Struktur und Zufall in der Menge der Primzahlen

Vortrag zum Tag der Mathematik 2013

PD Dr. Karin Halupczok

2. März 2013, LVM in Münster

Primzahlen zählen: von Euklid bis Riemann

Primzahlmuster finden: viele offene Fragen

Fazit: Die Rolle des Zufalls in der Menge der Primzahlen

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und p).

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und p).

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

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und p).

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

Folge der Primzahlen: 2, 3, 5, 7, 11, 13, 17, ...

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und p).

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

Folge der Primzahlen: 2, 3, 5, 7, 11, 13, 17, ...

Satz von Euklid (ca. 300 v. Chr.)

Es existieren unendlich viele Primzahlen.

Primzahlen

Die Zahlentheorie untersucht die Menge $\mathbb{Z}$ der ganzen Zahlen.

Teilbarkeit in $\mathbb{Z}$: a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = ac$

Eine natürliche Zahl p heißt *prim* bzw. Primzahl, wenn sie genau zwei natürliche Teiler hat (nämlich 1 und p).

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

Folge der Primzahlen: 2, 3, 5, 7, 11, 13, 17, ...

Satz von Euklid (ca. 300 v. Chr.)

Es existieren unendlich viele Primzahlen.

Größte bekannte Primzahl aktuell: $2^{57.885.161} - 1$ mit 17.425.170 Stellen (Projekt GIMPS, 25.1.2013)

Der Beweis des Satzes von Euklid

Konstruktiver Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen.

Der Beweis des Satzes von Euklid

Konstruktiver Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen.

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

Der Beweis des Satzes von Euklid

Konstruktiver Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen.

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

Sei p_{k+1} einer dieser Primteiler. So können unendlich viele Primzahlen $p_1, p_2, \ldots$ gewonnen werden. qed

Der Beweis des Satzes von Euklid

Konstruktiver Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen.

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

Sei p_{k+1} einer dieser Primteiler. So können unendlich viele Primzahlen $p_1, p_2, \ldots$ gewonnen werden. qed

Bemerkung: $p_1 \cdots p_k + 1$ muss selbst nicht prim sein, wie das Beispiel $2 * 3 * 5 * 7 * 11 * 13 + 1 = 30031 = 59 * 509$ zeigt. Manche Formulierungen des euklidischen Beweises als Widerspruchsbeweis suggerieren dies, aber es ist falsch.

Der Beweis des Satzes von Euklid

Konstruktiver Beweis: Seien $p_1, \ldots, p_k$ verschiedene Primzahlen.

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

Sei p_{k+1} einer dieser Primteiler. So können unendlich viele Primzahlen $p_1, p_2, \ldots$ gewonnen werden. qed

Bemerkung: $p_1 \cdots p_k + 1$ muss selbst nicht prim sein, wie das Beispiel $2 * 3 * 5 * 7 * 11 * 13 + 1 = 30031 = 59 * 509$ zeigt. Manche Formulierungen des euklidischen Beweises als Widerspruchsbeweis suggerieren dies, aber es ist falsch.

Der konstruktive euklidische Beweis ist nicht nur einfacher als die Formulierung als Widerspruchsbeweis, er liefert bereits erste Abschätzungen für die Primzahlzählfunktion:

Die Primzahlzählfunktion $\pi(x)$

Für reelle Zahlen $x > 1$ betrachten wir die Primzahlzählfunktion

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

also z. B. $\pi(3.5) = 2$, $\pi(12) = 5$ usw., sie stellt im Schaubild eine monoton steigende Stufenfunktion dar. Klar: $\pi(x) \leq x$.

Die Primzahlzählfunktion $\pi(x)$

Für reelle Zahlen $x > 1$ betrachten wir die Primzahlzählfunktion

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

also z. B. $\pi(3.5) = 2$, $\pi(12) = 5$ usw., sie stellt im Schaubild eine monoton steigende Stufenfunktion dar. Klar: $\pi(x) \leq x$.

Der konstruktive Euklid-Beweis, mit etwas Zusatzüberlegung versehen, zeigt $\pi(x) > \log_2(\log_2 x)$.

Die Primzahlzählfunktion $\pi(x)$

Für reelle Zahlen $x > 1$ betrachten wir die Primzahlzählfunktion

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

also z. B. $\pi(3.5) = 2$, $\pi(12) = 5$ usw., sie stellt im Schaubild eine monoton steigende Stufenfunktion dar. Klar: $\pi(x) \leq x$.

Der konstruktive Euklid-Beweis, mit etwas Zusatzüberlegung versehen, zeigt $\pi(x) > \log_2(\log_2 x)$.

Für $x = 100000$ ist diese untere Schranke nur etwa bei 4.05.

Die Primzahlzählfunktion $\pi(x)$

Für reelle Zahlen $x > 1$ betrachten wir die Primzahlzählfunktion

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

also z. B. $\pi(3.5) = 2$, $\pi(12) = 5$ usw., sie stellt im Schaubild eine monoton steigende Stufenfunktion dar. Klar: $\pi(x) \leq x$.

Der konstruktive Euklid-Beweis, mit etwas Zusatzüberlegung versehen, zeigt $\pi(x) > \log_2(\log_2 x)$.

Für $x = 100000$ ist diese untere Schranke nur etwa bei 4.05.

Was sind bessere untere Schranken?
Was sind gute obere Schranken?
Welche stetigen Funktionen in x beschreiben $\pi(x)$ am besten?

Die Vermutung von Gauß über $\pi(x)$

Vermutung von Gauß (1849): Das logarithmische Integral

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

ist eine approximierende Funktion an $\pi(x)$, d. h. es gilt

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

Bemerkung: log ist hier der Logarithmus zur Basis e.

Die Vermutung von Gauß über $\pi(x)$

Vermutung von Gauß (1849): Das logarithmische Integral

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

ist eine approximierende Funktion an $\pi(x)$, d. h. es gilt

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

Bemerkung: log ist hier der Logarithmus zur Basis e.

Nach dieser Vermutung von Gauß sind die Funktionen $\mathrm{li}(x)$ und $\frac{x}{\log x}$ beide Approximationen an $\pi(x)$.

Die Vermutung von Gauß über $\pi(x)$

Vermutung von Gauß (1849): Das logarithmische Integral

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

ist eine approximierende Funktion an $\pi(x)$, d. h. es gilt

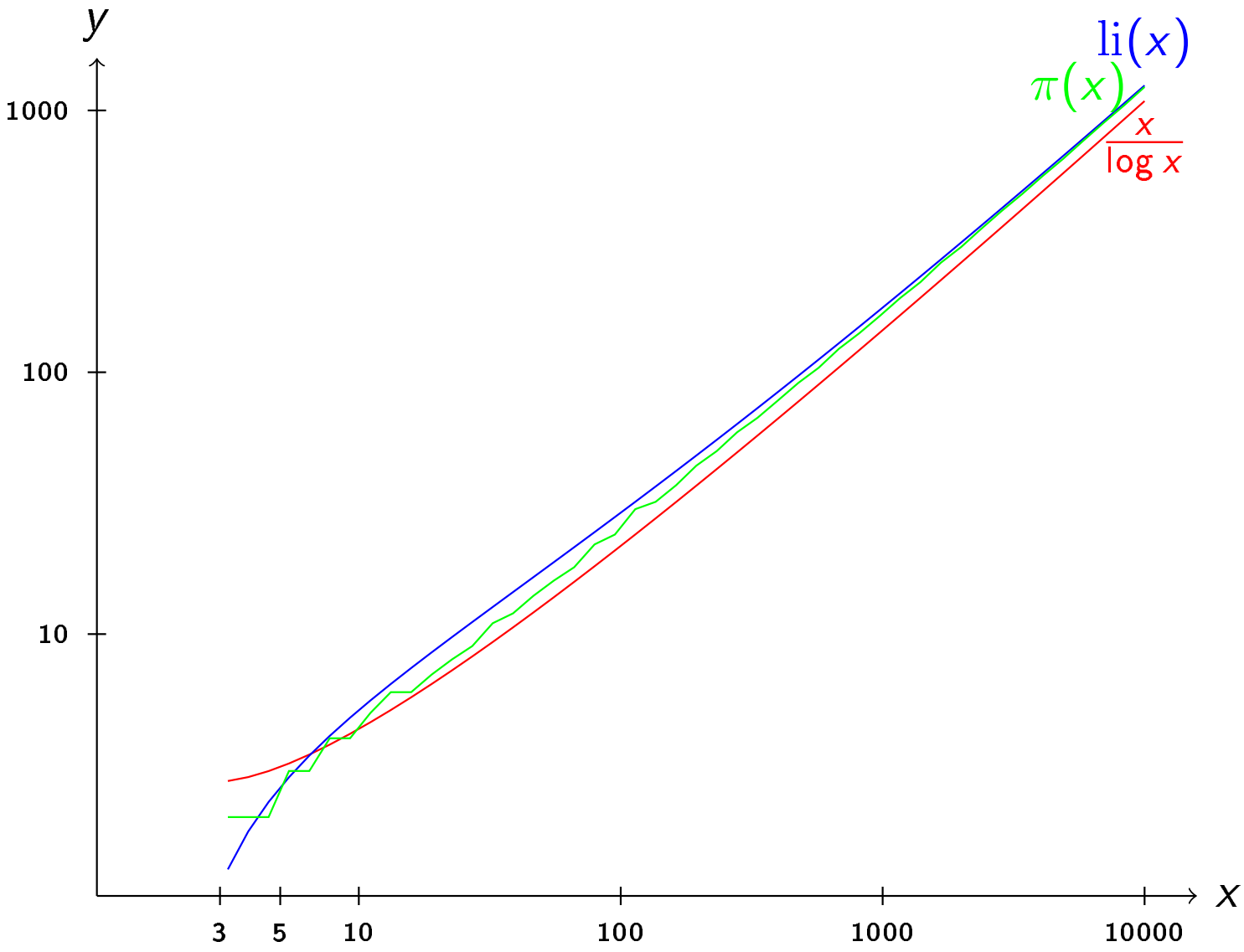
$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1.$$

Bemerkung: log ist hier der Logarithmus zur Basis e.

Nach dieser Vermutung von Gauß sind die Funktionen $\mathrm{li}(x)$ und $\frac{x}{\log x}$ beide Approximationen an $\pi(x)$.

Darstellung der Funktionen $\pi(x)$, $\mathrm{li}(x)$ und $\frac{x}{\log x}$ im Schaubild:

Schaubild von $\pi(x)$, $\mathrm{li}(x)$ und $x/\log x$:



Primzahlsatz

Die numerischen Werte geben Gauß recht, zu seiner Zeit war aber noch kein Beweis für dieses asymptotische Verhalten von $\pi(x)$ in Sicht.

Primzahlsatz

Die numerischen Werte geben Gauß recht, zu seiner Zeit war aber noch kein Beweis für dieses asymptotische Verhalten von $\pi(x)$ in Sicht.

Hadamard und de la Vallée–Poussin (1896): Beweis der Gaußschen Vermutung, heute bekannt als:

Primzahlsatz:

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

Primzahlsatz

Die numerischen Werte geben Gauß recht, zu seiner Zeit war aber noch kein Beweis für dieses asymptotische Verhalten von $\pi(x)$ in Sicht.

Hadamard und de la Vallée–Poussin (1896): Beweis der Gaußschen Vermutung, heute bekannt als:

Primzahlsatz:

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

Dieser Satz kann auch umformuliert werden als
$\pi(x) = \mathrm{li}(x) + o(\mathrm{li}(x))$, wobei $o(\mathrm{li}(x))$ einen Fehlerterm bezeichnet, der langsamer wächst als $\mathrm{li}(x)$, genau: $o(\mathrm{li}(x))/\mathrm{li}(x) \underset{x\to\infty}{\longrightarrow} 0$.

Primzahlsatz

Die numerischen Werte geben Gauß recht, zu seiner Zeit war aber noch kein Beweis für dieses asymptotische Verhalten von $\pi(x)$ in Sicht.

Hadamard und de la Vallée–Poussin (1896): Beweis der Gaußschen Vermutung, heute bekannt als:

Primzahlsatz:

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

Dieser Satz kann auch umformuliert werden als
$\pi(x) = \mathrm{li}(x) + o(\mathrm{li}(x))$, wobei $o(\mathrm{li}(x))$ einen Fehlerterm bezeichnet, der langsamer wächst als $\mathrm{li}(x)$, genau: $o(\mathrm{li}(x))/\mathrm{li}(x) \underset{x\to\infty}{\longrightarrow} 0$.
Da $\mathrm{li}(x)$ und $\frac{x}{\log x}$ Approximationen voneinander sind, kann man den Primzahlsatz auch als $\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$ schreiben.

Approximationsgüte

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

Das (im wesentlichen) beste bewiesene Ergebnis bis heute ist

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

von Vinogradov und Korobov (1958).

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?
Das (im wesentlichen) beste bewiesene Ergebnis bis heute ist

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

von Vinogradov und Korobov (1958).
Bekannt ist: Ist der Fehlerterm $\mathrm{O}(\sqrt{x}\log x)$, so gilt die (bislang unbewiesene) Riemannsche Vermutung, und umgekehrt!

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?
Das (im wesentlichen) beste bewiesene Ergebnis bis heute ist

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

von Vinogradov und Korobov (1958).
Bekannt ist: Ist der Fehlerterm $\mathrm{O}(\sqrt{x}\log x)$, so gilt die (bislang unbewiesene) Riemannsche Vermutung, und umgekehrt!

Die Riemannsche Vermutung (RH):

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

Approximationsgüte

Wie gut ist die Approximation von $\pi(x)$ an $\mathrm{li}(x)$?
Das (im wesentlichen) beste bewiesene Ergebnis bis heute ist

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

von Vinogradov und Korobov (1958).
Bekannt ist: Ist der Fehlerterm $\mathrm{O}(\sqrt{x}\log x)$, so gilt die (bislang unbewiesene) Riemannsche Vermutung, und umgekehrt!

Die Riemannsche Vermutung (RH):

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

Bemerkung: Die Funktion $\zeta(s)$ wird für $s \in \mathbb{C}$, $\mathrm{Re}\, s > 1$, durch $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + 1/2^s + 1/3^s + \ldots$ definiert und mit

$$\zeta(s) := 1 + \frac{1}{s-1} - s\int_1^{\infty} \frac{x - [x]}{x^{s+1}}\,dx$$

zu einer Funktion auf $\mathrm{Re}\, s > 0$, $s \neq 1$, analytisch fortgesetzt.

Primzahlen zählen: von Euklid bis Riemann

Primzahlmuster finden: viele offene Fragen

Fazit: Die Rolle des Zufalls in der Menge der Primzahlen

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$.

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$.

Muster sind sich wiederholende Strukturen in einer beliebigen Teilmenge T der natürlichen Zahlen und sind interessant, wenn sie unendlich oft auftauchen. Dann soll ihre Häufigkeit, mit der diese in T auftreten, auch quantitativ untersucht werden.

Strukturen und Muster in der Menge der Primzahlen

Wie können Strukturen und Muster in der Menge $\mathbb{P}$ der Primzahlen gefunden und untersucht werden?

Strukturen sind interessante Konstellationen endlich vieler natürlicher Zahlen, z. B. Paare mit festem Abstand oder Zahlen in einer Restklasse $\equiv a \bmod q$.

Muster sind sich wiederholende Strukturen in einer beliebigen Teilmenge T der natürlichen Zahlen und sind interessant, wenn sie unendlich oft auftauchen. Dann soll ihre Häufigkeit, mit der diese in T auftreten, auch quantitativ untersucht werden.

Wir sprechen von Primzahlstrukturen und Primzahlmustern, wenn die untersuchte Menge $T = \mathbb{P}$ ist.

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Konsequenz u. a.: Unendlich viele Primzahlen haben jeweils die Endziffer 1, 3, 7, oder 9, und zwar mit einem Anteil von 25% unter allen Primzahlen.

Ein bekanntes Ergebnis zum einfachsten Primzahlmuster: Primzahlen in Restklassen

Satz von Dirichlet (1837):

Zu gegebenen teilerfremden Zahlen a und q gibt es unendlich viele Primzahlen $p \equiv a \bmod q$.

Konsequenz u. a.: Unendlich viele Primzahlen haben jeweils die Endziffer 1, 3, 7, oder 9, und zwar mit einem Anteil von 25% unter allen Primzahlen.

Analog für andere Basen als 10.

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p + 2k$?

(Zwillingsvermutung von de Polignac, 1849)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p + 2k$?

(Zwillingsvermutung von de Polignac, 1849)

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

(Sophie Germain, 1805)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p+2k$?

(Zwillingsvermutung von de Polignac, 1849)

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

(Sophie Germain, 1805)

Ist jede gerade Zahl $n \geq 4$ Summe zweier Primzahlen?
Oder umformuliert: Gibt es für jedes gerade $n \geq 4$ eine Primzahl p so, dass $n - p$ auch prim ist?

(Goldbach-Vermutung, 1742)

Weitere einfache Primzahlmuster:

Gibt es unendlich viele Primzahlpaare $p, p+2k$?

(Zwillingsvermutung von de Polignac, 1849)

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

(Sophie Germain, 1805)

Ist jede gerade Zahl $n \geq 4$ Summe zweier Primzahlen?
Oder umformuliert: Gibt es für jedes gerade $n \geq 4$ eine Primzahl p so, dass $n-p$ auch prim ist?

(Goldbach-Vermutung, 1742)

Bis heute sind diese Fragen unbeantwortet!

Eine Vermutung zu linearen Primzahlmustern

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem “linearen” Primzahlmusterproblem im Stil des Dirichletschen Satzes:

Eine Vermutung zu linearen Primzahlmustern

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes:

Prim-k-Tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1 + q_1 x, a_2 + q_2 x, \ldots, a_k + q_k x \in \mathbb{Z}[x]$, die $q_i \neq 0$, zulässig, d. h. keine Primzahl teilt $\prod_{i=1}^{k}(a_i + q_i n)$ für alle $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1 + q_1 n, a_2 + q_2 n, \ldots, a_k + q_k n$ prim (Prim-k-Tupel).

Eine Vermutung zu linearen Primzahlmustern

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes:

Prim-k-Tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1 + q_1 x, a_2 + q_2 x, \ldots, a_k + q_k x \in \mathbb{Z}[x]$, die $q_i \neq 0$, zulässig, d. h. keine Primzahl teilt $\prod_{i=1}^{k}(a_i + q_i n)$ für alle $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1 + q_1 n, a_2 + q_2 n, \ldots, a_k + q_k n$ prim (Prim-k-Tupel).

Schon lange bewiesen: Fall $k = 1$ (Ist genau der Satz von Dirichlet!)

Eine Vermutung zu linearen Primzahlmustern

Verallgemeinerung des Zwillings-, Goldbach- und Sophie-Germain-Zwillingsproblems zu einem "linearen" Primzahlmusterproblem im Stil des Dirichletschen Satzes:

Prim-k-Tupel-Vermutung von Hardy-Littlewood-Dickson:
Seien $a_1 + q_1 x, a_2 + q_2 x, \ldots, a_k + q_k x \in \mathbb{Z}[x]$, die $q_i \neq 0$, zulässig, d. h. keine Primzahl teilt $\prod_{i=1}^{k}(a_i + q_i n)$ für alle $n \in \mathbb{N}$. Dann gibt es unendlich viele $n \in \mathbb{N}$ mit $a_1 + q_1 n, a_2 + q_2 n, \ldots, a_k + q_k n$ prim (Prim-k-Tupel).

Schon lange bewiesen: Fall $k = 1$ (Ist genau der Satz von Dirichlet!)

Die Formulierung ist ein "mehrdimensionaler" Satz von Dirichlet.

Heuristik mit Zufall

Es gibt auch eine quantitative Version dieser Vermutung. Sie macht eine Aussage über die Häufigkeitsverteilung der Prim-k-Tupel in Form einer asymptotischen Formel, ähnlich wie die Formel im Primzahlsatz oben.

Heuristik mit Zufall

Es gibt auch eine quantitative Version dieser Vermutung. Sie macht eine Aussage über die Häufigkeitsverteilung der Prim-k-Tupel in Form einer asymptotischen Formel, ähnlich wie die Formel im Primzahlsatz oben.

Die quantitative Form im Fall $k = 1$ heißt heute Primzahlsatz in Progressionen.

Heuristik mit Zufall

Es gibt auch eine quantitative Version dieser Vermutung. Sie macht eine Aussage über die Häufigkeitsverteilung der Prim-k-Tupel in Form einer asymptotischen Formel, ähnlich wie die Formel im Primzahlsatz oben.

Die quantitative Form im Fall $k = 1$ heißt heute Primzahlsatz in Progressionen.

Hardy und Littlewood gelangten um 1920 zur Prim-k-Tupel- und anderen Vermutungen über die Verteilung von Primzahlmustern.

Heuristik mit Zufall

Es gibt auch eine quantitative Version dieser Vermutung. Sie macht eine Aussage über die Häufigkeitsverteilung der Prim-k-Tupel in Form einer asymptotischen Formel, ähnlich wie die Formel im Primzahlsatz oben.

Die quantitative Form im Fall $k = 1$ heißt heute Primzahlsatz in Progressionen.

Hardy und Littlewood gelangten um 1920 zur Prim-k-Tupel- und anderen Vermutungen über die Verteilung von Primzahlmustern.

Sie benutzten dafür ein einfaches Zufallsprinzip als Heuristik:
Der Primzahlsatz/die Riemannsche Vermutung legt den Ansatz nahe, dass eine zufällig gewählte natürliche Zahl $n \geq 3$ mit Wahrscheinlichkeit $1/\log n$ prim ist. (Cramérsches Modell)
Dies modelliert das pseudozufällige Auftreten der Primzahlen.

Ein Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Balog (1990):

Die Prim-k-tupel-Vermutung gilt im Mittel. (D. h. im Mittelwert über die Tupel $(a_1, \ldots, a_k)$.)

Ein Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Balog (1990):

Die Prim-k-tupel-Vermutung gilt im Mittel. (D. h. im Mittelwert über die Tupel $(a_1, \ldots, a_k)$.)

Konsequenz 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.

Ein Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Balog (1990):

Die Prim-k-tupel-Vermutung gilt im Mittel. (D. h. im Mittelwert über die Tupel $(a_1, \ldots, a_k)$.)

Konsequenz 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.

Beispiel für einen 3-dimensionalen "Balog-Würfel":

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

Ein Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Balog (1990):

Die Prim-k-tupel-Vermutung gilt im Mittel. (D. h. im Mittelwert über die Tupel $(a_1, \ldots, a_k)$.)

Konsequenz 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.

Beispiel für einen 3-dimensionalen "Balog-Würfel":

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

Damit blieb aber zunächst ungelöst: Gibt es unendlich viele Balogwürfel mit längerer Seitenlänge als 3?

Der Satz von Green-Tao

Ein weiterer Durchbruch in Richtung Prim-k-Tupel-Vermutung (Fields-Medaille an T. Tao 2006):

Satz von Green-Tao:

Es gibt unendlich viele lineare Polynome $f(x) = a + qx \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

Der Satz von Green-Tao

Ein weiterer Durchbruch in Richtung Prim-k-Tupel-Vermutung (Fields-Medaille an T. Tao 2006):

Satz von Green-Tao:

Es gibt unendlich viele lineare Polynome $f(x) = a + qx \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

(D. h. es gibt unendlich viele arithmetische Progressionen $a, a+q, a+q\cdot 2, \ldots, a+q\cdot(k-1)$ der Länge k, die nur aus Primzahlen bestehen.)

Der Satz von Green-Tao

Ein weiterer Durchbruch in Richtung Prim-k-Tupel-Vermutung (Fields-Medaille an T. Tao 2006):

Satz von Green-Tao:

Es gibt unendlich viele lineare Polynome $f(x) = a + qx \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

(D. h. es gibt unendlich viele arithmetische Progressionen $a, a+q, a+q\cdot 2, \ldots, a+q\cdot(k-1)$ der Länge k, die nur aus Primzahlen bestehen.)

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

Der Satz von Green-Tao

Ein weiterer Durchbruch in Richtung Prim-k-Tupel-Vermutung (Fields-Medaille an T. Tao 2006):

Satz von Green-Tao:

Es gibt unendlich viele lineare Polynome $f(x) = a + qx \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

(D. h. es gibt unendlich viele arithmetische Progressionen $a, a+q, a+q\cdot 2, \ldots, a+q\cdot(k-1)$ der Länge k, die nur aus Primzahlen bestehen.)

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

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

Der Satz von Green-Tao

Ein weiterer Durchbruch in Richtung Prim-k-Tupel-Vermutung (Fields-Medaille an T. Tao 2006):

Satz von Green-Tao:

Es gibt unendlich viele lineare Polynome $f(x) = a + qx \in \mathbb{N}[x]$, für die $f(0), f(1), \ldots, f(k-1)$ alle prim sind.

(D. h. es gibt unendlich viele arithmetische Progressionen $a, a+q, a+q\cdot 2, \ldots, a+q\cdot(k-1)$ der Länge k, die nur aus Primzahlen bestehen.)

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

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

Rekord (Benoãt Perichon, PrimeGrid 2010): Länge $k = 26$:
$4314274659571419 1 + 23681770 \cdot 223092870 \cdot n;\ 0 \leq n \leq 25$

Zum Beweis des Satzes von Green-Tao

Der Beweis ist ein Mix aus harmonischer Analysis, Ergodentheorie (einem Teilgebiet der Stochastik, der sich mit dynamischen Systemen beschäftigt), und Siebmethoden.

Zum Beweis des Satzes von Green-Tao

Der Beweis ist ein Mix aus harmonischer Analysis, Ergodentheorie (einem Teilgebiet der Stochastik, der sich mit dynamischen Systemen beschäftigt), und Siebmethoden.

Der Beweis des Satzes von Green-Tao ist nicht konstruktiv. Er kann aber effektiv ausgeführt werden (d. h. so, dass Schranken berechnet werden können). Eine solche Analyse zeigt dann:
Es gibt eine Primzahl-AP der Länge k mit Primzahlen unterhalb von

Zum Beweis des Satzes von Green-Tao

Der Beweis ist ein Mix aus harmonischer Analysis, Ergodentheorie (einem Teilgebiet der Stochastik, der sich mit dynamischen Systemen beschäftigt), und Siebmethoden.

Der Beweis des Satzes von Green-Tao ist nicht konstruktiv. Er kann aber effektiv ausgeführt werden (d. h. so, dass Schranken berechnet werden können). Eine solche Analyse zeigt dann:
Es gibt eine Primzahl-AP der Länge k mit Primzahlen unterhalb von

$$2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}$$

Zum Beweis des Satzes von Green-Tao

Der Beweis ist ein Mix aus harmonischer Analysis, Ergodentheorie (einem Teilgebiet der Stochastik, der sich mit dynamischen Systemen beschäftigt), und Siebmethoden.

Der Beweis des Satzes von Green-Tao ist nicht konstruktiv. Er kann aber effektiv ausgeführt werden (d. h. so, dass Schranken berechnet werden können). Eine solche Analyse zeigt dann:
Es gibt eine Primzahl-AP der Länge k mit Primzahlen unterhalb von

$$2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}$$

Diese Schranke müsste eher bei etwa $k!$ sein. Und: Wird die Riemannsche Vermutung angenommen, kann in der Schranke lediglich eine Exponentialstufe weggelassen werden!

Einige Folgerungen aus dem Satz von Green-Tao:

Einige Folgerungen 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.

Einige Folgerungen 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:* Das "Eulersche" Polynom $x^2 + x + 41$ hat Primzahlwerte für $x = 0, 1, 2, \ldots, 39$.)

Einige Folgerungen 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:* Das "Eulersche" Polynom $x^2 + x + 41$ hat Primzahlwerte für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren unendlich viele Paare $a, b \in \mathbb{Z}$, 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 dann $f(x) = ax^2 + ax + b$. qed

Einige Folgerungen 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:* Das "Eulersche" Polynom $x^2 + x + 41$ hat Primzahlwerte für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren unendlich viele Paare $a, b \in \mathbb{Z}$, 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 dann $f(x) = ax^2 + ax + b$. qed

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

Einige Folgerungen 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:* Das "Eulersche" Polynom $x^2 + x + 41$ hat Primzahlwerte für $x = 0, 1, 2, \ldots, 39$.)

Beweis: Nach Green-Tao existieren unendlich viele Paare $a, b \in \mathbb{Z}$, 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 dann $f(x) = ax^2 + ax + b$. qed

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

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

Bsp.:

17	89	71
113	59	5
47	29	101

oder

41	89	83
113	71	29
59	53	101

Weiterer Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Green, Tao und Ziegler (2010/12)

Die Prim-k-Tupel-Vermutung (in der quantitativen Version, für lineare Polynome in d Variablen) stimmt für alle Fälle mit "endlicher Komplexität".

Weiterer Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Green, Tao und Ziegler (2010/12)

Die Prim-k-Tupel-Vermutung (in der quantitativen Version, für lineare Polynome in d Variablen) stimmt für alle Fälle mit "endlicher Komplexität".

Die Ausnahmen von "unendlicher Komplexität" sind etwa das oben genannte Zwillings-, Goldbach- und Sophie-Germain-Problem, also die "binären Fälle", die weiterhin offen bleiben!

Weiterer Durchbruch zur Prim-k-Tupel-Vermutung

Satz von Green, Tao und Ziegler (2010/12)

Die Prim-k-Tupel-Vermutung (in der quantitativen Version, für lineare Polynome in d Variablen) stimmt für alle Fälle mit "endlicher Komplexität".

Die Ausnahmen von "unendlicher Komplexität" sind etwa das oben genannte Zwillings-, Goldbach- und Sophie-Germain-Problem, also die "binären Fälle", die weiterhin offen bleiben!

Der Beweis verwendet tiefe Methoden der Ergodentheorie.

Neuere Fortschritte zu binären Fällen:

Ansatz zur Zwillingsvermutung:
Zählen von Primzahlpaaren mit kleinen Abständen

Neuere Fortschritte zu binären Fällen:

Ansatz zur Zwillingsvermutung:
Zählen von Primzahlpaaren mit kleinen Abständen

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

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

sogar:

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

Neuere Fortschritte zu binären Fällen:

Ansatz zur Zwillingsvermutung:
Zählen von Primzahlpaaren mit kleinen Abständen

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

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

sogar:

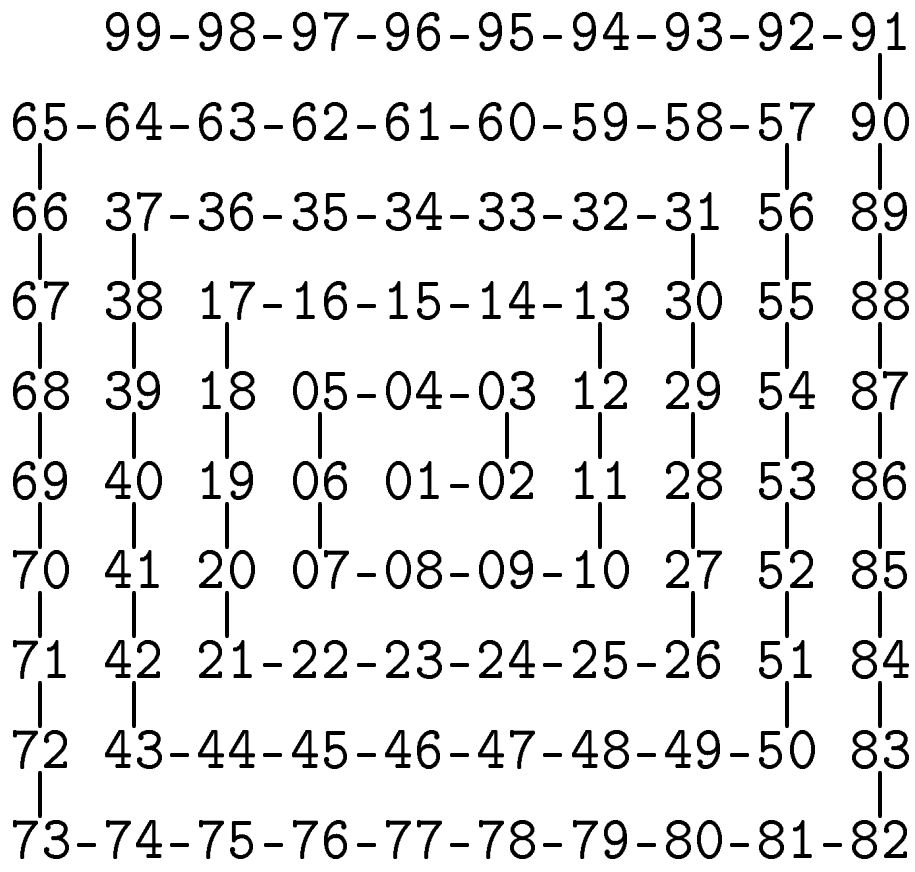
$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty$$

Unter Annahme der Elliott-Halberstam-Vermutung (schwächer als die Riemann-Vermutung) folgt die "bounded gap conjecture"

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

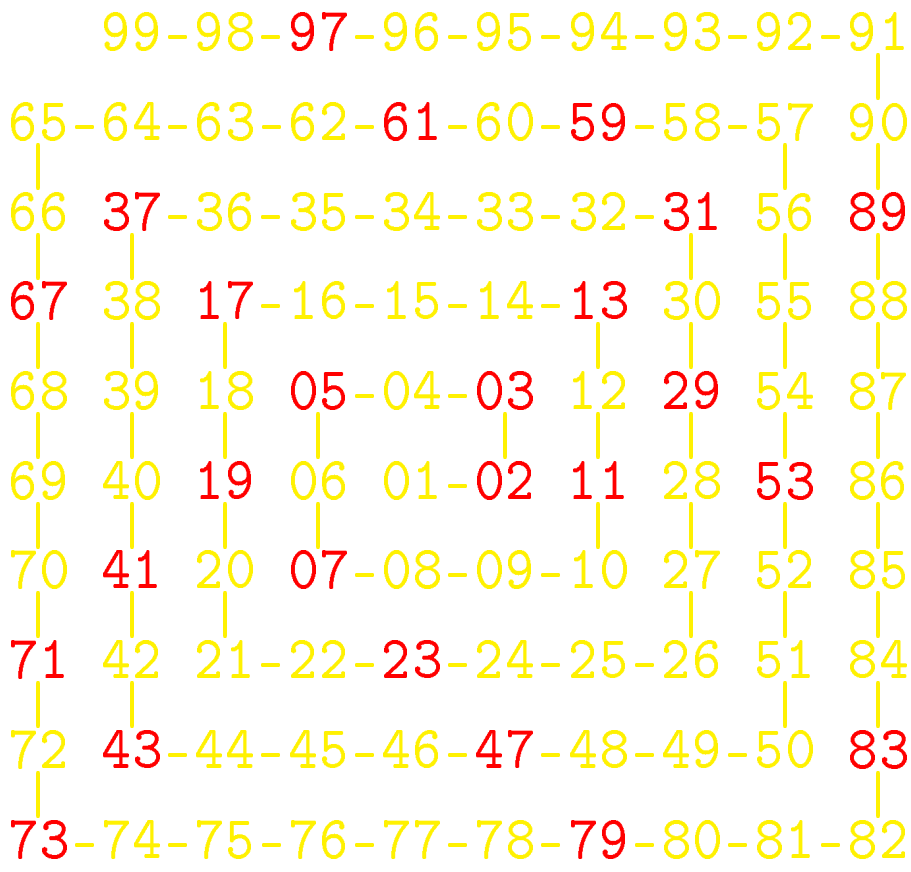
Weitere Muster mit Primzahlen: Die Ulam-Spirale

In einer spiralförmigen Anordnung der natürlichen Zahlen werden die Primzahlen markiert:



Weitere Muster mit Primzahlen: Die Ulam-Spirale

In einer spiralförmigen Anordnung der natürlichen Zahlen werden die Primzahlen markiert:



Die Primzahlen erscheinen in manchen schräg verlaufenden Geraden häufiger als in anderen.

Eine größere Ulam-Spirale

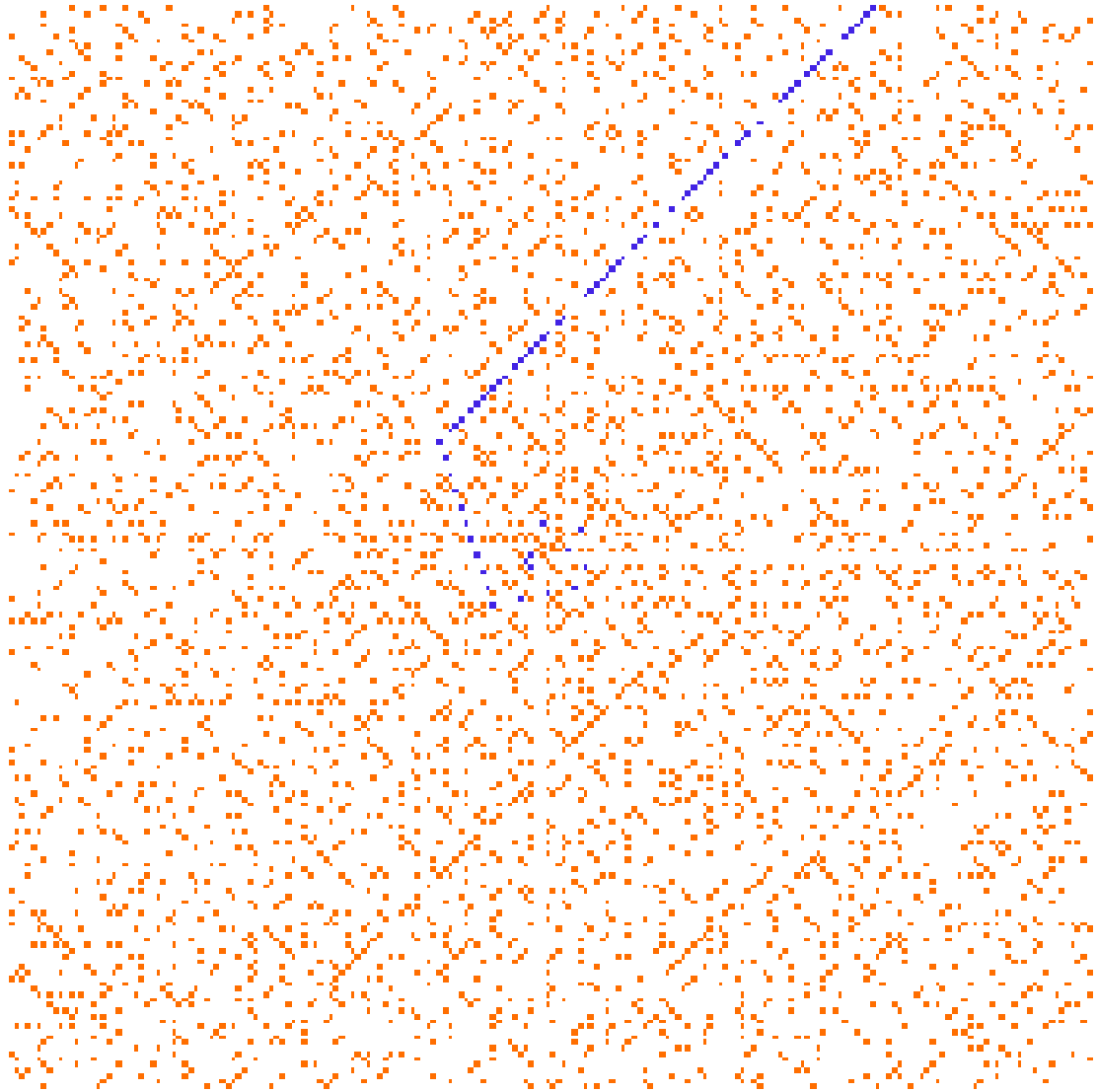


Abbildung: aus der Wikipedia, in blau: Primzahlen der Form $4n^2 - 2n + 41$, $n = 0, 1, 2, 3, \ldots$

Erklärung der Geraden in der Ulam-Spirale

Die Ulam-Spirale zeigt numerisch/visualisiert,
dass manche quadratische Polynome der Form $4n^2 + bn + c$ für $n = 1, 2, 3, \ldots$ häufiger Primzahlwerte annehmen als andere Polynome.

Erklärung der Geraden in der Ulam-Spirale

Die Ulam-Spirale zeigt numerisch/visualisiert,
dass manche quadratische Polynome der Form $4n^2 + bn + c$ für $n = 1, 2, 3, \ldots$ häufiger Primzahlwerte annehmen als andere Polynome.

Dieses Verhalten der Ulamspirale (und Varianten davon) ist ein Spezialfall der Vermutung "F" von Hardy und Littlewood, die 1923 formuliert wurde. Deren Vermutung "F" ist das Analogon der Prim-k-Tupel-Vermutung mit (geeigneten) Polynomen $\in \mathbb{Z}[x]$ statt Linearformen und ist bis heute offen für nichtlineare Polynome.

Erklärung der Geraden in der Ulam-Spirale

Die Ulam-Spirale zeigt numerisch/visualisiert,
dass manche quadratische Polynome der Form $4n^2 + bn + c$ für $n = 1, 2, 3, \ldots$ häufiger Primzahlwerte annehmen als andere Polynome.

Dieses Verhalten der Ulamspirale (und Varianten davon) ist ein Spezialfall der Vermutung "F" von Hardy und Littlewood, die 1923 formuliert wurde. Deren Vermutung "F" ist das Analogon der Prim-k-Tupel-Vermutung mit (geeigneten) Polynomen $\in \mathbb{Z}[x]$ statt Linearformen und ist bis heute offen für nichtlineare Polynome.

Die von Hardy und Littlewood vorhergesagte Formel erklärt sehr gut, welche quadratischen Polynome (also welche Geraden in der Ulam-Spirale) mehr Primzahltreffer haben als andere.

Primzahlen zählen: von Euklid bis Riemann

Primzahlmuster finden: viele offene Fragen

Fazit: Die Rolle des Zufalls in der Menge der Primzahlen

Grenzen des Wahrscheinlichkeitsmodells für Primzahlen

Die Wahrscheinlichkeitstheorie ist das beste Mittel zum Studium der Primzahlen, oder?

Grenzen des Wahrscheinlichkeitsmodells für Primzahlen

Die Wahrscheinlichkeitstheorie ist das beste Mittel zum Studium der Primzahlen, oder?

Viele Voraussagen des oben genannten Cramérschen Wahrscheinlichkeitsmodells konnten bei Primzahlmusterproblemen bestätigt werden.

Grenzen des Wahrscheinlichkeitsmodells für Primzahlen

Die Wahrscheinlichkeitstheorie ist das beste Mittel zum Studium der Primzahlen, oder?

Viele Voraussagen des oben genannten Cramérschen Wahrscheinlichkeitsmodells konnten bei Primzahlmusterproblemen bestätigt werden.

Eine Konsequenz des Cramér-Modells ist die asymptotische Formel

$$\pi(x + \log^N x) - \pi(x) \sim \log^{N-1} x \text{ für } x \to \infty,$$

wobei $N > 2$ eine beliebige feste natürliche Zahl ist.

Grenzen des Wahrscheinlichkeitsmodells für Primzahlen

Die Wahrscheinlichkeitstheorie ist das beste Mittel zum Studium der Primzahlen, oder?

Viele Voraussagen des oben genannten Cramérschen Wahrscheinlichkeitsmodells konnten bei Primzahlmusterproblemen bestätigt werden.

Eine Konsequenz des Cramér-Modells ist die asymptotische Formel

$$\pi(x + \log^N x) - \pi(x) \sim \log^{N-1} x \text{ für } x \to \infty,$$

wobei $N > 2$ eine beliebige feste natürliche Zahl ist.

Zur Überraschung aller Experten konnte H. Maier im Jahr 1985 diese Aussage für die Menge der Primzahlen widerlegen. Mittlerweile gibt es aber auch noch weitere Widersprüche des Modells.

Verfeinerung des Cramérschen Modells

Das Cramérsche Modell konnte inzwischen so verfeinert werden, dass diese Widersprüche behoben wurden (A. Granville, 1995).

Verfeinerung des Cramérschen Modells

Das Cramérsche Modell konnte inzwischen so verfeinert werden, dass diese Widersprüche behoben wurden (A. Granville, 1995).

Nach dieser Verfeinerung müsste eine natürliche Zahl n ohne Primfaktoren $\leq T$, vereinfacht gesagt, mit Wahrscheinlichkeit

$$\frac{1}{\log n} \cdot \prod_{p \leq T} \frac{p}{p-1}$$

prim sein, wobei T groß genug ist.

Verfeinerung des Cramérschen Modells

Das Cramérsche Modell konnte inzwischen so verfeinert werden, dass diese Widersprüche behoben wurden (A. Granville, 1995).

Nach dieser Verfeinerung müsste eine natürliche Zahl n ohne Primfaktoren $\leq T$, vereinfacht gesagt, mit Wahrscheinlichkeit

$$\frac{1}{\log n} \cdot \prod_{p \leq T} \frac{p}{p-1}$$

prim sein, wobei T groß genug ist.

Es ist noch längst nicht verstanden, welche Rolle der Zufall in der Menge der Primzahlen genau spielt.

Verfeinerung des Cramérschen Modells

Das Cramérsche Modell konnte inzwischen so verfeinert werden, dass diese Widersprüche behoben wurden (A. Granville, 1995).

Nach dieser Verfeinerung müsste eine natürliche Zahl n ohne Primfaktoren $\leq T$, vereinfacht gesagt, mit Wahrscheinlichkeit

$$\frac{1}{\log n} \cdot \prod_{p \leq T} \frac{p}{p-1}$$

prim sein, wobei T groß genug ist.

Es ist noch längst nicht verstanden, welche Rolle der Zufall in der Menge der Primzahlen genau spielt.

Tiefliegende offene Vermutungen wie die Riemannsche Vermutung und ihre Verallgemeinerungen hängen mit diesen Fragen eng zusammen.

Vielen Dank!