1.4 Euklidischer Algorithmus

Es seien n, m pos. nat. Zahlen.

(1.) Das kleinste gemeinsame Vielfache von n und m, symb.: $\mathrm{kgV}(n,m)$, ist die kleinste nat. Zahl $k>0$ mit $n \mid k$ und $m \mid k$.

(2.) Der größte gemeinsame Teiler von n und m, symb.: $\mathrm{ggT}(n,m)$, ist die größte nat. Zahl k mit $k \mid n$ und $k \mid m$.

Beispiele:

1. $\mathrm{kgV}(3,5) = 15$, $\quad \mathrm{ggT}(3,5) = 1$
2. $\mathrm{kgV}(3,6) = 6$, $\quad \mathrm{ggT}(3,6) = 3$
3. $\mathrm{kgV}(4,6) = 12$, $\quad \mathrm{ggT}(4,6) = 2$

Lemma 3. (siehe Skriptum)

Beispiel: $\mathrm{kgV}(120,36) = 2^3 \cdot 3^2 \cdot 5^1 = 360$, $\mathrm{ggT}(120,36) = 2^2 \cdot 3^1 \cdot 5^0 = 12$
$(120 = 2^3 \cdot 3^1 \cdot 5^1,\ 36 = 2^2 \cdot 3^2 \cdot 5^0)$

Satz 4.

Es seien n und m pos. nat. Zahlen. Dann gilt:

$$n \cdot m = \mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m) \qquad \blacksquare$$

Frage: Wie bestimmen wir $\mathrm{ggT}(n,m)$?

Lemma 5.

Sind n, m pos. nat. Zahlen mit $m \leq n$ und $m \nmid n$, so gilt

$$\mathrm{ggT}(m,n) = \mathrm{ggT}(m, n-m)$$

Beweis: Wir zeigen: Jeder Teiler von n und m ist auch ein

Teiler von $n-m$ und m und umgekehrt.

Es sei d ein Teiler von n und m, d.h. $d | n$ und $d | m$, d.h. $n = c \cdot d$, $m = c' \cdot d$ für geeignete c, c'. Somit gilt

$$n - m = c \cdot d - c' \cdot d = (c - c') \cdot d$$

D.h. $d \,/\, n-m$.

Es sei d ein Teiler von $n-m$ und m, d.h. $d \,/\, n-m$ und $d | m$, d.h. $n-m = c \cdot d$, $m = c' \cdot d$ für geeignete c, c'. Somit gilt:

$$n = n - m + m = c \cdot d + c' \cdot d = (c + c') \cdot d$$

D.h. $d | n$ $\blacksquare$

Korollar 6.

Sind m, n pos. nat. Zahlen mit $m \leq n$ und $m \nmid n$, so gilt:

$$ggT(m,n) = ggT(mod(n,m), m)$$

Beweis: Es sei $n = k \cdot m + mod(n,m)$ für geeignetes $k > 0$. Dann gilt:

$$\begin{aligned} ggT(m,n) &= ggT(m, n-m) \\ &= ggT(m, n-2m) \\ &\;\vdots \\ &= ggT(m, n-km) \\ &= ggT(m, mod(n,m)) \end{aligned}$$

$\blacksquare$

Algorithmus: Euklid

Eingabe: pos. nat. Zahlen m, n mit $m \leq n$

Ausgabe: $ggT(m,n)$

(1) **if** m teilt n **then**

(2) **return** m

(3) else
(4) return Euklid(mod(n,m), m)

Beispiele:

1. Euklid(36, 120) = Euklid(12, 36) = 12
2. Euklid(89, 144) = Euklid(55, 89)
   = Euklid(34, 55)
   = Euklid(21, 34)
   = Euklid(13, 21)
   = Euklid(8, 13)
   = Euklid(5, 8)
   = Euklid(3, 5)
   = Euklid(2, 3)
   = Euklid(1, 2)
   = 1

Fibonacci-Zahlen: $F_n =_{def} F_{n-1} + F_{n-2}$ für $n \geq 2$, $F_1 =_{def} 1$, $F_0 =_{def} 0$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13 ...
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233 ...

Euklidischer Alg. kann benutzt werden, um teilerfremde Brüche zu berechnen:

Es gilt $\frac{n}{ggT(n,m)}$ und $\frac{m}{ggT(n,m)}$ sind teilerfremd, d.h.

$$ggT\left(\frac{n}{ggT(n,m)}, \frac{m}{ggT(n,m)}\right) = 1$$

Weiterhin ist:

$$\frac{n}{m} = \frac{n}{m} \cdot \frac{ggT(n,m)}{ggT(n,m)} = \frac{\frac{n}{ggT(n,m)}}{\frac{m}{ggT(n,m)}}$$

Beispiel: $2{,}7\overline{1828} = \frac{271.801}{99.990}$ teilerfremd

3. Induktion

3.1 Vollständige Induktion

Problem:

Wie weisen wir nach, dass alle nat. Zahlen eine bestimmte Eigenschaft E erfüllen?

Lösungsmethode: vollständige Induktion von $n-1$ nach n

(IA) Induktionsanfang: Erfüllt 0 die Eigenschaft E und
(IS) Induktionsschritt: folgt für alle $n>0$ die Gültigkeit von E für n aus der Tatsache, dass $n-1$ die Eigenschaft E erfüllt (Induktionsvoraussetzung; IV),

so erfüllen alle Zahlen die Eigenschaft E.

Beispiele:

1. Definiere für $n \geq 0$: $a_n =_{def} \sum_{k=0}^{n} k$

Wollen zeigen: Für alle n gilt $a_n = \frac{n(n+1)}{2}$ $(E(n))$

(IA) $n=0$: $a_0 = \sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2}$, d.h. $E(0)$ wahr

(IS) $n>0$:
$$a_n = n + a_{n-1} \overset{(IV)}{=} n + \frac{(n-1)n}{2} = \frac{2n + (n-1)n}{2} = \frac{n(2+(n-1))}{2} = \frac{n(n+1)}{2}$$

2.) Definiere für $n \geq 0$: $a_n =_{def} \sum_{k=0}^{n} (2k+1)$ $E(0): a_0 = (0+1)^2$

Wollen zeigen: Für alle n gilt $a_n = (n+1)^2$ $\leftarrow E(n)$

(IA) $n=0$: $a_0 = \sum_{k=0}^{0} (2k+1) = 1 = (0+1)^2$ $E(n-1): a_{n-1} = ((n-1)+1)^2 = n^2$

(IS) $n>0$: $\underset{k=0,1,\dots,n}{a_n} = \underset{k=n}{2n+1} + \underset{k=0,1,\dots,n-1}{a_{n-1}}$

$\overset{(IV)}{=} 2n+1 + n^2$

$= (n+1)^2$

3.) Geometrische Reihe (für $q \neq 1$)

Definiere für $n \geq 0$: $s_n =_{def} \sum_{k=0}^{n} q^k$ $E(0): s_0 = \frac{q^{0+1}-1}{q-1} = 1$

Wollen zeigen: Für alle n gilt $s_n = \frac{q^{n+1}-1}{q-1}$ $\leftarrow E(n)$

(Insbesondere: $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$) $E(n-1): s_{n-1} = \frac{q^{(n-1)+1}-1}{q-1} = \frac{q^n-1}{q-1}$

(IA) $n=0$: $s_0 = \sum_{k=0}^{0} q^k = q^0 = 1 = \frac{q^{0+1}-1}{q-1}$

(IS) $n>0$: $\underbrace{\sum_{k=0}^{n} q^k}_{s_n} = q^n + \underbrace{\sum_{k=0}^{n-1} q^k}_{s_{n-1}}$

$\overset{(IV)}{=} q^n + \frac{q^n-1}{q-1}$

$= \frac{q^n(q-1) + q^n - 1}{q-1}$

$= \frac{q^{n+1} - q^n + q^n - 1}{q-1} = \frac{q^{n+1}-1}{q-1}$

4.) Wollen zeigen: Für alle $n \geq 0$ gilt $\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

(IA) $n=0$: $\sum_{k=0}^{0} k^2 = 0^2 = 0 = \frac{0(0+1)(2 \cdot 0+1)}{6}$

(IS) $n>0$: $\sum_{k=0}^{n} k^2 = n^2 + \sum_{k=0}^{n-1} k^2$

$$\overset{(IV)}{=} n^2 + \frac{(n-1)n(2n-1)}{6}$$

$$= \frac{6n^2 + (n-1)n(2n-1)}{6}$$

$$= \frac{n(6n + (n-1)(2n-1))}{6}$$

$$= \frac{n(6n + 2n^2 - 3n + 1)}{6}$$

$$= \frac{n(2n^2 + 3n + 1)}{6}$$

$$= \frac{n(n+1)(2n+1)}{6}$$