

Eine Erweiterung des Lemmas von Bézout

Florian Severin

9. September 2009

1 Einleitung

Das Lemma von Bézout ist ein bekanntes und wichtiges Instrument der Zahlentheorie.

Lemma 1 (Lemma von Bézout). *Für alle ganzen Zahlen $a, b \in \mathbb{Z}$ existieren $x, y \in \mathbb{Z}$, so dass*

$$ax + by = \text{ggT}(a, b) \tag{1}$$

gilt.

Dabei bezeichnet $\text{ggT}(a, b)$ den größten gemeinsamen Teiler von a und b .

Der größte gemeinsame Teiler zweier ganzer Zahlen lässt sich also immer als Linearkombination der Zahlen darstellen.

In diesem kurzen Artikel soll eine einfache aber interessante Erweiterung von Bézouts Lemma angegeben und bewiesen werden.

2 Erweiterung

Man sieht sofort ein, dass genau eine der Zahlen x, y in (1) negativ sein muss, die andere positiv. Denn bei gleicher Parität wäre $ax + by$ entweder kleiner als 0 oder größer als a und b .

Wegen der Symmetrie der Gleichung (1) und der des ggT können wir also ohne Beschränkung der Allgemeinheit

$$ax - by = \text{ggT}(a, b) \text{ mit } x, y \in \mathbb{N} \tag{2}$$

annehmen.

Diese Formulierung hilft uns beim konstruktiven Beweis des folgenden Lemmas, das zeigt, dass sich schnell ein Paar $(x, y) \in \mathbb{N}^2$ mit den gesuchten Eigenschaften finden lässt.

Lemma 2 (erweitertes Lemma von Bézout). *Für ganze Zahlen $a, b \in \mathbb{Z}$ existieren $x, y \in \mathbb{Z}$, die (1) erfüllen und für die $|x| < b$ und $|y| < a$ gilt.*

Beweis. Das Lemma Bézouts soll hier nicht bewiesen werden ¹, wir nehmen die Existenz von $x, y \in \mathbb{N}$ mit $ax - by = ggT(a, b)$ an wie oben erläutert. Ist dabei $x < b$, so folgt daraus direkt

$$\begin{aligned} ggT(a, b) &= ax - by < ab - by = b(a - y) \\ \implies 0 &< ggT(a, b) < b(a - y) \\ \implies a - y &> 0 \\ \implies y &< a \end{aligned}$$

und wir sind fertig.

Sei also nun $x \geq b$.

Definieren wir dann $x' = x - \lambda b$ mit $x' < b$ als den Rest von x bei Division durch b und $y' = y - \lambda a$ mit $\lambda, x' \in \mathbb{N}, y' \in \mathbb{Z}$, so gilt

$$\begin{aligned} ax' - by' & \\ &= a(x - \lambda b) - b(y - \lambda a) \\ &= ax - \lambda ab - by + \lambda ab \\ &= ax - by \\ &= ggT(a, b). \end{aligned}$$

Es ist also $ax' - by' = ggT(a, b)$ und $x' < b$ nach Definition. Wie oben folgt daraus, dass auch $y' < a$ ist.

Der Beweis ist damit vollendet. □

3 Schlusswort

Andersherum betrachtet zeigt der Beweis dieser Erweiterung eine andere interessante Tatsache auf: Zu einem Paar (x, y) mit den geforderten Eigenschaften erfüllt auch das Paar (x', y') mit

$$\begin{aligned} x' &:= x + \lambda b \\ y' &:= y + \lambda a \end{aligned}$$

für beliebige $\lambda \in \mathbb{Z}$ das Lemma Bézouts.

Es gibt also nicht nur endlich viele Paare ganzer Zahlen, die Bézouts bemerkenswertes Lemma erfüllen.

¹Der interessierte Leser findet z.B. im Internet eine Fülle von Beweisen dieses bekannten Resultats.