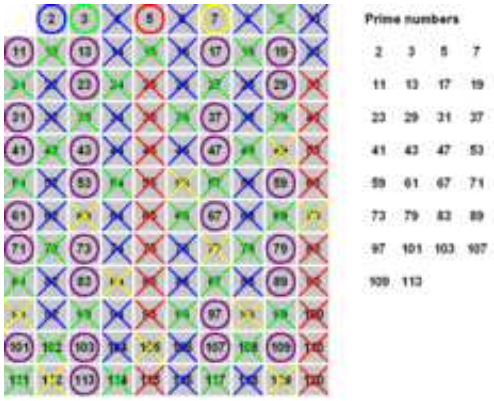
Prof. Dr. H. Brenner **Osnabrück WS 2014/2015**

Vorkurs Mathematik

Vorlesung 2

Primzahlen



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.

DEFINITION 2.1. 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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$.

SATZ 2.2. *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. Von der kleineren Zahl 35 ist die Zerlegung $35 = 5 \cdot 7$ nach Induktionsvoraussetzung schon bekannt 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. Weiter unten werden wir zeigen, dass die Primfaktorzerlegung bis auf Reihenfolge eindeutig ist, was keineswegs selbstverständlich ist und einiger Vorbereitungen bedarf.

SATZ 2.3. *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, ist diese Zahl durch keine der Primzahlen p_i teilbar. Andererseits besitzt N nach Satz 2.2 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. □

Teilerfremdheit

DEFINITION 2.4. Zwei natürliche Zahlen heißen *teilerfremd*, wenn sie keinen gemeinsamen Teiler ≥ 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. 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.

AUFGABE 2.5. Die Wasserspedition „Alles im Eimer“ verfügt über einen 7- und einen 10-Liter-Eimer, die allerdings keine Markierungen haben. Sie erhält den Auftrag, insgesamt genau einen Liter Wasser von der Nordsee in die Ostsee zu transportieren. Kann sie diesen Auftrag erfüllen?

Die Aufgabe ist lösbar: Man macht fünfmal den 10-Liter-Eimer in der Nordsee voll und transportiert dies in die Ostsee. Danach (oder gleichzeitig) macht man siebenmal den 7-Liter-Eimer in der Ostsee voll und transportiert dies in die Nordsee. Unterm Strich hat man dann $5 \cdot 10 - 7 \cdot 7 = 1$ Liter transportiert. Die dieser Überlegung zugrunde liegende Aussage heißt *Lemma von Bezout*.

SATZ 2.6. *Es seien $a, b \in \mathbb{N}$ zwei teilerfremde natürliche Zahlen. Dann gibt es ganze Zahlen $r, s \in \mathbb{Z}$ mit $ra + sb = 1$.*

Beweis. Wir beweisen die Aussage durch Induktion über das Maximum von a und b, wobei wir ohne Einschränkung $a \leq b$ wählen können. Wenn das Maximum 0 ist, so sind beide Zahlen 0 und somit nicht teilerfremd. Wenn das Maximum 1 ist, so ist $b = 1$ und somit ist $r = 0$ und $s = 1$ eine Darstellung der 1. Seien nun $a \leq b$ teilerfremd, $b \geq 2$ und die Aussage sei für alle Zahlenpaare, deren Maximum kleiner als b ist, schon bewiesen. Dann ist $a < b$, da bei $a = b$ die beiden Zahlen nicht teilerfremd sind. Ebenso können wir $a = 0$ ausschließen. Wir betrachten das Zahlenpaar $(a, b-a)$ und wollen darauf die Induktionsvoraussetzung anwenden. Das Maximum dieses neuen Paares ist jedenfalls kleiner als b. Allerdings müssen wir, damit die Induktionsvoraussetzung wirklich eingesetzt werden kann, wissen, dass auch a und $b - a$ teilerfemd sind. Dazu führen wir einen Widerspruchsbeweis. Nehmen wir also an, dass a und $b - a$ nicht teilerfremd sind. Dann gibt es eine natürliche Zahl $t \geq 2$, die sowohl a als auch $b - a$ teilt. Dies bedeutet wiederum, dass es natürliche Zahlen m, n gibt mit $a = mt$ und $b - a = nt$. Doch dann ist

$$b = (b - a) + a = nt + mt = (n + m)t$$

ebenfalls ein Vielfaches von t, im Widerspruch zur Teilerfremdheit von a und b. Die Induktionsvoraussetzung ist also auf a und $b-a$ anwendbar und somit gibt es ganze Zahlen r, s mit

$$ra + s(b - a) = 1.$$

Dann ist aber auch

$$(r-s)a+sb \;=\; ra+s(b-a) \;=\; 1$$

und wir haben eine Darstellung der 1 mit a und b gefunden. □

Der Hauptsatz der elementaren Zahlentheorie

Wir möchten nun zur Primfaktorzerlegung, deren Existenz wir bereits 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 Reihenfolge gemeint. Um dies zu zeigen brauchen wir zunächst das sogenannte *Lemma von Euklid*, das eine wichtige Eigenschaft einer Primzahl beschreibt.

Satz 2.7. *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 Satz 2.5 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 $a_1a_2\cdots a_n$ teilt, dann teilt p mindestens einen Faktor. Man wendet das Lemma einfach auf $(a_1a_2\cdots a_{n-1})\cdot a_n$ an (formal ist das eine Induktion über die Anzahl der Faktoren). Dies wird im Beweis des folgenden *Hauptsatzes der elementaren Zahlentheorie* verwendet.

Satz 2.8. *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 2.2 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 2.6 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. □

Primzahlprobleme

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

Die ersten Beispiele für Primzahlzwillinge sind

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

Übrigens ist $3, 5, 7$ der einzige Primzahldrilling, siehe Aufgabe 2.12.

Problem 2.10. 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 2.11. 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

Quelle = New Animation Sieve of Eratosthenes.gif , Autor = Benutzer M.qrius auf Commons, Lizenz = CC-by-sa 3.0 1

Quelle = Kielcanal.PNG , Autor = Benutzer Grunners auf Commons, Lizenz = PD 3