Letztes Mal:

$(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gruppe g.d.w p eine Primzahl ist

Zentrales Problem im Beweis

Lemma Sei p eine Primzahl und sei $a \neq 0$; $a < p$ dann ex eine Zahl b $0 < b < p$ mit

$$b \cdot a - k \cdot p = 1$$

für geeignetes $k \in \mathbb{N}$

- Wie berechnet man b aus p und a algorithmisch.

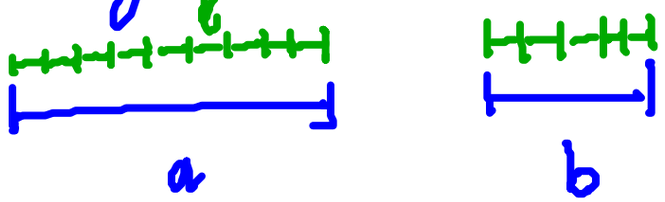
Verwandte Probleme:

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

  ↑ größter gem. Teiler

- Kürzen von Brüchen a/b

- Kommensurabilität: Gegeben zwei Längen a, b



gibt es eine „Messlatte" l so daß sowohl a als auch b ist Vielfaches von l.

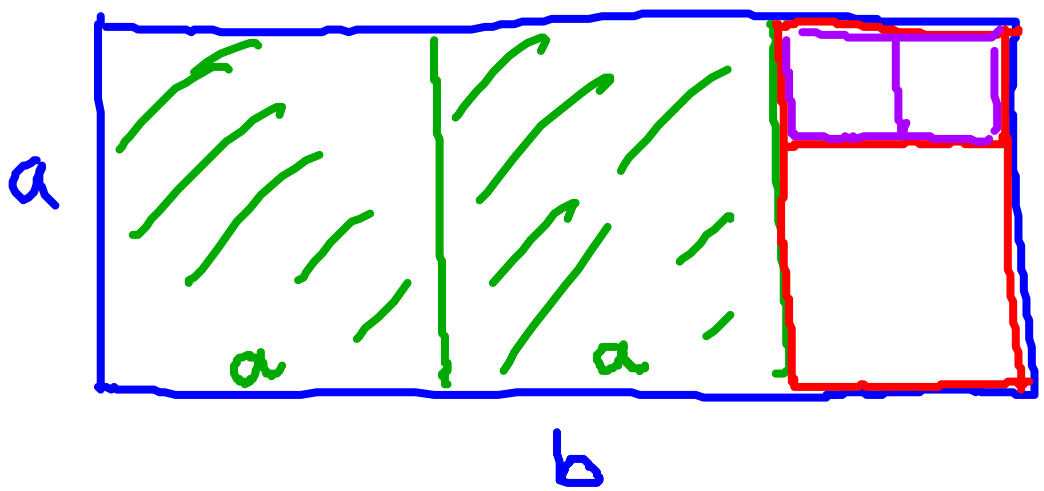
- Zahlen Raten: gegeben $x \in \mathbb{R}^+$ Entscheide ist $x = a/b$, $a, b \in \mathbb{N}$

Def $t \in \mathbb{Z}$ ist ein ggT von a, b wenn:
(i) $t \mid a$ und $t \mid b$
(ii) falls $t' \mid a$ und $t' \mid b$ dann $t' \mid t$

Kommensurabilität:

a, b als Längen gegeben

• Zeichne Rechteck a, b



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

• Spalte Quadrate ab.

• Bleibt ein Rechteck übrig?

Ja

Betrachte
Dieses Rechteck

Nein

Messlatte gefunden

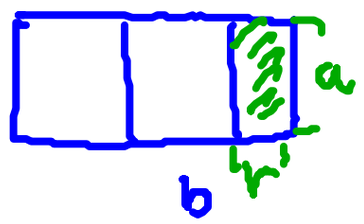
Algorithmisch

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

```
while a ≠ 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 $k, r \in \mathbb{N}$
$a - k \cdot b = r$; $r < b$



Beispiel 816, 294

$816 = 294 \cdot 2 + 228$

$294 = 228 \cdot 1 + 66$

$228 = 66 \cdot 3 + 30$

$66 = 30 \cdot 2 + 6$

$30 = 6 \cdot 5 + 0$

ggT

$a_1 \geq a_2$

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

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

$\vdots$

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

(n-1) $a_{n-1} = a_n \cdot q_n + 0$ $\leftarrow$ Muss erreicht werden

$a_2 > a_3 > \ldots\ldots > a_n > 0$

<u>Bew:</u> (i) Zeige a_n teilt a_1 und a_2

$a_n | a_n$, $a_n | a_{n-1}$ $\;a_n | a_{n-2}$ $\;a_n | a_{n-3}$ $\ldots\ldots a_n | a_2, a_n | a_1$

(n-2) (n-3)

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

$t | a_1$, $t | a_2$ $\;t | a_3$ $\;t | a_4 \ldots\ldots\; t | a_n$

(1) (2)

(i), (ii) $\Rightarrow$ a_n ist ggT von a_1, a_2

Erweiterter Eukl. Algorithmus:

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

Bsp $816, 294$

$816 = 294 \cdot 2 + 228$

$294 = 228 \cdot 1 + 66$

$228 = 66 \cdot 3 + 30$

$66 = 30 \cdot 2 + 6$

$30 = \underline{6} \cdot 5 + 0$

$6 = 7 \cdot 294 - 9 \cdot (816 - 2 \cdot 294) = \boxed{25} \cdot 294 - \boxed{9} \cdot 816$

$6 = -2 \cdot 228 + 7 \cdot (294 - 1 \cdot 228) = 7 \cdot 294 - 9 \cdot 228$

$6 = 66 - 2 \cdot (228 - 3 \cdot 66) = 7 \cdot 66 - 2 \cdot 228$

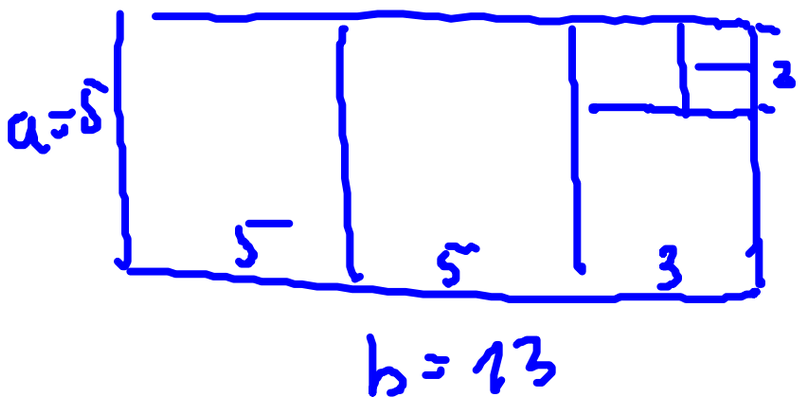
$6 = 66 - 30 \cdot 2$

Inverse Finden: → Annahme $0 < a < p$, p Prim

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

$1 = a \cdot r - s \cdot p$ | Setze $a' = r \bmod p \Rightarrow a \cdot a' \bmod p = 1$

Kettenbrüche:



Eingabe $x \in \mathbb{R}^+$

```
while (x ∉ ℕ) {
    a = Floor(x);
    Print(a)
    x = 1/(x - Floor(x))
}
Print(x)
```

Beobachtung: Quadrate abspalten hängt nur vom Verhältnis b/a ab

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

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

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

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

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