



Zahlentheorie I

Thomas Huber

Aktualisiert: 1. August 2016
vers. 1.0.0

Inhaltsverzeichnis

1	Teilbarkeit	2
2	ggT und kgV	3
3	Abschätzungen	6

1 Teilbarkeit

Im Folgenden sind a und b ganze Zahlen. Gibt es ein $k \in \mathbb{Z}$ mit $a = kb$, dann sagt man, a sei durch b teilbar oder b sei ein Teiler von a . In Zeichen: $b \mid a$. Jede ganze Zahl n ist durch ± 1 und $\pm n$ teilbar und jede ganze Zahl ist ein Teiler von 0. Ist $a > 0$, dann hat sich eingebürgert, dass man unter den *Teilern* von a nur die positiven Teiler versteht. $p \in \mathbb{N}$ heisst *prim* oder *Primzahl*, wenn p und 1 die einzigen Teiler von p sind.

Es gelten die folgenden einfachen aber wichtigen Fakten:

- $a \mid b$ und $b \mid c \implies a \mid c$
- $a \mid b_1, \dots, a \mid b_n$, dann gilt für beliebige ganze Zahlen c_1, \dots, c_n

$$a \mid \sum_{i=1}^n b_i c_i.$$

- $a \mid b$ und $c \mid d \implies ac \mid bd$
- p prim und $p \mid ab \implies p \mid a$ oder $p \mid b$
- $a \in \mathbb{N}, b \in \mathbb{Z}$ und $a \mid b \implies b = 0$ oder $a \leq |b|$

Beispiel 1. Finde alle natürlichen Zahlen x, y mit

$$x^2 - y! = 2001.$$

Lösung. 2001 ist durch 3 teilbar aber nicht durch 9. Ist $y \geq 3$, dann ist $y!$ durch 3 teilbar, also auch x . Dann ist x^2 aber sogar durch 9 teilbar. Für $y \geq 6$ ist auch $y!$ durch 9 teilbar, also müsste dies auch für 2001 gelten, was nicht der Fall ist. Es bleiben die Möglichkeiten $y = 1, 2, 3, 4, 5$, durchtesten dieser Fälle liefert die einzige Lösung $(x, y) = (45, 4)$. \square

Bekanntlich kann man ganze Zahlen stets mit Rest teilen. Genauer lautet diese Aussage wie folgt:

Satz 1.1 (Division mit Rest). *Seien a, b ganze Zahlen mit $b > 0$. Dann existieren eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < b$, sodass gilt*

$$a = qb + r,$$

r heisst Rest der Division und es ist $r = 0$ genau dann, wenn $b \mid a$.

Einer der zentralen Punkte der ganzen Zahlentheorie ist die Tatsache, dass jede natürliche Zahl eindeutig als Produkt von Primzahlen geschrieben werden kann:

Theorem 1.2 (Primfaktorzerlegung). *Zu jeder natürlichen Zahl a existieren verschiedene Primzahlen p_1, p_2, \dots, p_r und natürliche Zahlen n_1, n_2, \dots, n_r mit*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

Die p_i und die n_i sind durch a eindeutig bestimmt.

Man beweist diesen Satz induktiv mit Hilfe der Division mit Rest, wir gehen aber nicht darauf ein. Der Fall $a = 1$ entspricht dem leeren Produkt auf der rechten Seite, d.h. es gibt überhaupt keine Primfaktoren und es gilt $r = 0$. Dieser Satz hat viele wichtige Konsequenzen, wir erwähnen hier zwei davon. Sei $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ die Primfaktorzerlegung der natürlichen Zahl a , dann gilt:

- a besitzt genau $(n_1 + 1)(n_2 + 1) \cdots (n_r + 1)$ verschiedene positive Teiler.
- a ist genau dann eine m -te Potenz einer natürlichen Zahl, wenn alle Exponenten n_k durch m teilbar sind.

Als weitere Anwendung bringen wir noch ein klassisches Resultat, das auf EUKLID zurückgeht:

Satz 1.3. *Es gibt unendlich viele Primzahlen.*

Beweis. Nehme an, es gäbe nur endlich viele Primzahlen p_1, p_2, \dots, p_n und betrachte die Zahl $N = p_1 p_2 \cdots p_n + 1$. Wegen $N > 1$ gibt es nach Theorem 1.2 einen Primteiler q von N . Nun ist N aber durch keine der Primzahlen p_k teilbar, denn sonst würde $p_k \mid 1$ folgen, was absurd ist. Also ist q verschieden von p_1, p_2, \dots, p_n , im Widerspruch zur Annahme. \square

2 ggT und kgV

Für zwei ganze Zahlen a, b bezeichnet $\text{ggT}(a, b)$ den *grössten gemeinsamen Teiler* von a und b , mit anderen Worten die grösste positive Zahl, die ein Teiler von a und ein Teiler von b ist. $\text{kgV}(a, b)$ bezeichnet das *kleinste gemeinsame Vielfache*, also die kleinste positive Zahl, die a und b als Teiler besitzt. Analog definiert man den ggT und das kgV von mehr als zwei Zahlen und verwendet die abkürzende Notation (a_1, a_2, \dots, a_n) und $[a_1, a_2, \dots, a_n]$ für den ggT bzw. das kgV. Formal kann man den ggT wie folgt charakterisieren:

Es ist äquivalent:

- (a) $c = \text{ggT}(a, b)$
- (b) $c > 0$ ist ein Teiler von a und b und für jede positive Zahl x gilt

$$x \mid a, x \mid b \implies x \mid c.$$

Analoges gilt für das kgV. Ist $\text{ggT}(a, b) = 1$, dann heissen a und b *teilerfremd*. Es gelten die folgenden Fakten:

- $\text{ggT}(a, b) = \text{ggT}(b, a)$
- $\text{ggT}(a, b, c) = \text{ggT}(\text{ggT}(a, b), c)$
- $c \mid ab$ und $\text{ggT}(a, c) = 1 \implies c \mid b$
- $a \mid c, b \mid c$ und $\text{ggT}(a, b) = 1 \implies ab \mid c$
- Ist $d = \text{ggT}(a, b)$, dann existieren *teilerfremde* ganze Zahlen x und y mit $a = xd$ und $b = yd$. Ausserdem ist dann $\text{kgV}(a, b) = xyd$ (vgl. Satz 2.1).
- Sind a, b teilerfremde natürliche Zahlen, sodass ab eine m -te Potenz ist, dann sind a und b beide m -te Potenzen.

Unter Verwendung der Primfaktorzerlegung lassen sich ggT und kgV explizit angeben:

Satz 2.1. Seien $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ und $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ die Faktorisierungen von a und b mit verschiedenen Primzahlen p_k und Exponenten $\alpha_k, \beta_k \geq 0$, dann gilt

$$\begin{aligned} \text{ggT}(a, b) &= p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}} \\ \text{kgV}(a, b) &= p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}} \end{aligned}$$

Ausserdem folgt daraus mit Hilfe der Formel $\min\{x, y\} + \max\{x, y\} = x + y$ sofort

$$\text{ggT}(a, b) \cdot \text{kgV}(a, b) = ab.$$

Beispiel 2. (Russland 95) Seien m und n natürliche Zahlen mit

$$\text{ggT}(m, n) + \text{kgV}(m, n) = m + n.$$

Zeige, dass eine der beiden Zahlen durch die andere teilbar ist.

Lösung. Sei d der grösste gemeinsame Teiler von m und n . Schreibe $m = ad, n = bd$, dann gilt $\text{kgV}(m, n) = abd$ nach Satz 2.1. Die Gleichung wird zu $d + abd = ad + bd$ oder $d(ab - a - b + 1) = 0$. Faktorisieren der linken Seite gibt $d(a - 1)(b - 1) = 0$, also ist $a = 1$ oder $b = 1$. Im ersten Fall gilt $m = d$, also $m \mid n$, im zweiten Fall folgt analog $n \mid m$. \square

Mit den Formeln in Satz 2.1 lässt sich der ggT im Prinzip immer berechnen. Das Problem dabei ist der enorme Aufwand, grosse Zahlen zu faktorisieren. Es gibt aber zum Glück ein einfaches und sehr effizientes Berechnungsverfahren, nämlich den *EUKLIDischen Algorithmus*, der auch vom theoretischen Standpunkt aus interessant ist. Grundlage dafür ist die Tatsache, dass für alle ganzen Zahlen a, b und n die folgende Gleichung gilt:

$$(a, b) = (a, b + na). \tag{1}$$

Beweis. Es genügt, dies für $n = \pm 1$ zu zeigen, der allgemeine Fall folgt dann durch wiederholte Anwendung. Ist c ein gemeinsamer Teiler von a und b , dann teilt c auch $b \pm a$, also gilt $(a, b) \mid (a, b \pm a)$. Sei umgekehrt c ein gemeinsamer Teiler von a und $b + a$ bzw. $b - a$, dann teilt c auch $(b + a) - a = b$ bzw. $(b - a) + a = b$. Daraus folgt $(a, b \pm a) \mid (a, b)$. \square

Als Zahlenbeispiel berechnen wir damit $(2541, 1092)$, indem wir die Gleichung (1) solange anwenden, bis das Ergebnis klar ist:

$$\begin{aligned}(2541, 1092) &= (2541 - 2 \cdot 1092, 1092) = (357, 1092) \\ &= (1092 - 3 \cdot 357, 357) = (21, 357) \\ &= (357 - 17 \cdot 21, 21) = (0, 21) = 21.\end{aligned}$$

Die Idee ist offenbar, dass man mit dem Rest der Division der grösseren durch die kleinere Zahl weiterrechnet. Formalisiert wird das im EUKLID'schen Algorithmus:

Algorithmus 2.2 (EUKLID). *Berechnung von (a, b) für $a, b \geq 0$.*

1. Setze $a_1 = \max\{a, b\}$ und $a_2 = \min\{a, b\}$ sowie $n = 2$.
2. Schreibe $a_{n-1} = q_n a_n + a_{n+1}$ mit $0 \leq a_{n+1} < a_n$ (Division mit Rest).
3. Ist $a_{n+1} = 0$, dann gilt $(a, b) = a_n$, sonst erhöhe n um 1 und gehe zu Schritt 2.

Die Richtigkeit dieses Algorithmus ergibt sich unmittelbar aus (1). Für unser Zahlenbeispiel sind dann also die folgenden Rechnungen anzustellen:

$$\begin{aligned}2541 &= 2 \cdot 1092 + 357 \\ 1092 &= 3 \cdot 357 + 21 \\ 357 &= 17 \cdot 21 + 0.\end{aligned}$$

Weil die Division in der letzten Zeile aufgeht, gilt also $(2541, 1092) = 21$.

Satz 2.3 (BÈZOUT). *Sind a, b teilerfremd, dann gibt es ganze Zahlen x, y mit*

$$xa + yb = 1.$$

Allgemeiner: Ist $d = \text{ggT}(a, b)$, dann existieren ganze Zahlen x, y mit

$$xa + yb = d.$$

Beweis. Das folgt aus dem Euklidischen Algorithmus: Aus der vorletzten Zeile des Algorithmus erhält man die Gleichung $\text{ggT}(a, b) = a_n$. Setzt man diesen Ausdruck für a_n in die $(n-1)$ -te Zeile ein und die entstehenden Ausdrücke für a_k in die $(k-1)$ -te Zeile für immer kleinere k , dann folgt schliesslich eine Gleichung der Form $\text{ggT}(a, b) = xa + yb$. \square

In unserem Beispiel erhält man der Reihe nach

$$\begin{aligned}21 &= 1 \cdot 1092 - 3 \cdot 357 \\ &= 1 \cdot 1092 - 3(2541 - 2 \cdot 1092) \\ &= (-3) \cdot 2541 + 7 \cdot 1092.\end{aligned}$$

Als Anwendung besprechen wir noch die lineare Diophant'sche Gleichung in zwei Variablen.

Satz 2.4. Seien a, b, c ganze Zahlen. Die Gleichung

$$ax + by = c$$

hat genau dann eine Lösung (x, y) mit $x, y \in \mathbb{Z}$, wenn $d = \text{ggT}(a, b) \mid c$. Ist dies der Fall und (x_0, y_0) eine Lösung, dann sind alle Lösungen gegeben durch

$$(x, y) = \left(x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d} \right), \quad k \in \mathbb{Z}.$$

Beweis. Nehme an, (x, y) sei eine Lösung. Dann ist d ein Teiler der linken Seite, also auch von c . Ist umgekehrt $d \mid c$, dann folgt die Existenz einer Lösung (x_0, y_0) direkt aus dem Satz von Bézout. Sei (x, y) eine weitere Lösung, dann gilt $a(x - x_0) + b(y - y_0) = c - c = 0$, also

$$\frac{a}{d} \cdot (x - x_0) = -\frac{b}{d} \cdot (y - y_0).$$

Nun sind $\frac{a}{d}$ und $\frac{b}{d}$ teilerfremd, daher ist $(x - x_0)$ durch $\frac{b}{d}$ teilbar und $(y - y_0)$ durch $\frac{a}{d}$. Daraus folgt unmittelbar, dass alle Lösungen von der angegebenen Gestalt sind. Einsetzen zeigt, dass es auch wirklich Lösungen sind. \square

3 Abschätzungen

Ein sehr wichtiges Element beim Lösen von zahlentheoretischen Problemen ist das Abschätzen von bestimmten Grössen. Oft kann man dadurch alles auf ein paar wenige Fälle reduzieren, die dann einfach zu lösen sind. Es geht dabei darum, bei Gleichungen irgendwie das Wachstumsverhalten der involvierten Grössen gegeneinander abzuwägen. Was damit genau gemeint ist, sehen wir nun an einer Reihe recht verschiedener Beispiele.

Beispiel 3. Finde alle natürlichen Zahlen n mit $n^2 + 11 \mid n^3 + 13$.

Was hat das nun mit Abschätzungen zu tun? Schauen wir's uns an:

Lösung. $n^2 + 11$ ist ein Teiler von $n^3 + 13$, also auch von $n(n^2 + 11) - (n^3 + 13) = 11n - 13$. Offenbar ist $n = 1$ keine Lösung, für $n \geq 2$ ist aber $11n - 13 > 0$ und da diese Zahl durch $n^2 + 11$ teilbar sein soll, muss gelten

$$n^2 + 11 \leq 11n - 13.$$

Hier ist nun also die Abschätzung. Da die linke Seite quadratisch in n ist, die rechte nur linear, kann diese Ungleichung nur für kleine Werte von n erfüllt sein. Sie ist äquivalent zu $n^2 - 11n + 24 = n(n - 11) + 24 \leq 0$. Für $n \geq 12$ gilt nun aber stets $n(n - 11) + 24 \geq 12 \cdot 1 + 24 > 0$, folglich ist $n \leq 11$. Durchtesten dieser Fälle ergibt die beiden Lösungen $n = 3$ und $n = 8$. \square

Der entscheidende Punkt war hier die einfache Bemerkung, dass aus $a \mid b$ und $b > 0$ stets $|a| \leq b$ folgt. Dieses Prinzip ist oft anwendbar, auch bei einer ganzen Reihe von IMO Aufgaben. Merkt es euch!

Beispiel 4. (*England 95*) Bestimme alle Lösungen in natürlichen Zahlen der Gleichung

$$\left(1 + \frac{1}{a}\right) \left(1 + \frac{1}{b}\right) \left(1 + \frac{1}{c}\right) = 2.$$

Hier ist die rechte Seite konstant, die linke wird offenbar immer kleiner, wenn a, b und c grösser werden. Sind alle drei Variablen sehr gross, dann ist jeder der Faktoren rechts ungefähr gleich 1 und die Gleichung kann nicht erfüllt sein. Dies müssen wir nun präzisieren.

Lösung. Die Gleichung ist symmetrisch in a, b und c , wir können daher OBdA $a \geq b \geq c$ annehmen. Dann ist die linke Seite einerseits gleich 2, andererseits aber höchstens gleich $(1 + \frac{1}{c})^3$. Eine kurze Rechnung zeigt aber, dass $(1 + \frac{1}{c})^3 < 2$ gilt für $c \geq 4$, folglich ist $c \leq 3$. Wir unterscheiden nun drei Fälle:

$c = 1$: Wegen $(1 + \frac{1}{a}) > 1$ und $(1 + \frac{1}{c}) = 2$ ist die linke Seite grösser als 2, ein Widerspruch.

$c = 2$: Die Gleichung wird zu $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{4}{3}$ und ähnlich wie oben erhält man die Abschätzung $\frac{4}{3} \leq (1 + \frac{1}{b})^2$, also $b \leq 6$. Wegen $(1 + \frac{1}{a}) > 1$ ist ausserdem $b \geq 4$. Einsetzen der 3 möglichen Werte für b liefert die Lösungen $(7, 6, 2)$, $(9, 5, 2)$ und $(15, 4, 2)$.

$c = 3$: Die Gleichung wird zu $(1 + \frac{1}{a})(1 + \frac{1}{b}) = \frac{3}{2}$ und analog zu vorher erhält man $b \leq 4$ und $b \geq c = 3$. Einsetzen ergibt die Lösungen $(8, 3, 3)$ und $(5, 4, 3)$.

Insgesamt sind die Lösungen also alle symmetrischen Vertauschungen von

$$(7, 6, 2), (9, 5, 2), (15, 4, 2), (8, 3, 3), (5, 4, 3).$$

□

Durch mehrfaches Abschätzen haben wir der Reihe nach obere Schranken für c und b gefunden und mussten dann noch einige wenige Fälle durchprobieren. Mit Teilbarkeitsbetrachtungen allein hätte man diese Aufgabe wohl kaum gelöst.

Beispiel 5. Bestimme alle Lösungen in natürlichen Zahlen der Gleichung

$$abc = ab + bc + ca + 12.$$

Hier wächst die linke Seite offenbar stärker als die rechte, wenn a, b und c alle gross werden. Die linke ist vom Grad 3, die rechte nur vom Grad 2 + Störterm. Wie können wir das quantifizieren?

Lösung. OBdA sei $a \geq b \geq c$. Wie wir uns überlegt haben, muss c klein sein. In der Tat, für $c \geq 4$ erhalten wir sofort $abc \geq 4ab \geq ab + bc + ca + 4^2 > ab + bc + ca + 12$, Widerspruch. Also ist $c \leq 3$.

$c = 3$: $3ab = ab + 3a + 3b + 12 \Leftrightarrow ab + (a-3)(b-3) = 21$. Wegen $a \geq b \geq 3$ ist dann $ab \leq 21$ und für (a, b) kommen nur die Paare $(7, 3), (6, 3), (5, 3), (4, 3), (3, 3), (5, 4), (4, 4)$ in Frage. Durchtesten zeigt, dass davon nur das erste eine Lösung ist.

$c = 2$: $2ab = ab + 2a + 2b + 12 \Leftrightarrow (a-2)(b-2) = 16$. Wegen $a \geq b \geq 2$ erhalten wir die Lösungen $(a, b) = (18, 3), (10, 4), (6, 6)$.

$c = 1$: $ab = ab + a + b + 12 \Leftrightarrow a + b = -12$ hat keine positive Lösung.

Insgesamt sind die Lösungen (a, b, c) die symmetrischen Vertauschungen von

$$(18, 3, 2), (10, 4, 2), (6, 6, 2), (7, 3, 3).$$

□

Beispiel 6. Bestimme alle positiven ganzzahligen Lösungen von $x^3 - y^3 = xy + 61$.

Hier ist die linke Seite von der Ordnung 3, die rechte hat Ordnung 2, dennoch kann man offensichtlich die linke Seite auch für grosse x und y klein halten. Das Argument der letzten Aufgabe ist hier also nicht direkt anwendbar. Vielmehr ist entscheidend, wie gross die Differenz der beiden Zahlen ist. Mit ihr wächst die linke Seite stärker als die rechte.

Lösung. Um dies genauer zu ergründen, setzen wir $d = x - y$. Da die rechte Seite der Gleichung stets positiv ist, gilt $d > 0$. Einsetzen liefert $(y+d)^3 - y^3 = (y+d)y + 61 \Leftrightarrow (3d-1)y^2 + (3d^2-d)y + d^3 = 61$, insbesondere ist $d^3 \leq 61$, also $d \leq 3$, denn die beiden Klammern links sind nicht negativ. Für $d = 1$ erhalten wir die Gleichung $y^2 + y - 30 = 0$ mit der einzigen positiven Lösung $y = 5 \Rightarrow x = 6$. Für $d = 2, 3$ haben die entsprechenden Gleichungen keine ganzzahligen Lösungen. Das einzige Lösungspaar ist $(x, y) = (6, 5)$. □

Eine weitere wichtige Tatsache ist, dass zwischen zwei *aufeinanderfolgenden* Quadraten (n -ten Potenzen, Zweierpotenzen etc.) keine weitere liegt. Damit kommt man z.B. oft dann weiter, wenn man Grössen hat, die in der Nähe einer Quadratzahl liegen und von denen man weiss, dass sie selbst eine sind.

Beispiel 7. (Deutschland 95) Finde alle Paare (x, y) nichtnegativer ganzer Zahlen, welche die folgende Gleichung erfüllen:

$$x^3 + 8x^2 - 6x + 8 = y^3.$$

Lösung. Hier kann man nicht viel Abschätzen, was das Wachstum betrifft. Die Idee ist die folgende: Die linke Seite muss ja eine dritte Potenz sein (nämlich y^3), liegt aber irgendwie auch nahe bei x^3 . Das wollen wir quantifizieren. Wir suchen also mal in der Nähe von x :

$$\begin{aligned} (x+2)^3 &= x^3 + 6x^2 + 12x + 8, \\ (x+3)^3 &= x^3 + 9x^2 + 27x + 27. \end{aligned}$$

Betrachtet man jeweils den Koeffizient von x^2 , dann scheint das erste eher kleiner, das zweite eher grösser als die linke Seite unserer Gleichung zu sein. Rechnen wir es aus:

$$(x+2)^3 < x^3 + 8x^2 - 6x + 8 \Leftrightarrow 2x^2 - 18x > 0 \Leftrightarrow x > 9,$$

$$(x+3)^3 > x^3 + 8x^2 - 6x + 8 \Leftrightarrow x^2 + 33x + 15 > 0 \quad \text{gilt für alle } x \geq 0.$$

Für $x > 9$ liegt die linke Seite also zwischen zwei dritten Potenzen und muss selbst eine sein, Widerspruch. Daher ist $x \leq 9$ und durchtesten dieser Fälle liefert die beiden Lösungen $(0, 2)$ und $(9, 11)$. □