home.in.tum.de/~~fischbec~~/Atringer.html
/~fischbec/

Letzte Stunde:

Einführung Gruppen: Menge + Operation
Es neutrales Element
Es inverses Elemente
Assoziativität

$(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gruppe wenn p Primzahl

Zentrales Problem im Beweis:
Sei p eine Primzahl und sei $a \neq 0, a < p$
Dann ex k und $0 < b < p$ mit

$$\underline{\underline{\underline{b}}} \cdot a - k \cdot p = 1$$

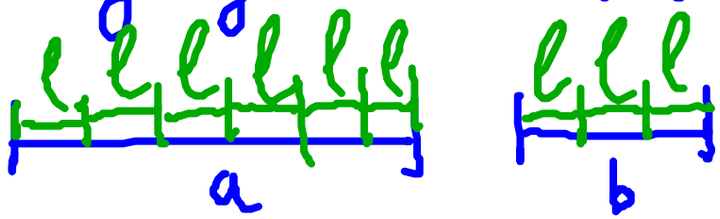
Thema heute: Wie berechnet man b algorithm. Ver wan dte Probleme

- Finde den ggT von $a, b \in \mathbb{N}$

ggT = größter gem Teiler

> Def $t \in \mathbb{N}$ ist der ggT von a, b wenn
> (i) $t \mid a$ und $t \mid b$
> (ii) falls $t' \mid a$ und $t' \mid b$ dann ist $t' \mid t$.

- Kürzen von Brüchen a/b
- Kommensurabilität:
  Gegeben zwei Längen a, b

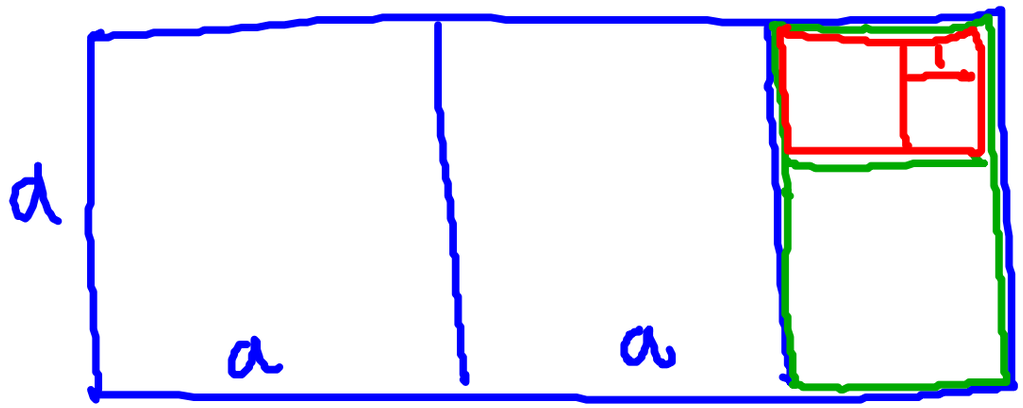


gibt es ein „Messlatte" ℓ, so dass sowohl a als auch b Vielfaches von ℓ ist

- Zahlentaten: gegeben $x \in \mathbb{R}^+$: Entscheide: ist $x = a/b$, $a, b \in \mathbb{N}$

Kommensurabilität:
a, b als Längen gegeben

- Zeichne Rechteck a,b



- Spalte Quadrate ab
- Bleibt Rechteck übrig?

Ja → Behandle Dieses Rechteck

Nein → Maßstab gefunden

Bsp.
$a, b \in \mathbb{N}$
$\Rightarrow \ell$ ist ggT

Algorithmisch

Eingabe $a, b \in \mathbb{N}$, $a \leq b$

While $a \neq 0$ {

r = Rest von b:a;

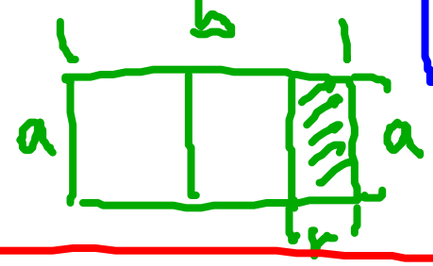
b = a;

a = r; }

return b;

Euklidischer Algorithmus

Satz: Sei $a, b \in \mathbb{N}$
Es gibt eindeutige Zahlen $k, r \in \mathbb{N}$
$r < b$
$a - k \cdot b = r$



15 − 2·6 = 3 Rest bzgl b

Beispiel: 816, 294 / Satz der Eukl. Alg. berechnet einen ggT von a und b

816 = 294 · 2 + 228
294 = 228 · 1 + 66
228 = 66 · 3 + 30
66 = 30 · 2 + 6
30 = 6 · 5 + 0

6 = ggT

$a_1 \geq a_2$

(1) $a_1 = a_2 q_2 + a_3$ $\quad 0 \leq a_3 < a_2$

(2) $a_2 = a_3 q_3 + a_4$ $\quad 0 \leq a_4 < a_3$

$\vdots$

$a_{n-2} = a_{n-1} \cdot q_{n-1} + a_n$

(n-1) $a_{n-1} = a_n \cdot q_n + 0$ ← Muss irgendwann erreicht werden wegen $0 \leq \ldots\ldots \leq a_4 \leq a_3 \leq a_2$

a_n ist ggT

Bew (i) a_n teilt a_1 und a_2

$a_n \mid a_n$ $\quad a_n \mid a_{n-1}$ $\quad a_n \mid a_{n-2}$ $\quad a_n \mid a_{n-3} \ldots a_n \mid a_2, a_n \mid a_1$

(n-2) (n-3)

(ii) Sei $t \mid a_1$ und $t \mid a_2 \Rightarrow t \mid a_n$

$t \mid a_1$ $\quad t \mid a_2$ $\quad \Rightarrow t \mid a_3 \Rightarrow t \mid a_4 \ldots\ldots t \mid a_n$

(1)

(i), (ii) ⇒ a_n ist ggT von a_1, a_2

Erweiterter Eukl. Algorithmus

$ggT(a,b) = r \cdot a - s \cdot b \quad , r,s \in \mathbb{Z}$

Bsp 816, 294

$816 = 294 \cdot 2 + 228$
$294 = 228 \cdot 1 + 66$
$228 = 66 \cdot 3 + 30$
$66 = 30 \cdot 2 + 6$
$30 = \underline{6} \cdot 5 + 0$

$6 = 7 \cdot 294 - 9 \cdot (816 - 2 \cdot 294) = \boxed{25} \cdot 294 - \boxed{9} \cdot 816$
$6 = -2 \cdot 228 + 7 \cdot (294 - 1 \cdot 228) = 7 \cdot 294 - 9 \cdot 228$
$6 = 66 - 2 \cdot (228 - 3 \cdot 66) = 7 \cdot 66 - 2 \cdot 228$
$6 = 66 - 30 \cdot 2$

Anwendung: $0 < a < p$, p Prim

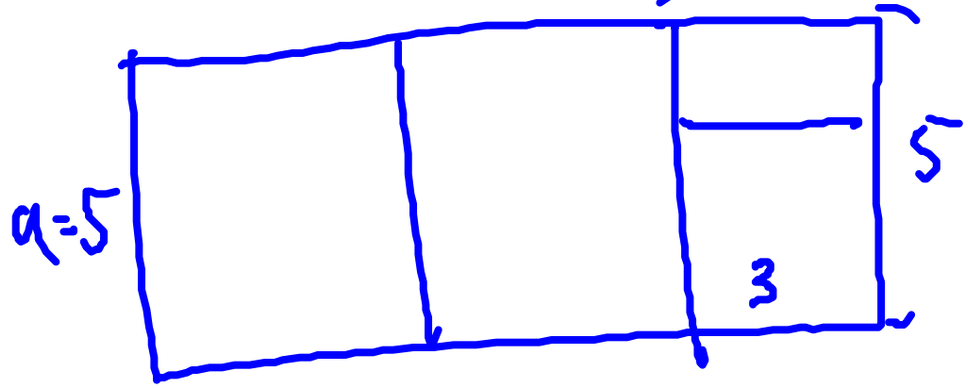
$\Rightarrow ggT(a,p) = 1$

$1 = a \cdot r - s \cdot p$

Setze $a' = r \bmod p \Rightarrow a \odot_p a' = 1$

Kettenbrüche

Beobachtung: Quadratabspalte bildet hängt nur von Längenverhältnis a/b ab.



$x = \frac{b}{a} = 2 + \frac{3}{5}$

$\frac{13}{5}$

$= 2 + \frac{1}{\left(\frac{5}{3}\right)}$

$= 2 + \frac{1}{1 + \frac{2}{3}}$

$= 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}$

```
Eingabe x ∈ R+
while (x ≠ Floor(x)){
    a = Floor (x)
    Print(a)
    X = 1/(x - Floor(x))}
Print(x)
```