Mathematik I

Zahlentheorie I

Prof. Dr. Doris Bohnet

Sommersemester 2020

Zeitplan Vorlesung

		Datum	Bemerkung	Inhalt
Grund-lagen			Selbststudium	Grundlagen: Mengen
			Selbststudium	Grundlagen: Relationen
			Selbststudium	Grundlagen: Abbildungen
Zahlen-theorie	1	22.04.	Einmalig Mi.	Wiederholung & Zusammenfassung Selbststudium
	2	**27.04.**		**Zahlentheorie I**
	3	28.04.		Zahlentheorie II
Algebra	4	04.05.		Gruppen
	5	11.05.		Ringe, Körper
	6	12.05.		Kryptographie
	7	18.05.		Vektorräume
Lineare Algebra	8	25.05.		Lineare Gleichungssysteme
	9	26.05.		Lineare Gleichungssysteme
	10	01.06.	Pfingstmontag	--
	11	08.06.		Matrizen
	12	09.06.		Lineare Abbildungen

Lernziele

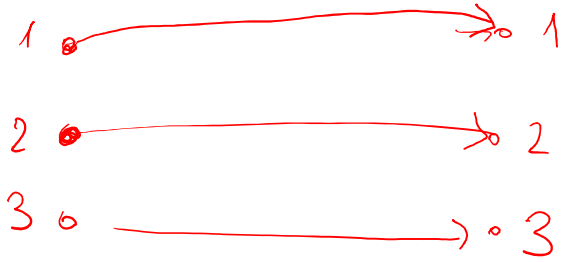
- **Begriffe bzw. Aussagen kennen:**
  - ✓ Teiler bzw. größter gemeinsamer Teiler (ggT)
  - ✓ Primzahl
  - ✓ natürliche, ganze, rationale und reelle Zahlenmengen

- und üben,
  - ✓ Beweise mit Hilfe der vollständigen Induktion durchzuführen;
  - ✓ mit Hilfe des euklidischen Algorithmus den ggT zweier ganzer Zahlen zu berechnen;
  - ✓ in Restklassen zu rechnen (Modulorechnung);

- ✓ (optional: Anwendung von ISBN-Prüfziffern und IBAN-Prüfziffern kennen.)

Wiederholung: Abbildungen

$f: \{1,2,3\} \longrightarrow \{1,2,3\}$



bijektiv

Wieviele Abbildungen $f: \{1,2,3\} \to \{1,2,3\}$ bijektiv gibt es?

$3 \cdot 2 \cdot 1 = 3!$ „3 Fakultät"

Vermutung: $n!$ bijektive Abbildungen von $\{1,\dots n\} \to \{1,\dots,n\}$

$A(n)$ $n \in \mathbb{N}$

Beweisprinzip Vollständige Induktion

Satz: Seien A, B endliche Mengen mit $|A| = |B| = n$.
Dann gibt es genau $n!$ Verschiedene bijektive Abbildungen $f: A \to B$.

Vollständige Induktion

Induktionsanfang: I.A. $A(1)$

$f: \{1\} \to \{1\}$, nur eine bijektive Abb. ✓

Induktionsvoraussetzung: I.V. $A(n)$ sei richtig für $n \in \mathbb{N}$

Induktionsschritt: $A(n) \Rightarrow A(n+1)$

$f: \{1, 2, \dots, n+1\} \longrightarrow \{1, \dots, n+1\}$

↳ $n+1$ ver. Punkte, auf die $(n+1)$ abgebildet werden kann

also unter I.V.: $(n+1) \cdot n! = (n+1)!$ Abbildungen

$n! := n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1$

□

Beweisprinzip Vollständige Induktion

Bsp: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

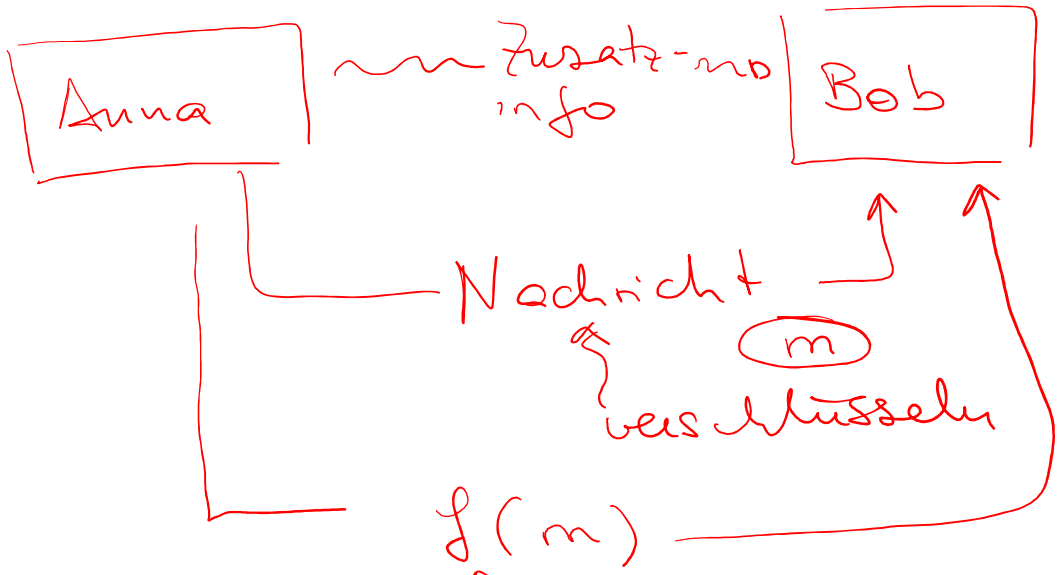
Induktionsanfang: $n=1$: $\sum_{k=1}^{1} k = 1 = \frac{1\cdot(1+1)}{2}$ ✓

Induktionsvoraussetzung (I.V.): $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ sei wahr für $n \in \mathbb{N}$

Induktionsschritt: Wir zeigen die Aussage für $(n+1)$ unter Verwendung der I.V.

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) \overset{\text{I.V.}}{=} \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$ □

Motivation - Verschlüsselungstechnik



z.B. Produkt: $n \cdot m$

$f(m)$ schnell zu rechnen

aber $f^{-1}(f(m)) = m$ schwer

Teiler finden

zu rechnen, aber mit Zusatzinfo leicht.

Größter gemeinsamer Teiler

Eine natürliche Zahl d heißt **Teiler** einer Zahl $a \in \mathbb{Z}$, falls eine ganze Zahl $k \in \mathbb{Z}$ existiert, so dass:

$$a = k \cdot d$$

Man schreibt kurz: $d \mid a$

$a = 42, \quad 7 \mid 42$

$42 = 6 \cdot 7$

$a = k \cdot d$

Eine natürliche Zahl d , die

- zwei Zahlen $a, b \in \mathbb{Z}$ teilt ($d \mid a$ und $d \mid b$), und
- für jeden Teiler d' von $a, b \in \mathbb{Z}$ gilt: $d' \leq d$

heißt **größter gemeinsamer Teiler** von $a, b \in \mathbb{Z}$.

Man schreibt: $ggT(a, b) = d$

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremd**, falls $ggT(a, b) = 1$ gilt.

$a = 42, \quad b = 24$

$ggT(24, 42) = 6$

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

$42 = 2 \cdot 3 \cdot 7$

Primzahl & Primfaktorzerlegung

Eine natürliche Zahl $p \geq 2$ heißt **Primzahl**, falls sie nur die Teiler 1 und p besitzt.

Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige **Primfaktorzerlegung**, d.h. es existieren Primzahlen $p_1 < \cdots < p_k$ und natürliche Zahlen $a_1, \ldots, a_k$ so dass

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

gilt.

$24 = 2^3 \cdot 3$

Beispiel:
Die Zahl 42 besitzt die Primfaktorzerlegung: $42 = 2 \cdot 3 \cdot 7$
Die Zahl 28 besitzt die Primfaktorzerlegung: $28 = 2^2 \cdot 7$
Die Zahl 48 besitzt die Primfaktorzerlegung: $48 = 2^4 \cdot 3$

Division mit Rest

Für beliebige Zahlen $a, b \in \mathbb{Z}$ gibt es genau eine Darstellung

$$a = bq + r$$

mit $q, r \in \mathbb{Z}, 0 \leq r < |b|$.

Man schreibt auch kurz: $a = r \; mod \; b$

$4 \nmid 15 \quad : \quad 15 : 4 = 3 \; R \; 3$

$15 = 3 \bmod 3$

$15 = 3 \cdot 4 + 3$

$b \quad q \quad = r$

Euklidischer Algorithmus - Beispiel

$a = 127 = r_0$
$b = 24 = r_1$

$r_0 \leq r_1$

↳ Berechnung des ggT

$127 = 5 \cdot 24 + 7$
$24 = 3 \cdot 7 + 3$
$7 = 2 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$

113 ←

$ggT(127, 24) = 1$

$r_{j+1} \mid r_0$ und $r_{j-1} \mid r_1$
⋮
$r_{j+1} \mid r_{j-1}$ ←
$r_{j+1} \mid r_j$ ←

$r_0 = k \cdot r_1 + r_2$
$r_1 = k \cdot r_2 + r_3$
$r_{j-1} = k \cdot r_j + r_{j+1}$
$r_j = k \cdot r_{j+1} + r_{j+2} = 0$

bis $r_{j+2} = 0$

Euklidischer Algorithmus

Man kann den größten gemeinsamen Teiler mit Hilfe des euklidischen Algorithmus iterativ berechnen:

Input: $n, m \in \mathbb{Z}, m \leq n$
Output: $ggT(n, m)$

Algorithmus $euklid(n, m)$

Falls $n = k \cdot m$, setze $ggT(n, m) = m$ und return.
Sonst: $n = k \cdot m + r, r < m$, setze $n = m, m = r$ und rechne $euklid(n, m)$.

Erweiterter euklidischer Algorithmus

Input: $a, b \in \mathbb{Z}, a \leq b$
Output: $ggT(a,b), x, y: d = ax + by$

Setze $x_0 = 0, x_1 = 1, y_0 = 1, y_1 = 0$.

Algorithmus $euklid(a, b, x_0, x_1, y_0, y_1)$.

Falls $a = k \cdot b$, setze $ggT(a,b) = b, x = x_0, y = y_0$ und return.
Sonst: $\mathrm{r} = a - k \cdot b, r < b$, $x_2 = x_0 - kx_1, y_2 = y_0 - ky_1$,
setze $\mathrm{a} = \mathrm{b}, \mathrm{b} = \mathrm{r}, \mathrm{x}_2 = x_0 - kx_1, \mathrm{y}_2 = y_1, y_1 = y_0$ und rechne $euklid(a, b, x_0, x_1, y_0, y_1)$.

Erweiterter euklidischer Algorithmus

$a, b \in \mathbb{Z} \Rightarrow ggT(a,b) = d$

$x, y \in \mathbb{Z} : d = ax + by$

$a = 104, b = 47$

i	a	b	x	y	k
0	104	47	1	0	—
1	47	10	0	1	2
2	10	7	1	−2	4
3	7	3	−4	9	1
4	3	1	5	−11	2
5	1	0	−14	31	3

Rest = 0 : Tabelle ist zu Ende!

$ggT(104, 47) = 1$

$1 = (-14) \cdot 104 + 31 \cdot 47$

Erweiterter euklidischer Algorithmus

Satz: Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd $\Leftrightarrow \exists x, y\colon\ 1 = ax + by$.

Restklassen - Beispiel

$n = 4$:

$3 : 4 = 0 \text{ R } 3 \quad = 0 \cdot 4 + 3 = 3 \bmod 4$

$7 : 4 = 1 \text{ R } 3 \quad = 1 \cdot 4 + 3 = 3 \bmod 4$

$12 : 4 = 3 \text{ R } 0 \quad = 3 \cdot 4 + 0 = 0 \bmod 4$

"Äquivalenzrelation

$$a \equiv_4 b \quad :\Longleftrightarrow \quad a - b = 0 \bmod 4$$

↖ a, b haben denselben Rest, wenn durch 4 geteilt

"Äquivalenzklasse = Restklasse

$[0] = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$

$[1] = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$

$[2] = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$

$[3] = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$

$[4] = [0]$

Restklassen

Auf $\mathbb{Z}$ ist für jedes $n \in \mathbb{N}$ eine Äquivalenzrelation definiert durch:

$$a \equiv_n b \Leftrightarrow a = b \; mod \; n$$

Man liest: „a gleich b modulo n“.
Die Äquivalenzbeziehung $\equiv_n$ besitzt genau n Äquivalenzklassen:

$$[0] = \{a \in \mathbb{Z} |\; a = 0 \; mod \; \text{n}\}, [1] = \{a \in \mathbb{Z} |\; a = 1 \; mod \; \text{n}\}, \dots, [n-1] = \{a \in \mathbb{Z} |\; a = (n-1) \; mod \; \text{n}\}$$

Wir nennen diese Äquivalenzklassen **Restklassen** und schreiben kurz für die Menge der Äquivalenzklassen:

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}, |\mathbb{Z}_n| = n$$

Beispiel:
Es gibt nur eine Restklasse von 1, deswegen ist $\mathbb{Z}_1 = \{[0]\} = \mathbb{Z}$.
Es gibt zwei Restklassen von 2, deswegen ist $\mathbb{Z}_2 = \{[0], [1]\}$. Die Restklassen enthalten die geraden bzw. ungeraden Zahlen.

Modulorechnung (Rechnen mit Restklassen)

Seien $n_1 = a \; mod \; m, n_2 = b \; mod \; m.$

Addition:

$$(n_1 + n_2) \; = (a + b) \; mod \; m$$

Multiplikation:

$$(n_1 \cdot n_2) = (a \cdot b) \; mod \; m$$

Beispiel:

Wir berechnen $7^{66} mod \; 13$.

$$7^2 \; mod \; 13 = 10$$
$$7^4 \; mod \; 13 = 100 \; mod \; 13 = 9$$
$$7^8 \; mod \; 13 = 81 \; mod \; 13 = 3$$
$$7^{16} \; mod \; 13 = 9 \; mod \; 13 = 9$$
$$7^{32} \; mod \; 13 = 81 \; mod \; 13 = 3$$
$$7^{64} \; mod \; 13 = 9 \; mod \; 13 = 9$$

Dann ist $7^{66} mod \; 13 = 7^{64} mod \; 13 \cdot 7^2 mod 13 = 9 \cdot 10 \; mod \; 13 = 12$

Modulorechnung (Rechnen mit Restklassen)

Beispiel:Teilbarkeitsregeln.

$$a = \sum_i a_i 10^i$$

$$a \; mod \; 3 = \sum_i a_i 10^i \; mod \; 3 = \sum_i a_i \; mod \; 3 \;\; \cdot 1^i = 0 \Leftrightarrow \left(\sum_i a_i \right) mod \; 3 = 0$$

Anwendung: Prüfziffern

Eine ISBN-Nummer besteht aus 13 Ziffern, die letzte Ziffer ist eine Prüfziffer. Die Prüfziffer berechnet sich aus der Modulorechnung wie folgt:

ISBN: $a_1 a_2 \dots a_9$
Prüfziffer: Man wählt die Prüfziffer a_{13}, so dass

$$(1 \cdot a_1 + 3 \cdot a_2 + 1 \cdot a_3 + \cdots + 3 \cdot a_{12} + 1 \cdot a_{13}) mod\ 10 = 0$$

Beispiel:
Wir überprüfen die ISBN-Nummer

978−3−540−89106−2

Prüfziffer: $(9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 5 + 3 \cdot 4 + 0 + 3 \cdot 8 + 9 + 3 \cdot 1 + 0 + 3 \cdot 6) mod\ 10 = 118\ mod\ 10 = 8$
Also ist die Prüfziffer 2.

Anwendung: Prüfziffern

Vertippt man sich an einer Stelle, beispielsweise

979−3−540−89106−2

Berechnet sich die Prüfziffer als wegen

$$(9 + 3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 4 + 0 + 3 \cdot 8 + 9 + 3 \cdot 1 + 0 + 3 \cdot 6) mod\ 10 = 119\ mod 10 = 9$$

als 1. Also wird dieser Tippfehler erkannt.

Vertauschen wir aus Versehen zwei Ziffern

973−8−540−89106−2

Prüfziffer: $(9 + 3 \cdot 7 + 3 + 3 \cdot 8 + 5 + 3 \cdot 4 + 0 + 3 \cdot 8 + 9 + 3 \cdot 1 + 0 + 3 \cdot 6) mod\ 10 = 128\ mod\ 10 = 8$

Also ist die Prüfziffer 2.

Der Fehler wird nicht erkannt.