TEILBARKEITSUNTERSUCHUNGEN UND DER EUKLIDISCHE ALGORITHMUS

Von F. Padberg

1. Die Behandlung der elementaren Teilbarkeitslehre führt man heute im Unterricht der 5. oder 6. Klasse zu Beginn i. a. mit Hilfe von Teiler*mengen* durch. So bestimmt man die gemeinsamen Teiler zweier oder mehrerer Zahlen über die Schnittmenge der zugehörigen Teilermengen und kann der Schnittmenge auch leicht den größten gemeinsamen Teiler, den ggT, entnehmen.
   Die Anwendung der elementaren Mengenlehre in dieser Form ist allerdings nur so lange mit Gewinn möglich, wie die zu untersuchenden Zahlen klein bzw. teilerarm sind; denn bei großen bzw. teilerreichen Zahlen wird dieses Verfahren unübersichtlich und damit für den Unterricht unbrauchbar. Daher geht man an dieser Stelle in fast allen Schulbüchern von der Untersuchung der *Teilermengen* über zur Bestimmung der *Primfaktorzerlegungen* der Zahlen und bestimmt mit ihrer Hilfe den ggT. Dieser *Bruch* in der Behandlungsart der elementaren Teilbarkeitslehre ist meines Erachtens unbefriedigend und überflüssig. Unbefriedigend, weil er den Eindruck erweckt, als wäre die Mengenkonzeption in diesem Abschnitt dem traditionellen Verfahren der ggT-Bestimmung mittels der Primfaktorzerlegung nur unorganisch und gekünstelt aufgepfropft, überflüssig, weil der Bruch in der Konzeption sich vermeiden läßt, wenn man die ggT-Bestimmung bei großen bzw. teilerreichen Zahlen statt über die Primfaktorzerlegung mittels des Euklidischen Algorithmus[1] durchführt. Hierbei bietet der Euklidische Algorithmus neben der durchgängigen Anwendungsmöglichkeit der Begriffsbildungen und Aussagen der elementaren Mengenlehre den weiteren Vorteil, daß er in vielen Fällen wesentlich kürzer und eleganter zum Ziel führt als der Weg über die —oft mühselige — Primfaktorzerlegung. Außerdem ist bei der traditionellen ggT-Bestimmung mittels der Primfaktorzerlegung der beweistechnisch nicht leichte Hauptsatz der elementaren Zahlentheorie die entscheidende Grundlage — ein Satz, der in den betreffenden Schulbüchern in diesem Zusammenhang vielfach nicht deutlich genug herausgestellt wird, dessen wichtige Funktion für dieses Verfahren erst recht nicht klar genug verdeutlicht wird und dessen Beweis für die betreffende Altersstufe nicht in Betracht kommen kann —, während bei dem Verfahren mittels des euklidischen Algorithmus nicht einmal der Begriff Primzahl bekannt zu sein braucht.
2. Aus den vorstehenden Gründen heraus scheint es mir daher in den Klassen 5 bzw. 6 sinnvoll und empfehlenswert zu sein, die Bestimmung des ggT bei größeren bzw. teilerreichen Zahlen statt über die Primfaktorzerlegung besser über den Euklidischen Algorithmus durchführen zu lassen. Im folgenden soll daher ein gangbarer Weg skizziert werden.
   Wir *setzen* bei ihm *voraus*, daß die Schüler bis zu diesem Zeitpunkt schon

die Anfangsgründe der elementaren Teilbarkeitslehre auf der — in den neueren Schulbüchern üblichen — mengentheoretischen Basis kennengelernt haben und ihnen also insbesondere auch die Teilbarkeitsrelation, einige Eigenschaften der Teilbarkeitsrelation, [insbesondere: für alle a, b, c und $s \in \mathbb{Z}^2$ gilt: $a \mid b$ und $a \mid c \Rightarrow a \mid b \pm c$ wie auch $a \mid b \Rightarrow a \mid sb$) sowie einige Aussagen über Teilermengen (so z. B. $a \mid b \Rightarrow T(a) \subseteq$[3] $T(b)$ und $T(a) \cap T(b) = T(a)$] inhaltlich geläufig sind. Außerdem sollten sie – etwa bei der Einführung der Teilbarkeitsrelation — an konkreten Beispielen den Inhalt des Satzes über die Division mit Rest[4] kennengelernt haben.

3. *Skizze des Unterrichtsweges*

3. 1 Einleitend führt man am günstigsten die Bestimmung der gemeinsamen Teiler (gT) und des ggT bei großen bzw. teilerreichen Zahlen mittels der zugehörigen Teilermengen durch. Hierdurch sollen die Schüler erkennen, daß dieses Verfahren in diesen Fällen sehr arbeitsaufwendig ist, um sie so für das Suchen nach einem leichteren Weg zu motivieren.

3. 2 Im Sonderfall $a \mid b$ ist die gT- und die ggT-Bestimmung auch bei großen Zahlen leicht möglich, da dann gilt: $T(a) \cap T(b) = T(a)$ und $ggT(a, b) = a$. Daher ist es bei der Vorgabe zweier beliebiger natürlicher Zahlen naheliegend, zunächst dividieren zu lassen. Gilt $b = q \cdot a + 0$ (also $a \mid b$), so können wir nach den vorstehenden Angaben leicht die $gT(a, b)$ und den $ggT(a, b)$ bestimmen. Es stellt sich die Frage, ob auch im allgemeinen Fall, bei dem bei der Division von b durch a der (nichtnegative kleinste) Rest r bleibt und in dem wir schreiben $b = q \cdot a + r$ (mit $0 \leqq r < a$) eine Arbeitsvereinfachung möglich ist. An konkreten Beispielen wird man zunächst die Vermutung: $T(a) \cap T(b) = T(a)$ als in diesem Fall unzutreffend verifizieren und statt dessen anhand der Beispiele feststellen lassen: $T(a) \cap T(b) \subset T(a)$. Da im betrachteten Fall gegenüber dem Sonderfall $a \mid b$ nur der Rest $r \neq 0$ neu hinzutritt, wird man – dies ist ein möglicher Anlauf – die Teilmenge $T(a) \cap T(b)$ von $T(a)$ dadurch auf eine leichtere Art zu gewinnen versuchen, daß man die Teilmenge $T(a) \cap T(r)$ von $T(a)$ bestimmt. Der Vergleich der Mengen $T(a) \cap T(b)$ und $T(a) \cap T(r)$ bei hinreichend vielen Beispielen führt zu der (berechtigten) Vermutung, daß für alle natürlichen Zahlen a, b mit $b = q \cdot a + r$ gilt: $T(a) \cap T(b) = T(a) \cap T(r)$. Diese Aussage bedeutet in der Praxis eine i. a. starke Arbeitsvereinfachung, da die Komponenten des Zahlenpaares (a, r) i. a. kleiner sind als die entsprechenden Komponenten des Zahlenpaares (b, a).

Beispiel: $b = 565$, $a = 70$ $\quad 565 = 8 \cdot 70 + 5$. $\quad$ Folglich:
$T(565) \cap T(70) = T(70) \cap T(5)$ $[= T(5)]$
Statt also die gemeinsamen und den größten gemeinsamen Teiler von 565 und 70 über die Teilermengen T(565) und T(70) bestimmen zu lassen, können wir sie über die Teilermengen T(70) und T(5) wesentlich einfacher bestimmen.

Je nach der Leistungsfähigkeit der Klasse wird man sich beim Nachweis der obigen Vermutung mit einer experimentellen Abklärung an einer größeren Zahl von Beispielen begnügen oder aber auch an *konkreten* Beispielen zeigen, daß die Aussage immer gelten muß, wobei wir hierbei *inhaltlich* den folgenden Beweisgang zugrundelegen können.

Satz:

Seien $a, b \in \mathbb{N}$ und sei $b = q \cdot a + r$ mit $q, r \in \mathbb{N}_0$ und $0 \leq r < a$, dann gilt: $T(a) \cap T(b) = T(a) \cap T(r)$, d. h. a, b und a, r haben dieselben gT und denselben ggT.

Beweis:

Wir zeigen: $T(a) \cap T(b) \subseteq T(a) \cap T(r)$ und umgekehrt.
Wir können uns hier auf die erste Teilaussage beschränken, da der Beweis der 2. Teilaussage völlig analog verläuft.
$t \in T(a) \cap T(b)$, t beliebig, dann gilt nach Def.:
$t \mid a$ und $t \mid b$, also gilt auch $t \mid q \cdot a$ und $t \mid b - qa$, d. h. $t \mid r$.
$t \mid a$, $t \mid r$, also: $t \mid a$ und $t \mid r$, daher: $t \in T(a) \cap T(r)$
und daher: $T(a) \cap T(b) \subseteq T(a) \cap T(r)$.

3. 3 Nachdem man die vorstehende Aussage genügend benutzt und geübt hat, wird man anschließend Beispiele auswählen, bei denen die *einmalige* Anwendung dieses Satzes noch nicht hinreichend vereinfachend wirkt, um somit die Schüler zu motivieren, den Satz mehrfach anzuwenden.

Beispiel: Man bestimme die gT und den ggT von 1690, 370.

$$
\begin{array}{rll}
1690 = 4 \cdot 370 + 210 & & T(1690) \cap T(370) = T(370) \cap T(210) \\
370 = 1 \cdot 210 + 160 & & T(370) \cap T(210) = T(210) \cap T(160) \\
210 = 1 \cdot 160 + 50 & & T(210) \cap T(160) = T(160) \cap T(50) \\
160 = 3 \cdot 50 + 10 & & T(160) \cap T(50) = T(50) \cap T(10) \\
50 = 5 \cdot 10 + 0 & & T(50) \cap T(10) = T(10) \cap T(0) = T(10)
\end{array}
$$

Wir können dem Beispiel entnehmen:
$gT(1690, 370) = T(1690) \cap T(370) = T(10) = \{1, 2, 5, 10\}$ und
$ggT(1690, 370) = 10$

Nach der Behandlung weiterer Beispiele wird man versuchen, die Schüler die Begründung finden zu lassen, warum die Gleichungskette (bei gesichertem eindeutigen Ablauf wegen des Satzes von der Division mit Rest) immer so bequem mit einem Rest $r = 0$ endet, so daß der Durchschnitt der gegebenen Teilermengen immer gleich der Teilermenge *einer* Zahl — in unserem Beispiel: 10 — ist und sie so inhaltlich den Satz vom Euklidischen Algorithmus erarbeiten lassen:

Satz (Eukl. Alg.):
Seien $a, b \in \mathbb{N}$, so gibt es einen Index n, so daß gilt:

$$
\begin{array}{ll}
b = q_1 \cdot a + r_1 & 0 \leqq r_1 < a \\
a = q_2 r_1 + r_2 & 0 \leqq r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 \leqq r_3 < r_2 \\
\vdots & \vdots
\end{array}
$$

$\vdots \qquad\qquad \vdots$

$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1} \quad 0 \leq r_{n+1} < r_n$

$r_n = q_{n+2} \cdot r_{n+1} + 0$

und man erhält:

$T(a) \cap T(b) = T(r_{n+1})$ und $ggT(a, b) = r_{n+1}$

Beweis:

Wegen $a > r_1 > r_2 > r_3 > \ldots \geqq 0$ bilden die Reste eine streng monoton fallende Folge nichtnegativer ganzer Zahlen. Folglich muß nach spätestens a Schritten ein Rest 0 werden und wir erhalten als letzte Gleichung:

$r_n = q_{n+2} \cdot r_{n+1} + 0.$

Die wiederholte Anwendung des Satzes von 3.2 auf die Gleichungen obiger Gleichungskette ergibt:

$T(b) \cap T(a) = T(a) \cap T(r_1) = T(r_1) \cap T(r_2) = \ldots$

$= T(r_n) \cap T(r_{n+1}) = T(r_{n+1})$, also:

$T(a) \cap T(b) = T(r_{n+1})$ und $ggT(a, b) = r_{n+1}$

4. *Einige Anwendungen des Euklidischen Algorithmus*

4.1 Als unmittelbare Folgerung aus dem Satz vom Euklidischen Algorithmus erhalten wir:

$T(a) \cap T(b) = T(r_{n+1}) = T(ggT(a, b))$, d. h.

der Durchschnitt zweier Teilermengen ergibt immer wieder — im Gegensatz zur Vereinigungsmengenbildung! — eine Teilermenge, und zwar die Teilermenge des zugehörigen ggT.

4.2 Nach Kenntnis des Zusammenhangs zwischen ggT und kgV ($ggT(a, b) \cdot kgV(a, b) = a \cdot b$) kann man mittels des Euklidischen Algorithmus zunächst den ggT(a, b) berechnen und dann in Anwendung obiger Beziehung das kgV(a, b) selbst bei größeren Zahlen einfach bestimmen lassen.

4.3 Der Kalkül des „Euklidischen Algorithmus" eignet sich gut zur Erarbeitung des Begriffs des „Flußdiagramms" (man vergl. auch F. Haeberlein: Ein Weg zum Euklid.-Algorithmus, in: Praxis der Mathematik, 5/1971, p 113—115) und somit zu Vorarbeiten für die wichtige Einsicht, daß Kalküle durch Computer bearbeitbar sind.

[1] Der Name „Euklidischer Algorithmus" weist darauf hin, daß dieses Rechenverfahren – *nicht* in der im folgenden zu entwickelnden Form, jedoch in seinem mathematischen *Kern* – schon in den Elementen Euklides erwähnt wird.

[2] $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

[3] „$\subseteq$" bedeutet: „echte oder unechte Teilmenge von"

[4] Satz von der Division mit Rest: Sind $a, b, \in \mathbb{N}$,[5] so gibt es genau ein Paar $q, r, \in \mathbb{N}_0$[5] mit $0 \leqq r < a$, so daß gilt: $b = q \cdot a + r$

[5] $\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 3, \ldots\}$

Bem. der Red. zu 3.3: Es ist für die Übersicht nützlich, bei dem hier (in 3.3) gegebenen Beispiel (und entsprechend bei den folgenden Beispielen) die Zahl 370 in der ersten Zeile mit der Zahl 370 der zweiten durch Bleistiftstrich zu verbinden. Entsprechen mit 210, 160, 50 usw. zu verfahren.