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

# Grundkurs Mathematik I

## Vorlesung 12

Man muss auch teilen können.

---

### Teilbarkeitseigenschaften

Wir besprechen nun die Eigenschaft, dass eine natürliche Zahl eine weitere natürliche Zahl teilt.

DEFINITION 12.1. Man sagt, dass die natürliche Zahl $a$ die natürliche Zahl $b$ *teilt* (oder dass $b$ von $a$ *geteilt* wird, oder dass $b$ ein *Vielfaches* von $a$ ist), wenn es eine natürliche Zahl $c$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Beispielsweise sind $1, 2, 5, 10$ Teiler von 10 und $1, 3, 9, 27, 81$ die Teiler von 81. Eine Zerlegung

$$n = st$$

nennt man auch eine *Faktorzerlegung* von $n$. Wenn $a$ ein Teiler von $b$ ist und

$$a \neq 0,$$

so ist die Zahl $c$ mit $b = ac$ nach der Kürzungsregel eindeutig bestimmt. Man nennt diese Zahl den *Gegenteiler* oder *komplementären Teiler* und schreibt dafür $\frac{b}{a}$. Da wir im Moment die rationalen Zahlen noch nicht zur Verfügung haben, ist dies nur dann eine erlaubte Schreibweise, wenn die Teilerbeziehung vorliegt und $a \neq 0$ ist (so wie die Schreibweise $a - b$ bisher nur erlaubt ist, wenn $b \leq a$ ist). Es ist also 0 ein Teiler der 0, der Ausdruck $0/0$ ist aber nicht definiert.

LEMMA 12.2. *Es sei $n \neq 0$ eine natürliche Zahl und $t$ ein Teiler von $n$. Dann ist $t \leq n$. Insbesondere besitzt $n$ nur endlich viele Teiler.*

*Beweis.* Da der Teiler 0 ausgeschlossen ist, sind bei einer Faktorzerlegung $n = tc$ beide Faktoren $\geq 1$. Wegen Satz 10.5 (3) ist daher

$$n = tc \geq t \cdot 1 = t.$$

Der Zusatz ist klar, da es unterhalb von $n$ überhaupt nur endlich viele natürliche Zahlen gibt. □

Wenn man also alle Teiler einer natürlichen Zahl $n$ finden möchte, so muss man einfach die Zahlen

$$a \leq n$$

der Reihe nach durchgehen und ihre Vielfachen

$$1a = a, 2a, 3a, \ldots$$

durchgehen, bis die Zahl $n$ auftaucht (in welchem Fall $a$ ein Teiler ist) oder eine Zahl $> n$ auftaucht (dann liegt kein Teiler vor). Übrigens muss man nicht die Zahlen bis $n$ durchprobieren, sondern lediglich bis zur ersten Zahl $r$ mit $r^2 \geq n$ (man muss also nur bis zur Größenordnung der Quadratwurzel aus $n$ gehen). Dann muss man aber für jeden Teiler

$$t \leq r$$

auch den Gegenteiler mitanführen, siehe Aufgabe 12.7. Für 105 muss man maximal bis 11 gehen. Es ergeben sich die Zerlegungen

$$105 = 1 \cdot 105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$$

und die Teiler sind somit $1, 3, 5, 7, 15, 21, 35, 105$.

Eine durch 2 teilbare Zahl, also ein Vielfaches von 2, heißt *gerade*, eine nicht durch 2 teilbare Zahl heißt *ungerade*. Für einige Zahlen gibt es einfache Tests, ob sie ein Teiler einer gewissen Zahl sind, die allerdings auf dem Dezimalsystem beruhen. Eine weitere wichtige Möglichkeit ist die Division mit Rest. Auch der dritte Teil des folgenden Lemmas hilft: Wenn $a$ kein Teiler von $n$ ist, so sind sämtliche Vielfache von $a$ ebenfalls kein Teiler von $n$.

LEMMA 12.3. *In $\mathbb{N}$ gelten folgende Teilbarkeitsbeziehungen.*

(1) *Für jede natürliche Zahl $a$ gilt $1 \mid a$ und $a \mid a$.*
(2) *Für jede natürliche Zahl $a$ gilt $a \mid 0$.*
(3) *Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.*
(4) *Gilt $a \mid b$ und $c \mid d$, so gilt auch $ac \mid bd$.*
(5) *Gilt $a \mid b$, so gilt auch $ac \mid bc$ für jede natürliche Zahl $c$.*
(6) *Gilt $a \mid b$ und $a \mid c$, so gilt auch $a \mid (rb + sc)$ für beliebige natürliche Zahlen $r, s$.*

*Beweis.* (1) Ist klar wegen

$$a = a \cdot 1.$$

(2) Ist klar wegen

$$0 = a \cdot 0.$$

(3) Die beiden Voraussetzungen bedeuten die Existenz von $s, t \in \mathbb{N}$ mit $b = as$ und $c = bt$. Somit ist

$$c = bt = (as)t = a(st)$$

und $a$ ist auch ein Teiler von $c$.

(4) Aus den Voraussetzungen $b = as$ und $d = tc$ ergibt sich direkt

$$bd = astc = acts,$$

also ist $ac$ ein Teiler von $bd$.

(5) Aus der Voraussetzung $b = as$ ergibt sich direkt

$$bc = acs,$$

also ist $ac$ ein Teiler von $bc$.

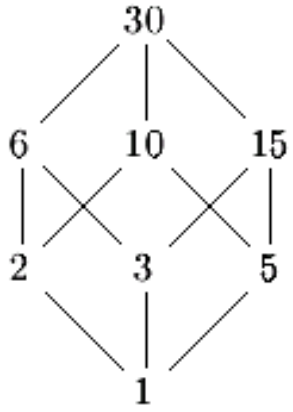
(6) Aus den Voraussetzungen $b = at$ und $c = au$ ergibt sich direkt mit dem Distributivgesetz

$$rb + sc = rat + sau = a(rt + su),$$

also ist $a$ ein Teiler von $rb + sc$.

□

Beispiel 12.4. Wir betrachten die positiven natürlichen Zahlen $\mathbb{N}_+$ zusammen mit der Teilbarkeitsbeziehung. Dies ergibt eine Ordnung auf $\mathbb{N}_+$. Die Teilbarkeitsrelation ist in der Tat reflexiv, da stets $n|n$ ist, wie $m = 1$ zeigt. Die Transitivität wurde in Lemma 12.3 (3) gezeigt. Die Antisymmetrie folgt so: Aus $n = ak$ und $k = bn$ folgt $n = (ab)n$. Da wir uns auf positive natürliche Zahlen beschränken, folgt mit der Kürzungsregel $ab = 1$ und daraus wegen $a, b \leq ab$ auch $a = b = 1$. Also ist $k = n$. Einfache Beispiele wie 2 und 3 zeigen, dass hier keine totale Ordnung vorliegt, da weder 2 von 3 noch umgekehrt geteilt wird.




## Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 12.5. Seien $a_1, \ldots, a_k$ natürliche Zahlen. Dann heißt eine natürliche Zahl $t$ *gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn $t$ jedes $a_i$ teilt für $i = 1, \ldots, k$.

Eine natürliche Zahl $g$ heißt *größter gemeinsamer Teiler* der $a_1, \ldots, a_k$, wenn $g$ ein gemeinsamer Teiler ist und wenn $g$ unter allen gemeinsamen Teilern der $a_1, \ldots, a_k$ der (bezüglich der Ordnungsrelation auf den natürlichen Zahlen) Größte ist.

Beispielsweise haben die Zahlen $100, 75, 125$ die gemeinsamen Teiler $1, 5, 25$, und 25 ist der größte gemeinsame Teiler.

Definition 12.6. Zwei natürliche Zahlen heißen *teilerfremd*, wenn sie keinen gemeinsamen Teiler $\geq 2$ besitzen.

Beispielsweise sind 12 und 25 teilerfremd, 15 und 25 sind nicht teilerfremd, da 5 ein gemeinsamer Teiler ist. Die 1 ist zu jeder natürlichen Zahl (auch zu 0 und 1) teilerfremd.

Definition 12.7. Zu einer Menge von natürlichen Zahlen

$$a_1, \ldots, a_n$$

heißt eine natürliche Zahl $b$ ein *gemeinsames Vielfaches*, wenn $b$ ein Vielfaches von jedem $a_i$ ist, also von jedem $a_i$ geteilt wird.

Die Zahl $b$ heißt das *kleinste gemeinsame Vielfaches* der $a_1, \ldots, a_n$, wenn $b$ ein gemeinsames Vielfaches ist und unter allen gemeinsamen Vielfachen $\neq 0$ der $a_1, \ldots, a_n$, das Kleinste ist.

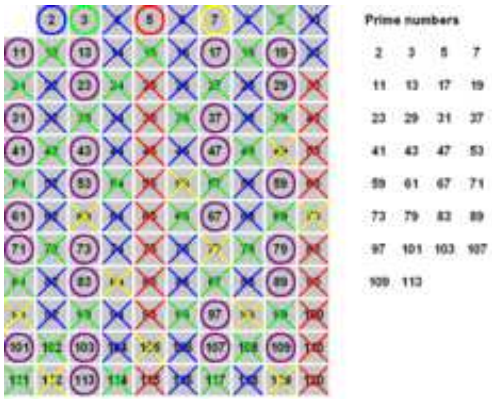
Die Existenz eines größten gemeinsamen Teilers ist wegen Lemma 12.2 klar. Die Existenz des kleinsten gemeinsamen Vielfachen ist ebenfalls klar, da das Produkt der Zahlen ein gemeinsames Vielfaches ist. Wir werden später als eine Anwendung der eindeutigen Primfaktorzerlegung (Satz 20.8) sehen, dass jeder gemeinsame Teiler den größten gemeinsamen Teiler teilt und dass jedes gemeinsame Vielfache ein Vielfaches des kleinsten gemeinsamen Vielfachen ist.

## Primzahlen

Definition 12.8. Eine natürliche Zahl $n \geq 2$ heißt eine *Primzahl*, wenn die einzigen natürlichen Teiler von ihr 1 und $n$ sind.

Eine Primzahl ist also eine natürliche Zahl, die genau zwei Teiler hat, nämlich 1 und $n$, und die müssen verschieden sein. 1 ist also keine Primzahl.

Die ersten Primzahlen sind $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$. Für eine Primzahl $p$ und eine natürliche Zahl $n$ gilt folgende Alternative: Entweder teilt $p$ die Zahl $n$, oder aber $p$ und $n$ sind teilerfremd. Ein gemeinsamer Teiler muss ja ein Teiler von $p$ sein, und da kommen nur 1 und $p$ in Frage.




Das *Sieb des Eratosthenes* liefert eine einfache Methode, eine Liste von Primzahlen unterhalb einer bestimmten Größe $k$ zu erstellen. Man streicht einfach die echten Vielfachen der kleinen (kleiner als oder gleich $\sqrt{k}$) schon etablierten Primzahlen durch, die verbleibenden Zahlen sind prim.

Ein wichtiger Satz ist der Satz über die eindeutige Primfaktorzerlegung. Eine einfache Version davon ist der folgende Satz.

Satz 12.9. *Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, besitzt eine Zerlegung in Primfaktoren.*

*D.h. es gibt eine Darstellung*

$$n = p_1 \cdot p_2 \cdots p_r$$

*mit Primzahlen $p_i$.*

*Beweis.* Wir beweisen die Existenz durch Induktion über $n$. Für $n = 2$ liegt eine Primzahl vor. Bei $n \geq 3$ ist entweder $n$ eine Primzahl, und diese bildet die Primfaktorzerlegung, oder aber $n$ ist keine Primzahl. In diesem Fall gibt es eine nichttriviale Zerlegung $n = ab$ mit kleineren Zahlen $a, b < n$. Für diese Zahlen gibt es nach Induktionsvoraussetzung jeweils eine Zerlegung in Primfaktoren, und diese setzen sich zu einer Primfaktorzerlegung für $n$ zusammen. □

Für 105 beispielsweise findet man den Primfaktor 3 und kann daher $105 = 3 \cdot 35$ schreiben. Für 35 hat man die Zerlegung $35 = 5 \cdot 7$ und man erhält

$$105 = 3 \cdot 5 \cdot 7.$$

Wenn man mit dem Primfaktor 5 startet, so ergibt sich $105 = 5 \cdot 21 = 5 \cdot 3 \cdot 7$, insgesamt kommen also die gleichen Primfaktoren vor. Gelegentlich betrachten wir die Gleichung $1 = 1$ als die Primfaktorzerlegung der 1, hier tritt jeder Primfaktor mit dem Exponenten 0 auf, das leere Produkt ist 1. Später werden wir zeigen, dass die Primfaktorzerlegung bis auf die Reihenfolge eindeutig ist, was keineswegs selbstverständlich ist, einiger Vorbereitungen bedarf und am besten innerhalb der ganzen Zahlen bewiesen wird.

Der folgende Satz wird Euklid zugeschrieben.

Euklid (4. Jahrhundert v. C.)

SATZ 12.10. *Es gibt unendlich viele Primzahlen.*

*Beweis.* Angenommen, die Menge aller Primzahlen sei endlich, sagen wir $\{p_1, p_2, \ldots, p_r\}$ sei eine vollständige Auflistung aller Primzahlen. Man betrachtet die natürliche Zahl

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_r + 1.$$

Da bei Division von $N$ durch $p_i$ immer der Rest 1 übrigbleibt (bzw. nach Aufgabe 12.6), ist diese Zahl durch keine der Primzahlen $p_i$ teilbar. Andererseits besitzt $N$ nach Satz 12.9 eine Primfaktorzerlegung. Insbesondere gibt es eine Primzahl $p$, die $N$ teilt (dabei könnte $N = p$ sein). Doch damit muss $p$ gleich einem der $p_i$ aus der Liste sein, und diese sind keine Teiler von $N$. Dies ist ein Widerspruch, da ein $p_i$ nicht gleichzeitig ein Teiler und kein Teiler von $N$ sein kann. Also muss die Annahme (nämlich die Endlichkeit der Primzahlmenge) falsch gewesen sein. □

## Primzahlprobleme

In der Vorlesung Grundkurs Mathematik geht es um Sachverhalte, die allesamt seit mindestens 120 Jahren gut verstanden sind und zu einem großen Teil sogar bis in die griechische Antike zurückreichen. Wir unterbrechen die allgemeine Darstellung und gehen kurz auf die Frage ein, was Mathematiker in der Forschung machen. Das ist im Allgemeinen schwierig zu vermitteln, im zahlentheoretischen Kontext gibt es aber einige Beispiele, die sich leicht erläutern lassen.

Die treibende Kraft der Mathematik ist es, Probleme zu lösen. Schwierige Probleme gibt es in allen Bereichen der Mathematik, besonders prägnant sind sie in der Zahlentheorie, da es dort eine Vielzahl von elementar formulierten ungelösten Problemen gibt. Als Beispiel besprechen wir das Problem der Primzahlzwillinge, zu dem es kürzlich (2013) einen wichtigen Fortschritt gab.

Definition 12.11. Ein *Primzahlzwilling* ist ein Paar bestehend aus $p$ und $p+2$, wobei diese beiden Zahlen Primzahlen sind.

Die ersten Beispiele für Primzahlzwillinge sind

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\dots\ .$$

Übrigens ist $3,5,7$ der einzige Primzahldrilling, siehe Aufgabe 12.28.

Problem 12.12. Gibt es unendlich viele Primzahlzwillinge?

Eine Lösung dieses Problems wäre ein mathematischer Satz, der entweder besagt, dass es unendlich viele Primzahlzwillinge gibt, oder dass es nur endlich viele Primzahlzwillinge gibt. D.h. das eine oder das andere müsste bewiesen werden. Bei schwierigen Problemen erwartet man nicht, dass jemand plötzlich einen Beweis hinschreibt, sondern dass eine neue und weit verzweigte Theorie entwickelt wird, mit der man letztlich einen Beweis geben kann.

Bemerkung 12.13. Die Frage, ob es unendlich viele Primzahlzwillinge gibt, besitzt verschiedene schwächere Varianten. Man kann sich zum Beispiel fragen, ob es unendlich oft vorkommt, dass es in einem Zehnerintervall zwei Primzahlen gibt, oder dass es in einem Hunderterintervall zwei Primzahlen gibt, und so weiter. Die ersten Primzahlen vermitteln dabei ein Bild, dass Primzahlen ziemlich häufig sind. Sie werden aber zunehmend seltener, so dass es für hohe Hunderterintervalle, sagen wir für die Zahlen von

$$1000000000000000 \text{ bis } 1000000000000100$$

ziemlich unwahrscheinlich ist, eine Primzahl zu enthalten, geschweige denn zwei Primzahlen. Bis vor kurzem war es nicht bekannt, ob es überhaupt eine Zahl $m$ mit der Eigenschaft gibt, dass es unendlich viele Intervalle der Länge $m$ gibt, die zwei Primzahlen enthalten ($m=2$ wäre die positive Lösung des Primzahlzwillingsproblems). Im Jahr 2013 bewies Zhang Yitang, dass man

$$m = 70000000$$

nehmen kann, dass es also unendlich viele Intervalle der Form

$$[k, k+70000000]$$

gibt, in denen zwei Primzahlen liegen. Dieses Resultat ist ein Durchbruch in der Primzahlzwillingforschung, da es erstmals zeigt, dass sich Primzahlen unendlich oft „ziemlich nahe“ kommen. Zwischenzeitlich wurde die Schranke von 70000000 auf 252 gesenkt, siehe http://arxiv.org/pdf/1402.4849v2.pdf.

# Abbildungsverzeichnis