Diskrete Mathematik

Inhalte 7. Vorlesungswoche

Sebastian Iwanowski
FH Wedel

Referenz zum Nacharbeiten:

Beutelspacher 5.6, 5.7

4. Zahlentheorie

4.3 Primzahlen

In diesem Abschnitt repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, ***natürliche*** *Zahlen (Elemente von $\mathbb{N}$).*

Definition

Eine natürliche Zahl p > 1 heißt Primzahl, wenn p und 1 die einzigen Teiler von p sind
(p heißt Primzahl :⇔ $(p \in \mathbb{N}) \wedge (p > 1) \wedge (((n \in \mathbb{N}) \wedge (n \mid p)) \Rightarrow ((n = 1) \vee (n = p)))$)

Bestimmung von Primzahlen: Sieb des Eratosthenes

1) Füge alle Zahlen von 2 bis n in das Sieb ein.
2) Setze p := 2.
3) Solange $p \leq \sqrt{n}$, führe folgende Aktionen aus:
   a) Streiche alle Zahlen durch, die Vielfache von p sind.
   b) Setze p gleich der nächsten nicht durchgestrichenen Zahl.

Behauptung: Am Ende enthält das Sieb alle Primzahlen zwischen 2 und n.

4. Zahlentheorie

4.3 Primzahlen

Anzahl von Primzahlen

1) Es gibt unendlich viele Primzahlen.

2) Die Primzahlen sind im Durchschnitt fast gleich verteilt:
Jede ln (n) – te Zahl bis n ist im Durchschnitt eine Primzahl.

4. Zahlentheorie

4.3 Primzahlen

Hauptsatz der elementaren Zahlentheorie:
Existenz und Eindeutigkeit der Primzahlzerlegung

Jede natürliche Zahl n > 1 lässt sich als Produkt von Primzahlpotenzen darstellen:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$$

Die Primzahlen dieser Darstellung und die Exponenten (d.h. die Häufigkeit ihres Auftretens) sind eindeutig, d.h. die Darstellung als Produkt von Primzahlpotenzen ist bis auf die Reihenfolge eindeutig.

Anwendungen des Hauptsatzes

- Charakterisierung und Bestimmung vom ggT und kgV
- Beweis des Zusammenhangs zwischen ggT und kgV
- Charakterisierung von teilerfremden Zahlen
- Beweis der Teilbarkeitsregel für teilerfremde Zahlen

4. Zahlentheorie

4.4 Modulare Arithmetik

Definition einer Restklasse modulo n

Sei $a \in \mathbb{Z}$:

Die Menge $[a]_n := \{b \in \mathbb{Z}: b \bmod n = a \bmod n\}$ heißt *Restklasse* von a modulo n

Eigenschaften von Restklassen:

Diese Definition einer Restklasse induziert eine Äquivalenzrelation auf $\mathbb{Z}$.

Die Restklassen sind die Äquivalenzklassen bzgl. dieser Äquivalenzrelation.

Mit $\mathbb{Z}_n$ wird die Menge der Restklassen bezeichnet.

$\mathbb{Z}_n = \{ [0] , [1] , ... , [n-1] \}$ ($\mathbb{Z}_n$ besteht also aus genau n Elementen)

4. Zahlentheorie

4.4 Modulare Arithmetik

Rechnen mit Restklassen

Addition: $[a]_n + [b]_n := [a+b]_n$

Multiplikation: $[a]_n \bullet [b]_n := [a \cdot b]_n$

Satz: Addition und Multiplikation sind wohldefiniert.

Definition von neutralen und inversen Elementen bzgl. Verknüpfungen:

Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Funktion $f: M \times M \rightarrow M$ mit $f(a,b) = a \circ b$

e heißt *neutrales Element* bzgl. einer Verknüpfung $\circ$, wenn $\forall m \in M: e \circ m = m \circ e = m$

m^{-1} heißt *inverses Element* von m bzgl. einer Verknüpfung $\circ$, wenn $m^{-1} \circ m = m \circ m^{-1} = e$

Anm.: Bei nichtkommutativen Verknüpfungen unterscheidet man zwischen links- und rechtsneutralen Elementen sowie zwischen links- und rechtsinversen Elementen.

4. Zahlentheorie

4.4 Modulare Arithmetik

Neutrale und inverse Elemente von Restklassen

$[0]_n$ ist das neutrale Element der Addition: $\forall a \in \mathbb{Z}: [0]_n + [a]_n = [a]_n + [0]_n = [a]_n$

$[n-a]_n$ ist das inverse Element von $[a]_n$ der Addition: $\forall a \in \mathbb{Z}: [n-a]_n + [a]_n = [a]_n + [n-a]_n = [0]_n$

$[1]_n$ ist das neutrale Element der Multiplikation: $\forall a \in \mathbb{Z}: [1]_n \bullet [a]_n = [a]_n \bullet [1]_n = [a]_n$

Ein inverses Element von $[a]_n$ der Multiplikation existiert nicht immer!

Satz: Ein inverses Element von $[a]_n$ der Multiplikation existiert genau dann, wenn a und n teilerfremd sind.

Korollar: Ein inverses Element von $[a]_n$ der Multiplikation existiert für alle $a \neq 0$, wenn n eine Primzahl ist.