome $f(x) \in \mathbb{Z}[x]$ mit $f(0), f(1), \ldots, f(k)$ prim.

(Erinnerung: $x^2 + x + 41$ ist prim für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren $a, b \in \mathbb{Z}$, für die $aj + b$ prim ist für $0 \leq j \leq k^2 + k$, also ist $a(i^2 + i) + b$ prim für $0 \leq i \leq k$, setze $f(x) = ax^2 + ax + b$. $\square$

Ungelöst: Quadratische *normierte* Polynome?

Korollar 2: Es gibt unendlich viele k^d-Balog-Würfel.

Korollar 3: Es gibt unendlich viele magische $k \times k$-Quadrate aus Primzahlen.

Beweis des Satzes von Green-Tao:

Beweis des Satzes von Green-Tao:

1. Teil:

Verallgemeinerung des Satzes von Szemerédi zum Satz von Szemerédi-Green-Tao:

Beweis des Satzes von Green-Tao:

1. Teil:
Verallgemeinerung des Satzes von Szemerédi zum Satz von Szemerédi-Green-Tao: Der Beweis ist ein Mix aus harmonischer Analysis und Ergodentheorie.

Beweis des Satzes von Green-Tao:

1. Teil:
Verallgemeinerung des Satzes von Szemerédi zum Satz von Szemerédi-Green-Tao: Der Beweis ist ein Mix aus harmonischer Analysis und Ergodentheorie.

2. Teil:
Der Satz von Szemerédi-Green-Tao lässt sich (mit Tricks!) für die Menge der Primzahlen anwenden.

Beweis des Satzes von Green-Tao:

1. Teil:
Verallgemeinerung des Satzes von Szemerédi zum Satz von Szemerédi-Green-Tao: Der Beweis ist ein Mix aus harmonischer Analysis und Ergodentheorie.

2. Teil:
Der Satz von Szemerédi-Green-Tao lässt sich (mit Tricks!) für die Menge der Primzahlen anwenden.

Für den 2. Teil: Siebmethoden nach Goldston, Yıldırım: eine Variante des bekannten Selberg-Siebs aus der Siebtheorie

Vielen Dank!