Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kap. 4: Zahlentheorie

Referenzen zum Nacharbeiten:

Iwanowski/Lang 4
Beutelspacher 5
Steger 3

4. Zahlentheorie

In diesem Kapitel repräsentieren die Variablen aller Definitionen und Sätze (Regeln), wenn nicht anders spezifiziert, ***ganze*** *Zahlen (Elemente von $\mathbb{Z}$). Fast alle Definitionen und Sätze können auch auf $\mathbb{N}$ beschränkt werden.*

4.1 Teilbarkeit

Definition von Teilbarkeit

Eine ganze Zahl m ≠ 0 ***teilt*** eine ganze Zahl n, wenn es eine ganze Zahl q gibt mit: n = q·m

$$(\forall\, m, n \in \mathbb{Z}: m \mid n :\Leftrightarrow \exists q \in \mathbb{Z}: n = q \cdot m)$$

Teilbarkeitssätze über Summen, Differenzen und Produkte

1) $m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 + n_2)$

2) $m \mid n_1 \wedge m \mid n_2 \Rightarrow m \mid (n_1 - n_2)$

3) $m \mid n_1 \Rightarrow m \mid (n_1 \cdot n_2)$

4. Zahlentheorie

4.1 Teilbarkeit

Größenbeschränkungen für Teiler und Vielfache

1) Sei $n \neq 0$: Für jeden echten Teiler $m \neq 1,n,-n$ von n gilt: $m \leq |\, n / 2 \,|$

2) Für zwei Teiler p,q von n mit $p \cdot q = n$ gilt: $(p \leq \sqrt{|n|}) \vee (q \leq \sqrt{|n|})$

3) Die einzigen Vielfachen n von m mit $|\, n \,| \leq |\, m \,|$ sind $-m$, 0 und m

4. Zahlentheorie

4.1 Teilbarkeit

Zahlendarstellungen mit Hilfe von Zahlenbasen

$n = \pm (a_i \cdot b^i + a_{i-1} \cdot b^{i-1} + \ldots + a_0 \cdot b^0)$ wobei $\forall j \in \{0,\ldots,i\}: a_j \in \{0,1,\ldots,b-1\}$

Kurzdarstellung: $n = \pm [a_i\ a_{i-1}\ \ldots\ a_0]_b$

Dezimale Darstellung: $b = 10$

Binäre Darstellung: $b = 2$

Definition der Quersumme $Q_b(n)$ in Abhängigkeit von der Zahlenbasis b:

Es sei $n = \pm [a_i\ a_{i-1}\ \ldots\ a_0]_b$ $Q_b(n) := a_i + a_{i-1} + \ldots + a_0$

Quersummenregeln

$3 \mid n \Leftrightarrow 3 \mid Q_{10}(n)$

$9 \mid n \Leftrightarrow 9 \mid Q_{10}(n)$ Allgemein: $b-1 \mid n \Leftrightarrow b-1 \mid Q_b(n)$

Für die *binäre* Quersumme gibt das keine hilfreiche Quersummenregel.

4. Zahlentheorie

4.1 Teilbarkeit

Definition von ggT und kgV

$a = ggT(m,n) :\Leftrightarrow (a \mid m) \wedge (a \mid n) \wedge [(b \mid m) \wedge (b \mid n) \Rightarrow (b \leq a)]$

$a = kgV(m,n) :\Leftrightarrow (m \mid a) \wedge (n \mid a) \wedge (a > 0) \wedge [(m \mid b) \wedge (n \mid b) \wedge (b \neq 0) \Rightarrow (a \leq |b|)]$

Zusammenhang zwischen ggT und kgV

$\forall\, m,n \in \mathbb{N}\setminus\{0\}: \qquad ggT(m,n) \cdot kgV(m,n) = m \cdot n$

Teilbarkeitsregel für teilerfremde Zahlen

Definition: Zwei ganze Zahlen m,n heißen teilerfremd $:\Leftrightarrow ggT(m,n) = 1$

Satz: Für zwei teilerfremde Zahlen m,n und eine ganze Zahl a gilt :
$m \mid a \wedge n \mid a \Rightarrow m \cdot n \mid a$

4. Zahlentheorie

4.2 Teilen mit Rest

Definition von ganzzahligem Quotienten und Rest

(1) Sei $n = q \cdot m + r$ für ganze Zahlen n,m,q,r, $0 \leq r < |m|$

Dann ist q der ganzzahlige Quotient von n geteilt durch m ($q = n \text{ DIV } m$)

Dann ist r der ganzzahlige Rest von n geteilt durch m ($r = n \text{ MOD } m$)

Eindeutigkeit und Existenz von ganzzahligem Quotienten und Rest

Für beliebige zwei ganze Zahlen n und $m \neq 0$ gibt es die Darstellung (1)

Die Darstellung (1) ist eindeutig,
d.h. q und r sind zu gegebenen n,m eindeutig bestimmt.

4. Zahlentheorie

4.2 Teilen mit Rest

Euklidischer Algorithmus zur Bestimmung von ggT und kgV

Satz: Sei $n = q \cdot m + r$ für ganze Zahlen n,m,q,r, $0 \leq r < m$

Dann gilt: $ggT(n,m) = ggT(m,r)$

Seien $n,m > 0$:

Algorithmus:

1) Berechne q und r für n und m

2) Falls r = 0: Setze ggT := m, fertig!
   Anderenfalls: Setze n := m und m := r und gehe zu 1)

Was machen wir, wenn n oder m negativ sind?

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 :$\Leftrightarrow$ $(p \in \mathbb{N}) \wedge (p > 1) \wedge (((n \in \mathbb{N}) \wedge (n \mid p)) \Rightarrow ((n = 1) \vee (n = p)))$)

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

- Das Sieb des Eratosthenes ist nicht effizient für große Zahlen.
- Es gibt effizientere Verfahren zur Primzahl**bestimmung**.
- Es sind keine effizienteren Verfahren zur **allgemeinen** Primfaktor**zerlegung** bekannt.
- Kryptographische Verfahren verwenden Produkte riesiger Primzahlen
  und halten ihre Zerlegung geheim.
- Sicher sind nur Faktoren mit mehr als 1000 bits (Stand: 2013)

Anzahl von Primzahlen: Relevant für die Suche nach sicheren Faktoren

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:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$$

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.

4. Zahlentheorie

4.3 Primzahlen

Anwendungen des Hauptsatzes

Charakterisierung und Bestimmung vom ggT und kgV:

Seien $m = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_s^{m_s}$ und $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_s^{n_s}$

$$ggT(m,n) = p_1^{\min\{m_1,n_1\}} \cdot p_2^{\min\{m_2,n_2\}} \cdot \ldots \cdot p_s^{\min\{m_s,n_s\}}$$

$$kgV(m,n) = p_1^{\max\{m_1,n_1\}} \cdot p_2^{\max\{m_2,n_2\}} \cdot \ldots \cdot p_s^{\max\{m_s,n_s\}}$$

Aus Folie DM4-5:

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.

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

4. Zahlentheorie

4.4 Modulare Arithmetik

Rechnen mit Restklassen

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

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

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: $\forall a \in \mathbb{Z}: [1]_n \cdot [a]_n = [a]_n \cdot [1]_n = [a]_n$

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.

4. Zahlentheorie

4.4 Modulare Arithmetik

Beispiele für das Rechnen in Restklassen:

$\mathbb{Z}_2$

$\oplus$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\mathbb{Z}_5$

$\oplus$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

$\odot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

$\mathbb{Z}_6$

$\oplus$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$\odot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$