

Elementare Zahlentheorie

Vorlesung mit Übung

Prof. Dr. Gerald Warnecke

6. Juli 2026

- Wintersemester 2026/27: 3V + 1Ü (6 CP)
- Für Studiengänge Mathematik oder Lehrämter
- Wahlpflicht für Bachelor oder Master möglich
- Voraussetzungen: keine
- Mögliche Fortsetzung: Analytische Zahlentheorie
Sommersemester 2024: 3V + 1Ü (6 CP)

- Euklidischer Algorithmus, Primzahlen (Fundamentalsatz der Arithmetik)
- Kettenbrüche, erweiterter Euklidischer Algorithmus
- Farey-Sequenzen
- Zahlentheoretische Funktionen
- Kongruenzen, Restklassengruppen
- Eventuell: Quadratische Reste

Euklidischer Algorithmus, Primzahlen

Ganze Zahlen: $\dots, -2, -1, 0, 1, 2, 3, \dots$

Euklidischer Algorithmus findet den größten gemeinsamen Teiler (ggT) zweier ganzer Zahlen durch Division mit Rest

Beweis, dass der Algorithmus das leistet

Beweis: Jede ganze Zahl besitzt eine eindeutige Primzahlzerlegung

Beweis: Es gibt unendlich viele Primzahlen

Kettenbrüche

$$x = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 - \frac{1}{q_4 + \frac{1}{\ddots}}}}}$$

mit $q_0 \in \mathbb{Z}$, $q_1, q_2, q_3, \dots \in \mathbb{N}$

$x \in \mathbb{Q} \quad \Leftrightarrow \quad$ der Kettenbruch ist endlich

$x \in \mathbb{R} \setminus \mathbb{Q} \quad \Leftrightarrow \quad$ der Kettenbruch ist unendlich

Erweiterter Euklidischer Algorithmus und Kettenbrüche

Farey-Sequenzen

Gekürzte Brüche aus $[0, 1] \subset \mathbb{R}$

n -te Sequenz: Nenner maximal n , geordnet nach Größe der Zahl

n	Brüche der n -ten Farey-Sequenz										
1	$\frac{0}{1}$ $\frac{1}{1}$										
2	$\frac{0}{1}$	$\frac{1}{2}$								$\frac{1}{1}$	
3	$\frac{0}{1}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{1}{1}$						
4	$\frac{0}{1}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{1}{1}$				
5	$\frac{0}{1}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{2}{5}$	$\frac{1}{2}$	$\frac{3}{5}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{4}{5}$	$\frac{1}{1}$
$\vdots$	$\dots$										

$$\frac{1}{3}, \frac{1}{2} \rightarrow \frac{2}{5}$$

$\frac{a}{b}, \frac{a'}{b'}$ zwei Brüche $\rightarrow$ **Mediante** $\frac{a+a'}{b+b'}$ liegt dazwischen

Zahlentheoretische Funktionen

Abbildungen $f : \mathbb{N} \rightarrow \mathbb{C}$

Eine andere Sicht auf Folgen: $(a_n)_{n \in \mathbb{N}} \subset \mathbb{C}$ als $a_n = f(n)$

Beispiele:

$\tau(n)$ = Anzahl der Teiler von n (**Teilerfunktion**)

$\varphi(n)$ = Anzahl der zu n teilerfremden Zahlen kleiner als n
(**Euler-Funktion**)

Dirichlet-Faltung, Möbius-Funktion μ

Kongruenzen, Restklassengruppen

Division mit Rest $\Rightarrow$ Restklassen

Arithmetik (Rechnen) mit Restklassen

Restklassengruppen, Restklassenringe, endliche Körper