11. Der Euklidische Algorithmus

Der Euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen ist einer der ältesten Algorithmen der Mathematik (über 2000 Jahre alt) und auch noch heute im Computer-Zeitalter aktuell. Bevor wir zur Beschreibung des Algorithmus kommen, soll zunächst der Begriff des größten gemeinsamen Teilers präzisiert werden.

Schreibweise. Für ganze Zahlen m, n schreibt man $m \mid n$, (und spricht: m teilt n), wenn m die Zahl n ohne Rest teilt, d.h. wenn es eine ganze Zahl q gibt mit $n = qm$.

Definition. Seien $a, b \in \mathbb{Z}$, nicht beide gleich 0. Eine Zahl $d \in \mathbb{Z}$ heißt *größter gemeinsamer Teiler* von a und b, wenn gilt:

a) d ist gemeinsamer Teiler von a und b, d.h. $d \mid a$ und $d \mid b$.
b) Für jeden gemeinsamen Teiler d' von a und b gilt: $d' \mid d$.

Für $a = b = 0$ wird der größte gemeinsame Teiler als 0 definiert.

Bemerkung. Der größte gemeinsame Teiler ist bis auf das Vorzeichen eindeutig bestimmt. (Wir unterstellen hierbei, dass es immer mindestens einen größten gemeinsamen Teiler gibt, was sich aber später mit dem Euklidischen Algorithmus von selbst ergeben wird.)

Beweis. Seien d_1 und d_2 größte gemeinsame Teiler von a und b, (a und b nicht beide gleich 0). Aus der Definition folgt dann

$$\begin{aligned} & d_1 \mid d_2 \quad \text{und} \quad d_2 \mid d_1 \\ \Longrightarrow\quad & d_2 = q_1 d_1 \quad \text{und} \quad d_1 = q_2 d_2 \quad \text{mit } q_1, q_2 \in \mathbb{Z} \\ \Longrightarrow\quad & d_2 = q_1 q_2 d_2 \\ \Longrightarrow\quad & q_1 q_2 = 1 \quad \Longrightarrow \quad q_1 = \pm 1, \end{aligned}$$

also $d_2 = \pm d_1$, q.e.d.

Im folgenden wählen wir immer den nicht-negativen größten gemeinsamen Teiler zweier ganzer Zahlen a, b und bezeichnen ihn mit

$$\gcd(a, b).$$

(Die Bezeichnung ist abgeleitet von engl. *greatest common divisor.*)

Offenbar gilt

$$\gcd(a, 0) = |a|, \quad \gcd(0, b) = |b|, \quad \gcd(\pm a, \pm b) = \gcd(a, b).$$

Die **Schulmethode**
zur Bestimmung des größten gemeinsamen Teilers zweier ganzer Zahlen a, b benutzt die Primfaktorzerlegung. Wir können annehmen, dass $a > 0$ und $b > 0$. Seien

$$a = \prod_p p^{e(a,p)} \quad \text{und} \quad b = \prod_p p^{e(b,p)}$$

die Primfaktorzerlegungen der beiden Zahlen. Dabei wird das Produkt formal über alle Primzahlen p erstreckt, aber für alle Primzahlen, die nicht in a als Faktor auftreten, ist der Exponent $e(a,p)$ gleich 0 (und entsprechend für b), so dass effektiv nur endlich viele Faktoren auftreten. Setze

$$\gamma(p) := \min(e(a,p), e(b,p)).$$

Dann gilt

$$\gcd(a,b) = \prod_p p^{\gamma(p)}.$$

Beispiel. Sei

$$\begin{aligned} a &:= 980 = 2^2 \cdot 5 \cdot 7^2, \\ b &:= 126 = 2 \cdot 3^2 \cdot 7. \end{aligned}$$

Damit folgt $\gcd(a,b) = \gcd(980, 126) = 2 \cdot 7 = 14$.

Die Schulmethode eignet sich zur Bestimmung des größten gemeinsamen Teilers kleiner Zahlen, ist aber für große (z.B. hundertstellige) Zahlen, wie sie heute in manchen Anwendungen (z.B. in der Kryptographie) auftreten, gänzlich ungeeignet, denn die Faktorzerlegung großer Zahlen ist ein schwieriges Problem. Hier kommt nun der Euklidische Algorithmus zu Hilfe. Er stützt sich auf das Teilen mit Rest: Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit

$$a = qb + r \quad \text{und} \quad 0 \leq r < |b|.$$

Lemma. *Seien $a, b \in \mathbb{Z}$, $b \neq 0$, und $a = qb + r$ mit $q, r \in \mathbb{Z}$. Dann gilt*

$$\gcd(a,b) = \gcd(b,r).$$

Beweis. Es ist nur zu zeigen

$$d \mid a,\ d \mid b \iff d \mid b,\ d \mid r.$$

"$\Rightarrow$" Es ist $r = a - qb$. Falls d die Zahlen a und b teilt, so teilt d auch r.
"$\Leftarrow$" Aus $a = qb + r$ folgt: Falls d die Zahlen b und r teilt, so teilt d auch a.

Wir können jetzt den Euklidischen Algorithmus beschreiben.

Euklidischer Algorithmus. Seien a, b ganze Zahlen > 0. Setze $a_0 := a$, $a_1 := b$ und führe sukzessive Divisionen mit Rest aus, bis die Division aufgeht:

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2, & 0 < a_2 < a_1,\\
a_1 &= q_2 a_2 + a_3, & 0 < a_3 < a_2,\\
&\vdots\\
a_{n-2} &= q_{n-1} a_{n-1} + a_n, & 0 < a_n < a_{n-1},\\
a_{n-1} &= q_n a_n + 0.
\end{aligned}$$

(Da $a_1 > a_2 > \ldots > 0$, muss das Verfahren nach endlich vielen Schritten abbrechen.) Dann gilt

$$a_n = \gcd(a_0, a_1).$$

Beweis. Nach dem Lemma ist

$$a_n = \gcd(a_n, 0) = \gcd(a_{n-1}, a_n) = \ldots = \gcd(a_1, a_2) = \gcd(a_0, a_1).$$

Beispiel. Für das oben betrachtete Zahlenpaar 980, 126 ergibt der Euklidische Algorithmus

$$\begin{aligned}
980 &= 7 \cdot 126 + 98,\\
126 &= 1 \cdot 98 + 28,\\
98 &= 3 \cdot 28 + 14,\\
28 &= 2 \cdot 14,
\end{aligned}$$

also $\gcd(980, 126) = 14$.

Bemerkung. Wir werden später mithilfe der Fibonacci-Zahlen eine Abschätzung für die Anzahl der Schritte, die beim Euklidischen Algorithmus nötig sind, ableiten.

Matrizen-Schreibweise. Die Gleichungen des Euklidischen Algorithmus lassen sich in Matrizen-Schreibweise umformen:

$$\begin{aligned}
\begin{pmatrix} a_i \\ a_{i+1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} a_{i-1} \\ a_i \end{pmatrix}, \quad i = 1, \ldots, n-1,\\
\begin{pmatrix} a_n \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix}.
\end{aligned}$$

Setzt man zur Abkürzung

$$Q_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix},$$

so ergibt sich durch Einsetzen der Gleichungen ineinander

$$\begin{pmatrix} a_n \\ 0 \end{pmatrix} = Q_n Q_{n-1} \cdot \ldots \cdot Q_2 Q_1 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$

Mit

$$Q := Q_n Q_{n-1} \cdot \ldots \cdot Q_2 Q_1 =: \begin{pmatrix} u & v \\ s & t \end{pmatrix}$$

erhält man

$$\begin{pmatrix} a_n \\ 0 \end{pmatrix} = Q \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} u & v \\ s & t \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \quad \Longrightarrow \quad a_n = ua + vb.$$

Damit haben wir folgende Aussage bewiesen.

Satz. *Der größte gemeinsame Teiler d zweier ganzer Zahlen a, b lässt sich als ganzzahlige Linearkombination von a und b darstellen, d.h. es gibt $u, v \in \mathbb{Z}$ mit*

$$d = ua + vb.$$

Anwendung. Wir betrachten den Spezialfall, dass $b = p$ eine Primzahl ist und $0 < a < p$. Dann gilt natürlich $\gcd(a, p) = 1$. Nach dem obigen Satz gibt es dann $u, v \in \mathbb{Z}$ mit

$$1 = ua + vp.$$

Betrachtet man diese Gleichung modulo p, heißt dies $1 \equiv ua \bmod p$, also

$$\overline{1} = \overline{u} \cdot \overline{a} \quad \text{in } \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

Daher ist $\overline{u}$ das Inverse von $\overline{a}$ im Körper $\mathbb{F}_p$. Dies lässt sich zu einem effizienten Algorithmus zur Bestimmung des Inversen im Körper $\mathbb{F}_p$ ausbauen. Die Implementierung sei dem Studenten als Programmier-Übung empfohlen.