Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

Dr.-Ing. Miriam Hommel

Gliederung

1. Zahlentheorie

- 1.1 Teilbarkeit
- 1.2 Primzahlen
- 1.3 Kongruenzen
- 1.4 RSA Public-Key-Kryptosytem

2. Algebra

- 2.1 Algebraische Strukturen
- 2.2 Vektoren und Matrizen
- 2.3 Lineare Gleichungssysteme
- 2.4 Determinanten

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Teilbarkeitsrelation und Teilermenge

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Teilbarkeitsrelation

Hinweis: Die Grundmenge in diesem Abschnitt ist $\mathbb{Z}$, die Menge der ganzen Zahlen.

Definition 1:

Für zwei Zahlen $m, n \in \mathbb{Z}$ mit $m > 0$ ist m ein Teiler von n, falls es ein $t \in \mathbb{Z}$ gibt, so dass

Kurzschreibweise: lies:

Beispiele:
- $2 \quad 6$, da
- $2 \quad 7$, da

1. Zahlentheorie

1.1 Teilbarkeit – Teilbarkeitsrelation

Für jedes $n \in \mathbb{Z}$ gilt

Ist $n > 0$, dann gilt auch

Hinweis: Ist $n < 0$, dann gilt $n \nmid n$, da der Teiler laut Definition > 0 sein muss.

Spezialfall: $n = 0$:

Dann gilt $\forall\, m \in \mathbb{N}\backslash\{0\}$:

1. Zahlentheorie

1.1 Teilbarkeit – Teilermenge

Definition 2:

Die Menge aller (positiven) Teiler von $n \in \mathbb{Z}$ ist

Beispiele:

- $T_6 =$
- $T_7 =$
- $T_{20} =$
- $T_0 =$

1. Zahlentheorie

1.1 Teilbarkeit – Teilbarkeitsrelation und Teilermengen

Kontrollfragen:

1. Was muss für m gelten, damit es ein Teiler von $n \in \mathbb{Z}$ ist?

2. Ist 3 ein Teiler von 45? Begründen Sie Ihre Antwort.

3. Ist -3 ein Teiler von -45? Begründen Sie Ihre Antwort.

4. Wie lautet die Definition der Teilermenge?

5. Bestimmen Sie T_{45}.

6. Bestimmen Sie T_{-45}.

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Ist m kein Teiler von n, so bleibt bei der Division ein Rest.

Für $n, t, m, r \in \mathbb{Z}$ mit $m, r > 0$ können wir schreiben:

(1.1)

Dabei wählen wir t maximal, so dass $tm \leq n$ ist, also $t = \left\lfloor \frac{n}{m} \right\rfloor$.

Zur Erinnerung:

Eulersche Ganzzahlfunktion:

$\lfloor x \rfloor = max\{a \in \mathbb{Z} \mid a \leq x\}$ wobei $x \in \mathbb{R}$, d.h. $\lfloor x \rfloor$ ist die größte ganze Zahl y mit $y \leq x$.

1. Zahlentheorie

$$n = t \cdot m + r \quad (1.1)$$

1.1 Teilbarkeit – Division mit Rest

Eingesetzt in Gleichung (1.1) ergibt sich:

(1.2)

Da $\left\lfloor \frac{n}{m} \right\rfloor \cdot m \leq n,$ ist

Andererseits ist $r < m$, da $\left\lfloor \frac{n}{m} \right\rfloor$ der größte Faktor t ist, so dass $t \cdot m \leq n$.

Folglich gilt

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Definition 3:

Die Menge der möglichen Reste, die sich bei der Division von n durch $m \in \mathbb{Z}, m > 0$ ergeben, lautet

Bei der ganzzahligen Division von n durch m bezeichnet man $\boldsymbol{m}$ als **Modul** und den **Rest** $\boldsymbol{r}$ als $\boldsymbol{n}$ **modulo** $\boldsymbol{m}$.

Kurzschreibweise:

Der Rest r ist also der Abstand vom nächst kleineren Vielfachen von m.

1. Zahlentheorie

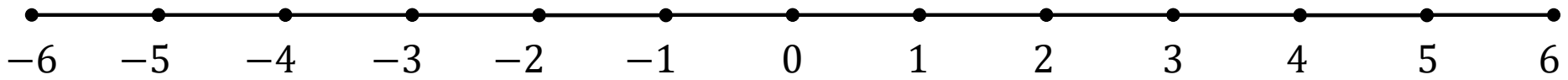
1.1 Teilbarkeit – Division mit Rest

$$r = n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor \cdot m$$

Beispiele:

- $m = 3,\ n = 5$

- $m = 3,\ n = -5$



1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Folgerung 1:

Für $n, m \in \mathbb{Z}$ mit $m > 0$ und $r = n \bmod m$ gilt:

Beweis:

Beispiele von oben:

- $5 - 2 = 3$ und $\frac{3}{3} = 1$
- $-5 - 1 = -6$ und $\frac{-6}{3} = -2$

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Eine Zahl n kann für feste m auf viele Arten in der Form $n = t \cdot m + r$ geschrieben werden.

Beispiel: $n = 11, \quad m = 3$

Beschränkt man r auf den Bereich $\{0; 1; \ldots; m - 1\}$, dann gibt es nur noch eine Darstellung $n = t \cdot m + r$.

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Theorem 1:

Für $m, n \in \mathbb{Z},\ m > 0$ ist die Darstellung $n = t \cdot m + r$ mit $0 \leq r < m$ eindeutig.

Beweis:

Angenommen es gäbe neben der Darstellung $n = t \cdot m + r$ noch eine weitere der Form $n = t' \cdot m + r'$:

$$n = t \cdot m + r = t' \cdot m + r' \qquad \text{mit} \qquad 0 \leq r, r' < m \tag{1.3}$$

1. Zahlentheorie

$$(t - t')m = r - r' \quad (1.3)$$

1.1 Teilbarkeit – Division mit Rest

Nach Gleichung (1.3) ist $r - r'$ ein Vielfaches von m.

Da $0 \leq r, r' < m$, liegt die Differenz $r - r'$ im Bereich

Das einzige Vielfache von m in diesem Bereich ist 0.

D.h. die beiden Darstellungen von n sind gleich.

□

1. Zahlentheorie

1.1 Teilbarkeit – Division mit Rest

Kontrollfragen:

1. Wie lautet die Menge der möglichen Reste, die sich bei der Division von $n \in \mathbb{Z}$ durch 5 ergeben?
2. Wie wird der Rest r bei der ganzzahligen Division von $n \in \mathbb{Z}$ durch $m \in \mathbb{Z}, m > 0$ bezeichnet?
3. Wie kann der Zusammenhang mathematisch dargestellt werden?
4. Weshalb gilt für $n, m \in \mathbb{Z}$ mit $m > 0$ und $r = n \bmod m$: $m | n - r$?

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Gemeinsame Teiler, ggT, kgV

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit

Definition 4:

Für zwei Zahlen $m, n \in \mathbb{Z}$ ist $T_{m;n}$ die Menge der gemeinsamen Teiler von m und n. Es gilt:

Definition 5:

Für zwei Zahlen $m, n \in \mathbb{Z}$ mit $(m; n) \neq (0; 0)$ ist der größte gemeinsame Teiler, kurz $\mathrm{ggT}(m; n)$, die größte Zahl in $T_{m;n}$, also $\max T_{m;n}$:

1. Zahlentheorie

1.1 Teilbarkeit

Definition 6:

Das kleinste gemeinsame Vielfache von $m, n \in \mathbb{Z}$ mit $m, n > 0$, kurz $\mathrm{kgV}(m; n)$, ist die kleinste Zahl, die von m und n geteilt wird:

1. Zahlentheorie

1.1 Teilbarkeit

Beispiele:

- $T_{12} =$

  $T_{18} =$

  $T_{12;18} =$

  $\mathrm{ggT}(12;18) =$

  $\mathrm{kgV}(12;18) =$

- $\mathrm{ggT}(0;n) =$

1. Zahlentheorie

1.1 Teilbarkeit – gemeinsame Teiler, ggT, kgV

Kontrollfragen – Teil 1:

1. Welche Elemente enthält die Menge $T_{m;n}$ $(m, n \in \mathbb{Z})$?

2. Wie lautet die Definition des größten gemeinsamen Teilers zweier Zahlen $m, n \in \mathbb{Z}$ mit

   $(m; n) \neq (0; 0)$?

3. Wie lautet die Definition des kleinsten gemeinsamen Vielfachen zweier Zahlen $m, n \in \mathbb{Z}$ mit

   $m, n > 0$?

1. Zahlentheorie

1.1 Teilbarkeit – gemeinsame Teiler, ggT, kgV

Kontrollfragen – Teil 2:

4. Bestimmen Sie:

- T_{15}
- T_{35}
- $T_{15;35}$
- $\mathrm{ggT}(15; 35)$
- $\mathrm{kgV}(15; 35)$

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Eigenschaften der Teilermengen

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit

Ziel:

Möglichst effizientes Verfahren zur Berechnung des größten gemeinsamen Teilers zweier Zahlen.

Dazu zeigen wir zunächst einige Eigenschaften der Teilermengen.

1. Zahlentheorie

1.1 Teilbarkeit

Lemma 1:

Für alle $a, b \in \mathbb{Z}$ ist

Beweis:

Sei $k \in T_{m;n}$ ein beliebiger Teiler von m und n.

Es gibt also $s, t \in \mathbb{Z}$, so dass

Dann gilt:

$$am + bn =$$

und folglich D.h. □

1. Zahlentheorie

1.1 Teilbarkeit

$T_{m;n} \subseteq T_{am+bn}$

Speziell gilt also für den ggT und für alle $a, b \in \mathbb{Z}$

Beispiel: $m = 12, \quad n = 18, \quad a = -1, \quad b = 2$

$$am + bn =$$

1. Zahlentheorie

1.1 Teilbarkeit

⇒ Die Teilermenge T_{am+bn} enthält im Allgemeinen mehr Zahlen als $T_{m;n}$

(z.B. ist $4 \in T_{24}$, aber $4 \notin T_{12;18}$).

Für bestimmte Aufgaben wäre es also von Vorteil, mindestens eine der Zahlen m, n zu verkleinern, ohne $T_{m;n}$ zu verändern.

1. Zahlentheorie

1.1 Teilbarkeit – Eigenschaften der Teilermengen

Kontrollfragen:

1. Zeigen Sie für $m = 15, \quad n = 21, \quad a = 2, \quad b = -1,$ dass die Beziehung $T_{m;n} \subseteq T_{am+bn}$ erfüllt ist?

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Hinführung zum Euklidischer Algorithmus

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit

Folgerung 2:

Für alle $a \in \mathbb{Z}$ ist

Beweis: Idee: Zeige, dass $T_{m;n} \subseteq T_{m;n-am}$ und $T_{m;n} \supseteq T_{m;n-am}$ also $T_{m;n-am} \subseteq T_{m;n}$

$\Rightarrow$ $T_{m;n} \subseteq T_{m;n-am} = T_m \cap T_{n-am}$

Zu zeigen: $T_{m;n}$ ist enthalten in T_m und in T_{n-am}

- $T_{m;n} \subseteq T_m$ gilt, da $T_{m;n} = T_m \cap T_n \subseteq T_m$
- $T_{m;n} \subseteq T_{n-am}$ folgt nach Lemma 1 ($T_{m;n} \subseteq T_{am+bn}$), wenn dort b durch 1 und a durch $-a$ ersetzt wird.

1. Zahlentheorie

1.1 Teilbarkeit

Beweis: Idee: Zeige, dass $T_{m;n} \subseteq T_{m;n-am}$ und $T_{m;n} \supseteq T_{m;n-am}$ also $T_{m;n-am} \subseteq T_{m;n}$

$\Leftarrow$ $T_{m;n} \supseteq T_{m;n-am}$ also $T_{m;n-am} \subseteq T_{m;n} = T_m \cap T_n$

Zu zeigen: $T_{m;n-am}$ ist enthalten in T_m und in T_n

- $T_{m;n-am} \subseteq T_m$ gilt, da $T_{m;n-am} = T_m \cap T_{n-am} \subseteq T_m$
- $T_{m;n-am} \subseteq T_n$ folgt nach Lemma 1 ($T_{m;n} \subseteq T_{am+bn}$), da sich n wie folgt als Linearkombination von m und $n - am$ darstellen lässt:

Da sowohl $T_{m;n} \subseteq T_{m;n-am}$ als auch $T_{m;n} \supseteq T_{m;n-am}$ gilt, muss $T_{m;n} = T_{m;n-am}$ gelten. □

1. Zahlentheorie

1.1 Teilbarkeit

$$T_{m;n} = T_{m;n-am}$$

Wählt man in Folgerung 2 $a \geq 1$, so verkleinert sich das Zahlenpaar $(m;n)$ zu $(m;n-am)$.

Trotzdem bleiben die gemeinsamen Teiler die selben.

Je kleiner $n-am$ wird, desto einfacher kann der ggT bestimmt werden.

Folglich wählen wir a maximal, so dass $n-am \geq 0$ ist.

Das gilt offensichtlich für $a = \left\lfloor \frac{n}{m} \right\rfloor$.

Dann haben wir:

1. Zahlentheorie

1.1 Teilbarkeit

Folgerung 3:

Für alle $m > 0$ gilt

Spezialfall: $n \bmod m = 0$

Dann erhalten wir $T_{m;0}$.

Da jede positive Zahl Teiler von 0 ist, gilt

und damit

1. Zahlentheorie

1.1 Teilbarkeit

$$T_{m;n} = T_{m;n \bmod m}$$

Beispiel: Berechnung des ggT von 12 und 18:

$$\mathrm{ggT}(12;18) = \max T_{12;18}$$

D.h. die gemeinsamen Teiler von 12 und 18 sind die Teiler von 6.

$$\mathrm{ggT}(12;18) = \max T_{12;18} = \max T_6 = 6$$

1. Zahlentheorie

1.1 Teilbarkeit

Allgemein: Sei $0 \leq m < n$:

$$\text{ggT}(m; n) = \max T_{m;n}$$

$$= \max T_{m;n \bmod m}$$

$$= \max T_{n \bmod m;\, m} \qquad \text{da} \quad n \bmod m < m$$

$$= \text{ggT}(n \bmod m; m)$$

$$T_{m;n} = T_{m;n \bmod m}$$

$$T_{m;n} = T_{n;m}$$

⇒ effizienter Algorithmus zur Bestimmung des ggT: Euklidischer Algorithmus

1. Zahlentheorie

1.1 Teilbarkeit – Hinführung zum Euklidischen Algorithmus

Kontrollfragen:

1. Zeigen Sie, dass für $m = 12$ und $n = 18$ die Beziehung $T_{m;n} = T_{m;n \bmod m}$ erfüllt ist.

2. Bestimmen Sie den $\mathrm{ggT}(15; 35)$ mit Hilfe des Euklidischen Algorithmus.

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Euklidischer Algorithmus (rekursiv)

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Wiederholung

Allgemein: Sei $0 \leq m < n$:

$$\text{ggT}(m; n) = \max T_{m;n}$$

$$= \max T_{m;n \bmod m}$$

$$= \max T_{n \bmod m;\, m} \qquad \text{da} \quad n \bmod m < m$$

$$= \text{ggT}(n \bmod m; m)$$

$$T_{m;n} = T_{m;n \bmod m}$$

$$T_{m;n} = T_{n;m}$$

⇒ effizienter Algorithmus zur Bestimmung des ggT: Euklidischer Algorithmus

1. Zahlentheorie

1.1 Teilbarkeit – Rekursive Formulierung des Euklidischen Algorithmus

Die einfachste Formulierung des Euklidischen Algorithmus ist als rekursive Prozedur.

Sei $0 \leq m < n$:

EUKLID(m, n)

```
1    if m = 0 then
2        return n
3    else
4        return EUKLID(n mod m, m)
```

1. Zahlentheorie

1.1 Teilbarkeit – Rekursive Formulierung des Euklidischen Algorithmus

Beispiel: **EUKLID** (15,10)

```
EUKLID(m, n)
1   if m = 0 then
2       return n
3   else
4       return EUKLID(n mod m, m)
```

1. Zahlentheorie

1.1 Teilbarkeit

EUKLID(m, n)

```
1   if m = 0 then
2       return n
3   else
4       return EUKLID(n mod m, m)
```

- Ausgehend von m und n wird die größere der beiden Zahlen, also n, durch $r = n \bmod m$ ersetzt.
- Wiederholung dieses Schrittes mit r und m.
- Nach Folgerung 3 bleibt die gemeinsame Teilermenge gleich.

$$T_{m;n} = T_{m;n \bmod m}$$

- Prozess endet, wenn die Division ohne Rest aufgeht, d.h. eine der beiden Zahlen 0 ist.
- Da die Zahlen immer kleiner werden, ist dies spätestens dann der Fall, wenn eine der beiden Zahlen 1 ist.
- Sind 0 und d die Zahlen im letzten Schritt, dann ist $T_{m;n} = T_d$ und insbesondere $d = \mathrm{ggT}(m; n)$.

1. Zahlentheorie

1.1 Teilbarkeit

Folgerung 4:

Jeder gemeinsame Teiler von n und m teilt folglich $\mathrm{ggT}(m;n)$.

1. Zahlentheorie

1.1 Teilbarkeit – Euklidischer Algorithmus (rekursiv)

Kontrollfragen:

1. Wie kann der euklidische Algorithmus als rekursive Prozedur formuliert werden?
2. Wann endet die Prozedur?
3. Wie oft muss die Prozedur durchlaufen werden, wenn Sie mit den Argumenten $(15,12)$ aufgerufen wird? Welcher Wert wird dann zurückgegeben?

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Euklidischer Algorithmus (iterativ)

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Iterative Formulierung des Euklidischen Algorithmus

Der Euklidische Algorithmus lässt sich auch als iterativer Algorithmus formulieren (performantere Implementierung).

EUKLID-ITERATIV(m, n)

```
1    while m > 0 do
2        r ← n mod m
3        n ← m
4        m ← r
5    return n
```

1. Zahlentheorie

1.1 Teilbarkeit – Iterative Formulierung des Euklidischen Algorithmus

Beispiel: **EUKLID-ITERATIV**(15,10)

Schritt	r	n	m

EUKLID-ITERATIV(m, n)

```
1  while m > 0 do
2      r ← n mod m
3      n ← m
4      m ← r
5  return n
```

1. Zahlentheorie

1.1 Teilbarkeit – Euklidischer Algorithmus (iterativ)

Kontrollfragen:

1. Wie kann der euklidische Algorithmus als iterative Prozedur formuliert werden?

2. Wann endet die Prozedur?

3. Wie oft muss die Schleife der Prozedur durchlaufen werden, wenn die Prozedur mit den Argumenten $(15,12)$ aufgerufen wird? Welcher Wert wird dann zurückgegeben?

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – ggT als Linearkombination

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – ggT als Linearkombination

Der $\mathrm{ggT}(m;n)$ von m und n lässt sich als Linearkombination von m und n darstellen.

Theorem 2:

Es gibt $x, y \in \mathbb{Z}$, so dass

Beweis:

Mittels vollständiger Induktion über die Zahlenfolge des euklidischen Algorithmus und zwar vom Ende her kommend.

1. Zahlentheorie

1.1 Teilbarkeit – ggT als Linearkombination

$$x \cdot m + y \cdot n = \mathrm{ggT}(m; n)$$

Beweis: Vollständige Induktion

IA: Der Induktionsanfang ist der Rekursionsabbruch des euklidischen Algorithmus, d.h. es ist

$n > m = 0$.

Für $x = 0$ und $y = 1$ gilt dann:

$$x \cdot m + y \cdot n =$$

IV: Für $r = n \bmod m$ und m gibt es x' und $y' \in \mathbb{Z}$, so dass gilt:

1. Zahlentheorie

1.1 Teilbarkeit – ggT als Linearkombination

$$x \cdot m + y \cdot n = \text{ggT}(m; n)$$

Beweis: Vollständige Induktion

IV: $x' \cdot (n \bmod m) + y' \cdot m = \text{ggT}(n \bmod m; m)$

IS (zu zeigen: $\text{ggT}(m; n) = x \cdot m + y \cdot n$):

Nach Folgerung 3 gilt: $\text{ggT}(m; n) = \text{ggT}(n \bmod m; m)$

$$n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor \cdot m$$

D.h. mit $x =$ und $y =$ gilt: $x \cdot m + y \cdot n = \text{ggT}(m; n)$

□

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Der erweiterte euklidische Algorithmus

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Erweiterter euklidischen Algorithmus

Der euklidische Algorithmus kann zum erweiterten euklidischen Algorithmus erweitert werden.

Dieser berechnet neben $d = \text{ggT}(m; n)$ zusätzlich x und y mit $xm + yn = \text{ggT}(m; n)$.

ERWEITERTER-EUKLID(m, n) Rückgabewert: (d, x, y)

```
1   if m = 0 then
2       return (n, 0, 1)
3   else
4       (d, x', y') ← ERWEITERTER−EUKLID(n mod m, m)
5       x = y' − ⌊n/m⌋ · x'
6       y = x'
7       return (d, x, y)
```

1. Zahlentheorie

1.1 Teilbarkeit – Erweiterter euklidischen Algorithmus

Beispiel: **ERWEITERTER-EUKLID**(30,21)

m	n	d	$x = y' - \left\lfloor \frac{n}{m} \right\rfloor \cdot x'$	$y = x'$
30	21	3	$-2 - \left\lfloor \frac{21}{30} \right\rfloor \cdot 3 = -2$	3
$21 \bmod 30 = 21$	30	3	$1 - \left\lfloor \frac{30}{21} \right\rfloor \cdot (-2) = 3$	-2
$30 \bmod 21 = 9$	21	3	$0 - \left\lfloor \frac{21}{9} \right\rfloor \cdot 1 = -2$	1
$21 \bmod 9 = 3$	9	3	$1 - \left\lfloor \frac{9}{3} \right\rfloor \cdot 0 = 1$	0
$9 \bmod 3 = 0$	3	3	0	1

d.h. $\mathrm{ggT}(30; 21) =$

ERWEITERTER-EUKLID(m, n)

```
1  if m = 0 then
2      return (n, 0, 1)
3  else
4      (d, x', y') ← ERW−EUKL(n mod m, m)
5      x = y' − ⌊n/m⌋ · x'
6      y = x'
7      return (d, x, y)
```

1. Zahlentheorie

1.1 Teilbarkeit – Erweiterter euklidischen Algorithmus

Anwendung: z.B. beim Kürzen von Brüchen

- Größter gemeinsamer Faktor in $\frac{a}{b}$ ist der $\mathrm{ggT}(a; b)$:

$$\frac{a}{b} =$$

- Beispiel:

$$\frac{21}{30} =$$

1. Zahlentheorie

1.1 Teilbarkeit – Erweiterter euklidischen Algorithmus

Kontrollfragen:

1. Wie kann der erweiterte euklidische Algorithmus als Prozedur formuliert werden?

2. Wann endet die Prozedur?

3. Welche Werte gibt die Prozedur zurück? Welche Bedeutung haben sie?

4. Warum werden für $m = 0$ die Werte $(n, 0, 1)$ zurückgegeben?

Anwendungsbeispiel erweiterter euklidischer Algorithmus

Sie haben zwei Messlatten mit den Längen $l_1 = 48\ \mathrm{cm}$ und $l_2 = 27\ \mathrm{cm}$.

Wie können Sie mit diesen eine Strecke von $9\ \mathrm{cm}$ abmessen?

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Anwendung euklidischer Algorithmus

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Anwendung des euklidischen Algorithmus

Aufgabe: Kürzen Sie den Bruch $\frac{1029}{1071}$ so weit wie möglich.

Hochschule Aalen

Diskrete Mathematik und Lineare Algebra

1. Zahlentheorie

1.1 Teilbarkeit – Anwendung euklidischer Algorithmus

Dr.-Ing. Miriam Hommel

1. Zahlentheorie

1.1 Teilbarkeit – Anwendung des erweiterten euklidischen Algorithmus

Aufgabe: Wenden Sie den erweiterten euklidischen Algorithmus auf das Zahlenpaar $(28; 42)$ an.