Arithmetische Progressionen von Primzahlen

Sei $\mathbb{N} := \{1, 2, 3, \dots\}$ die Menge der natürlichen Zahlen.

Definition

Eine Primzahl ist eine natürliche Zahl > 1, die nur durch 1 und durch sich selbst teilbar ist.

Beispiel

$$2, 3, 5, 7, 11, \dots, 2^{32582657} - 1, \dots$$

Sei $\mathbb{N} := \{1, 2, 3, \dots\}$ die Menge der natürlichen Zahlen.

Definition

Eine Primzahl ist eine natürliche Zahl > 1, die nur durch 1 und durch sich selbst teilbar ist.

Beispiel

$$2, 3, 5, 7, 11, \dots, 2^{32582657} - 1, \dots$$

Theorem (Eindeutige Primfaktorzerlegung)

Jede natürliche Zahl lässt sich als Produkt von Primzahlen schreiben, und diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

Es gibt unendlich viele Primzahlen. Sogar:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots=\sum_{p \text{ Primzahl}}\frac{1}{p} \text{ divergiert.}$$

Es gibt unendlich viele Primzahlen. Sogar:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots=\sum_{p \text{ Primzahl}}\frac{1}{p} \text{ divergiert.}$$

Viele andere Fragen über die Struktur der Menge der Primzahlen sind offen, zum Beispiel

Vermutung

Es gibt unendlich viele Primzahlzwillinge, also Primzahlen p, so dass auch $p+2$ eine Primzahl ist.

Definition

Eine arithmetische Progression von Primzahlen der Länge k ist eine Folge $p_1, p_2, \ldots, p_k$ von Primzahlen, derart dass je zwei aufeinander folgende Glieder der Folge den gleichen Abstand haben:

$$p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1} \neq 0$$

Definition

Eine arithmetische Progression von Primzahlen der Länge k ist eine Folge $p_1, p_2, \ldots, p_k$ von Primzahlen, derart dass je zwei aufeinander folgende Glieder der Folge den gleichen Abstand haben:

$$p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1} \neq 0$$

Beispiel

$5, 11, 17, 23, 29$ (Länge 5, Abstand 6)

$5 + 12 \cdot i, \quad i = 0, 1, \ldots, 4.$

$56.211.383.760.397 + 44.546.738.095.860i, \ i = 0, 1, \ldots, 22$

(M. Frind, P. Jobling, P. Underwood 2004)

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156
157	158	159	160	161	162	163	164	165	166	167	168
169	170	171	172	173	174	175	176	177	178	179	180

Theorem (Green, Tao 2004)

Zu jeder natürlichen Zahl k gibt es unendlich viele arithmetische Progressionen von Primzahlen der Länge k.

Theorem (Green, Tao 2004)

Zu jeder natürlichen Zahl k gibt es unendlich viele arithmetische Progressionen von Primzahlen der Länge k.

Vorher bekannte Resultate:

van der Corput 1939: Es gibt unendlich viele arithmetische Progressionen von Primzahlen der Länge 3.

Offensichtliche Einschränkungen:
Ist $p, p + r, \ldots, p + (k-1)r$ eine AP von Primzahlen der Länge k, mit Abstand r, so gilt

Alle Primzahlen $< k$ teilen r.

Offensichtliche Einschränkungen:
Ist $p, p+r, \ldots, p+(k-1)r$ eine AP von Primzahlen der Länge k, mit Abstand r, so gilt

Alle Primzahlen $< k$ teilen r.

Beispiel (k=23)

- $r \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 223.092.870$
- Frind, Jobling, Underwood: $r = 44.546.738.095.860$

Offensichtliche Einschränkungen:
Ist $p, p+r, \ldots, p+(k-1)r$ eine AP von Primzahlen der Länge k, mit Abstand r, so gilt

Alle Primzahlen $< k$ teilen r.

Beispiel (k=23)

- $r \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 223.092.870$
- Frind, Jobling, Underwood: $r = 44.546.738.095.860$

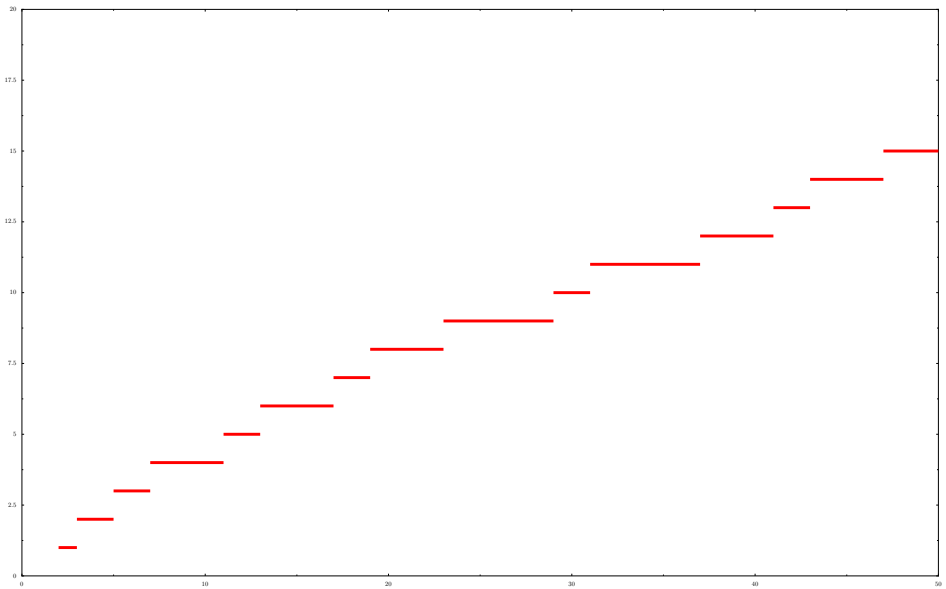
Abschätzung nach oben

- Green, Tao: möglich ist $p+(k-1)r \leq 2^{2^{2^{2^{2^{2^{100k}}}}}}$
- Vermutung: möglich ist $p+(k-1)r \leq k!+1$,
  für $k = 23$: $23!+1 = 25.852.016.738.884.976.640.001$

Der Primzahlsatz

Sei

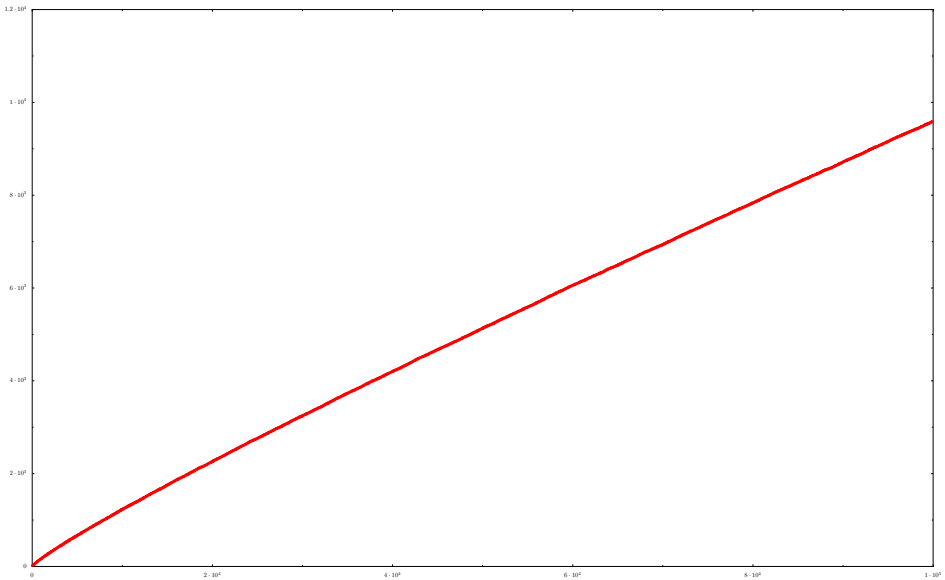
$$\pi(x) = |\{p \in \mathbb{N};\ p \text{ Primzahl}, p \leq x\}|.$$



Der Primzahlsatz

Sei

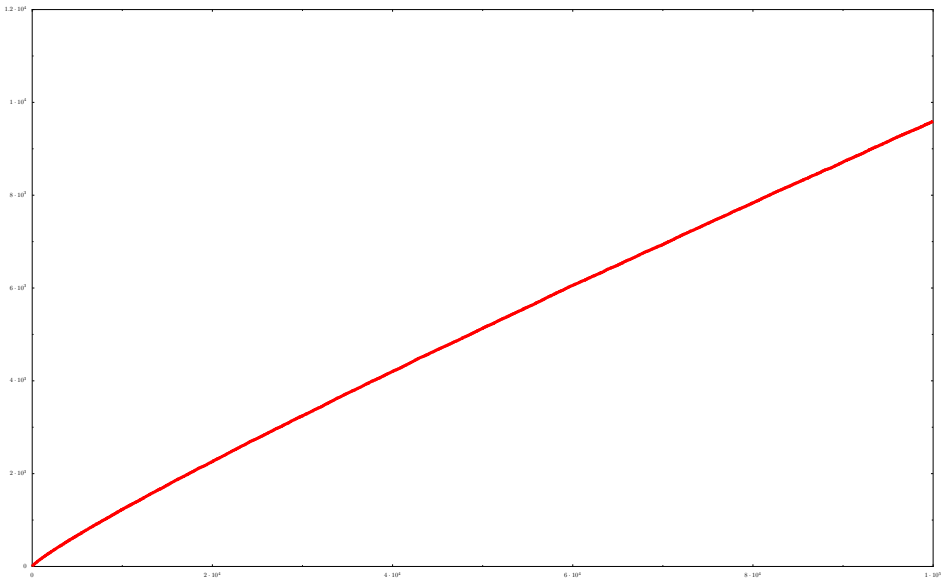
$$\pi(x) = |\{p \in \mathbb{N};\ p \text{ Primzahl}, p \leq x\}|.$$



Der Primzahlsatz

Sei

$$\pi(x) = |\{p \in \mathbb{N};\ p \text{ Primzahl}, p \leq x\}|.$$



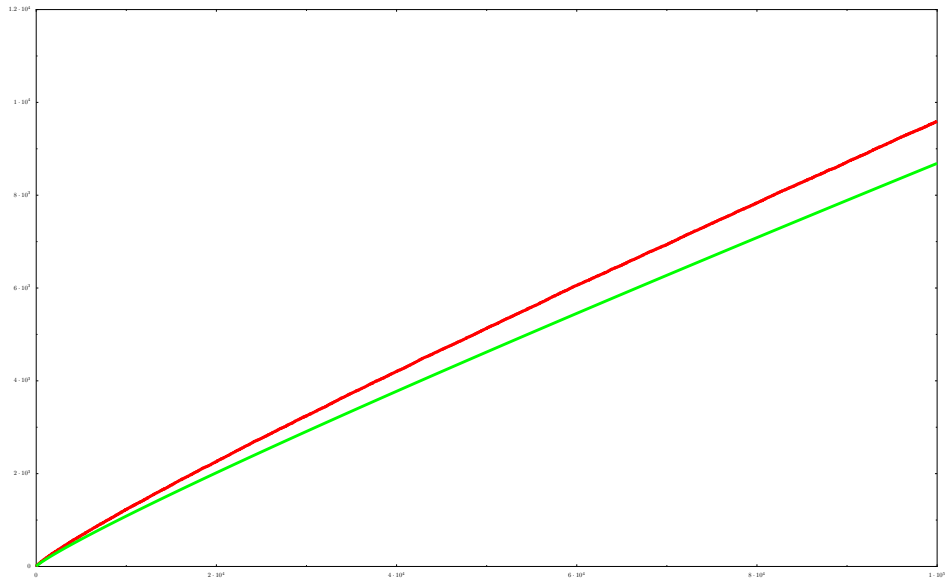
Theorem (Hadamard, de la Vallée-Poussin 1896)

$$\pi(x) \sim \frac{x}{\log x}.$$

Der Primzahlsatz

Sei

$$\pi(x) = |\{p \in \mathbb{N};\ p \text{ Primzahl}, p \leq x\}|.$$



Theorem (Hadamard, de la Vallée-Poussin 1896)

$$\pi(x) \sim \frac{x}{\log x}.$$

Die Hardy-Littlewood-Vermutung

Wir können den Primzahlsatz benutzen, um eine **heuristische Überlegung** durchzuführen, wie viele arithmetische Progressionen von Primzahlen wir erwarten sollten.

Die Hardy-Littlewood-Vermutung

Wir können den Primzahlsatz benutzen, um eine **heuristische Überlegung** durchzuführen, wie viele arithmetische Progressionen von Primzahlen wir erwarten sollten.

"Wahrscheinlichkeit", dass $x \in \{1, 2, \ldots, N\}$ prim ist: $\frac{1}{log(N)}$

Sei $1 \leq r \leq N$. Wir können hoffen, dass die Ereignisse, dass x bzw. $x + r$ prim sind, im wesentlichen unabhängig sind, also

$$P(x \text{ prim und } x + r \text{ prim}) = P(x \text{ prim})P(x + r \text{ prim}) = \frac{1}{\log(N)^2}.$$

Wir führen das fort, lassen außerdem den Startpunkt x und den Abstand r variieren, und erhalten heuristisch, dass für x, r im Bereich $\{1, 2, \ldots, N\}$ ungefähr

$$\frac{N^2}{\log(N)^k}$$

arithmetische Progressionen von Primzahlen der Länge k existieren sollten.

Wir führen das fort, lassen außerdem den Startpunkt x und den Abstand r variieren, und erhalten heuristisch, dass für x, r im Bereich $\{1, 2, \ldots, N\}$ ungefähr

$$\frac{N^2}{\log(N)^k}$$

arithmetische Progressionen von Primzahlen der Länge k existieren sollten.

Diese Argumentation ist offensichtlich zu naiv: wir haben schon gesehen, dass r von allen Primzahlen $\leq k$ geteilt werden muss.

Wir führen das fort, lassen außerdem den Startpunkt x und den Abstand r variieren, und erhalten heuristisch, dass für x, r im Bereich $\{1, 2, \ldots, N\}$ ungefähr

$$\frac{N^2}{\log(N)^k}$$

arithmetische Progressionen von Primzahlen der Länge k existieren sollten.

Diese Argumentation ist offensichtlich zu naiv: wir haben schon gesehen, dass r von allen Primzahlen $\leq k$ geteilt werden muss.

Vermutung (Hardy, Littlewood 1923)

Für alle k gilt

$$|\{\textit{AP von PZ der Länge } k \textit{ mit Startpkt., Abstand in } \{1, \ldots, N\}\}| = \frac{\gamma_k N^2}{\log(N)^k}(1 + o(1)).$$

Die Vermutung von Erdös und Turán

Statt nach der Struktur der Menge aller Primzahlen zu fragen, kann man auch fragen, unter welchen Bedingungen eine Teilmenge $A \subseteq \mathbb{N}$ arithmetische Progressionen beliebiger Länge enthalten muss.

Die Vermutung von Erdös und Turán

Statt nach der Struktur der Menge aller Primzahlen zu fragen, kann man auch fragen, unter welchen Bedingungen eine Teilmenge $A \subseteq \mathbb{N}$ arithmetische Progressionen beliebiger Länge enthalten muss.

Vermutung (Erdös, Turán 1936)

Ist $A \subseteq \mathbb{N}$ eine Teilmenge, so dass

$$\sum_{a \in A} \frac{1}{a} \quad \textit{divergiert},$$

dann enthält A arithmetische Progressionen beliebiger Länge.

Der Satz von Szemerédi

Theorem (Szemerédi 1975)

Sei $A \subseteq \mathbb{N}$ eine Teilmenge mit positiver oberer Dichte, d. h.

$$\limsup_{N \to \infty} \frac{|A \cap [1, N]|}{N} > 0$$

Dann enthält A arithmetische Progressionen beliebiger Länge.

Allerdings ist die Dichte von $\{p \text{ Primzahl}\} \subset \mathbb{N}$ gleich 0.

Furstenbergs Beweis

Theorem (Furstenberg 1977)

Sei $(X, \mathscr{B}, \mu)$ ein Wahrscheinlichkeitsraum, $T : X \longrightarrow X$ eine maßerhaltende Abbildung, d. h. $\mu(T^{-1}(M)) = \mu(M)$ für alle $M \in \mathscr{B}$. Seien $A \in \mathscr{B}$ mit $\mu(A) > 0$ und $k \in \mathbb{N}$.
Dann existiert $n \in \mathbb{N}$, so dass

$$\mu\Big(\bigcap_{j=0}^{k-1} T^{-jn} A\Big) > 0.$$

Wende dies an wie folgt: Sei $\Lambda \subseteq \mathbb{Z}$ eine Teilmenge mit positiver Dichte.

- Definiere $T : \mathscr{P}(\mathbb{Z}) \longrightarrow \mathscr{P}(\mathbb{Z})$ durch $TM := \{n \in \mathbb{Z};\ n+1 \in M\}$.
- Sei X der Abschluss von $\{T^n\Lambda;\ n \in \mathbb{Z}\}$ in $\mathscr{P}(\mathbb{Z})$,
- sei $A = \{M \in X;\ 0 \in M\}$.
- Definiere ein T-invariantes Maß μ auf X mit $\mu(A) > 0$ und folgere

$$T^{n'}\Lambda \in \bigcap_{j=0}^{k-1} T^{-jn}A$$

für n, n' geeignet.

Der schwach mischende Fall

Bernoulli-System:

Seien $p_1, \ldots, p_r \in \mathbb{R}_{\geq 0}$ mit $\sum_{i=1}^{r} p_i = 1$.

Betrachte $(X, \mathscr{B}, \mu, T)$ gegeben durch

- $X = \{(\omega_i)_{i \in \mathbb{Z}}; \omega_i \in \{1, 2, \ldots, r\}\}$,
- $\mathscr{B}$ die kleinste σ-Algebra, so dass alle Abb. $(\omega_i)_i \mapsto \omega_{i_0}$ messbar sind,
- μ das Produktmaß

$$\mu(\omega_{i_1} = j_1, \omega_{i_2} = j_2, \ldots, \omega_{i_n} = j_n) = p_{j_1} \cdots p_{j_n}.$$

- $T((\omega_i)_i) = (\omega_{i+1})_i$.

Satz

Sei $(X, \mathscr{B}, \mu, T)$ ein Bernoulli-System, und seien $A_0, \ldots, A_k \in \mathscr{B}$. Dann gilt

$$\lim_{n \to \infty} \mu(A_0 \cap T^{-n} A_1 \cap \cdots \cap T^{-kn} A_k) = \mu(A_0)\mu(A_1) \cdots \mu(A_k).$$

Der kompakte Fall

Sei $X = \mathbb{R}/\mathbb{Z}$, $\mathscr{B}$ die Borel-σ-Algebra und μ das vom Lebesgue-Maß auf $\mathbb{R}$ induzierte W-Maß auf X. Sei $T : X \longrightarrow X$ gegeben durch $x \mapsto x + \alpha$, $\alpha \in \mathbb{R}$.

Satz

In dieser Situation gilt für alle $k \geq 1$:

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu(A \cap T^{-n}A \cap \cdots \cap T^{-kn}A) > 0.$$

Umformulierung von Szemerédis Satz

Identifiziere $\{1, \ldots, N\} = \mathbb{Z}/N$.

Für eine Funktion $f : \mathbb{Z}/N \longrightarrow \mathbb{R}$ und $A \subseteq \mathbb{Z}/N$ setze

$$E(f(n)|n \in A) = \frac{1}{|A|} \sum_{n \in A} f(n).$$

Theorem (Szemerédi)

Sei $k \geq 3$, $0 < \delta \leq 1$, und sei $N \geq 1$ eine Primzahl. Sei $f : \mathbb{Z}/N \longrightarrow \mathbb{R}$ mit

$$0 \leq f(n) \leq 1 \text{ für alle } n \in \mathbb{Z}/N, \text{ und}$$
$$E(f(n)|n \in \mathbb{Z}/N) \geq \delta.$$

Dann gilt

$$E(f(n)f(n+r)\cdots f(n+(k-1)r)|n, r \in \mathbb{Z}/N) \geq c(k, \delta) - o_\delta(1).$$

Die Idee von Green und Tao

Finde $\mathbb{P} \subseteq A \subseteq \mathbb{N}$, so dass $\mathbb{P}$ in A relative Dichte > 0 hat, und dass A so beschaffen ist, dass Szemerédis Satz auch für Teilmengen von A gilt.

Die Idee von Green und Tao

Finde $\mathbb{P} \subseteq A \subseteq \mathbb{N}$, so dass $\mathbb{P}$ in A relative Dichte > 0 hat, und dass A so beschaffen ist, dass Szemerédis Satz auch für Teilmengen von A gilt.

1. Schritt: Verallgemeinere den Satz von Szemerédi.

Theorem (Green, Tao)

Sei $k \geq 3$, $0 < \delta \leq 1$. Sei $\nu : \mathbb{Z}/N \longrightarrow \mathbb{R}_{\geq 0}$ eine k-Pseudozufallsdichte. Sei $f : \mathbb{Z}/N \longrightarrow \mathbb{R}_{\geq 0}$, so dass

$$0 \leq f(n) \leq \nu(n) \text{ für alle } n \in \mathbb{Z}/N, \text{ und}$$
$$E(f(n)|n \in \mathbb{Z}/N) \geq \delta.$$

Dann gilt

$$E(f(n)f(n+r)\cdots f(n+(k-1)r)|n, r \in \mathbb{Z}/N) \geq c(k,\delta) - o_{\delta,\nu}(1).$$

Pseudo-Zufallsdichten

Definition

Eine k-Pseudozufallsdichte ist eine Familie von Funktionen

$$\nu_N : \mathbb{Z}/N \longrightarrow \mathbb{R}_{\geq 0}, \quad N \in \mathbb{N}$$

die eine

- "Linearformenbedingung" und eine
- "Korrelationsbedingung"

erfüllen.

Beispiel (Konsequenzen der Linearformenbedingung)

- $E(\nu) = 1 + o(1)$
- $E(\nu(x)\nu(x+h_1)\nu(x+h_2)\nu(x+h_1+h_2)|x, h_1, h_2 \in \mathbb{Z}/N) = 1 + o(1)$

Anwendung auf die Primzahlen

Seien $k \geq 1$, $N \in \mathbb{N}$, $W = \prod_{\substack{p \in \mathbb{P} \\ p \leq w(N)}} p$, $\epsilon_k = \frac{1}{2^k (k+4)!}$.

von Mangoldt-Funktion

$$\Lambda(n) = \begin{cases} \log p & \text{wenn } n = p^r, \ p \text{ prim}, \\ 0 & \text{sonst.} \end{cases}$$

Anwendung auf die Primzahlen

Seien $k \geq 1$, $N \in \mathbb{N}$, $W = \prod_{\substack{p \in \mathbb{P} \\ p \leq w(N)}} p$, $\epsilon_k = \frac{1}{2^k (k+4)!}$.

von Mangoldt-Funktion

$$\Lambda(n) = \begin{cases} \log p & \text{wenn } n = p^r, \ p \text{ prim}, \\ 0 & \text{sonst.} \end{cases}$$

W-Trick

$$\widetilde{\Lambda}(n) = \begin{cases} \frac{\phi(W)}{W} \log(Wn+1) & \text{wenn } Wn+1 \text{ prim}, \\ 0 & \text{sonst.} \end{cases}$$

Anwendung auf die Primzahlen

Seien $k \geq 1$, $N \in \mathbb{N}$, $W = \prod_{\substack{p \in \mathbb{P} \\ p \leq w(N)}} p$, $\epsilon_k = \frac{1}{2^k (k+4)!}$.

von Mangoldt-Funktion

$$\Lambda(n) = \begin{cases} \log p & \text{wenn } n = p^r, \ p \text{ prim}, \\ 0 & \text{sonst.} \end{cases}$$

W-Trick

$$\widetilde{\Lambda}(n) = \begin{cases} \frac{\phi(W)}{W} \log(Wn+1) & \text{wenn } Wn+1 \text{ prim}, \\ 0 & \text{sonst.} \end{cases}$$

$$f(n) = \begin{cases} k^{-1} 2^{-k-5} \widetilde{\Lambda}(n) & \text{wenn } \epsilon_k N \leq n \leq 2\epsilon_k N, \\ 0 & \text{sonst.} \end{cases}$$

Es gilt

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d).$$

Definiere abgeschnittene Version von Λ (nach Goldston, Yildirim):

$$\Lambda_R(n) = \sum_{\substack{d|n \\ d \leq R}} \mu(d) \log(R/d).$$

Theorem

Seien $R = N^{k^{-1}2^{-k-4}}$ *und* $\epsilon_k = \frac{1}{2^k(k+4)!}$. *Definiere*

$$\nu(n) := \begin{cases} \frac{\phi(W)}{W} \frac{\Lambda_R(Wn+1)^2}{\log R} & \text{wenn } \epsilon_k N \leq n \leq 2\epsilon_k N, \\ 1 & \text{sonst.} \end{cases}$$

Dann ist ν *eine* k*-Pseudozufallsdichte, die* f *majorisiert.*