Innermathematische Beziehungen
Zahlentheorie (Übung)

Prof. Dr. Markus Vogel
Fabian Grünig

Sommersemester 2018
Mittwoch, 14:00 Uhr, H009

Der Erweiterte Euklidische Algorithmus (EEA) liefert für zwei Zahlen $a, b \in \mathbb{Z}$ die Darstellung des $\operatorname{ggT}(a,b)$ als Linearkombination $\operatorname{ggT}(a,b) = x \cdot a + y \cdot b$. Auf diesem Übungszettel entwickeln wir eine Tabellendarstellung für der Erweiterten Euklidischen Algorithmus (EEA), in der die gesuchten x, y Koeffizienten direkt „von oben" mitberechnet werden.

Zusatzaufgabe 6 *(Bestimmung der Linearkombinationen „von oben")*
Es seien $a, b \in \mathbb{Z}$. Der Euklidische Algorithmus liefert Zahlenpaare $q_i, r_i \in \mathbb{Z}$ und die folgende Gleichungskette:

$$\begin{aligned} a &= q_0 \cdot b + r_0 & &\vdots \\ b &= q_1 \cdot r_0 + r_1 & r_{n-2} &= q_n \cdot r_{n-1} + r_n \\ r_0 &= q_2 \cdot r_1 + r_2 & r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

(i) Stelle r_0 als Linearkombination von a und b dar. Wie lauten die Koeffizienten?

(ii) Stelle r_1 als Linearkombination von a und b dar. Wie lauten die Koeffizienten?

(iii) Es sei bereits möglich r_{k-2} und r_{k-1} als Linearkombination von a und b darzustellen, etwa via

$$r_{k-2} = x_{k-2} \cdot a + y_{k-2} \cdot b, \qquad r_{k-1} = x_{k-1} \cdot a + y_{k-1} \cdot b.$$

Zeige, dass sich dann auch r_k als Linearkombination von a und b darstellen lässt. Wie lauten die Koeffizienten?

Diese Aufgabe zeigt uns, dass wir jeden entstehenden Rest r_k als Linearkombination von a und b schreiben können. Um die Koeffizienten x_k, y_k zu berechnen, brauchen wir die jeweiligen Koeffizienten aus den *beiden* vorherigen Schritten. Wir setzen die Tabellendarstellung wie folgt an.

k	a	b	q	r	x	y
0	a	b	q_0	r_0	1	$-q_0$
1	b	r_0	q_1	r_1	$1-q_1$	$1-q_1 q_0$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	r_{k-4}	r_{k-3}	q_{k-2}	r_{k-2}	x_{k-2}	y_{k-2}
$k-1$	r_{k-3}	r_{k-2}	q_{k-1}	r_{k-1}	x_{k-1}	y_{k-1}
k	r_{k-2}	r_{k-1}	q_k	r_k	$\boxed{x_{k-2} - q_k \cdot x_{k-1}}$	$\boxed{y_{k-2} - q_k \cdot y_{k-1}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	r_{n-2}	r_{n-1}	q_n	r_n	$\boxed{x_n}$	$\boxed{y_n}$
$n+1$	r_{n-1}	r_n	q_{n+1}	0		

Als Ergebnis erhalten wir

$$\operatorname{ggT}(a,b) = r_n = x_n \cdot a + y_n \cdot b.$$