Zum $ggT(a_1, a_2, \ldots a_n)$

0. Als Teiler nur positive ganze Zahlen

1. Gegeben: $a_1, a_2, \ldots a_n \in \mathbb{Z} \setminus \{0\}$

2. Behauptung: Es gibt genau einen gemeinsamen Teiler d von $a_1, a_2, \ldots, a_n$ mit:

(I) d ist durch jeden gemeinsamen Teiler von $a_1, a_2, \ldots, a_n$ teilbar

(Bezeichnung: $ggT(a_1, a_2, \ldots, a_n)$)

(II) d läßt sich als Vielfachsumme der a_i schreiben:

$$d = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n$$

mit $m_i \in \mathbb{Z} \setminus \{0\}$

(Unter allen gemeinsamen Teilern von $a_1, \ldots, a_n$ ist d durch (II) eindeutig bestimmt)

Bew.: (i) Es ex. höchstens ein gem. Teiler von $a_1, \ldots a_n$ mit (I). Denn gäbe es d' mit (I), so wäre $d \mid d'$ und $d' \mid d$.

(ii) d ist größter gem. T. von $a_1, \dots, a_n$, denn für jeden gem. T. t der a_i gilt auch $t \mid d$, dh $t \leq d$.

(iii) Jeder gem. Teiler t von $a_1, \dots, a_n$ mit Eigenschaft II erfüllt (I)

Sei $t = m_1 a_1 + \dots + m_n a_n$.
Für jeden gem. T. t' von $a_1, \dots, a_m$ ist dann $t' \mid m_i a_i$ also $t' \mid t$
Also gibt es höchstens einen gem. T. der a_i mit II.

(iv) Konstruktion des g.g.T.: Erst für $n = 2$: Euklidscher Algorithm.
Voraus. $a_1 > a_2$: Sukzessive Division

$$a_1 = a_2 q_1 + r_1 \quad , \quad 0 < r_1 < a_2$$
$$a_2 = r_1 q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$
$$r_2 = r_3 q_4 + r_4 \quad , \quad 0 < r_4 < r_3$$

Da $r_i \in \mathbb{N}$, exist. p mit $r_p = 0$.
Dann $r_{p-1} \mid a_2$ und $r_{p-1} \mid a_1$

Permutationen

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = A$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = B$

$= (1\ 2\ 3)$ $= (1)(2\ 3)$

$AB = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$= (1\ 3)(2)$ $= (1\ 2)(3)$

$A^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ $B^{-1} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix}$

$= (1\ 3\ 2)$ $= (1)(2\ 3)$

$= A^2$ $B^2 = id$

$\{A, A^2, B, AB, BA, id\}$

Volle Permutationsgruppe von $\{1, 2, 3\}$