ggT und kgV verdienen die schlechte Behandlung nicht

Hermann Karcher, Bonn

Im Winter 1996/97 bin ich von den Mathematiklehrern einer benachbarten Schule gebeten worden, bei der Beurteilung von zwei Schulbuchreihen zu helfen. Ich habe in beiden Reihen die Behandlung von ggT und kgV so schlecht gefunden, dass ich meine Kritik und meine daran anschließenden Vorschläge und Kommentare nicht nur gegenüber den Lehrern jener Schule formulieren möchte. Wer wollte bestreiten, dass die Mathematik ihrer Argumentationen wegen wichtig ist und derentwegen gelehrt wird, so wie, dass auswendig gelernte Mathematik außerhalb von Prüfungen wenig hilft? Ich bin sehr dafür, das kleine Einmaleins auswendig zu lernen, aber das Ausprobieren oder gar Auswendiglernen von Primzahlzerlegungen ist *kein* Ausbildungsziel.
Wer versucht, vor Laien über Anwendungen der Mathematik zu reden, für den sind die Verschlüsselungsmethoden mit Hilfe großer Primzahlen ein gutes Beispiel. Diese Verfahren beruhen darauf, dass das Faktorisieren sehr großer Zahlen außerordentlich viel Zeit kostet. Mathematica braucht (vor 1997) laut Handbuch auf einer Workstation 3.5 Stunden, um die 38-stellige Zahl $2^{128}+1$ in zwei große Faktoren zu zerlegen; für je zwei Stellen mehr braucht man 10-mal so lange. Bei diesem Tempo kann man das Faktorisieren 100-stelliger Zahlen nicht abwarten, weil ein Jahr nur etwa 9000 Stunden hat. Anders als beim Faktorisieren hat man mit Euklids Verfahren zur Berechnung des ggT ein Musterbeispiel für ein schnelles Verfahren: Man könnte in nur 60 - 100 Stunden den ggT zweier 100-stelliger Zahlen nach Euklid *ohne Hilfsmittel* berechnen.
Argumentieren lernt man in kleinen Schritten, und zur Teilbarkeitslehre gehören schon in Klasse 6 die folgenden grundlegenden Einsichten (alle im Text vorkommenden Zahlen sind ganz, $a, ..., z \in \mathbb{Z}$):

1) Wenn k Teiler der Zahlen a und b ist, so ist k auch Teiler aller Linearkombinationen $m \cdot a + n \cdot b$.
   Als Übung zum Klammerrechnen etwa: $51 \cdot 27 + 51 \cdot 13 = 51 \cdot (27 + 13)$, usw..
2) Eine zielstrebige Folgerung, nützlich beim Kürzen, ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - b)$.
3) Noch etwas zielstrebiger erhält man einen Schritt des Euklidschen Verfahrens unter Verwendung der Division mit Rest: Wenn a größer als b ist, so kann man a schreiben als $a = q \cdot b + r$ mit einem Rest r, der *kleiner* als b ist. Also gilt: $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Zum Beispiel ist der ggT aufeinander folgender (ungerader) Zahlen 1: *ohne* weitere Faktorsuche gilt $\mathrm{ggT}(937, 939) = 1$. Die Einsicht ist doch auch schon für Schüler bemerkenswert, dass sie den größten gemeinsamen Teiler von zwei vier- bis sechsstelligen Zahlen a, b ohne weiteres finden können, obwohl die Zahlen a, b so groß sind, dass die Aufgabe, deren Primfaktorzerlegungen herzustellen, schon eine Strafarbeit ist.
Leider wird nun in beiden Schulbüchern gelehrt, dass man den ggT von a und b dadurch bestimmt, dass man die Primzahlzerlegungen von a und b herstellt und die Faktoren sortiert, erstaunlicher Weise, obwohl das euklidische Verfahren beschrieben wird.

Man geht also Argumenten der Teilbarkeitslehre aus dem Weg, und man erschwert ein späteres Verständnis der Verschlüsselungstechnik. Im Anschluß an diese uneffektive und nicht lehrreiche ggT- Bestimmung wird das kgV nicht etwa aus der schönen (aber unerwähnten) Beziehung

$a \cdot b = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$

(mit $\mathrm{kgV} = b \cdot (a/\mathrm{ggT})$, nicht etwa $\mathrm{kgV} = (a \cdot b)/\mathrm{ggT}$)

gewonnen, sondern man betrachtet tatsächlich die Vielfachen von a und sucht unter diesen das kleinste, das durch b teilbar ist. (Durch Sortieren der gewonnenen Primfaktoren wird das kgV dann auch bestimmt.) - Ältere Lehrer erinnern sich vielleicht, dass ich schon vor zwanzig Jahren Lehrpläne und Schulbücher zu kritisieren hatte. Trotzdem kam mir diese Art Teilbarkeitslehre unerwartet, ich habe es als Schüler von Heinz Schwarze besser gehabt. Es heißt, die kgV-Bestimmung würde für die Bruchrechnung benötigt, um Brüche auf Hauptnenner zu bringen. Ursprünglich war das als *Vereinfachung* gedacht, aber wenn man das kgV derart umständlich berechnet, dann ist es besser, einfach das Produkt als Hauptnenner zu verwenden.

Vielleicht ist das folgende eine Erklärung für die Verbreitung des geschilderten Vorgehens: Für die drei kleinsten Primzahlen 2, 3 und 5 hat man sehr einfache (hoffentlich begründete) Teilbarkeitsregeln, und im bevorzugten Zahlenraum bis 120 ist eine Zahl, die nicht durch 2,3,5 teilbar ist, schon beinahe eine Primzahl. Von diesem "Satz" gibt es nur zwei ernsthafte Ausnahmen, $91 = 7 \cdot 13$ und $119 = 7 \cdot 17$, sowie zwei weitere Zahlen, deren Zerlegung klar ist, 77 und 49. Jenseits von 120 wird das Faktorisieren rasch mühsamer: Die guten Erfahrungen, die unterhalb 120 mit den Teilbarkeitsregeln gemacht werden, erweisen sich als untypisch.

Ich beginne mit Beispielen zu besonders einfachen Teilbarkeitsargumenten; in kleinen Schritten werden die Beispiele komplizierter, bis man gerne mit der Eindeutigkeit der Primzahlzerlegung argumentieren möchte. Faktorisiert man Zahlen, so wird die Neugier fast von allein auf die Primzahlen gelenkt. Die Frage: "Wieviele gibt es eigentlich?" ist alt und natürlich. Die 2000 Jahr alte Antwort hat eine Standardform angenommen, die nicht ganz geeignet ist, in Klasse 6 oder 7 behandelt zu werden. Zum Beispiel Wagenschein [W] hat darauf hingewiesen, dass die erstarrte Standardantwort zu wenig Variationsmöglichkeiten anbietet. Ich finde, Wagenscheins Vorschläge rücken Argumente der Teilbarkeitslehre in den Vordergrund; ich werde seine Variationen erweitern. Als nicht empfehlenswert, nämlich nicht variierbar und nicht auf Beispiele anwendbar, beschreibe ich zunächst den indirekten Beweis für die Aussage:

Es gibt unendlich viele Primzahlen.

Angenommen es gäbe nur endlich viele, dann könnte man sie alle multiplizieren und dazu 1 addieren. Die erhaltene Zahl besäße eine Primzahlzerlegung, in der keine der multiplizierten Primzahlen als Faktor vorkommen kann - ein Widerspruch, weil man ja alle (endlich vielen) Primzahlen multipliziert hatte.

Inhaltlich besagt die folgende, mit demselben Argument direkt bewiesene Behauptung dasselbe:

Zu jeder endlichen Menge von Primzahlen kann man neue Primzahlen konstruieren.
Aber die umformulierte Aussage kann an Beispielen betrachtet werden; diese sind schon lehrreich, wenn man nur zwei Primzahlen für das Produkt benutzt:
$2 \cdot 3 + 1 = 7,\ 2 \cdot 5 + 1 = 11,\ 2 \cdot 7 + 1 = 3 \cdot 5,\ 3 \cdot 5 + 1 = 2 \cdot 2 \cdot 2 \cdot 2,\ 2 \cdot 3 \cdot 5 + 1 = 31.$
Zu vermitteln ist hier vor allem die Einsicht, dass die konstruierte Zahl, Produkt + 1, keine der verwendeten Primzahlen als Faktor enthält, weil ja bei Division der Rest 1 bleibt! Um das Argument zu variieren, *subtrahieren* wir 1 oder wir verwenden Faktoren mehrfach:

$2 \cdot 3 - 1 = 5,\ 2 \cdot 5 - 1 = 3 \cdot 3,\ 2 \cdot 7 - 1 = 13,\ 3 \cdot 5 - 1 = 2 \cdot 7.$

$2 \cdot 2 \cdot 3 \pm 1 = 13(11),\ 2 \cdot 2 \cdot 2 \cdot 3 \pm 1 = 5 \cdot 5(23),\ 2 \cdot 2 \cdot 3 \cdot 3 \pm 1 = 37(5 \cdot 7).$

Weiterhin gilt, die konstruierte Zahl Produkt ± 1 ist nicht durch die verwendeten Faktoren teilbar, weil man ja den Rest $\pm 1 \neq 0$ kennt; die Zahl hat also *andere* Primfaktoren. (Weil $(1 + 4)$ durch 5 teilbar ist, usw. für andere Divisoren p, benutze ich -1 als (äquivalente) Abkürzung für den größten Rest $p - 1$.)
Das Argument wird anders, wenn man versucht, um ± 2 zu ändern. Offenbar darf dann die Primzahl 2 unter den multiplizierten Faktoren nicht vorkommen, aber diese Einschränkung genügt:

$3 \cdot 5 \pm 2 = 17(13),\ 3 \cdot 7 \pm 2 = 23(19),\ 3 \cdot 3 \cdot 5 \pm 2 = 47(43).$

Bei Division durch die in dem Produkt verwendeten Faktoren gilt noch wie bisher: Der Rest ist $\pm 2 \neq 0$. Neu ist: Bei Division durch 2 bleibt der Rest 1, weil die konstruierte Zahl *ungerade* ist.

Die nächste Frage erlaubt weitere Experimente im Bereich kleiner Zahlen, und sie führt in eine neue Situation: Kann man alle Primzahlen unter 120 so schreiben, dass sie offensichtlich nicht durch $2, 3, 5, 7$ teilbar sind, so dass man ihnen die Primzahleigenschaft unmittelbar ansieht?

$71 = 2 \cdot 5 \cdot 5 + 3 \cdot 7,\ 73 = 2 \cdot 5 \cdot 7 + 3,\ 79 = 2 \cdot 5 \cdot 7 + 3 \cdot 3,\ 83 = 2 \cdot 3 \cdot 3 \cdot 5 - 7.$

Die neue Schwierigkeit ist: Warum ist $2 \cdot 5 \cdot 5 + 3 \cdot 7$ nicht durch 3 teilbar? Natürlich können wir $3 \cdot 7$ abziehen, aber warum ist $2 \cdot 5 \cdot 5$ nicht durch 3 teilbar? Ich erwarte als Antwort: *"Wegen der Eindeutigkeit der Primfaktorzerlegung!"* Aber hiermit haben wir einen traurigen Punkt der Schulmathematik berührt: Es ist zwar richtig, dass viele Abiturienten "wissen", dass die Primfaktorzerlegung eindeutig ist. Aber kaum jemand hat mitbekommen, dass diese Eindeutigkeit *nicht* auf Grund der Definition offensichtlich richtig ist, dass sie also eines Beweises bedarf, und dass ein Beweis zum Beispiel aus der Division mit Rest oder aus Eigenschaften des ggT folgt. Im Gegensatz zu der Nicht-Thematisierung der Eindeutigkeit der Primfaktorzerlegung wird übrigens oft Mühe darauf verwandt, den Schülern klar zu machen, dass die Multiplikation kommutativ ist, einer Aussage, die ja in $\mathbb{Z}$ ebenfalls ohne Gegenbeispiel ist. Daher will ich zur Eindeutigkeit der Primzahlzerlegung etwas sagen, notwendigerweise vermischt mit Kommentaren zur Division mit Rest, zu ggT und kgV. Als erstes hebe ich hervor, dass die Frage einfacher wird, wenn man sie für eine bestimmte (insbesondere kleine) Primzahl stellt, statt für alle Primzahlen auf einmal: Gibt es

Zahlen, die man *auf zwei Weisen als Produkt unzerlegbarer Faktoren schreiben kann, so dass die Zahl 2 in den beiden Produkten verschieden oft als Faktor vorkommt?*
Da Kürzen von gleichen Faktoren kein Problem ist, brauchen wir nur zu fragen:

Kann 2 Teiler eines Produktes ungerader Faktoren sein?

Hierdurch wird die Aufmerksamkeit auf das Verhalten der Reste konzentriert. Produkte wurden schon bei der Erläuterung des Kommutativgesetzes durch Rechtecke veranschaulicht. Greift man das wieder auf, so sehen auch schon Schüler einer Klasse 6: Das Produkt zweier ungerader Zahlen läßt bei Division durch 2 den Rest 1. Und deshalb ist unsere Frage für die Primzahl 2 beantwortet. Das Verhalten der Reste bei Division durch 3 ist für die Quersummenregeln wichtig. Zunächst kann man die Teilbarkeit einer Zahl durch 3 an der Teilbarkeit der Quersumme ablesen, weil die für unsere Zahldarstellungen wichtigen Potenzen von 10 bei Division durch 3 alle den Rest 1 lassen. Aber die Regel sagt mehr: Der Dreierrest eines Produktes ist Produkt der Dreierreste der Faktoren. Also stellen wir uns wieder ein Produkt als Rechteck vor und überprüfen das Multiplikationsverhalten der Reste. Wir finden insbesondere: Die von null verschiedenen Reste 1, 2 haben Produkte 1, 2, 4, die in der Tat nicht durch 3 teilbar sind. Damit ist auch für 3 argumentiert: Ein Produkt von nicht durch 3 teilbaren Zahlen ist wirklich nicht durch 3 teilbar. - Die Fortführung dieser Diskussion hat durch Gauß eine sehr elegante Wendung bekommen, ich gehe am Schluss noch darauf ein.

Weiter, gibt es Gegenbeispiele zu eindeutigen Faktorzerlegungen? Das folgende Beispiel kenne ich von Herrn Harder, und er kennt es von Bundessiegern. Es kommt also aus der Schule: Wir verabreden, Faktorisierungen nur in der Menge der geraden Zahlen zu betrachten; alle Faktoren müssen dann gerade sein, und die gerade-unzerlegbaren Zahlen bleiben auch hier im Sieb des Erathostenes hängen.

Also sind $2, 6, 10, 14, ..., 30, ..., 42, ..., 70$ unzerlegbar in Produkte gerader Zahlen, aber $420 = 6 \cdot 70 = 10 \cdot 42 = 14 \cdot 30$ ist auf *verschiedene* Weise in gerade-unzerlegbare Faktoren zerlegt.

Manchen stört hier das Fehlen einer 1, aber das hat mit der eindeutigen Faktorzerlegung nichts zu tun. Das einfachste Beispiel eines Ringes R mit 1, das ich kenne, ist der folgende Unterring der komplexen Zahlen:

$$R := \{m \cdot 1 + n \cdot \sqrt{-3};\ m, n \in \mathbb{Z}\}.$$

Die invertierbaren Elemente ("Einheiten") sind ± 1, die nächst längeren (also unzerlegbaren) Elemente sind $\pm\sqrt{-3}$. Mit dem Sieb des Erathostenes suchen wir weitere unzerlegbare Elemente: Alle, die kürzer sind als die Vielfachen $(\sqrt{-3})^2$ von $\pm\sqrt{-3}$, sind sicher unzerlegbar. Also sind die Elemente der Länge 2 unzerlegbar:

$$\pm 2, \pm 1 \pm \sqrt{-3}.$$

Wir finden, dass

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$$

auf zwei *verschiedene* Weisen Produkt unzerlegbarer Faktoren ist. Auch wenn man dieses Beispiel nicht in der Teilbarkeitslehre besprechen kann, so könnte es doch Lehrer (und Schulbuchautoren) dazu bringen, vor der Eindeutigkeit der Primfaktor-

zerlegung etwas mehr Respekt zu haben, so dass das Argument *"Wie soll es denn sonst sein"* seine außerhalb der Mathematik übliche Wirkung weniger ungestraft entfalten kann.
Als nächstes fasse ich wirklich einfache Eigenschaften des ggT zusammen so wie Folerungen daraus bis zum Beweis der Eindeutigkeit der Primfaktorzerlegung. Ich hoffe, man wird zustimmen, dass die Schwierigkeiten allein bei der *Einsicht in die Beweisnotwendigkeit* zu suchen sind. Der folgende Abschnitt ist daher mehr für Lehrer als für Schüler. Zunächst, weit wichtiger als die ggT-Bestimmung durch Suchen von Faktoren in (eventuell gelernten) Multiplikationstabellen ist die argumentierte Einsicht in $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,\mathrm{a}-b)$. Nach kurzem Üben wird daraus ein Schritt des euklidischen Verfahrens:

ggT - Bestimmung:
Zerlegt man $a > b$ mit Hilfe der Division mit Rest: $a = q \cdot b + r,\ r < b$,
so gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,r)$.

Dieser Schritt ist schon eine große Hilfe, wenn man ihn nur zwei- dreimal wiederholt und seine Benutzung darf nicht dadurch behindert werden, dass man ihn von Anfang an als Teil eines abbrechenden Verfahrens mit klangvollem Namen beschreibt. Natürlich, wenn der Unterricht gut läuft, ist es schön, wenn einige Schüler schließlich formulieren können, dass die Wiederholung dieses Schrittes immer zum Ziel führt, weil die Reste bei jedem Schritt kleiner werden. Den Einzelschritt aber sollte jeder mitbekommen. Schreibt man die durchgeführten Schritte des euklidischen Verfahrens auf, so führt das zu der ersten "höheren" Eigenschaft des ggT:

Darstellung des ggT:
Zu a, b gibt es Zahlen $m, n \in \mathbb{Z}$ so dass gilt $\mathrm{ggT}(a,b) = m \cdot a + n \cdot b$.

Diese Aussage ist nützlich, außerdem ist sie unerwartet und die Zahlen m, n sind nicht leicht zu raten (auch nicht wenn man die Faktorzerlegungen von a, b kennt). Dadurch wird noch einmal die Leistungsfähigkeit des euklidischen Verfahrens demonstriert. Der Beweis wird dem Leser bekannt sein, er wird von Mathematikern als Induktionsbeweis formuliert, aber der Beweis ist ein Verfahren, das auch in jedem Einzelfall von Schülern durch Einsetzen durchgeführt werden kann: Zwei Schritte ggT-Bestimmung: $21 = 1 \cdot 15 + 6,\ 15 = 2 \cdot 6 + 3$, Abbruch wegen $6 = 2 \cdot 3 + 0$, und daraus rückwärts:
$\mathrm{ggT}(21,15) = 3 = 1 \cdot 15 - 2 \cdot 6 = 1 \cdot 15 - 2 \cdot (21 - 1 \cdot 15) = 3 \cdot 15 - 2 \cdot 21$.
Allgemein gilt, wenn man schon die Darstellung $\mathrm{ggT}(b,r) = m_1 \cdot b + n_1 \cdot r$ erreicht hat, so kann man in die vorhergehende Zeile $a = q \cdot b + r$ zurückgehen und $r = a - q \cdot b$ einsetzen: $\mathrm{ggT}(a,b) = n_1 \cdot a + (m_1 - n_1 \cdot q) \cdot b$.

Anwendung der Darstellung des ggT: $a \cdot b = \mathbf{ggT}(a,b) \cdot \mathbf{kgV}(a,b)$.

Diese nützliche Formel ist selbstverständlich, wenn ggT und kgV mit sortierten Primfaktoren beschrieben werden. Ich beweise sie mit Hilfe der komplementären Faktoren, ohne Primzahlen zu erwähnen: Direkt aus den Definitionen von ggT und kgV folgen die Faktorisierungen $\mathrm{ggT}(a,b) \cdot r = a$, $\mathrm{ggT}(a,b) \cdot s = b$, $\mathrm{kgV}(a,b) = a \cdot t$. Offenbar ist erstens $t \leq s$, weil man $\mathrm{ggT} \cdot r \cdot s$ schon als ein gemeinsames Vielfaches kennt. Weiter,

da $b = s\cdot$ggT Teiler von $\mathrm{kgV}(a,b) = a \cdot t$ ist, kann man durch $\mathrm{ggT}(a,b)$ kürzen und findet s teilt $r \cdot t$. Wir zeigen gleich, s ist Teiler von t, wegen $t \leq s$ also $s = t$ und damit wie behauptet $a \cdot b = a\cdot$ ggT$\cdot s = \mathrm{ggT}(a,b) \cdot a \cdot t = \mathrm{ggT}(a,b)\cdot$ kgV(a,b).
Dazu wird die Darstellung des ggT durch ggT geteilt und mit t multipliziert:

$\mathrm{ggT}(a,b) = m \cdot a + n \cdot b$, also $1 = m \cdot r + n \cdot s$ und $t = m \cdot (r \cdot t) + (n \cdot t) \cdot s$.

Der eine Summand in der Darstellung von t enthält s als Faktor, im anderen Summanden ist $r \cdot t$ schon als durch s teilbar bewiesen, also ist t durch s teilbar, wie behauptet. Für den Spezialfall, dass $b = p$ eine Primzahl ist, die ja nach Definition nur die Faktoren $1, p$ hat, zeigt derselbe Beweis die wichtige

Primzahleigenschaft: Teilt eine Primzahl p ein Produkt $a \cdot s$, aber nicht a, so ist p Teiler von s.

(Dies ist in dem erwähnten Unterring der komplexen Zahlen offenbar falsch, ebenso bei der besprochenen Faktorisierung gerader Zahlen nur in gerade Faktoren.)

Aus dieser Primzahleigenschaft folgt nun die *Eindeutigkeit der Primfaktorzerlegung* in naheliegender Weise (oder würden Sie anders anfangen?): Sei $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ eine Gleichung mit Primfaktoren. Man möchte diese Gleichung zunächst durch p_1 kürzen (und dann weiter durch $p_2, \ldots, p_r$). Und das geht, denn entweder ist $p_1 = q_1$ und man kürzt oder p_1 ist wegen der vorhergehenden Primzahleigenschaft ein Teiler des verbleibenden Faktors, des *kürzeren* Produktes $q_2 \cdot \ldots \cdot q_s$. Daher kann man die Suche nach dem Faktor p_1 wiederholen; spätetens nach s Schritten hat man Erfolg.

Obwohl die Werkzeuge dieses Beweises durchaus in Büchern der Klasse 6 zu finden sind, so kann man die Einsicht in die Beweisnotwendigkeit wohl nur selten ohne vorführbares Gegenbeispiel erreichen. Aber, wenn der Lehrer die Zusammenhänge kennt, so kann er wenigstens die Stellen betonen, an denen die Argumentation mit der Eindeutigkeit eine Hilfe ist – das ist an anderen Stellen in der Mathematik ja auch notwendig. Vielleicht hilft es, wenn einige einfache Aussagen über ggT und kgV angeführt werden, die einerseits mit der Eindeutigkeit der Faktorzerlegung offensichtlich sind, die man andererseits ohne diese Eindeutigkeit auch direkt aus den Definitionen beweisen kann. Zu dem schon behandelten Beispiel $a \cdot b = \mathrm{ggT}(a,b)\cdot$ kgV(a,b) füge ich folgende Aussagen hinzu. Dabei benutze ich für die Vielfachen von a die Abkürzung $a \cdot \mathbb{Z} := \{a \cdot m; m \in \mathbb{Z}\}$.

Wenn a, b Teiler von c sind, so ist auch $\mathrm{kgV}(a,b)$ Teiler von c. Anders ausgedrückt: $a \cdot \mathbb{Z} \cap b \cdot \mathbb{Z}$, d.h. der Durchschnitt der Vielfachen von a und der Vielfachen von b, besteht genau aus den Vielfachen von $\mathrm{kgV}(a,b)$.

Oder noch anders: Der ggT von a, b ist kgV aller gemeinsamen Teiler von a, b.

Beweis. $D := a \cdot \mathbb{Z} \cap b \cdot \mathbb{Z}$ enthält alle gemeinsamen Vielfachen von a, b und natürlich deren Vielfache, also $D \supseteq \mathrm{kgV}(a,b) \cdot \mathbb{Z}$. Tatsächlich gilt hier sogar Gleichheit: Denn gäbe es eine weitere Zahl $d \in D$, die nicht Vielfaches von $\mathrm{kgV}(a,b)$ ist, also $m\cdot\mathrm{kgV}(a,b) < d < (m+1)\cdot\mathrm{kgV}(a,b)$, so wäre $0 < d - m\cdot$ kgV(a,b) ein kleineres gemeinsames Vielfaches von a, b als $\mathrm{kgV}(a,b)$, im Widerspruch zur Definition des kleinsten gemeinsamen Vielfachen. Die übrigen Aussagen sind Umformulierungen. (Wo ist die Division mit Rest versteckt?)

Dieser Beweis argumentiert mit *Mengen von Vielfachen* und ist insofern typisch für viele leistungsfähige Argumente der Mathematik, andererseits ist er genau dadurch zu abstrakt für Klasse 6. Er zeigt dem Lehrer, dass die bewiesene Aussage ohne Bezug auf die Primzahlzerlegung direkt aus den Definitionen hergeleitet werden *kann*.

Ich hoffe, dass diese Diskussionen dazu beitragen, die argumentative Rolle der *eindeutigen Faktorzerlegung* so zu stärken, dass sie mindestens im Unterricht thematisiert wird. Ich finde, sie sollte im Kontext des Einübens der Buchstabenrechnung, z.B. in Klasse 8, bewiesen werden. - Später, in der Analysis, kann auch die Bestimmung des ggT wieder auftreten: Bekanntlich versagt das Newtonverfahren zur Nullstellenbestimmung von Polynomen an doppelten Nullstellen; eine doppelte Nullstelle ist aber gemeinsamer Faktor des Polynoms P und seiner Ableitung P'; die Polynomdivision mit Rest erlaubt $\mathrm{ggT}(P, P')$ mit dem Euklidschen Verfahren zu bestimmen.

Ich komme noch einmal zu der zentralen Frage: Warum wird in der Teilbarkeitslehre das Argumentieren unnötig konsequent vermieden? Vielleicht spielt wieder eine Rolle, dass die Argumente kaum variierbar scheinen, wie ja auch meine Ausführungen zum ggT wenig von der Standardform abweichen. Hier hat nun Gauß der Sache einen Blickpunkt hinzugefügt, der nicht nur diesen Mangel beseitigt, sondern auch noch zusätzliche Verbindungen mit anderen Themen der Schulmathematik ermöglicht. Wir hatten oben die Darstellung des ggT besonders in folgender Form benutzt:

> Sei p prim und m teilerfremd zu p, also $\mathrm{ggT}(p, m) = 1$. Dann gibt es Zahlen ℓ_1, ℓ_2, so dass gilt $\mathrm{ggT}(p, m) = 1 = \ell_1 \cdot p + \ell_2 \cdot m$.

Gauß hat dies folgendermaßen uminterpretiert (die Rückübersetzung ist einfach):

> Sei p prim und m teilerfremd zu p, dann gibt es ℓ, so dass gilt $m \cdot \ell = 1 \bmod p$, mit anderen Worten m ist mod p invertierbar mit Inversem ℓ.

Damit bilden die zu p teilerfremden Restklassen mod p eine kommutative Gruppe mit $p - 1$ Elementen, und *alle* Restklassen mod p, also die teilerfremden und 0 mod p, bilden einen Körper mit p Elementen. Auf diesen kann z.B. beim Lösen linearer Gleichungen und linearer Gleichungssysteme zurückgegriffen werden.

Aber warum ist Gauß' Betrachtungswechsel schon für kleine Schüler interessant? Während die ggT-Darstellung sich gut zum Argumentieren eignet, aber *nicht experimentell gesucht* werden sollte, kann Gauß Aussage mit Multiplikationstabellen für Reste *ausprobiert* werden! Für p = 2 reduziert sich die Aussage auf

ungerade × *ungerade* = *ungerade.*

Hier sind Multiplikationstabellen für die Reste $\neq 0$, mod 3, mod 5 und mod 7:

×	1	2
1	1	2
2	2	1

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Man kann anfangen, Gesetzmäßigkeiten in diesen Tabellen zu entdecken. Auf jeden Fall genügt diese einfache Aufzählung, um für die Primzahlen p = 2,3,5,7 die Gauß'sche Aussage "Die zu p teilerfremden Restklassen sind mod p invertierbar" zu beweisen; natürlich hat man für diese dann auch die Rückübersetzung in die ggT-Darstellung und die Eindeutigkeit *dieser* Primfaktoren in Produkten. Außerdem hat Gauß für seine Aussage einen konstruktiven Beweis gegeben, der zu einer effektiven Bestimmung der Inversen mod p benutzt werden kann, von Schülern exemplarisch für jede Primzahl einzeln.

Gauß' Beweis. Induktionsanfang: 1 ist invertierbar mod p.
Induktionsvoraussetzung: Die m kleinsten Restklassen k mod $p, 1 \leq k \leq m < p$ seien schon als invertierbar nachgewiesen.
Zu zeigen ist noch: Ist $(m+1) < p$, so ist $(m+1)$ invertierbar mod p.
Dazu sei ℓ die kleinste Zahl mit $\ell \cdot (m+1) > p$, also $p = \ell \cdot (m+1) - n$ (eine Variation der Division mit Rest). Weil $1 < m+1 < p$ und weil p Primzahl ist, folgt für n:

$$0 < n := \ell \cdot (m+1) - p \leq m.$$

Nach Induktionsvoraussetzung gibt es daher ℓ_1 mit $\ell_1 \cdot n = 1$ mod p, also

$$(\ell_1 \cdot \ell) \cdot (m+1) = 1 \text{ mod } p.$$

Damit ist das Inverse $(\ell_1 \cdot \ell)$ mod p für $(m+1)$ gefunden.

Zum Abschluss möchte ich noch einmal zusammenfassend begründen, warum ich die Behandlung der Teilbarkeitslehre in den beiden Buchreihen so schlimm finde. Meiner Meinung nach gibt es nur wenige mathematische Rezepte, bei denen schon das Auswendiglernen (ohne Einsicht) einen praktischen Nutzen hat. Ich rechne das kleine Einmaleins und das Addieren von Zahlenreihen (Preise auf Rechnungen) zu den (ohne Argumente) brauchbaren Rezepten. Aber, wenn man die Praxis der heutigen Geldgeschäfte ansieht, muss man zugeben, dass keine Regel der Prozentrechnung ohne Einsicht benutzbar ist. Ich rechne auch Teile der Ingenieurausbildung zu den brauchbaren Rezepten, weil dort der Kontext, in dem mathematische Rezepte benutzt werden sollen, sehr genau gelehrt wird. Von solchen Ausnahmen abgesehen gilt in fast allen Situationen, dass die Mathematik ihrer Argumente wegen erfolgreich ist und dass unverstandene Regeln nur in Prüfungen nützen. Und unsere high-tech Werkzeuge helfen dann auch nicht weiter: Wer (Beispiele aus Klasse 10) nicht ohne Taschenrechner durch 0.1 dividieren kann, hat eine so schwache Vorstellung von der Bedeutung von Dezimalzahlen, dass er die Zahlenangaben in Zeitung und Fernsehen nicht mehr als Information interpretieren kann. Da mathematisches Argumentieren nur in kleinen Schritten gelehrt werden kann, müssen *Gelegenheiten ergriffen* werden. Wenn in der Teilbarkeitslehre auf das Argumentieren verzichtet wird, dann kann man später nicht genug Algebra verstehen, um Formelmanipulatoren mit Gewinn benutzen zu können. Die Behandlung von ggT und kgV im Rahmen der Teilbarkeitslehre in den beiden Schulbuchreihen verzichtet in nicht vertretbarer Weise auf das Einüben mathematischer Argumentation.

[W] Wagenschein, M.: Ursprüngliches Verstehen und exaktes Denken, Band I. Stuttgart, Klett 1965.