Diskrete Strukturen

Vorlesung 15: Arithmetik

5. Februar 2019

Nächste Termine — Modul “Diskrete Strukturen”

Hörsaalübung (Mo. 9:15)	**Vorlesung (Di. 17:15)**
4.2. Tutorium (Klausurvorbereitung)	5.2. Arithmetik
11.2.	12.2.
18.2. Prüfungswoche	19.2. Prüfung am Fr., den 22.2. 10 Uhr (AudiMax, Hs. 3, Hs. 9)

Vorlesungsstruktur

1. Mathematische Grundlagen
   - Aussagen- und Prädikatenlogik
   - Naive Mengenlehre
   - Relationen und Funktionen

2. Diskrete Strukturen
   - Algebraische Strukturen
   - Bäume und Graphen
   - Arithmetik

Heutige Vorlesung

- Teilbarkeit und größte gemeinsame Teiler
- Modulares Rechnen
- Euklidischer Algorithmus
- erweiterter Euklidischer Algorithmus

Bitte Fragen direkt stellen!

Arithmetik — Motivation

Motivation:

- modulares Rechnen relevant
  (z.B. Rechnen mit Uhrzeiten, Wochentagen, Datumsangaben)
- Körper $(\mathbb{Z}_p, +_p, \cdot_p, (-\cdot), \cdot^{-1}, [0], [1])$ für p prim
  relevant in Kryptographie und Kodierungstheorie
- Einblick in die Natur ganzer Zahlen

Arithmetik — Wiederholung: Teilbarkeit

Definition (Teiler)

Sei $a \in \mathbb{N}$ und $b \in \mathbb{Z}$. Dann ist a Teiler von b gdw.
ein $k \in \mathbb{Z}$ existiert, so dass $b = k \cdot a$.
Wir schreiben $a \mid b$, falls a Teiler von b ist.

Arithmetik — Wiederholung: Teilbarkeit

Definition (Teiler)

Sei $a \in \mathbb{N}$ und $b \in \mathbb{Z}$. Dann ist a Teiler von b gdw.
ein $k \in \mathbb{Z}$ existiert, so dass $b = k \cdot a$.
Wir schreiben $a \mid b$, falls a Teiler von b ist.

Beispiele

- $11 \mid 121$ denn $121 = 11 \cdot 11$
- $n \mid 0$ für jedes $n \in \mathbb{N}$, denn $0 = 0 \cdot n$
- $2 \nmid 121$ denn $\frac{121}{2} = 60,5 \notin \mathbb{Z}$

Arithmetik — Wiederholung: Teilbarkeit

Definition (Menge der Teiler)

Sei $b \in \mathbb{Z}$. Dann sei

$$T_b = \{a \in \mathbb{N} \mid \text{ es gilt } a \mid b\}$$

die Menge aller Teiler von b.

Arithmetik — Wiederholung: Teilbarkeit

Definition (Menge der Teiler)

Sei $b \in \mathbb{Z}$. Dann sei

$$T_b = \{a \in \mathbb{N} \mid \text{ es gilt } a \mid b\}$$

die Menge aller Teiler von b.

Beispiele

- $T_8 = \{1, 2, 4, 8\}$
- $T_9 = \{1, 3, 9\}$
- $T_{12} = \{1, 2, 3, 4, 6, 12\}$

Arithmetik — Teilbarkeit

Notizen:

- wir wissen bereits, dass $|$ (Teilbarkeit) auf den natürlichen Zahlen eine Ordnungsrelation ist
- hier betrachten wir $|$ jedoch als Relation $| \subseteq \mathbb{N} \times \mathbb{Z}$

§15.1 Theorem

Sei $m \mid b$. Dann gilt $m \mid c$ gdw. $m \mid (b + c)$ für alle $c \in \mathbb{Z}$.

Arithmetik — Teilbarkeit

Notizen:

- wir wissen bereits, dass $|$ (Teilbarkeit) auf den natürlichen Zahlen eine Ordnungsrelation ist
- hier betrachten wir $|$ jedoch als Relation $| \subseteq \mathbb{N} \times \mathbb{Z}$

§15.1 Theorem

Sei $m \mid b$. Dann gilt $m \mid c$ gdw. $m \mid (b + c)$ für alle $c \in \mathbb{Z}$.

Beweis (beidseitige Implikationen).

($\rightarrow$) Gelten $m \mid b$ und $m \mid c$. Dann existieren $k, n \in \mathbb{Z}$, so dass $b = k \cdot m$ und $c = n \cdot m$. Also gilt $b + c = km + nm = (k + n) \cdot m$ und damit $m \mid (b + c)$.

Arithmetik — Teilbarkeit

Notizen:

- wir wissen bereits, dass $|$ (Teilbarkeit) auf den natürlichen Zahlen eine Ordnungsrelation ist
- hier betrachten wir $|$ jedoch als Relation $| \subseteq \mathbb{N} \times \mathbb{Z}$

§15.1 Theorem

Sei $m \mid b$. Dann gilt $m \mid c$ gdw. $m \mid (b + c)$ für alle $c \in \mathbb{Z}$.

Beweis (beidseitige Implikationen).

($\rightarrow$) Gelten $m \mid b$ und $m \mid c$. Dann existieren $k, n \in \mathbb{Z}$, so dass $b = k \cdot m$ und $c = n \cdot m$. Also gilt $b + c = km + nm = (k + n) \cdot m$ und damit $m \mid (b + c)$.

($\leftarrow$) Gelte $m \mid b$ und $m \mid (b + c)$. Dann existieren $k, n \in \mathbb{Z}$, so dass $b = k \cdot m$ und $b + c = n \cdot m$. Also gilt $c = (b + c) - b = nm - km = (n - k) \cdot m$ und damit $m \mid c$. □

§15.2 Korollar

Seien $a, b \in \mathbb{N}$. Dann gilt

$$T_a \cap T_b = T_{(a+b)} \cap T_b$$

§15.2 Korollar

Seien $a, b \in \mathbb{N}$. Dann gilt

$$T_a \cap T_b = T_{(a+b)} \cap T_b$$

Beweis (beidseitige Teilmengen).

($\subseteq$) Sei $m \in T_a \cap T_b$. Also $m \mid a$ und $m \mid b$. Gemäß §15.1 gilt dann $m \mid (a + b)$ und damit $m \in T_{(a+b)} \cap T_b$.

§15.2 Korollar

Seien $a, b \in \mathbb{N}$. Dann gilt

$$T_a \cap T_b = T_{(a+b)} \cap T_b$$

Beweis (beidseitige Teilmengen).

($\subseteq$) Sei $m \in T_a \cap T_b$. Also $m \mid a$ und $m \mid b$. Gemäß §15.1 gilt dann $m \mid (a+b)$ und damit $m \in T_{(a+b)} \cap T_b$.

($\supseteq$) Sei $m \in T_{(a+b)} \cap T_b$. Also $m \mid (a+b)$ und $m \mid b$. Gemäß §15.1 gilt dann $m \mid a$ und damit $m \in T_a \cap T_b$. $\square$

§15.2 Korollar

Seien $a, b \in \mathbb{N}$. Dann gilt

$$T_a \cap T_b = T_{(a+b)} \cap T_b$$

Beweis (beidseitige Teilmengen).

($\subseteq$) Sei $m \in T_a \cap T_b$. Also $m \mid a$ und $m \mid b$. Gemäß §15.1 gilt dann $m \mid (a+b)$ und damit $m \in T_{(a+b)} \cap T_b$.

($\supseteq$) Sei $m \in T_{(a+b)} \cap T_b$. Also $m \mid (a+b)$ und $m \mid b$. Gemäß §15.1 gilt dann $m \mid a$ und damit $m \in T_a \cap T_b$. □

Notizen:

- a und b haben die gleichen Teiler wie $a+b$ und b
- dies gilt sogar für die Teiler von a und b und die Teiler von $a+kb$ (für $k \in \mathbb{N}$) und b

§15.3 Theorem

Seien $a, b \in \mathbb{N}$. Es gilt für alle $k \in \mathbb{N}$

$$T_a \cap T_b = T_{(a+kb)} \cap T_b$$

§15.3 Theorem

Seien $a, b \in \mathbb{N}$. Es gilt für alle $k \in \mathbb{N}$

$$T_a \cap T_b = T_{(a+kb)} \cap T_b$$

Beweis (vollständige Induktion über k).

- IA: Für $k = 0$ ist dies offensichtlich.

§15.3 Theorem

Seien $a, b \in \mathbb{N}$. Es gilt für alle $k \in \mathbb{N}$

$$T_a \cap T_b = T_{(a+kb)} \cap T_b$$

Beweis (vollständige Induktion über k).

- IA: Für $k = 0$ ist dies offensichtlich.
- IH: Die Aussage gelte für k.
- IS: Gemäß IH gilt $T_a \cap T_b = T_{(a+kb)} \cap T_b$. Weiterhin gilt gemäß §15.2

$$T_{(a+kb)} \cap T_b = \underbrace{T_{(a+kb+b)}}_{=T_{(a+(k+1)b)}} \cap T_b$$

womit $T_a \cap T_b = T_{(a+(k+1)b)} \cap T_b$ bereits gezeigt ist. □

Arithmetik — Teilbarkeit

Notizen:

- $T_a \cap T_b \neq \emptyset$ für alle $a, b \in \mathbb{N}$
  denn $1 \in T_a$ und $1 \in T_b$
- $T_a \cap T_b$ ist endlich für alle $a, b \in \mathbb{N} \setminus \{0\}$
  denn $m \leq a$ und $m \leq b$ für alle $m \in T_a \cap T_b$

Notizen:

- $T_a \cap T_b \neq \emptyset$ für alle $a, b \in \mathbb{N}$
  denn $1 \in T_a$ und $1 \in T_b$
- $T_a \cap T_b$ ist endlich für alle $a, b \in \mathbb{N} \setminus \{0\}$
  denn $m \leq a$ und $m \leq b$ für alle $m \in T_a \cap T_b$

§15.4 Definition (größter gemeinsamer Teiler)

Seien $a, b \in \mathbb{N} \setminus \{0\}$. Dann ist

$$\mathrm{ggT}(a, b) = \max\,(T_a \cap T_b)$$

der größte gemeinsame Teiler von a und b.
Die Zahlen a und b sind teilerfremd gdw. $\mathrm{ggT}(a, b) = 1$.

Beispiele

- $T_8 = \{1, 2, 4, 8\}$ und $T_9 = \{1, 3, 9\}$ und $T_{12} = \{1, 2, 3, 4, 6, 12\}$
- also ist $\mathrm{ggT}(8, 12) = 4$ und $\mathrm{ggT}(8, 9) = 1$
- 1 ist teilerfremd zu jeder positiven natürlichen Zahl

§15.5 Theorem

Seien $a, b \in \mathbb{N}$ mit $b \geq 1$.
Dann existieren eindeutige $k, r \in \mathbb{N}$, so dass

$$a = kb + r \qquad \text{und} \qquad 0 \leq r < b$$

§15.5 Theorem

Seien $a, b \in \mathbb{N}$ mit $b \geq 1$.
Dann existieren eindeutige $k, r \in \mathbb{N}$, so dass

$$a = kb + r \qquad \text{und} \qquad 0 \leq r < b$$

Beweis (vollständige Induktion über a; 1/2).

Wir beweisen zunächst die Existenz.

- IA: Sei $a = 0$. Wir setzen $k = 0$ und $r = 0$. Dann gilt $a = kb + r$ und $0 \leq r < b$ wie gefordert.

§15.5 Theorem

Seien $a, b \in \mathbb{N}$ mit $b \geq 1$.
Dann existieren eindeutige $k, r \in \mathbb{N}$, so dass

$$a = kb + r \qquad \text{und} \qquad 0 \leq r < b$$

Beweis (vollständige Induktion über a; 1/2).

Wir beweisen zunächst die Existenz.

- IA: Sei $a = 0$. Wir setzen $k = 0$ und $r = 0$. Dann gilt $a = kb + r$ und $0 \leq r < b$ wie gefordert.
- IH: Seien $k, r \in \mathbb{N}$, so dass $a = kb + r$ und $0 \leq r < b$.
- IS: Wir unterscheiden nun 2 Fälle.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

  Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.
- Fall 2: Sei $r+1<b$. Dann gilt auch $a+1=(kb+r)+1$. Wir setzen also $m=k$ und $s=r+1$, womit $a+1=mb+s$.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

  Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.
- Fall 2: Sei $r+1<b$. Dann gilt auch $a+1=(kb+r)+1$. Wir setzen also $m=k$ und $s=r+1$, womit $a+1=mb+s$.

Damit ist die Existenz bewiesen. Seien nun $k, m, r, s \in \mathbb{N}$, so dass $a=kb+r$ und $a=mb+s$ und $0 \leq r<b$ und $0 \leq s<b$.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

  Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.
- Fall 2: Sei $r+1<b$. Dann gilt auch $a+1=(kb+r)+1$. Wir setzen also $m=k$ und $s=r+1$, womit $a+1=mb+s$.

Damit ist die Existenz bewiesen. Seien nun $k,m,r,s\in\mathbb{N}$, so dass $a=kb+r$ und $a=mb+s$ und $0\leq r<b$ und $0\leq s<b$. Also gilt auch $kb+r=mb+s$ und damit $(k-m)b=s-r$. Wir unterscheiden wieder zwei Fälle.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

  Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.
- Fall 2: Sei $r+1<b$. Dann gilt auch $a+1=(kb+r)+1$. Wir setzen also $m=k$ und $s=r+1$, womit $a+1=mb+s$.

Damit ist die Existenz bewiesen. Seien nun $k,m,r,s\in\mathbb{N}$, so dass $a=kb+r$ und $a=mb+s$ und $0\leq r<b$ und $0\leq s<b$. Also gilt auch $kb+r=mb+s$ und damit $(k-m)b=s-r$. Wir unterscheiden wieder zwei Fälle.

- Sei $k-m=0$. Dann ist $k=m$ und es gilt $0=s-r$, womit auch $r=s$ folgt.

Beweis (vollständige Induktion über a; 2/2).

- Fall 1: Sei $r+1=b$. Dann gilt auch

$$a+1=(kb+r)+1=kb+b=(k+1)b+0$$

  Wir setzen also $m=(k+1)$ und $s=0$, womit $a+1=mb+s$.
- Fall 2: Sei $r+1<b$. Dann gilt auch $a+1=(kb+r)+1$. Wir setzen also $m=k$ und $s=r+1$, womit $a+1=mb+s$.

Damit ist die Existenz bewiesen. Seien nun $k,m,r,s\in\mathbb{N}$, so dass $a=kb+r$ und $a=mb+s$ und $0\leq r<b$ und $0\leq s<b$. Also gilt auch $kb+r=mb+s$ und damit $(k-m)b=s-r$. Wir unterscheiden wieder zwei Fälle.

- Sei $k-m=0$. Dann ist $k=m$ und es gilt $0=s-r$, womit auch $r=s$ folgt.
- Sei $k-m\neq 0$. Dann ist $|(k-m)b|\geq b$, aber $|s-r|<b$. Folglich kann dieser Fall nicht eintreten, denn $(k-m)b=s-r$ ist unmöglich. □

§15.6 Definition (Rest- oder Modulo-Operation)

Seien $a, b \in \mathbb{N}$ mit $b \geq 1$. Dann existieren gemäß §15.5 eindeutige $k, r \in \mathbb{N}$, so dass $a = kb + r$ und $0 \leq r < b$.
Wir schreiben $r = a \bmod b$.

§15.6 Definition (Rest- oder Modulo-Operation)

Seien $a, b \in \mathbb{N}$ mit $b \geq 1$. Dann existieren gemäß §15.5 eindeutige $k, r \in \mathbb{N}$, so dass $a = kb + r$ und $0 \leq r < b$.
Wir schreiben $r = a \bmod b$.

Beispiele:

- $5 \bmod 2 = 1$ und $12 \bmod 2 = 0$
- $7 \bmod 4 = 3$ und $9 \bmod 4 = 1$

§15.7 Theorem

Seien $a, b \in \mathbb{N}$ und $m \in \mathbb{N}$. Folgende Aussagen sind äquivalent:

- $r_a = r_b$ wobei $r_a = a \bmod m$ und $r_b = b \bmod m$
- $m \mid (a - b)$

§15.7 Theorem

Seien $a, b \in \mathbb{N}$ und $m \in \mathbb{N}$. Folgende Aussagen sind äquivalent:

- $r_a = r_b$ wobei $r_a = a \bmod m$ und $r_b = b \bmod m$
- $m \mid (a - b)$

Beweis (direkt).

Da $|r_a - r_b| < m$ gilt

$$
\begin{aligned}
& m \mid (a - b) \\
\text{gdw. } & \exists k \big(k \in \mathbb{Z} \wedge a - b = km \big) \\
\text{gdw. } & \exists k \Big(k \in \mathbb{Z} \wedge \big(\lfloor \tfrac{a}{m} \rfloor \cdot m + r_a \big) - \big(\lfloor \tfrac{b}{m} \rfloor \cdot m + r_b \big) = km \Big) \\
\text{gdw. } & \exists k \Big(k \in \mathbb{Z} \wedge r_a - r_b = (k - \lfloor \tfrac{a}{m} \rfloor + \lfloor \tfrac{b}{m} \rfloor) \cdot m \Big) \\
\text{gdw. } & r_a = r_b
\end{aligned}
$$

□

§15.8 Theorem

Seien $a, b, c, d \in \mathbb{N}$ und $m \in \mathbb{N} \setminus \{0\}$, so dass
$a \bmod m = b \bmod m$ und $c \bmod m = d \bmod m$. Dann gelten

1. $(a + c) \bmod m = (b + d) \bmod m$
2. $(a \cdot c) \bmod m = (b \cdot d) \bmod m$

§15.8 Theorem

Seien $a, b, c, d \in \mathbb{N}$ und $m \in \mathbb{N} \setminus \{0\}$, so dass $a \bmod m = b \bmod m$ und $c \bmod m = d \bmod m$. Dann gelten

1. $(a + c) \bmod m = (b + d) \bmod m$
2. $(a \cdot c) \bmod m = (b \cdot d) \bmod m$

Beweis (direkt).

Beide Resultate folgen direkt aus den Resultaten zur Repräsentantenunabhängigkeit aus Vorlesung 11 (Seiten 14 und 51), denn $a \bmod m = b \bmod m$ und $c \bmod m = d \bmod m$ liefern $a \sim_m b$ und $c \sim_m d$ nach §15.7. Also auch $a + c \sim_m b + d$ und $a \cdot c \sim_m b \cdot d$ und damit folgen die Resultate gemäß §15.7. □

Notizen:

- damit haben wir bereits die wesentlichen Rechenregeln für das modulare Rechnen
- wir können jederzeit mit “kleinen Zahlen” rechnen (Zahlen aus $\{0, 1, \ldots, m-1\}$)

$\rightarrow$ modulares Rechnen sogar einfacher als Rechnen in $\mathbb{N}$

§15.9 Theorem

Seien $a, b, c \in \mathbb{N}$ und $m \in \mathbb{N} \setminus \{0\}$, so dass c und m teilerfremd sind und $(a \cdot c) \bmod m = (b \cdot c) \bmod m$.
Dann gilt auch $a \bmod m = b \bmod m$.

§15.9 Theorem

Seien $a, b, c \in \mathbb{N}$ und $m \in \mathbb{N} \setminus \{0\}$, so dass c und m teilerfremd sind und $(a \cdot c) \bmod m = (b \cdot c) \bmod m$.
Dann gilt auch $a \bmod m = b \bmod m$.

Beweis (direkt).

Gemäß §15.7 folgt $m \mid (ac - bc)$ und damit $m \mid (a - b)c$. Da m und c teilerfremd sind, muss $m \mid (a - b)$ gelten (dies folgt aus der Primfaktorzerlegung). Gemäß §15.7 gilt daher $a \bmod m = b \bmod m$. □

Arithmetik — Euklidischer Algorithmus

Motivation:

- Algorithmus zur Berechnung des größten gemeinsamen Teilers
- sehr effizient
- bereits uralt; Euklid präsentiert das Verfahren
  (ob er es gefunden hat, ist ungeklärt)
- ältester nicht-trivialer Algorithmus

Euklid von Alexandria (3. Jhd v. Chr.)

- griech. Mathematiker
- sammelte Wissen der Mathematik
- Vorreiter des strengen Beweises

Arithmetik — Euklidischer Algorithmus

§15.10 Theorem

Seien $a, b \in \mathbb{N} \setminus \{0\}$. Dann gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b)$$

§15.10 Theorem

Seien $a, b \in \mathbb{N} \setminus \{0\}$. Dann gilt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b)$$

Beweis (direkt).

Gemäß §15.5 existiert ein eindeutiges $k \in \mathbb{N}$, so dass $a = kb + r$ wobei $r = a \bmod b$. Weiterhin gilt

$$T_{(a \bmod b)} \cap T_b = T_{((a \bmod b)+kb)} \cap T_b$$

nach §15.3. Folglich gilt

$$T_a \cap T_b = \underbrace{T_{((a \bmod b)+kb)}}_{T_a} \cap T_b = T_{(a \bmod b)} \cap T_b \ ,$$

womit auch deren größte Elemente gleich sind. □

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	

- wir berechnen $e(127, 34)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	9
25	9	

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$
- da $34 \bmod 25 = 9 \to e(25, 9)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	9
25	9	7
9	7	

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$
- da $34 \bmod 25 = 9 \to e(25, 9)$
- da $25 \bmod 9 = 7 \to e(9, 7)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	9
25	9	7
9	7	2
7	2	

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$
- da $34 \bmod 25 = 9 \to e(25, 9)$
- da $25 \bmod 9 = 7 \to e(9, 7)$
- da $9 \bmod 7 = 2 \to e(7, 2)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	9
25	9	7
9	7	2
7	2	1
2	1	

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$
- da $34 \bmod 25 = 9 \to e(25, 9)$
- da $25 \bmod 9 = 7 \to e(9, 7)$
- da $9 \bmod 7 = 2 \to e(7, 2)$
- da $7 \bmod 2 = 1 \to e(2, 1)$

Arithmetik — Euklidischer Algorithmus

§15.11 Definition (rekursive Berechnung des ggT)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $e\colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$e(a,b) = \begin{cases} b & \text{falls } a \bmod b = 0 \\ e(b, a \bmod b) & \text{sonst} \end{cases}$$

a	b	$a \bmod b$
127	34	25
34	25	9
25	9	7
9	7	2
7	2	1
2	1	0

- wir berechnen $e(127, 34)$
- da $127 \bmod 34 = 25 \to e(34, 25)$
- da $34 \bmod 25 = 9 \to e(25, 9)$
- da $25 \bmod 9 = 7 \to e(9, 7)$
- da $9 \bmod 7 = 2 \to e(7, 2)$
- da $7 \bmod 2 = 1 \to e(2, 1)$
- da $2 \bmod 1 = 0$ liefern wir 1

Arithmetik — Euklidischer Algorithmus

§15.12 Theorem

Für alle $a, b \in \mathbb{N}_+$ gilt $e(a, b) = \mathrm{ggT}(a, b)$.

§15.12 Theorem

Für alle $a, b \in \mathbb{N}_+$ gilt $e(a, b) = \mathrm{ggT}(a, b)$.

Beweis (vollständige Induktion über b; 1/2).

- IA: Sei $b = 1$. Dann ist offensichtlich $\mathrm{ggT}(a, b) = b$ und ebenso $e(a, b) = b$, denn $a \bmod b = a \bmod 1 = 0$.

§15.12 Theorem

Für alle $a, b \in \mathbb{N}_+$ gilt $e(a,b) = \mathrm{ggT}(a,b)$.

Beweis (vollständige Induktion über b; 1/2).

- IA: Sei $b = 1$. Dann ist offensichtlich $\mathrm{ggT}(a,b) = b$ und ebenso $e(a,b) = b$, denn $a \bmod b = a \bmod 1 = 0$.
- IH: Die Aussage gelte für b und alle kleineren Werte.
- IS: Wir unterscheiden mehrere Fälle:
  - Sei $a \bmod (b+1) = 0$. Dann gilt $e(a, b+1) = b+1$ und ebenso $\mathrm{ggT}(a, b+1) = b+1$, denn $b+1$ ist Teiler von a und offensichtlich der größte Teiler von $b+1$.

§15.12 Theorem

Für alle $a, b \in \mathbb{N}_+$ gilt $e(a, b) = \mathrm{ggT}(a, b)$.

Beweis (vollständige Induktion über b; 1/2).

- IA: Sei $b = 1$. Dann ist offensichtlich $\mathrm{ggT}(a, b) = b$ und ebenso $e(a, b) = b$, denn $a \bmod b = a \bmod 1 = 0$.
- IH: Die Aussage gelte für b und alle kleineren Werte.
- IS: Wir unterscheiden mehrere Fälle:
  - Sei $a \bmod (b+1) = 0$. Dann gilt $e(a, b+1) = b+1$ und ebenso $\mathrm{ggT}(a, b+1) = b+1$, denn $b+1$ ist Teiler von a und offensichtlich der größte Teiler von $b+1$.
  - Sei $a \bmod (b+1) \neq 0$. Dann unterscheiden wir zwei weitere Fälle.

Beweis (vollständige Induktion; 2/2).

Wir sind im Induktionsschritt und es gilt $a \bmod (b+1) \neq 0$.

- Sei zuächst $a < b+1$. Dann gilt offensichtlich $a \bmod (b+1) = a$ und damit $e(a, b+1) = e(b+1, a)$. Da $a < b+1$ gilt $a \leq b$ und aus der IH folgt $e(b+1, a) = \mathrm{ggT}(b+1, a)$. Damit folgt

$$e(a, b+1) = e(b+1, a) = \mathrm{ggT}(b+1, a) = \mathrm{ggT}(a, b+1)$$

Beweis (vollständige Induktion; 2/2).

Wir sind im Induktionsschritt und es gilt $a \bmod (b+1) \neq 0$.

- Sei zuächst $a < b+1$. Dann gilt offensichtlich $a \bmod (b+1) = a$ und damit $e(a, b+1) = e(b+1, a)$. Da $a < b+1$ gilt $a \leq b$ und aus der IH folgt $e(b+1, a) = \mathrm{ggT}(b+1, a)$. Damit folgt

$$e(a, b+1) = e(b+1, a) = \mathrm{ggT}(b+1, a) = \mathrm{ggT}(a, b+1)$$

- Sei also nun $a > b+1$. Dann ist $a \bmod (b+1) < b+1$ und damit gilt

$$\begin{aligned} e(a, b+1) &= e(b+1, a \bmod (b+1)) && \text{(Def. } e\text{)} \\ &= \mathrm{ggT}(b+1, a \bmod (b+1)) && \text{(IH)} \\ &= \mathrm{ggT}(a \bmod (b+1), b+1) \\ &= \mathrm{ggT}(a, b+1) && \text{(§15.10)} \end{aligned}$$

womit die Induktion abgeschlossen ist. □

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	144
992	144	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	144
992	144	128
144	128	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	144
992	144	128
144	128	16
128	16	

Arithmetik — Euklidischer Algorithmus

Wir berechnen $e(16.607.184, 2.367.488)$:

a	b	$a \bmod b$
16.607.184	2.367.488	34.768
2.367.488	34.768	3.264
34.768	3.264	2.128
3.264	2.128	1.136
2.128	1.136	992
1.136	992	144
992	144	128
144	128	16
128	16	0

Arithmetik — Euklidischer Algorithmus

§15.13 Theorem

Für alle $a, b \in \mathbb{N}_+$ existieren $m, n \in \mathbb{Z}$ mit $e(a, b) = ma + nb$.

§15.13 Theorem

Für alle $a, b \in \mathbb{N}_+$ existieren $m, n \in \mathbb{Z}$ mit $e(a, b) = ma + nb$.

Beweis (vollständige Induktion; 1/2).

- IA: Die Berechnung von $e(a, b)$ terminiert sofort. Dann gilt $a \bmod b = 0$ und $e(a, b) = b$. Wir setzen $m = 0$ und $n = 1$. Dann gilt $e(a, b) = b = ma + nb$.

§15.13 Theorem

Für alle $a, b \in \mathbb{N}_+$ existieren $m, n \in \mathbb{Z}$ mit $e(a, b) = ma + nb$.

Beweis (vollständige Induktion; 1/2).

- IA: Die Berechnung von $e(a, b)$ terminiert sofort. Dann gilt $a \bmod b = 0$ und $e(a, b) = b$. Wir setzen $m = 0$ und $n = 1$. Dann gilt $e(a, b) = b = ma + nb$.
- IV: Gelte die Aussage für Aufrufe von e, die in k Schritten terminieren.
- IS: Sei $e(a, b)$ ein Aufruf, der in $k + 1$ Schritten terminiert. Es gilt offensichtlich $e(a, b) = e(b, a \bmod b)$ und gemäß IH existieren $m, n \in \mathbb{Z}$ mit $e(b, a \bmod b) = mb + n(a \bmod b)$.

$$\begin{aligned} mb + n(a \bmod b) &= mb + n(a - \lfloor \tfrac{a}{b} \rfloor \cdot b) \\ &= na + (m - n \cdot \lfloor \tfrac{a}{b} \rfloor) \cdot b \end{aligned}$$

Beweis (vollständige Induktion; 2/2).

Also gilt

$$\begin{aligned} e(a,b) &= \mathrm{ggT}(a,b) && \text{(§15.12)} \\ &= \mathrm{ggT}(a \bmod b, b) && \text{(§15.10)} \\ &= \mathrm{ggT}(b, a \bmod b) \\ &= e(b, a \bmod b) && \text{(§15.12)} \\ &= mb + n(a \bmod b) \\ &= na + (m - n \cdot \lfloor \tfrac{a}{b} \rfloor) \cdot b \end{aligned}$$

womit die Aussage für $m' = n$ und $n' = m - n\lfloor \frac{a}{b} \rfloor$ bewiesen ist. □

§15.14 Definition (erweiterter Euklid-Schritt)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $f : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+ \times \mathbb{Z} \times \mathbb{Z}$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$f(a,b) = \begin{cases} (b, 0, 1) & \text{falls } a \bmod b = 0 \\ (d, n, m - n\lfloor \frac{a}{b} \rfloor) & \text{sonst,} \\ & \text{wobei } (d, m, n) = f(b, a \bmod b) \end{cases}$$

Arithmetik — Erweiterter Euklidischer Algorithmus

§15.14 Definition (erweiterter Euklid-Schritt)

Sei $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$. Wir definieren die Funktion $f : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}_+ \times \mathbb{Z} \times \mathbb{Z}$ induktiv für alle $a, b \in \mathbb{N}_+$ durch

$$f(a,b) = \begin{cases} (b, 0, 1) & \text{falls } a \bmod b = 0 \\ (d, n, m - n\lfloor \frac{a}{b} \rfloor) & \text{sonst,} \\ & \text{wobei } (d,m,n) = f(b, a \bmod b) \end{cases}$$

Notizen:

- Korrektheit ergibt sich direkt aus §15.13
- (wesentlicher Teil) entdeckt von Claude Bachet
- für Polynome von Étienne Bézout
- wichtig für Berechnung von Inversen (siehe VL 11)

Arithmetik — Erweiterter Euklidischer Algorithmus

Claude Gaspard Bachet (* 1581; † 1638)

- franz. Mathematiker
- arbeitete an Zahlentheorie
- lieferte Werk für Fermats Notizen

Étienne Bézout (* 1730; † 1783)

- franz. Mathematiker
- inspiriert von Leonhard Euler
- arbeitete beim Militär

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144	128				
144	128					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144	128				
144	128	16				
128	16					

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144	128				
144	128	16				
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144	128				
144	128	16	16	0	1	-1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144				
992	144	128	16	1	-1	7
144	128	16	16	0	1	-1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992				
1.136	992	144	16	-1	7	-8
992	144	128	16	1	-1	7
144	128	16	16	0	1	-1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136				
2.128	1.136	992	16	7	−8	15
1.136	992	144	16	−1	7	−8
992	144	128	16	1	−1	7
144	128	16	16	0	1	−1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128				
3.264	2.128	1.136	16	-8	15	-23
2.128	1.136	992	16	7	-8	15
1.136	992	144	16	-1	7	-8
992	144	128	16	1	-1	7
144	128	16	16	0	1	-1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264				
34.768	3.264	2.128	16	15	−23	245
3.264	2.128	1.136	16	−8	15	−23
2.128	1.136	992	16	7	−8	15
1.136	992	144	16	−1	7	−8
992	144	128	16	1	−1	7
144	128	16	16	0	1	−1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768				
2.367.488	34.768	3.264	16	−23	245	−16.683
34.768	3.264	2.128	16	15	−23	245
3.264	2.128	1.136	16	−8	15	−23
2.128	1.136	992	16	7	−8	15
1.136	992	144	16	−1	7	−8
992	144	128	16	1	−1	7
144	128	16	16	0	1	−1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768	16	245	−16.683	117.026
2.367.488	34.768	3.264	16	−23	245	−16.683
34.768	3.264	2.128	16	15	−23	245
3.264	2.128	1.136	16	−8	15	−23
2.128	1.136	992	16	7	−8	15
1.136	992	144	16	−1	7	−8
992	144	128	16	1	−1	7
144	128	16	16	0	1	−1
128	16	0				

wir erhalten $f(16.607.184, 2.367.488)$

Arithmetik — Erweiterter Euklidischer Algorithmus

Wir berechnen $f(16.607.184, 2.367.488)$:

a	b	$a \bmod b$	d	m	n	$m - n\lfloor \frac{a}{b} \rfloor$
16.607.184	2.367.488	34.768	16	245	−16.683	117.026
2.367.488	34.768	3.264	16	−23	245	−16.683
34.768	3.264	2.128	16	15	−23	245
3.264	2.128	1.136	16	−8	15	−23
2.128	1.136	992	16	7	−8	15
1.136	992	144	16	−1	7	−8
992	144	128	16	1	−1	7
144	128	16	16	0	1	−1
128	16	0				

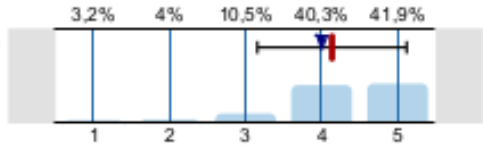
wir erhalten $f(16.607.184, 2.367.488) = (16, -16.683, 117.026)$

Auswertung
Evaluation

1. Aufbau & Struktur

1.1) Die Vorlesung ist gut auf die zum Modul gehörenden Lehrveranstaltungen abgestimmt.

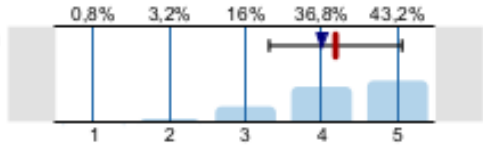
trifft gar nicht zu — trifft voll zu



n=124
mw=4,1
md=4
s=1

1.2) Die Ziele der Vorlesung sind klar und transparent.

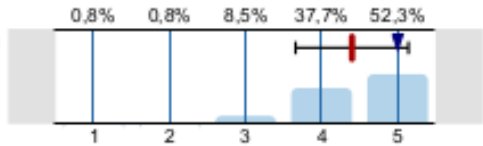
trifft gar nicht zu — trifft voll zu



n=125
mw=4,2
md=4
s=0,9

1.3) Die Vorlesung ist gut strukturiert.

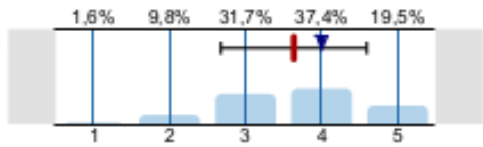
trifft gar nicht zu — trifft voll zu



n=130
mw=4,4
md=5
s=0,7

1.4) Die Inhalte der Vorlesung entsprechen meinen Erwartungen.

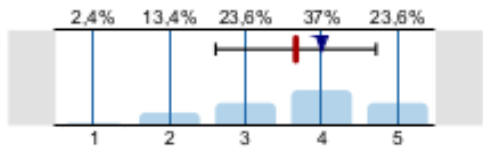
trifft gar nicht zu — trifft voll zu



n=123
mw=3,6
md=4
s=1

1.5) Die Argumentationen sind verständlich und nachvollziehbar.

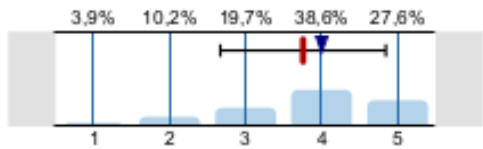
trifft gar nicht zu — trifft voll zu



n=127
mw=3,7
md=4
s=1,1

1.6) Einzelne Schritte werden hinreichend erklärt.

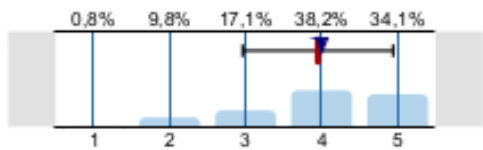
trifft gar nicht zu — trifft voll zu



n=127
mw=3,8
md=4
s=1,1

1.7) Der Stoff wird anhand von Beispielen veranschaulicht.

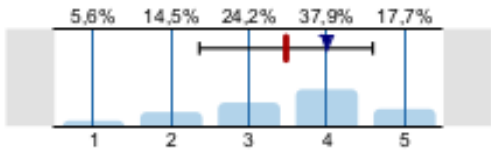
trifft gar nicht zu — trifft voll zu



n=123
mw=4
md=4
s=1

1.8) Die Vorlesung wird durch hilfreiche Materialien zur Vor- und Nachbereitung (z. B. Literaturliste, Handout) ergänzt.

trifft gar nicht zu — 5,6% 14,5% 24,2% 37,9% 17,7% — trifft voll zu

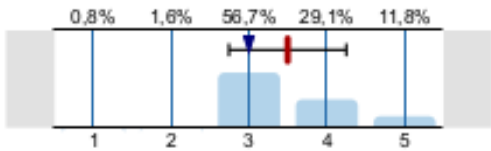


n=124
mw=3,5
md=4
s=1,1

2. Aufwand & Anforderungen

2.1) Das Tempo dieser Vorlesung ist...

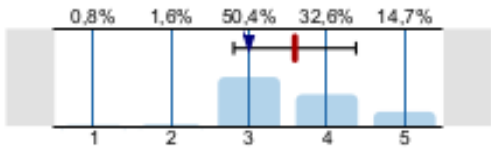
zu langsam — 0,8% 1,6% 56,7% 29,1% 11,8% — zu schnell



n=127
mw=3,5
md=3
s=0,8

2.2) Der Stoffumfang dieser Vorlesung ist...

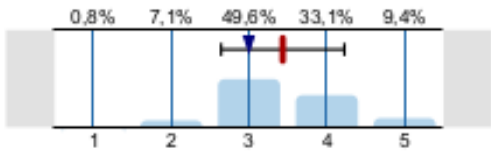
zu klein — 0,8% 1,6% 50,4% 32,6% 14,7% — zu groß



n=129
mw=3,6
md=3
s=0,8

2.3) Der Arbeitsaufwand für diese Vorlesung ist...

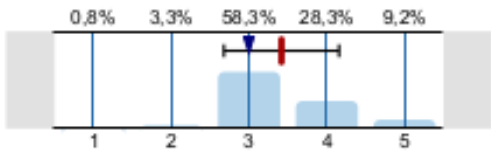
zu niedrig — 0,8% 7,1% 49,6% 33,1% 9,4% — zu hoch



n=127
mw=3,4
md=3
s=0,8

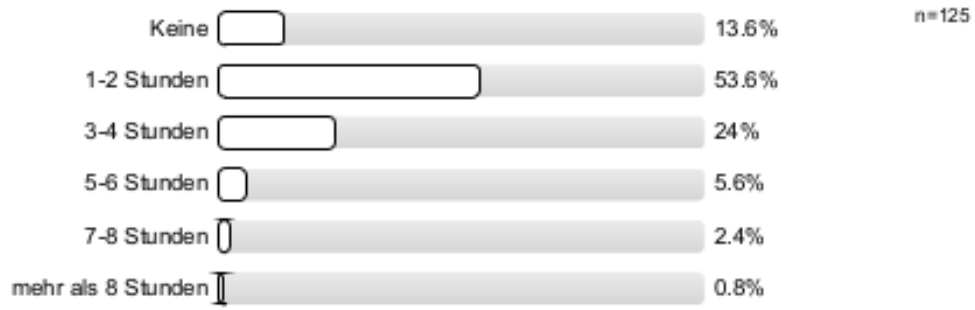
2.4) Die Anforderungen zum Erreichen der Leistungspunkte sind...

zu niedrig — 0,8% 3,3% 58,3% 28,3% 9,2% — zu hoch

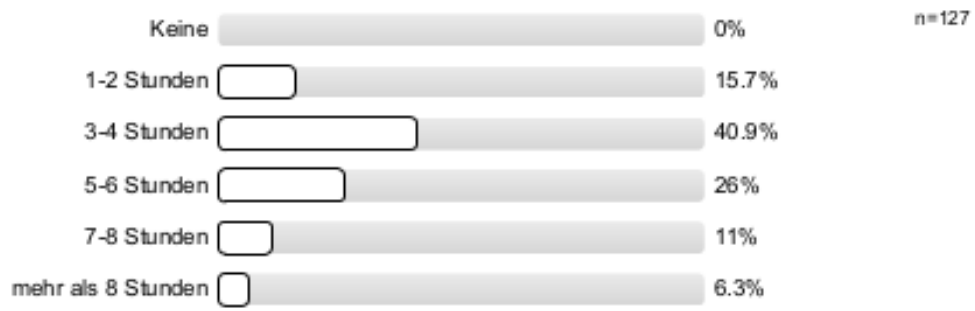


n=120
mw=3,4
md=3
s=0,7

2.5) Wie viel Zeit wenden Sie wöchentlich für die Vor- bzw. Nachbereitung dieser Vorlesung (ohne Übungsaufgaben) auf?

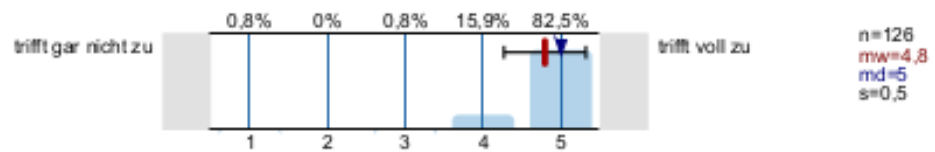


2.6) Wie viel Zeit wenden Sie wöchentlich für die Bearbeitung der Übungsaufgaben auf?

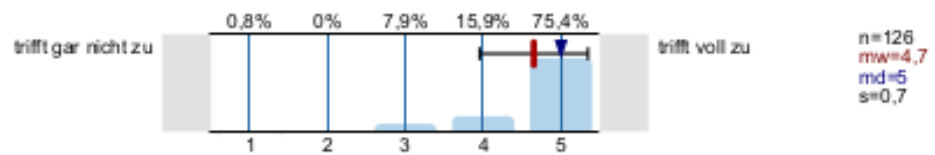


3. **Zur Lehrperson**

3.1) Die Dozentin/der Dozent wirkt gut vorbereitet.



3.2) Die Dozentin/der Dozent ist gut zu verstehen.



3.3) Die Dozentin/der Dozent gestaltet die Vorlesung interessant.

trifft gar nicht zu | 0,8% | 5,5% | 15% | 49,6% | 29,1% | trifft voll zu

1 2 3 4 5

n=127
mw=4
md=4
s=0,9

3.4) Die Dozentin/der Dozent kann schwierige Sachverhalte gut erklären.

trifft gar nicht zu | 0,8% | 6,3% | 15% | 52,8% | 25,2% | trifft voll zu

1 2 3 4 5

n=127
mw=4
md=4
s=0,9

3.5) Die Dozentin/der Dozent zeigt Interesse am Lernerfolg der Studierenden.

trifft gar nicht zu | 0,8% | 6,3% | 14,3% | 29,4% | 49,2% | trifft voll zu

1 2 3 4 5

n=126
mw=4,2
md=4
s=1

3.6) Die Dozentin/der Dozent geht ausreichend auf Fragen und Beiträge der Studierenden ein.

trifft gar nicht zu | 0% | 0,8% | 2,4% | 17,5% | 79,4% | trifft voll zu

1 2 3 4 5

n=126
mw=4,8
md=5
s=0,5

3.7) Die Dozentin/der Dozent gibt konstruktives Feedback auf erbrachte (Arbeits-) Leistungen.

trifft gar nicht zu | 5,9% | 7,6% | 34,7% | 28,8% | 22,9% | trifft voll zu

1 2 3 4 5

n=118
mw=3,6
md=4
s=1,1

4. Gesamtbewertung der Dozentin/ des Dozenten

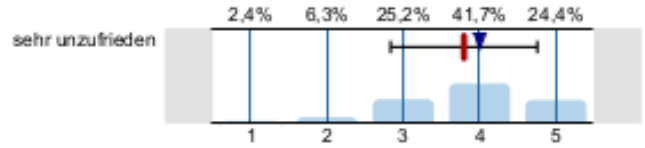
4.1) Insgesamt bin ich mit der Dozentin/dem Dozenten...

sehr unzufrieden | 0% | 1,6% | 6,3% | 40,2% | 52% | sehr zufrieden

1 2 3 4 5

n=127
mw=4,4
md=5
s=0,7

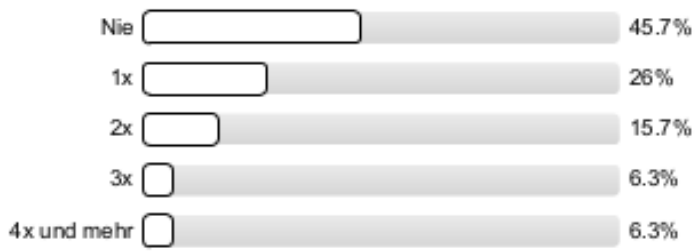
5.1) Insgesamt bin ich mit dieser Vorlesung...



n=127
mw=3,8
md=4
s=1

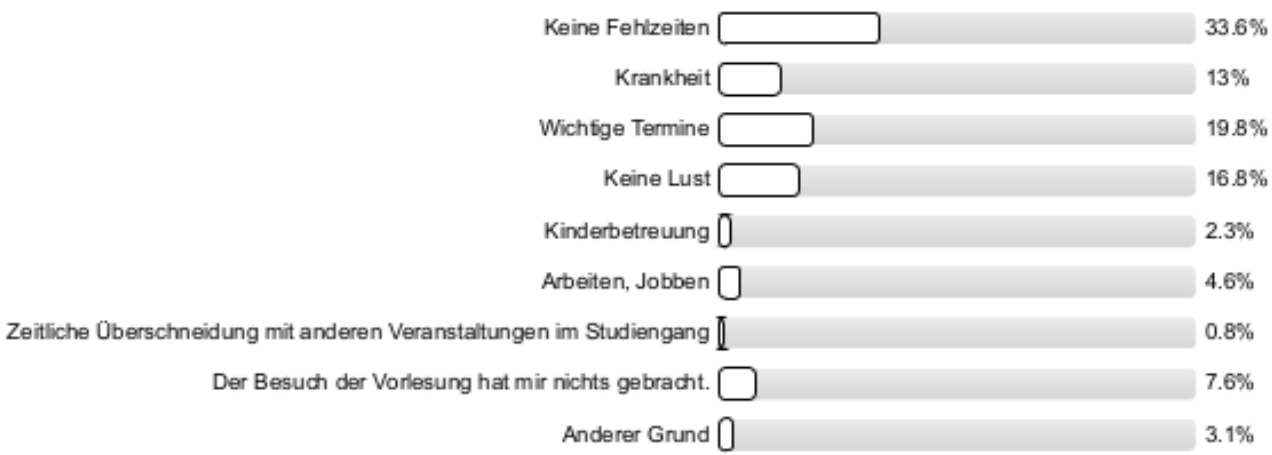
6. Allgemeine Angaben

6.1) Wie häufig blieben Sie der Vorlesung fern?



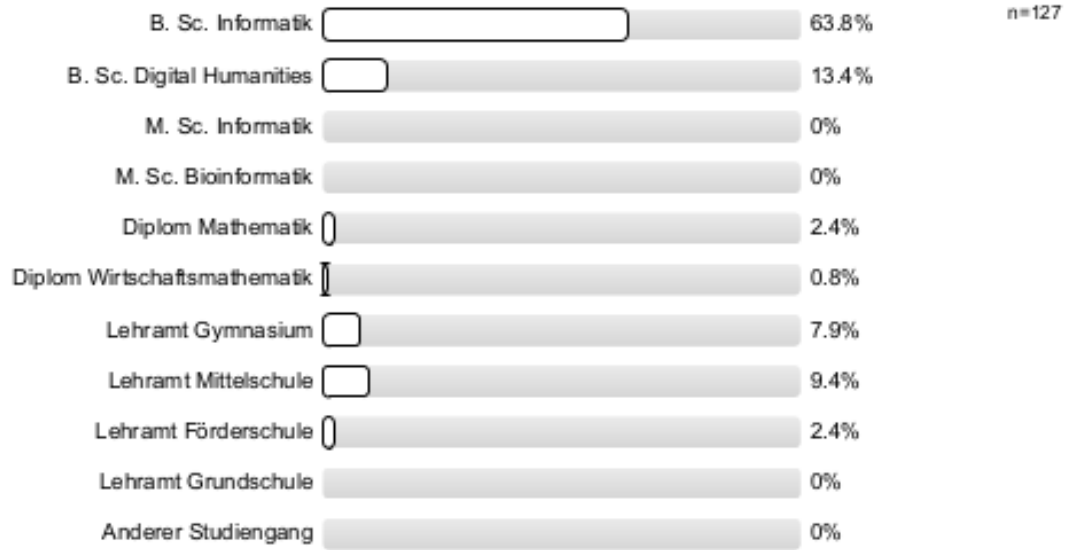
n=127

6.2) Was waren die Gründe für die Fehlzeiten? (Mehrfachantworten möglich.)

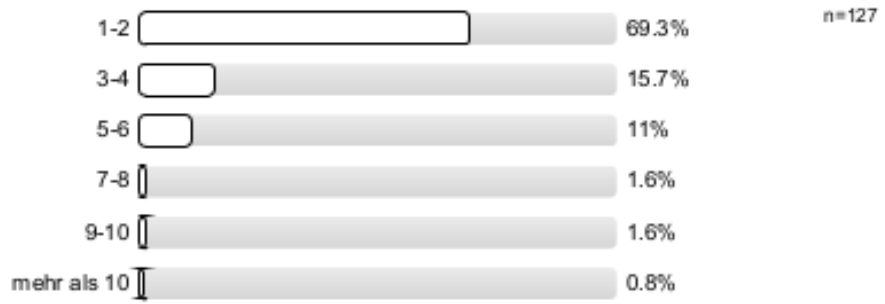


n=131

64) In welchem Studiengang sind Sie derzeit immatrikuliert?



66) Fachsemester laut Studierendenausweis:



52) Mein Lernprozess wurde unterstützt durch:

- Die Hörsaalübung.
  Mathematik für Informatiker von Teschl und Teschl.
- Steger - Diskrete Strukturen
  Folien des Dozenten
- Belege
- Bücher, online und Kommilitonen.
- Daniel Jung
- Das Skript. An einigen Stellen etwas zu lang (einzelne Schritte), aber sehr gut strukturiert und verständlich.
- Die Seminaraufgaben
- Die Übungen
- Folien, Lerngruppen
- Google und Literaturempfehlungen
- Gruppenarbeit
- Gruppenlernen
- Hauptsächlich duch eigene Recherche, die Übungen und die gute Struktur der Vorlesung.
- Horsaalübung, Online-Skript
- Internet (3 Nennungen)
- Kommilitonen (6 Nennungen)

- Kommilitonen, Internetrecherche
- Kommilitonen, die meist genauso verzweifelt waren, wie ich.
- Meine Eltern, die es bezahlen.
- Power Point Slides, Internet
- Selbstlearning, Bücher, Vorlesungen, Übungsgruppen
- Skript
- Wikipedia (2 Nennungen)
- YouTube (2 Nennungen)
- das verständliche Skript
- den offenen Mathe- bzw. Informatikraum
- die vorgeschlagene Literatur
- Übungen und Serien
- Übungsaufgaben

[53] Mein Lernprozess wurde erschwert durch:

- Sehr viel Stoff, wenig Rückkopplung zu Beispielen und Anwendungsfehlern aus der Realität.

  Zu späte Uhrzeit für so komplexe Materie.

Starke Unterschiede bei den Vorkenntnissen der Kommilitonen.

- Alle Module und der damit zusammenhängene Arbeitsaufwand
- Andere Module
- Das Anforderungsniveau bei der selbstständigen Bearbeitung der Hausaufgaben.
- Die zu hohe Schwierigkeit der Übungsaufgaben und fehlende anschauliche (!) Beispiele
- Fehlendes Vorwissen
- Folien
- Häufige Unterbrechungen durch Fragen unvorbereiteter StudentInnen (2 Nennungen)
- Meine Dummheit und Faulheit
- Meinen Netflix-Account
- Rechnen mathematischer Beweise auf Folien
- Schwierigkeitsgrad des Moduls
- Uhrzeit der Vorlesung (2 Nennungen)
- Unterschiedliche Kennzeichnungen in Vorlesungen verglichen mit den Hausaufgaben. Aufgabenstellungen sind oft nicht klar ersichtlich.
- Verständnisprobleme zu einzelnen Themen.
- Vorleistungen
- Vorlesungsfolien sind nicht ideal zum Nacharbeiten (Erklärungen durch Dozent gut, aber entsprechnde Erklärungen wären in Kurzfassung hilfreich)
- Vorlesungsfolien sind teils schwer zu verstehen/nachzuarbeiten, auch wenn man zu Vorlesung selbst da war.

- andere Jäcken, die auch viel Zeit brauchten.
- andere Module
- berufliche Tätigkeiten
- eine ungenügende Zeitplanung
- hohen Stoffumfang
- sehr abstraktes Thema
- sehr viel Inhalt
- teilweise sind Bsp. schwer verständlich
- zu anspruchsvolle Übungsaufgaben im Vergleich zum Behandelten in der VL
- zu komplizierte Aufgaben im Vergleich zu Vorlesungsinhalten
- zu viel Arbeitsaufwand im gesamten Studium
- zu viel Stoff (2 Nennungen)
- zu viele Definitionen
- zu viele Übungsaufgaben parallel in anderen Modulen
- zu wenig Zeit
- Übung aller 2 Wochen, Hörsaalübung hat Überschneidungen mit anderen Veranstaltungen
- Übung leider nur aller 2 Wochen

6.3) Anderer Grund und zwar:

- Uhrzeit.
  Anfangs war nicht möglich mitzuschreiben.
- Die Vorlesung selbst ist nicht schwierig zu verstehen, aber die Aufgaben in der Übung sind manchmal zu schwierig.
- Lernen
- Skatturnier
- unter anderem auch zum Lernen

6.5) Anderer Studiengang und zwar:

- BA Geschichte, BA Kulturwissenschaften
- Lehramt Mathe/Info
- Studium nach M. Ed. zur Ergänzung offener Module

7. **Lob, Kritik, Verbesserungsvorschläge:** (*Zur besseren Lesbarkeit bitte in DRUCKBUCHSTABEN schreiben!)*

7.1) Lob: Das hat mir besonders gut gefallen.

- Beweis eines jeden Themas.
  klare und logische Strukturierung der Vorlesung.
- Das Verständnis des Dozenten.
  Sein Humor.
- Der Dozent nimmt sich Zeit, auf die Fragen der Studierenden einzugehen.

  Gute Struktur der Vorlesungen, gute Organisation.
  Die Möglichkeit, dem Dozenten zu Anfang der Vorlesung Fragen zu stellen u.ä.

- Gute Arbeit des Dozenten mit guten Beispielen.

  Auch gut auf die Fragen eingegangen.

- Höflichkeit zu Beginn der Vorlesung Fragen zu stellen
  sehr ausführlich

- Lautstärke und Motivation des Dozenten
  Struktur und Transparenz
- Anschauliche Beispiele
- Auftreten des Dozenten
- Beantworten von Fragen von Hörerinnen zu Beginn der Vorlesung.
- Bonuspunkte
- Das Skript und der inhaltliche Aufbau der Themen (Reihenfolge wäre sinnvoll).
- Das zur Verfügungstellen der Folien bereits vor der VL
- Der Dozent (2 Nennungen)
- Der Dozent und das im Netz bereitgestellte Material.
- Der Dozent unterstützt die Studenten mit Rat und Tat.
- Die Art des Dozenten auf Fragen einzugehen.

- Die Kompetenz des Dozenten
- Die Zusammenfassung des Stoffes war leicht zu lernen. Man konnte durch die Folien den Stoff gut erfassen.
- Die interessante Vermittlung des manchmal trockenen Stoffes.
- Dozent bezieht Studierende während der Vorlesung mit ein und beantwortet alle Fragen ausführlich.
- Dr. Maletti ist sehr nett und verantwortlich
- Eingehen auf Fragen
- Folien von VL sehr gut und online verfügbar, Folien sehr umfassend.
- Folien, stückweise vorgehen, aufeinander aufbauend, kurze Wiederholungen
- Gute Folien
- Gute Folien. Bei Fragen wird sich Zeit für die Beantwortung genommen.
- Gute Vorlesungsfolien!
- Gute anschauliche Präsentationen
- Guter Dozent
- Herr Maletti ist sehr engagiert, ruft stets dazu auf, Fragen zu stellen und ist immer ansprechbar, wenn er im Büro ist.
- Humor des Dozenten
- Jede Frage wurde ausführlich und verständlich beantwortet.
- Maletti gibt viele Möglichkeiten Fragen zu stellen.
- Malettis Engagement
- Prof. Maletti geht intensiv auf Fragen ein und ermutigt, diese zu stellen. Die Hausaufgaben sind angemessen im Umfang.
- Prof. ist sehr sympathisch

- Prof. ist sympathisch
- Prof. wirkt sympathisch
- Quiz, Möglichkeit des Fragestellens
- Reflektierter Umgang mit der gelernten Wissenschaftsdisziplin zwecks Annahmen des Faches und Beschränkung.
- Sehr gut auf Fragen der Studenten eingegangen.
- Sprechen ohne Mikro, so kann es nicht nur bei Unruhe lauter gestellt werden, sondern SuS müssen leiser sein.
- Struktur mit guten Folien
- Strukturiertheit
- Strukturiertheit Strukturübersicht der Vorlesungen
- Strukturierung
- Sympathischer Dozent, er zeigt Interesse am Stoff.
- Veranschaulichung anhand von Beispielen sind so gut wie immer vorhanden.
- Vorlesungen sind trotz des trockenen Themas witzig und entspannt.
- Vortragsweise, viele Beispiele
- Witzeleien des Dozenten waren ganz locker. Lachender Smiley.
- die Beispiele
- gut strukturiert
- gute Folien, super Erklärungen
- nette Art des Dozenten

- sehr gut gefallen

[72] Kritik: Das war nicht so gut.

- Am Modul gefällt mir nicht, dass es für Informatiker ausgelegt ist und für Studenten des Lehramtes schwer verständlich ist.
  Kein zusätzliches Tutorium.

- Fülle und erforderliche Leistung für 5 LP zu viel.
  Ich studiere Mathematik und finde Formulierungen unpassend.

- Kapitel nicht immer zum Ende der Vorlesung beendet und beim nächsten Termin nicht zu Ende geführt.
  Übungsaufgaben unangemessen schwerer und nicht allein durch Vorlesungsbesucht zu lösen.

- Ablenkung durch andere Studenten.

- Anschaulichkeit der Beispiele.

- Auswahlaxiom ...

- Beispiele sind oft trivial und helfen nicht das Thema zu durchblicken.

- Beweise sind für mich teilweise nicht durchsichtig genug.

- Bisschen langweilig.

- Bonuspunktesystem für die Klausur. Das baute bei mir zusätzlichen Druck auf.

- Das zwingende Erbringen von Vorleistungen zur Zulassung zur Klausur

- Die Sprünge zwischen sehr einfachen Beispielen in der VL und den im Vergleich dazu schwierigen Hausaufgaben.

- Die Vorlesungen sind ganz unhilfreich, um die Serie aufzulösen.

- Die große(!) Inhomogenität führt zu sehr(!) unterschiedlichen Leistungsniveaus. Zusätzlich liegt die VL mit 17-19 Uhr recht spät, was sich negativ auf die generelle Konzentrationsfähigkeit auswirkt.

- Ein Student stellt während der VL unaufhörlich Fragen zu trivialen Themen, die durch Eigenrecherche hätten geklärt werden können. Der Dozent ist auf all diese Fragen eingegangen und die VL wurde aufgehalten und nicht zu Ende gebracht.
- Es fiel mir schwer mit zu halten mit der Schnelligkeit.
- Etwas schnell und zu viel Stoff.
- Folien sind manchmal schwer zu verfolgen, weil sie nicht ganz klar sind bzw. nicht auf Anhieb verständlich.
- Folien sind schwer zu Verfolgen, gerade bei Beweisen. Persönlich könnte ich z.B. immer etwas mehr Zeit zum Nachvollziehen gebrauchen, zum Beispiel bei Aussagenlogischen Aussagen, die in der Vorlesung eher schnell durchgegangen werden.
- Geringer Tiefgang bei abstrakten Problemen, dafür langgezogene technische Beweise.
- Lehrveranstaltung in meinen Augen total fehlplatziert im Mathe-Lehramtsstudium. Relevanz nicht erkennbar!
- Lösung Übungsserien bitte online stellen.
- Man hat nur in der A-Woche eine Übungswoche.
- Manche Inhalte sind abstrakt.
- Manchmal wurde über schwierigen Inhalt drüber gerannt, aber auf Nachfrage wurde eine gute Erklärung abgeliefert.
- Punkteverteilung der Aufgaben (sehr wenig Punkte für viel Aufwand)
- Stoff war sehr umfangreich
- VL-Folien kamen immer erst nach der VL.
- Viel zu viel Stoff
- Viele unnötige Fragen von Studierenden.
- manchmal ein bisschen trocken
- manchmal schnelles Tempo

- schwierige Beweise wurden zu schnell überflogen
- teilweise schwer zu verstehende Folien bei der Nachbearbeitung
- zu viel Stoff
- zu viel Theorie am Stück in der VL
- Übungen nur aller 2 Wochen

[73] Verbesserungsvorschläge: Das könnte verbessert werden.

- 10 LP pro Semester oder weniger Stoff oder Modul über 2 Semester
- Eindeutige Definitonen von VL und Übung, z.B. bei vollständige Induktion.
  Es fehlt in der VL die Zeit genau mitzukommen, da die alten Folien schneller durchlaufen werden als ich überhaupt lesen kann.
- Inhalte öfter mal an der Tafel entwickeln, das entschleunigt und lässt besser mitdenken.

  Einzelne Stoffgebiete langsamer, aber mit mehr Beispielen/Vertiefungen behandeln! Übungen jede Woche und nicht alle 2 Wochen.
- Stoffumfang auf Grundlagen stützen und Fälle eindämmen.
  Wichtige Sätze für Klausur/Übung hervorheben.
- mehr Grafiken
  weniger überladene Folien
- zwischendurch kleine Pausen oder extra Beispiele (Was zum Kopf frei kriegen)
  Nicht zu lange auf Fragen der Studierenden eingehen, die einfach zu weit hinter dem Stoff her sind.
- Abstrakte Sachverhalte können detailierter erklärt werden.
- Ausführliche Literaturliste und Linkliste für einzelne Themengebiete.

- Beim nächsten Mal, wenn ein und diesselbe Frage mehrmals gestellt wird (von derselben Person) bitte mit der VL weitermachen und ggf. nach der VL zu zweit sprechen.
- Beleuchtung des Vorlesungssales während der Vorlesung nicht so sehr abdunkeln.
- Benennung aller verwendeter Zeichen.
- Die Ausführung der Beweise
- Ein zusätzliches Tutorium könnte angeboten werden, bei dem die Begriffe aus der VL noch einmal aufgegriffen werden.
- Eine Gesellschaft, die nicht nur von lebenslangem Lernen redet, sondern diesen Ansatz real lebt. Lachender Smiley.
- Etwas langsamer
- Für D.H.-Studenten bessere Einblicke in außerhalb des Moduls liegenden, aber trotzdem benötigte Inhalte
- Hörleitungen im Skript nicht auf (gefühlt) 50.000 Folien splitten.
- Ich hoffe, dass es mehr Übungen geben wird, um es besser nachvollziehen zu können. Dankeschön!
- In den Folien könnten einige Definitionen mit Worten geschrieben werden, um Symbole/Formeln leichter zu verstehen.
- Lautstärke und Struktur des Dozenten
- Lösung der Aufgaben online ins Almaweb stellen.
- Mehr Beispiele in Folien der Vorlesung.
- Mehr Hinweisfolien mit wörtlichen Erklärungen, sodass auch schwierige Gleichungen etc. im Nachhinein nachvollzogen werden können.
- Mehr anschauliche Beispiele.
- Minimal langsamer
- Online-Abgabe von Übungen

- Schwierige Beweise/Sachverhalte langsamer und mit Beispielen erklären/behandeln.
- Skript mit Inhaltsverzeichnis und mehr wichtigen Überschriften (hervorgehoben)
- Skripte bitte kürzer halten
- Studiengänge, die Analysis machen, nicht zusammen mit Studiengängen, die kein Analysis machen müssen.
- Uhrzeit der Vorlesung
- Vielleicht ein bisschen mehr Infos an anderer Literatur (Bücher).
- Vorlesung und Serien besser aufeinander abstimmen.
- Wöchentliche Serien
- etwas genauer auf Übungen eingehen.
- mehr Beispiel, höhere Anschaulichkeit
- mehr Beispiel/ähnlich der Übungsaufgaben
- mehr Enthusiasmus
- wöchentliche Halbserien
- zu viel Stoff auf einmal, es wäre gut, wenn Hauptpunkte der VL in "Notizen" hochgeladen würden.

Zusammenfassung

- Teilbarkeit und größte gemeinsame Teiler
- Modulares Rechnen
- Euklidischer Algorithmus
- erweiterter Euklidischer Algorithmus

Sie haben es geschafft.

Vielen herzlichen Dank und viel Erfolg in der Prüfung!