1 Euklidischer Teileralgorithmus

Ziel ist es, den grössten gemeinsamen Teiler (ggt, gcd (greatest common divisor)) zweier Zahlen zu finden, die nicht relativ prim sind. Dazu zieht Euklid (~ 300 vC) folgende beiden Beobachtungen heran:

1. für zwei ganze Zahlen gilt:

$$b|a \Rightarrow ggt(a,b) = b$$

   Begründung: keine Zahl kann durch eine Zahl geteilt werden, die grösser ist als die Zahl selbst.

2. Rekursionsschritt:

$$a = bt + r \Rightarrow ggt(a,b) = ggt(b,r)$$

   (für $t, r \in N$)

   Jede Zahl, die a und b teilt, ist auch ein Divisor von r. Daher teilt ggt(a,b) auch r ($ggt(a,b)|r$), nicht nur b, sodass $ggt(a,b) \leq ggt(b,r)$, ebenso $ggt(a,b) \leq ggt(a,r)$. Wenn nun für den nächsten Schritt $a = b$ und $b = r$ gesetzt wird, kann das Verfahren so lange fortgesetzt werden, bis gilt $b|a$, also der Divisionsrest `a % b == 0`.

In der urpsruenglichen Version subtrahierte Euklid jeweils a von b, der Algorithmus waere also dann:

1. wenn `b > a`, dann vertausche `a` und `b`
2. wenn `a` durch `b` dividierbar ist, dann Ergebnis `ggt(a,b) == b` **ENDE**
3. subtrahiere `b` von `a`
4. gehe zu **1.**

1.1 Beispiel

1. $a = 9690, b = 3825 \Rightarrow r = 2040$
2. $a = 3825, b = 2040 \Rightarrow r = 1785$
3. $a = 2040, b = 1785 \Rightarrow r = 255$
4. $a = 1785, \mathbf{b = 255} \Rightarrow r = 0$

```
ggt(9690,2040) == 255
```

1.2 Schreibweise

$b \mid a$	b teilt a (`a % b == 0`)
$ggt(a, b)$	grösster gemeinsamer Teiler