Diskrete Strukturen
Großübung

Amelie Heindl

Lehrstuhl für Logik und Semantik

Technische Universität Berlin

Sommersemester 2024

Themenüberblick

Themenüberblick: Vorlesungswoche 9

- Teilbarkeit und Primzahlen
- Modulo
- Rechenregeln
- Algorithmus von Euklid

Teilgebiete der Mathematik

Teilgebiete der Mathematik: Überblick

Diskrete Mathematik

Die diskrete Mathematik untersucht endliche und abzählbar unendliche mathematische Strukturen und Probleme auf diesen. Sie enthält unter Anderem die Gebiete Graphentheorie und Kombinatorik.

Zahlentheorie

Die Zahlentheorie beschäftigt sich mit den Eigenschaften von Zahlen und dem Rechnen. Ein wichtiges (und das ursprüngliche) Teilgebiet betrachtet die ganzen Zahlen. Man spricht dann auch von Arithmetik.

Modulare Arithmetik

Die Modulare Arithmetik ist ein Teilgebiet der Zahlentheorie. Sie beschäftigt sich mit den Eigenschaften und Operationen von ganzen Zahlen modulo eines Wertes.

Algebra

Algebra beschäftigt sich mit Strukturen, die aus Mengen und Operationen auf den Mengenelementen bestehen. Algebraische Methoden und Erkenntnisse können in der Zahlentheorie genutzt werden.

Teilbarkeit und Primzahlen

Teilbarkeit und Primzahlen: Grundlagen

Wir definieren 'teilen' auf den ganzen Zahlen.

teilen

Seien $a, b \in \mathbb{Z}$. Dann gilt $a|b$, falls ein $q \in \mathbb{Z}$ existiert mit $q \cdot a = b$.
Man nennt a dann Teiler von b.

Nach dieser Definition kann eine Zahl also auch negative Teiler haben, wir interessieren und jedoch vorwiegend für die positiven.

Offensichtlich gilt $1 \cdot a = a$ für jedes $a \in \mathbb{Z}$ und damit sind 1 und a immer Teiler von a.
Welche anderen Teiler eine Zahl hat, ist weniger offensichtlich.

Primzahl

Sei $p \in \mathbb{Z}$ mit $p \geq 2$. Dann ist p eine Primzahl, falls 1 und p die einzigen positiven Teiler von p sind. Die Menge der Primzahlen wird manchmal mit $\mathbb{P}$ bezeichnet.

Teilbarkeit und Primzahlen: Eigenschaften

Primzahlen haben einige schöne und nützliche Eigenschaften.

Fundamentalsatz der Arithmetik

Jede natürliche Zahl $n > 1$ hat eine eindeutige Primfaktorzerlegung. Das bedeutet sie lässt sich eindeutig in der Form $n = \prod_{i=1}^{k} p_i^{e_i}$ mit $p_i \in \mathbb{P}$ und $e_i \in \mathbb{N}$ für $1 \leq i \leq k$ darstellen.

- Für Primzahlen p besteht die Primfaktorzerlegung aus einem Faktor, p selbst.
- Natürliche Zahlen, deren Primfaktorzerlegung mehr als einen Faktor hat, heißen zusammengesetzt.

Für den größten gemeinsamen Teiler $\mathrm{ggT}(a,b) := \max\{k \in \mathbb{N} \mid k \text{ teilt } a \text{ und } k \text{ teilt } b\}$ und das kleinste gemeinsame Vielfache $\mathrm{kgV}(a,b) := \min\{k \in \mathbb{N} \mid a \text{ teilt } k \text{ und } b \text{ teilt } k\}$ gilt bei Primzahlen $p, q \in \mathbb{P}$ mit $p \neq q$:

$$\mathrm{ggT}(p,q) = 1 \quad \text{und} \quad \mathrm{kgV}(p,q) = p \cdot q$$

Teilbarkeit und Primzahlen: Beispiele

Wir betrachten beispielhaft einige Zahlen und ihre Teilbarkeiten:

Ist diese Zahl prim?

- 23 Ja, denn 1 und 23 sind ihre einzigen positiven Teiler.
- 69 Nein, denn es gilt beispielsweise $23|69$, wegen $3 \cdot 23 = 69$.
- -23 Nein, denn $-23 \not\geq 2$.

Wie sieht die Primzahlzerlegung dieser Zahlen aus?

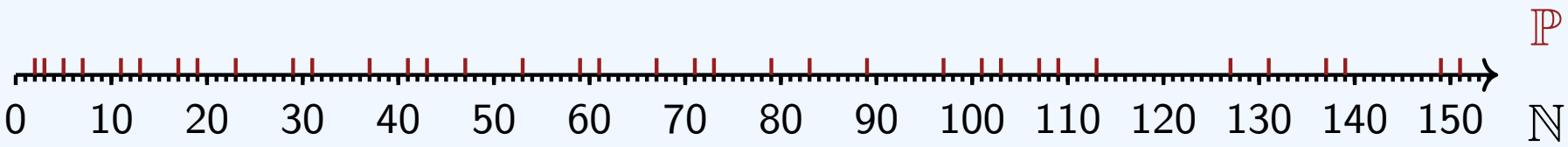
- $1024 = 2^{10}$ (wir haben also $p_1 = 2$ und $e_1 = 10$)
- $666 = 2 \cdot 3^2 \cdot 37$ (wir haben also $p_1 = 2, p_2 = 3, p_3 = 37$ und $e_1 = 1, e_2 = 2, e_3 = 1$)
- $100 = 2^2 \cdot 5^2$ (wir haben also $p_1 = 2, p_2 = 5$ und $e_1 = 2, e_2 = 2$)

Was ist der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache?

- $\mathrm{ggT}(11,13) = 1$ $\quad$ $\mathrm{kgV}(11,13) = 143$
- $\mathrm{ggT}(513,513) = 513$ $\quad$ $\mathrm{kgV}(513,513) = 513$
- $\mathrm{ggT}(-30,45) = 15$ $\quad$ $\mathrm{kgV}(-30,45) = 90$

Teilbarkeit und Primzahlen: Vorkommen

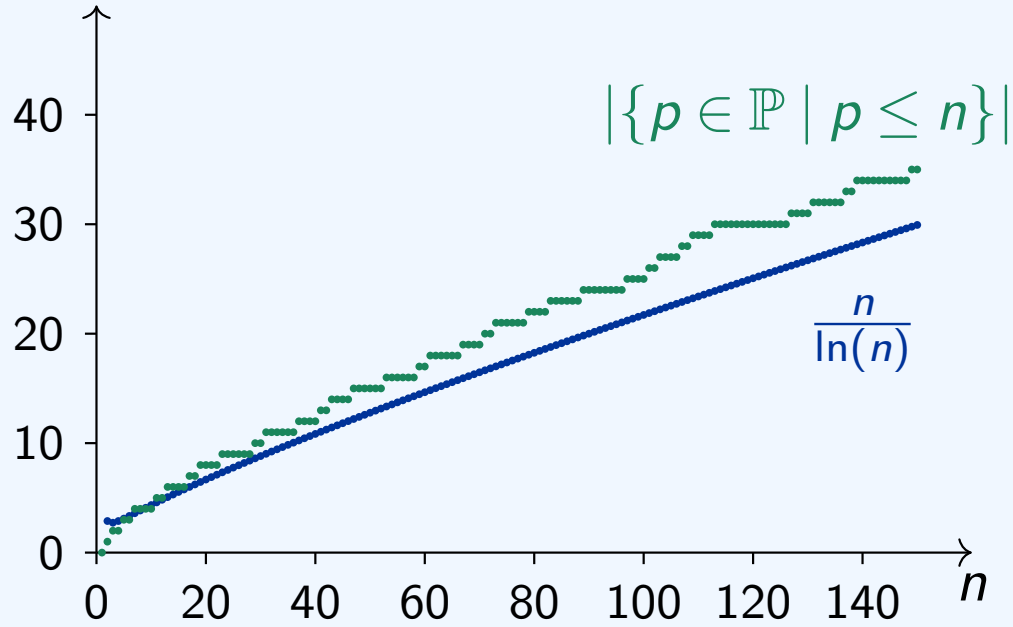
Trotz ihrer simplen Definition, ist das Auftauchen von Primzahlen recht unregelmäßig.



Einige Schranken und Abschätzungen für das Vorkommen und die Verteilung von Primzahlen sind bekannt.

Primzahlsatz: Für jedes $n \in \mathbb{N}$ mit $n > 1$ gibt es $(1 + o(1) \cdot \frac{n}{\ln(n)})$ viele Primzahlen, die höchstens so groß sind wie n.

$$\pi(n) \quad = \quad (1 + o(1)) \cdot \frac{n}{\ln(n)}.$$



Teilbarkeit und Primzahlen: Finden

Für einige Anwendungen, beispielsweise in der Kryptographie, ist es notwendig, Primzahlen zu finden.

Allerdings gibt es kein effizientes Verfahren, um Primzahlen zu generieren.

Stattdessen werden Zahlen ausgewählt und auf Primalität getestet.

In der Theorie ist das mit dem AKS-Test fehlerfrei in P möglich.

In der Praxis werden schnellere Test verwendet, die mit geringer Wahrscheinlichkeit ein falsches Ergebnis liefern.

Modulooperation

Modulooperation: Grundlagen

Eng verbunden mit dem Konzept der Teilbarkeit ist die Rechenoperation Modulo. Rechnet man eine Zahl modulo einer anderen ist das Ergebnis der Rest der Division dieser Zahlen.

Modulo

Seien $m, z \in \mathbb{Z}$ mit $m \geq 2$. Dann gibt es eindeutige Zahlen $q \in \mathbb{Z}$ und $r \in \{0, \ldots, m-1\}$ mit $z = q \cdot m + r$. Die Modulooperation ist dann definiert durch $z \bmod m = r$.

Beispiele:

z	m	q	r
56	9	6	2
56	7	8	0
-15	8	-2	1
5	12	0	5

Wir rechnen also Division mit Rest von z geteilt durch m.
Das ganzzahlige Ergebnis ist dann q und der Rest ist r.

Modulooperation: Grundlagen

z mod m ist also immer eine ganze Zahl zwischen 0 und $m-1$.

Insbesondere in der Programmierung ist es hilfreich, die Größe des Ergebnisses einer Operation so einschränken zu können.

Oft interessiert man sich dafür, welche Zahlen Modulo einem festen Wert m das gleiche Ergebnis liefern, also bei der Division durch m den gleichen Rest lassen.

Beispiel: Möchte man (in einem Programm) die Parität zweier Zahlen vergleichen, kann man testen, ob sie Modulo 2 das gleiche ergeben.

Modulo m zu rechnen, setzt verschiedene Zahlen miteinander in Relation. Das wollen wir nun formalisieren.

Relationen

Relationen: Grundlagen

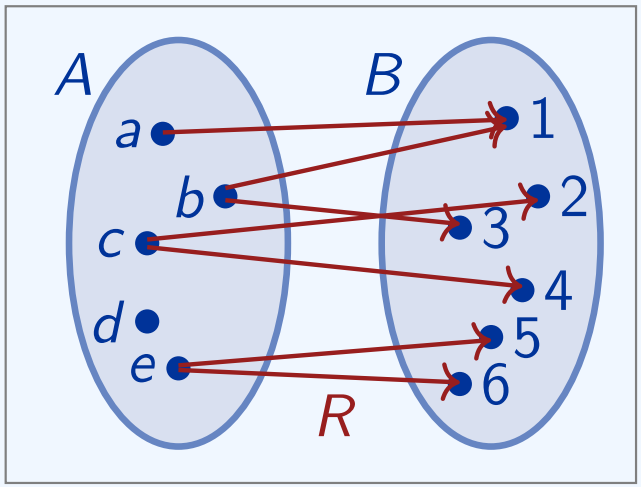
Relation verbinden Elemente von Mengen miteinander. Elemente, die miteinander verbunden sind, sind als Tupel in der Relation enthalten. Hier interessieren wir uns für binäre Relationen, diese enthalten 2-Tupel.

Relation

Seien A, B Mengen. Eine binäre Relation ist eine Teilmenge $R \subseteq A \times B$.

Beispiel:

$A = \{a, b, c, d, e\}$
$B = \{1, 2, 3, 4, 5, 6\}$
$R = \{(a, 1), (b, 1), (b, 3), (c, 2), (c, 4), (e, 5), (e, 6)\}$



Relationen: Grundlagen

Funktionen/Abbildungen stellen einen Spezialfall von Relationen dar, bei denen $|\{b \in B \mid (a,b) \in R\}| = 1$ für alle Elemente $a \in A$ gilt. Jedes Element aus A steht also mit genau einem Element von B in Relation.

Bei Relationen kann insbesondere auch $A = B$ gelten, also Elemente aus einer Menge mit Elementen aus der selben Menge in Relation gesetzt werden. Man nennt R dann eine Relation auf A.
Beispiel: In einem gerichteten Graphen G ist die Kantenmenge $E(G)$ als Teilmenge des kartesischen Produkts der Knotenmenge mit sich selbst definiert. $E(G)$ stellt also eine Relation auf $A = B = V(G)$ dar.

Relationen: Äquivalenzrelationen

Eine interessante Art von Relationen auf einer Menge A sind Äquivalenzrelationen.

Äquivalenzrelation

Sei $R \subseteq A \times A$ eine Relationen. Wenn R reflexiv, transitiv und symmetrisch ist, ist R eine Äquivalenzrelation.

- R ist reflexiv, falls $(a, a) \in R$ für alle $a \in A$ gilt.
- R ist transitiv, falls für alle $a, b, c \in A$, für die $(a, b), (b, c) \in R$ gilt, auch $(a, c) \in R$ gilt.
- R ist symmetrisch, falls für alle $a, b \in A$, für die $(a, b) \in R$ gilt, auch $(b, a) \in R$ gilt.

Eine Äquivalenzrelation auf einer algebraischen Struktur, die mit den Operationen der Struktur verträglich ist, heißt Kongruenzrelation.

Relationen: Beispiele

Welche Eigenschaften haben folgende Relationen?

Menge A	**Relation R auf A**	**Reflexiv?**	**Transitiv?**	**Symmetrisch?**
$\mathbb{Z}$	kleiner sein als	Nein	Ja	Nein
$\mathbb{N}$	Teiler sein von	Ja	Ja	Nein
$\mathscr{P}(\{a, b, c, d\})$	gleichmächtig sein	Ja	Ja	Ja
Personen auf der Welt	jemanden mögen	Nein	Nein	Nein
Wörter im Duden	Homophon sein zu	Nein	Nein	Ja

Relationen: Äquivalenzklassen

Jede Äquivalenzrelation R auf A erzeugt eine Partition von A. Die entstehenden Teilmengen werden Äquivalenzklasse genannt.

Jedes Element $a \in A$ ist also in genau einer Äquivalenzklasse enthalten. Zwei Elemente $a, b \in A$ sind genau dann in der gleichen Äquivalenzklasse, wenn sie in Relation stehen.

Ein Repräsentantensystem für eine Äquivalenzrelation ist eine Teilmenge $S \subseteq A$, die aus jeder Äquivalenzklasse genau ein Element enthält.

Beispiel: Sei A die Menge aller einfachen ungerichteten Graphen G mit $V(G) \subseteq \{v_1, \ldots, v_{10}\}$. Sei R die Relation auf A, die alle Paare (G_1, G_2) von Graphen enthält, für die $V(G_1) = V(G_2)$ gilt. R ist eine Äquivalenzrelation. Für jede Teilmenge von $\{v_1, \ldots, v_{10}\}$ gibt es eine Äquivalenzklasse, die alle Graphen mit dieser Knotenmenge enthält. Ein Repräsentantensystem wäre beispielsweise $\{G = (V, \emptyset) \mid V \in \mathscr{P}(\{v_1, \ldots, v_{10}\})\}$.

Modulo Kongruenzrelation

Modulo Kongruenzrelation: Grundlagen

同余关系

Für jede Zahl $m \geq 2$ kann man eine Kongruenzrelation auf $\mathbb{Z}$ definieren, bei der Elemente in Relation stehen, wenn sie modulo m das Gleiche ergeben.

Kongruenzrelation modulo m

Seien $a, b \in \mathbb{Z}$ und $m \geq 2$. Dann ist $\equiv (\bmod m)$ eine Kongruenzrelation auf $\mathbb{Z}$, definiert durch:

$$a \equiv b \pmod{m} \text{ genau dann, wenn } m \mid (a - b)$$

Die Relation $\equiv (\bmod m)$ erzeugt m viel Äquivalenzklassen. Die eindeutig definierte Zahl $(a \bmod m)$ ist beispielsweise ein geeigneter Repräsentant für die Äquivalenzklasse, die a enthält. Damit ergibt sich $\mathbb{Z}_m = \{0, \ldots, m-1\}$ als mögliches Repräsentantensystem.

Modulo Kongruenzrelation: Beispiel

Wir betrachten die Kongruenzrelation modulo 7.

- es gilt $50 \equiv 15 \pmod 7$, wegen $(50-15) = 35$ und $7 \mid 35$
- es gilt $30 \not\equiv 12 \pmod 7$, wegen $(30-12) = 18$ und $7 \nmid 18$
- es gibt sieben Äquivalenzklassen:

$$\{0, 7, 14, 21, 28, 35, 49, 56, 63, 70, \ldots\}$$
$$\{1, 8, 15, 22, 29, 36, 50, 57, 64, 71, \ldots\}$$
$$\{2, 9, 16, 23, 30, 37, 51, 58, 65, 72, \ldots\}$$
$$\{3, 10, 17, 24, 31, 38, 52, 59, 66, 73, \ldots\}$$
$$\{4, 11, 18, 25, 32, 39, 53, 60, 67, 74, \ldots\}$$
$$\{5, 12, 19, 26, 33, 40, 54, 61, 68, 75, \ldots\}$$
$$\{6, 13, 20, 27, 34, 41, 55, 62, 69, 76, \ldots\}$$

- ein Repräsentantensystem ist $\mathbb{Z}_m := \{0, 1, 2, 3, 4, 5, 6\}$

Rechenregeln

Rechenregeln: plus und mal modulo m

Wir haben gesehen, das das rechnen Modulo einer Zahl m immer Ergebnisse kleiner als m erzeugt. Da modulo m eine Kongruenzrelation ist, kann man das Verknüpfen ganzer Zahlen und anschließendes modulo m Rechnen vereinfachen, indem man erst die Operanden modulo m rechnet.

Es gilt für alle $a, b \in \mathbb{Z}$ und $m \geq 2$:

$$\begin{aligned} (a+b) \mod m &= ((a \mod m)+(b \mod m)) \mod m \\ (a \cdot b) \mod m &= ((a \mod m) \cdot (b \mod m)) \mod m. \end{aligned}$$

Beispiele:

$(270+55) \mod 6 = ((270 \mod 6)+(55 \mod 6)) \mod 6 = (0+1) \mod 6 = 1$

$$\begin{aligned} (120+70) \mod 11 &= ((120 \mod 11)+(70 \mod 11)) \mod 11 \\ &= (10+4) \mod 11 = 14 \mod 11 = 3 \end{aligned}$$

$(81 \cdot 42) \mod 5 = ((81 \mod 5) \cdot (42 \mod 5)) \mod 5 = (1 \cdot 2) \mod 5 = 2$

$$\begin{aligned} (100 \cdot 30) \mod 8 &= ((100 \mod 8) \cdot (30 \mod 8)) \mod 8 = (4 \cdot 6) \mod 8 \\ &= 24 \mod 8 = 0 \end{aligned}$$

Feedback, Fragen und Vorschläge zur Großübung gerne an:

a.heindl@tu-berlin.de