Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Grundkurs Mathematik I

Vorlesung 21

Ein guter Schüler lernt auch
bei einem schlechten Lehrer ...

Kleinstes gemeinsames Vielfaches und größter gemeinsamer Teiler

Zu einer ganzen Zahl a besteht $\mathbb{Z}a$ aus allen Vielfachen von a. Zu zwei Zahlen a, b besteht somit der Durchschnitt $\mathbb{Z}a \cap \mathbb{Z}b$ aus allen Zahlen, die sowohl von a als auch von b Vielfache sind, also aus allen gemeinsamen Vielfachen von a und b. In der Tat gilt die folgende Aussage.

LEMMA 21.1. *Es seien $a_1, \ldots, a_k$ ganze Zahlen. Dann ist*

$$\mathbb{Z}a_1 \cap \mathbb{Z}a_2 \cap \ldots \cap \mathbb{Z}a_k = \mathbb{Z}u,$$

wobei u das kleinste gemeinsame Vielfache der $a_1, \ldots, a_k$ ist.

Beweis. Nach Aufgabe 21.23 ist der Durchschnitt der Untergruppen $\mathbb{Z}a_i$ wieder eine Untergruppe von $\mathbb{Z}$. Nach Satz 20.4 gibt es ein eindeutig bestimmtes $c \geq 0$ mit

$$\mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_k = \mathbb{Z}c.$$

Wegen

$$\mathbb{Z}c \subseteq \mathbb{Z}a_i$$

für alle i ist c ein Vielfaches von jedem a_i, also ein gemeinsames Vielfaches der $a_1, \ldots, a_k$. Für jedes gemeinsame Vielfache v dieser Elemente gilt

$$\mathbb{Z}v \subseteq \mathbb{Z}a_1 \cap \ldots \cap \mathbb{Z}a_k.$$

Die Zahl c besitzt also die Eigenschaft, dass jedes gemeinsame Vielfache der Elemente ein Vielfaches von c ist. Daher ist c das kleinste gemeinsame Vielfache. □

Für ganze Zahlen setzen wird den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache stets positiv an, um Eindeutigkeit zu erzielen. Grundsätzlich hat jeweils das Negative dazu die gleichen Eigenschaften.

LEMMA 21.2. *Für natürliche Zahlen a, b, g gelten folgende Aussagen.*

(1) *Für teilerfremde a, b ist $\mathrm{kgV}(a, b) = ab$.*
(2) *Es gibt $c, d \in \mathbb{Z}$ mit $a = c \cdot \mathrm{ggT}(a, b)$ und $b = d \cdot \mathrm{ggT}(a, b)$, wobei c, d teilerfremd sind.*

(3) *Es ist* $\mathrm{kgV}\,(ga, gb) = g \cdot \mathrm{kgV}\,(a, b)$.
(4) *Es ist* $\mathrm{ggT}\,(a, b) \cdot \mathrm{kgV}\,(a, b) = ab$.

Beweis. (1) Zunächst ist natürlich das Produkt ab ein gemeinsames Vielfaches von a und b. Sei also f irgendein gemeinsames Vielfaches, also $f = ua$ und $f = vb$. Nach Satz 20.1 gibt es im teilerfremden Fall Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$. Daher ist

$$f \;=\; f \cdot 1 \;=\; f(ra + sb) \;=\; fra + fsb \;=\; vbra + uasb \;=\; (vr + us)ab$$

ein Vielfaches von ab.

(2) Die Existenz von c und d ist klar. Hätten c und d einen gemeinsamen Teiler $e \neq 1, -1$, so ergäbe sich sofort der Widerspruch, dass $e \cdot \mathrm{ggT}\,(a, b)$ ein größerer gemeinsamer Teiler wäre.

(3) Die rechte Seite ist offenbar ein gemeinsames Vielfaches von ga und gb. Sei n ein Vielfaches der linken Seite, also ein gemeinsames Vielfaches von ga und gb. Dann kann man schreiben $n = uga$ und $n = vgb$. Damit ist $uga = vgb$ und somit ist $k := ua = vb$ (bei $n \neq 0$
$n = 0$ ist erst recht ein Vielfaches der rechten Seite)
ein gemeinsames Vielfaches von a und b. Also ist $n = gk$ ein Vielfaches der rechten Seite.

(4) Wir schreiben unter Verwendung der ersten Teile

$$\begin{aligned}
\mathrm{ggT}\,(a, b) \cdot \mathrm{kgV}\,(a, b) &= \mathrm{ggT}\,(a, b) \cdot \mathrm{kgV}\,(c \cdot (\mathrm{ggT}\,(a, b)), d \cdot (\mathrm{ggT}\,(a, b))) \\
&= \mathrm{ggT}\,(a, b) \cdot \mathrm{ggT}\,(a, b) \cdot \mathrm{kgV}\,(c, d) \\
&= \mathrm{ggT}\,(a, b) \cdot \mathrm{ggT}\,(a, b) \cdot cd \\
&= c \cdot \mathrm{ggT}\,(a, b) \cdot d \cdot \mathrm{ggT}\,(a, b) \\
&= ab.
\end{aligned}$$

□

Der Teil (4) der vorstehenden Aussage erlaubt es, das kleinste gemeinsame Vielfache zu zwei Zahlen algorithmisch dadurch zu bestimmen, dass man ihren größten gemeinsamen Teiler mit Hilfe des euklidischen Algorithmus bestimmt und das Produkt durch diesen teilt.

Der Hauptsatz der elementaren Zahlentheorie

Wir möchten nun zur Primfaktorzerlegung, deren Existenz wir bereits in Satz 12.9 gezeigt haben, beweisen, dass sie eindeutig ist. Natürlich kann man

$$12 \;=\; 3 \cdot 2 \cdot 2 \;=\; 2 \cdot 3 \cdot 2 \;=\; 2 \cdot 2 \cdot 3$$

schreiben, mit eindeutig ist also eindeutig bis auf die Reihenfolge gemeint. Um dies zu zeigen brauchen wir zunächst das sogenannte *Lemma von Euklid*, das eine wichtige Eigenschaft einer Primzahl beschreibt.

Satz 21.3. *Es sei p eine Primzahl und p teile ein Produkt ab von natürlichen Zahlen $a, b \in \mathbb{N}$. Dann teilt p einen der Faktoren.*

Beweis. Wir setzen voraus, dass a kein Vielfaches von p ist (andernfalls sind wir fertig). Dann müssen wir zeigen, dass b ein Vielfaches von p ist. Unter der gegebenen Voraussetzung sind a und p teilerfremd. Nach dem Lemma von Bezout gibt es ganze Zahlen r, s mit

$$ra + sp = 1$$

Da ab ein Vielfaches von p ist, gibt es ein t mit

$$ab = tp.$$

Daher ist

$$b = b \cdot 1 = b(ra + sp) = abr + bsp = tpr + bsp = p\,(tr + bs)\,.$$

Also ist b ein Vielfaches von p. □

Aus dem Lemma von Euklid folgt sofort die etwas stärkere Aussage: Wenn eine Primzahl p ein beliebiges Produkt $a_1 a_2 \cdots a_n$ teilt, dann teilt p mindestens einen Faktor. Man wendet das Lemma einfach auf $(a_1 a_2 \cdots a_{n-1}) \cdot a_n$ an (formal ist das eine Induktion über die Anzahl der Faktoren). Dies wird im Beweis des folgenden *Hauptsatzes der elementaren Zahlentheorie* verwendet.

Satz 21.4. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine eindeutige Zerlegung in Primfaktoren.*

D.h. es gibt eine Darstellung

$$n = p_1 \cdots p_r$$

mit Primzahlen p_i, und dabei sind die Primfaktoren bis auf ihre Reihenfolge eindeutig bestimmt.

Beweis. Die Existenz der Primfaktorzerlegung wurde bereits in Satz 12.9 gezeigt. Die Eindeutigkeit wird durch Induktion über n gezeigt. Für $n = 2$ liegt eine Primzahl vor. Sei nun $n \geq 3$ und seien zwei Zerlegungen in Primfaktoren gegeben, sagen wir

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

Wir müssen zeigen, dass nach Umordnung die Primfaktorzerlegungen übereinstimmen. Die Gleichheit bedeutet insbesondere, dass die Primzahl p_1 das Produkt rechts teilt. Nach Satz 20.7 muss dann p_1 einen der Faktoren rechts teilen. Nach Umordnung können wir annehmen, dass q_1 von p_1 geteilt wird. Da q_1 selbst eine Primzahl ist, folgt, dass $p_1 = q_1$ sein muss. Daraus ergibt sich durch Kürzen, dass

$$p_2 \cdots p_r = q_2 \cdots q_s$$

ist. Nennen wir diese Zahl n'. Da $n' < n$ ist, können wir die Induktionsvoraussetzung auf n' anwenden und erhalten, dass links und rechts die gleichen Primzahlen stehen. □

In der *kanonischen Primfaktorzerlegung* schreibt man die beteiligten Primzahlen in aufsteigender Reihenfolge mit ihrem jeweiligen Exponenten, also beispielsweise

$$840 = 2^3 \cdot 3 \cdot 5 \cdot 7.$$

Damit ist insbesondere zu jeder ganzen Zahl $n \neq 0$ und jeder Primzahl p eindeutig bestimmt, ob p in der Primfaktorzerlegung überhaupt vorkommt und wenn ja mit welchem Exponenten.

Definition 21.5. Zu einer ganzen Zahl $n \neq 0$ und einer Primzahl p nennt man den Exponenten, mit dem p in der Primfaktorzerlegung von n vorkommt, den *p-Exponenten* von n. Er wird mit $\nu_p(n)$ bezeichnet.

Statt Exponent spricht man auch von der *Vielfachheit* oder der *Ordnung* von p in n. Wenn p in der Primfaktorzerlegung nicht vorkommt, so ist

$$\nu_p(n) = 0.$$

Die Primfaktorzerlegung einer Zahl $n \neq 0$ kann man damit abstrakt und kompakt als

$$n = \pm \prod_p p^{\nu_p(n)}$$

schreiben. Da in jeder Primfaktorzerlegung nur endlich viele Primzahlen wirklich vorkommen, ist dies ein endliches Produkt.

Zu $n = 14000$ ist die Primfaktorzerlegung gleich

$$14000 = 2^4 \cdot 5^3 \cdot 7$$

und somit gilt

$$\begin{aligned} \nu_2(14000) &= 4, \\ \nu_5(14000) &= 3, \\ \nu_7(14000) &= 1 \end{aligned}$$

und

$$\nu_p(14000) = 0$$

für alle weiteren Primzahlen p.

Lemma 21.6. *Es sei p eine Primzahl und*

$$\nu_p \colon \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N},\ n \longmapsto \nu_p(n),$$

der zugehörige p-Exponent. Dann gelten folgende Aussagen.

(1) *Die Zahl $p^{\nu_p(n)}$ ist die größte Potenz von p, die n teilt.*
(2) *Es ist*
$$\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n).$$
(3) *Es ist*
$$\nu_p(m+n) = \min(\nu_p(m), \nu_p(n))$$
(es sei $m + n \neq 0$ vorausgesetzt).

Beweis. Siehe Aufgabe 21.14. □

KOROLLAR 21.7. *Es seien n und k positive natürliche Zahlen. Dann wird n von k genau dann geteilt, wenn für jede Primzahl p die Beziehung*

$$\nu_p(n) \geq \nu_p(k)$$

gilt.

Beweis. (1) $\Rightarrow$ (2). Aus der Beziehung $n = kt$ folgt in Verbindung mit der eindeutigen Primfaktorzerlegung, dass die Primfaktoren von k mit mindestens ihrer Vielfachheit auch in n vorkommen müssen. (2) $\Rightarrow$ (1). Wenn die Exponentenbedingung erfüllt ist, so ist $t = \prod_p p^{\nu_p(n)-\nu_p(k)}$ eine natürliche Zahl mit $n = kt$. □

Aus diesem Kriterium ergibt sich, dass man zu einer gegebenen Zahl, deren Primfaktorzerlegung vorliegt, einfach alle Teiler angeben kann. Bei

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

sind die (positiven) Teiler genau die Zahlen

$$p_1^{s_1} p_2^{s_2} \cdots p_2^{s_k} \text{ mit } 0 \leq s_1 \leq r_1,\, 0 \leq s_2 \leq r_2, \ldots, 0 \leq s_k \leq r_k\,.$$

Davon gibt es $(r_1+1)(r_2+1)\cdots(r_k+1)$ Stück.

KOROLLAR 21.8. *Es seien n und m positive natürliche Zahlen mit den Primfaktorzerlegungen $n = \prod_p p^{\nu_p(n)}$ und $m = \prod_p p^{\nu_p(m)}$. Dann ist*

$$\mathrm{kgV}(n,m) = \prod_p p^{\max(\nu_p(n),\nu_p(m))}$$

und

$$\mathrm{ggT}(n,m) = \prod_p p^{\min(\nu_p(n),\nu_p(m))}.$$

Beweis. Dies folgt direkt aus Korollar 20.7. □

Für die beiden Zahlen $m = 2^3 \cdot 3^2 \cdot 7^2 \cdot 11$ und $m = 2^2 \cdot 3^3 \cdot 5 \cdot 11$ ist beispielsweise der größte gemeinsame Teiler gleich $2^2 \cdot 3^2 \cdot 11$ und das kleinste gemeinsame Vielfache gleich $2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11$.