4.2 Bestimmung des multiplikativen Inversen

Grundlage für die Bestimmung des multiplikativen Inversen einer Zahl a modulo einer Zahl m, wobei a und m teilerfremd sind, ist der Euklidische Algorithmus, mit dem man sehr einfach den größten gemeinsamen Teiler zweier Zahlen berechnen kann.

4.2.1 Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Es gibt verschiedene Möglichkeiten, um den größten gemeinsamen Teiler (ggT) zweier Zahlen a und b (kurz: $\mathrm{ggT}(a, b)$) zu bestimmen. Man kann dies beispielsweise über eine Primfaktorzerlegung der beiden Zahlen und anschließenden Abgleich der gemeinsamen Primfaktoren vornehmen oder auch mit dem Euklidischen Algorithmus. Dabei erfordert der Euklidische Algorithmus in vielen Fällen weniger Rechenaufwand als die Primfaktorzerlegung.

Nehmen wir beispielsweise an, wir wollen $\mathrm{ggT}(8, 5)$ bestimmen. Es gilt

$$8 : 5 = 1 \text{ Rest } 3 \ .$$

Basis des Euklidischen Algorithmus ist jetzt, dass ggT(8,5)=ggT(5,3) gilt, d.h. anstatt den ggT der beiden ursprünglichen Zahlen zu ermitteln, reicht es aus, den ggT aus der kleineren dieser beiden Zahlen und dem Rest, der entsteht, wenn wir die gegebenen beiden Zahlen durcheinander dividieren, zu bestimmen. Dies gilt allgemein; wir verzichten hier jedoch auf einen Beweis. Dieser Ansatz kann rekursiv angewendet werden:

$$5 : 3 = 1 \text{ Rest } 2 \qquad \Longrightarrow \qquad \mathrm{ggT}(5, 3) = \mathrm{ggT}(3, 2)$$

sowie

$$3 : 2 = 1 \text{ Rest } 1 \qquad \Longrightarrow \qquad \mathrm{ggT}(3, 2) = \mathrm{ggT}(2, 1)$$

und schließlich

$$2 : 1 = 2 \text{ Rest } 0 \ .$$

Der letzte von 0 verschiedene Rest ist dann der ggT der beiden ursprünglichen Zahlen. Also: $\mathrm{ggT}(8, 5) = \mathrm{ggT}(5, 3) = \mathrm{ggT}(3, 2) = \mathrm{ggT}(2, 1) = 1$.

Beispiel 4.1 *Ein weiteres Beispiel für den Euklidischen Algorithmus: Zu bestimmen sei ggT(120,72). Es gilt*

$$\begin{aligned} 120 : 72 &= 1 \ \mathit{Rest}\ 48 & \Longrightarrow \qquad & ggT(120, 72) = ggT(72, 48) \\ 72 : 48 &= 1 \ \mathit{Rest}\ 24 & \Longrightarrow \qquad & ggT(72, 48) = ggT(48, 24) \\ 48 : 24 &= 2 \ \mathit{Rest}\ 0 & \Longrightarrow \qquad & ggT(48, 24) = 24 \ . \end{aligned}$$

Wir haben also

$$ggT(120, 72) = ggT(72, 48) = ggT(48, 24) = 24 \ .$$

Das Arbeitsblatt *Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen* unterstützt die Schüler/-innen bei der Erarbeitung des Euklidischen Algorithmus zur Bestimmung des ggT zweier gegebener Zahlen.

Arbeitsblatt: Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier Zahlen

Es gibt verschiedene Möglichkeiten, um den größten gemeinsamen Teiler zweier Zahlen a und b, im folgenden kurz als $\mathrm{ggT}(a,b)$ bezeichnet, zu bestimmen. Man kann dies beispielsweise über eine Primfaktorzerlegung der beiden Zahlen und anschließenden Abgleich der gemeinsamen Primfaktoren vornehmen oder auch mit dem Euklidischen Algorithmus. Ist von keiner der beiden Zahlen die Primfaktorzerlegung bekannt, so ist der Euklidische Algorithmus das schnellste Verfahren zur Bestimmung des ggT.

Nehmen wir beispielsweise an, wir wollen $\mathrm{ggT}(8,5)$ bestimmen. Es gilt

$$8 : 5 = 1 \text{ Rest } 3 \ .$$

Basis des Euklidischen Algorithmus ist jetzt, dass ggT(8,5)=ggT(5,3) gilt, d.h. anstatt den ggT der beiden ursprünglichen Zahlen 8 und 5 zu ermitteln, reicht es aus, den ggT aus der kleineren dieser beiden Zahlen (hier 5) und dem Rest (hier 3), der entsteht, wenn wir die gegebenen beiden Zahlen durcheinander dividieren, zu bestimmen. (Dies gilt allgemein; wir verzichten hier jedoch auf einen Beweis.) Dieser Ansatz kann mehrfach angewendet werden:

$$5 : 3 = 1 \text{ Rest } 2 \qquad \Longrightarrow \qquad \mathrm{ggT}(5,3) = \mathrm{ggT}(3,2)$$

sowie

$$3 : 2 = 1 \text{ Rest } 1 \qquad \Longrightarrow \qquad \mathrm{ggT}(3,2) = \mathrm{ggT}(2,1)$$

und schließlich

$$2 : 1 = 2 \text{ Rest } 0 \ .$$

Der letzte von 0 verschiedene Rest ist dann der ggT der beiden ursprünglichen Zahlen. Es gilt somit: ggT(8,5)=ggT(5,3)=ggT(3,2)=ggT(2,1)=1 .

Ein weiteres Beispiel für den Euklidischen Algorithmus:
Zu bestimmen sei ggT(120,72). Es gilt

$$\begin{aligned} 120 : 72 = 1 \text{ Rest } 48 \qquad &\Longrightarrow \qquad \mathrm{ggT}(120,72) = \mathrm{ggT}(72,48) \\ 72 : 48 = 1 \text{ Rest } 24 \qquad &\Longrightarrow \qquad \mathrm{ggT}(72,48) = \mathrm{ggT}(48,24) \\ 48 : 24 = 2 \text{ Rest } 0 \qquad &\Longrightarrow \qquad \mathrm{ggT}(48,24) = 24 \ . \end{aligned}$$

Wir haben also

$$\mathrm{ggT}(120,72) = \mathrm{ggT}(72,48) = \mathrm{ggT}(48,24) = 24 \ .$$

Aufgabe 1: Bestimme mit dem Euklidischen Algorithmus den ggT von
a) 24 und 9
b) 36 und 18
c) 75 und 45
d) 720 und 288
e) 1071 und 1029