Euklidischer Algorithmus und Inverse in $\mathbb{Z}/p\mathbb{Z}$

Seien $a, b \in \mathbb{Z}$. Gesucht ist der grösste gemeinsame Teiler $d = ggT(a, b)$ von a, b, d.h. eine ganze Zahl d mit foldgenden Eigenschaften:

(i) $d|a$, $d|b$

(ii) Sei $d' \in \mathbb{Z}$ mit $d'|a$, $d'|b$, so folgt $d'|d$.

(iii) $d \geq 1$.

Wir benutzen hier die Kurzschreibweise $d|a$ für "d teilt a". Die Berechnung des $ggT(a, b)$ geschieht mit dem Euklidischen Algorithmus:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{k+1} &= \underbrace{r_{k-1} - \left[\frac{r_{k-1}}{r_k}\right] r_k}_{\text{Rest bei Division } r_{k-1}:r_k} \qquad (k \geq 1) \end{aligned} \tag{1}$$

1) Es gilt $0 \leq r_{k+1} < r_k$:

Beweis. Per Definition der Gauss'schen Klammer $[\cdot]$ gilt

$$\left[\frac{r_{k-1}}{r_k}\right] \leq \frac{r_{k-1}}{r_k} < \left[\frac{r_{k-1}}{r_k}\right] + 1$$

also

$$\frac{r_{k-1}}{r_k} - 1 < \left[\frac{r_{k-1}}{r_k}\right] \leq \frac{r_{k-1}}{r_k} \tag{2}$$

Ersetzen wir in (1) den Term $\left[\frac{r_{k-1}}{r_k}\right]$ durch seine untere bzw. obere Schranke gegeben in (2), erhalten wir

$$\underbrace{r_{k-1} - \frac{r_{k-1}}{r_k} r_k}_{=0} \leq \underbrace{r_{k-1} - \left[\frac{r_{k-1}}{r_k}\right] r_k}_{=r_{k+1}} < \underbrace{r_{k-1} - \left(\frac{r_{k-1}}{r_k} - 1\right) r_k}_{r_k}$$

$\square$

2) Nach 1) gibt es ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$ und $r_n \neq 0$. Dann ist $r_n = ggT(a, b)$:

Beweis. Zu zeigen ist, dass r_n alle drei Eigenschaften des ggT(a,b) erfüllt. Zuerst zeigen wir, dass $r_n | r_k$, $\forall k \leq n$. Insbesondere also $r_n | r_0$ und $r_n | r_1$. Wir beginnen mit der offensichtlichen Aussagen $r_n | r_{n+1}$, $r_n | r_n$ und gehen damit rückwärts durch den Euklidischen Algorithmus:

$$\begin{array}{rcll}
r_{n+1} & = & r_{n-1} - \left[\frac{r_{n-1}}{r_n}\right] r_n & \Rightarrow \; r_n | r_{n-1} \\
r_n & = & r_{n-2} - \left[\frac{r_{n-2}}{r_{n-1}}\right] r_{n-1} & \Rightarrow \; r_n | r_{n-2} \\
\vdots & & \vdots & \vdots \\
r_{k+1} & = & r_{k-1} - \left[\frac{r_{k-1}}{r_k}\right] r_k & \Rightarrow \; r_n | r_{k-1} \\
\vdots & & \vdots & \vdots \\
r_3 & = & r_1 - \left[\frac{r_1}{r_2}\right] r_2 & \Rightarrow \; r_n | r_1 = b \\
r_2 & = & r_0 - \left[\frac{r_0}{r_1}\right] r_1 & \Rightarrow \; r_n | r_0 = a
\end{array}$$

Sei nun $d' \in \mathbb{Z}$ mit $d'|a$, $d'|b$. Zu zeigen ist $d'|r_n$. Wir beginnen mit $d'|r_0$, $d'|r_1$ und gehen damit vorwärts durch den Euklidischen Algorithmus:

$$\begin{array}{rcll}
r_2 & = & r_0 - \left[\frac{r_0}{r_1}\right] r_1 & \Rightarrow \; d' | r_2 \\
\vdots & & \vdots & \vdots \\
r_{k+1} & = & r_{k-1} - \left[\frac{r_{k-1}}{r_k}\right] r_k & \Rightarrow \; d' | r_{k+1} \\
\vdots & & \vdots & \vdots \\
r_n & = & r_{n-2} - \left[\frac{r_{n-2}}{r_{n-1}}\right] r_{n-1} & \Rightarrow \; d' | r_n
\end{array}$$

Schliesslich ist nach Konstruktion $r_n \geq 1$. $\square$

3) Beispiel: $a = 495$, $b = 368$

$$\begin{array}{rcl}
127 & = & 495 - 1 \cdot 368 \\
114 & = & 368 - 2 \cdot 127 \\
13 & = & 127 - 1 \cdot 114 \\
10 & = & 114 - 8 \cdot 13 \\
3 & = & 13 - 1 \cdot 10 \\
1 & = & 10 - 3 \cdot 3 \\
0 & = & 3 - 3 \cdot 1
\end{array}$$

D.h. $ggT(495, 386) = 1$.

4) Es existieren $s, t \in \mathbb{Z}$ mit $a \cdot s + b \cdot t = ggT(a, b)$:

Beweis. Die Bedingung $a \cdot s + b \cdot t = ggT(a, b) = d$ lässt sich vektoriell formulieren als $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} d \\ s \\ t \end{pmatrix} = 0$. Um s, t zu finden erweitern wir im Euklidischen Algorithmus die Zahlen r_k zu Vektoren, deren erste Komponente gerade r_k ist:

$$\begin{aligned} \begin{pmatrix} r_0 \\ s_0 \\ t_0 \end{pmatrix} &= \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} r_1 \\ s_1 \\ t_1 \end{pmatrix} &= \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} r_{k+1} \\ s_{k+1} \\ t_{k+1} \end{pmatrix} &= \begin{pmatrix} r_{k-1} \\ s_{k-1} \\ t_{k-1} \end{pmatrix} - \left[\frac{r_{k-1}}{r_k} \right] \begin{pmatrix} r_k \\ s_k \\ t_k \end{pmatrix} \quad (k \geq 1) \end{aligned} \tag{3}$$

Es gilt $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} r_0 \\ s_0 \\ t_0 \end{pmatrix} = \begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix} = 0$, $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ s_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix} = 0$. Nun multiplizieren wir auch alle anderen Zeile des erweiterten Euklidischen Algorithmus (3) skalar mit dem Vektor $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix}$ und erhalten so schrittweise $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} r_k \\ s_k \\ t_k \end{pmatrix} = 0$. Für $k = n$ haben wir insbesondere $r_n = d$, d.h. $\begin{pmatrix} 1 \\ -a \\ -b \end{pmatrix} \cdot \begin{pmatrix} d \\ s_n \\ t_n \end{pmatrix} = 0$. Somit leisten die Zahlen $s = s_n$ und $t = t_n$ das verlangte. □

5) Beispiel $a = 495$, $b = 368$:

$$\begin{aligned} \begin{pmatrix} 127 \\ 1 \\ -1 \end{pmatrix} &= \begin{pmatrix} 495 \\ 1 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 368 \\ 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 114 \\ -2 \\ 3 \end{pmatrix} &= \begin{pmatrix} 368 \\ 0 \\ 1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 127 \\ 1 \\ -1 \end{pmatrix} \\ \begin{pmatrix} 13 \\ 3 \\ -4 \end{pmatrix} &= \begin{pmatrix} 127 \\ 1 \\ -1 \end{pmatrix} - 1 \cdot \begin{pmatrix} 114 \\ -2 \\ 3 \end{pmatrix} \\ \begin{pmatrix} 10 \\ -26 \\ 35 \end{pmatrix} &= \begin{pmatrix} 114 \\ -2 \\ 3 \end{pmatrix} - 8 \cdot \begin{pmatrix} 13 \\ 3 \\ -4 \end{pmatrix} \\ \begin{pmatrix} 3 \\ 29 \\ -39 \end{pmatrix} &= \begin{pmatrix} 13 \\ 3 \\ -4 \end{pmatrix} - 1 \cdot \begin{pmatrix} 10 \\ -26 \\ 35 \end{pmatrix} \\ \begin{pmatrix} 1 \\ -113 \\ 152 \end{pmatrix} &= \begin{pmatrix} 10 \\ -26 \\ 35 \end{pmatrix} - 3 \cdot \begin{pmatrix} 3 \\ 29 \\ -39 \end{pmatrix} \end{aligned}$$

D.h. $495 \cdot (-113) + 368 \cdot 152 = 1$.

6) a hat ein Inverses im Ring $\mathbb{Z}/b\mathbb{Z}$ genau dann wenn $ggT(a, b) = 1$.

Beweis. Sei $ggT(a, b) = 1$ dann existieren $s, t \in \mathbb{Z}$ mit

$$a \cdot s + b \cdot t = 1 \quad \Rightarrow \quad a \cdot s \equiv 1 \mod b$$

Mit anderen Worten ${[a]_b}^{-1} = [s]_b$ in $\mathbb{Z}/b\mathbb{Z}$.

Umgekehrt: es existiere ein Inverses ${[a]_b}^{-1} = [s]_b$, d.h. $a \cdot s \equiv 1 \mod b$. Dann exisiert ein $t \in \mathbb{Z}$ mit $a \cdot s + b \cdot t = 1$. Da die linke Seite per Def. durch $ggT(a, b)$ teilbar ist, muss dies auch für die rechte Seite gelten - also $ggT(a, b) = 1$ □