2.3. Primzahlen

Eine positive natürliche Zahl p heißt ***prim***, wenn sie genau zwei verschiedene positive Teiler hat. Diese sind dann 1 und p. Nach dieser Definition ist dann 1 keine Primzahl und die kleinste Primzahl ist 2. Eine positive natürliche Zahl, die nicht prim ist, wird auch eine ***zusammengesetzte*** Zahl genannt. Um Primzahlen zu suchen kann man naiv vorgehen: Eine Zahl n nehmen und einfach alle möglichen Teiler (zwischen 2 und $\sqrt{n}$) testen. Ist keine dieser Zahlen Teiler, hat man eine Primzahl. Will man mehrere (oder alle) Primzahlen zwischen 2 und n, geht es das sehr gut mit dem folgenden uralten Algorithmus.

Britannica:

Eratosthenes of Cyrene
born c. 276 BC, Cyrene, Libya
died c. 194, Alexandria, Egypt
Greek scientific writer, astronomer, and poet, the first man known to have calculated the Earth's circumference.
At Syene (now Aswan), some 800 km (500 miles) southeast of Alexandria in Egypt, the Sun's rays fall vertically at noon at the summer solstice. Eratosthenes noted that at Alexandria, at the same date and time, sunlight fell at an angle of about 7° from the vertical. He correctly assumed the Sun's distance to be very great; its rays therefore are practically parallel when they reach the Earth. Given estimates of the distance between the two cities, he was able to calculate the circumference of the Earth. The exact length of the units (stadia) he used is doubtful, and the accuracy of his result is therefore uncertain; it may have varied by 0.5 to 17 percent from the value accepted by modern astronomers. He also measured the degree of obliquity of the ecliptic (in effect, the tilt of the Earth's axis) with great accuracy and compiled a star catalog. His mathematical work is known principally from the writings of Pappus of Alexandria.

After study in Alexandria and Athens, Eratosthenes settled in Alexandria about 255 BC and became director of the great library there. He worked out a calendar that included leap years, and he tried to fix the dates of literary and political events since the siege of Troy. His writings include a poem inspired by astronomy, as well as works on the theatre and on ethics. Eratosthenes was afflicted by blindness in his old age, and he is said to have committed suicide by voluntary starvation.

ALGORITHM 2.3.1. *Sieb des Eratosthenes*

Dazu beginnt man mit der Menge $C := 2, 3, \ldots, n$ der Kandidaten und der Menge P der gefundenen Primzahlen. Nun sucht man die kleinste Zahl p (das ist die 2) aus C. Dies ist eine Primzahl, sie wird in P eingefügt. Nun streicht man p und alle Vielfachen davon aus C. Danach geht es weiter mit der nächsten kleinsten Zahl aus C. Am Ende ist C leer, und in P sind alle Primzahlen.

EXAMPLE 2.3.2. alle Primzahlen bis 30
$C = \{2, 3, 4, \ldots\}$; $P = \emptyset$;
$c = 2$;$P = \{2\}$;$C = \{3, 5, 7, 9, 11, \ldots, 29\}$;
$c = 3$; $P = \{2, 3\}$; $C = \{5, 7, 11, 13, 17, 19, 23, 25, 29\}$;
$c = 5$; $P = \{2, 3, 5\}$; $C = \{7, 11, 13, 17, 19, 23, 29\}$;
nun kann aufgehört werden, da $7 > \sqrt{30}$, und man weiß, C sind die restlichen Primzahlen ≤ 30.

THEOREM 2.3.3. *Eigenschaft von Primzahlen*
Sei p eine Primzahl. Seien a, b ganze Zahlen mit der Eigenschaft: p teilt das Produkt ab. Dann wird a oder b von p geteilt.

BEWEIS. Nehmen wir an p teilt nicht a. Dann ist $ggT(a, p) = 1$, also sind p und a teilerfremd. Damit teilt p das Produkt ab, also teilt p den Faktor b nach der Eigenschaft 2.2.8 teilerfremder Zahlen. □

COROLLARY 2.3.4. *Eigenschaft bei mehreren Faktoren*
Sei p eine Primzahl. Seien $a_1, \ldots, a_k$ ganze Zahlen mit der Eigenschaft: p teilt das Produkt $a_1 \ldots a_k$. Dann teilt p einen der Faktoren.

BEWEIS. Mit obigem Theorem 2.3.3 und vollständiger Induktion. □

Das wichtigste Ergebnis ist folgender Satz, der die Bedeutung der Primzahlen (als eine Art multiplikatives Atom) zeigt.

THEOREM 2.3.5. *Satz von der eindeutigen Primfaktorzerlegung*
Jede natürliche Zahl $n \geq 2$ kann geschrieben werden als Produkt von Primzahlen $p_1, \ldots, p_k$:

$$n = p_1 \ldots p_k.$$

Dieses Produkt ist bis auf die Reihenfolge eindeutig.

BEWEIS. Der Beweis besteht aus zwei Teilen. Der erste Teil zeigt, dass eine deratige 'Produktzerlegung' möglich ist und der zweite Teil zeigt, dass diese Schreibweise eindeutig ist.
Teil 1: Man beweist dies mit vollständiger Induktion über n. Der Induktionsanfang ist $n = 2$, dies ist eine Primzahl und hat daher die Zerlegung $2 = p_1$ mit $p_1 = 2$. Für den Induktionsschritt betrachtet man ein beliebiges $n > 2$ und man weiß, dass alle Zahlen $k < n$ ein Zerlegung als Produkt von Primzahlen hat. Man unterscheidet nun zwei Fälle:
Fall 1: n ist eine Primzahl, dann ist $n = n$ die gesuchte Produktzerlegung in Primzahlen.
Fall 2: $n = ab$ ist eine zusammengesetzte Zahl, dann kann man nach Induktionsannahme sowohl $a = p_1 \ldots p_k$ als auch $b = q_1 \ldots q_l$ als Produkt von Primzahlen schreiben, das gemeinsame Produkt $n = p_1 \ldots p_k q_1 \ldots q_l$ ist die gesuchte Zerlegung.
Teil 2: Für die Eindeutigkeit, zeigen wir per Induktion über k, dass eine Zerlegung $n = p_1 \ldots p_k$ eindeutig ist.
Induktionsanfang: $k = 1$. Wir nehmen an es gibt zwei Primfaktorzerlegungen $n = p_1 = q_1 \ldots q_s$. Aus $n = p_1$ wissen wir, dass n eine Primzahl ist. Aus der Zerlegung $n = q_1 \ldots q_s$ hat aber n die verschiedenen Faktoren $1, q_1, q_1 q_2$ was ein Widerspruch zur Primzahleigenschaft ist.
Induktionsschritt: Wir wissen also, dass aus einer Zerlegung in ein Produkt aus $k-1$ Primzahlen die Eindeutigkeit dieser Zerlegung folgt. Wir nehmen nun an, es gibt zwei Primfaktorzerlegungen:

$$n = p_1 \ldots p_k = q_1 \ldots q_l.$$

Wir wissen wegen $n = p_1 \ldots$, dass p_1 Teiler von n ist, also teilt wegen 2.3.4 p_1 auch eine der Primzahlen $q_1, \ldots, q_s$. Man kann ohne Probleme annehmen p_1 teilt q_1. Da aber $q_1$auch eine Primzahl ist, gilt also $p_1 = q_1$. Nun teilt man die obige rechte Hälfte der Gleichung durch p_1 und bekommt:

$$p_2 \ldots p_k = q_2 \ldots q_l.$$

Die linke Seite ist eine Primfaktorzerlegung in $k-1$ Teile, und diese ist nach Induktionsannahme eindeutig, also hat man $k = l$ und rechts ist ein bis auf Reihenfolge gleiches Produkt. Damit ist dann auch die Ausgangszerlegung eindeutig. □

Teil 1 war bereits bei Euklid. Ein zweites wichtiges Ergebnis (wieder von Euklid) ist die Erkenntnis, dass es unendlich viele Primzahlen gibt.

THEOREM 2.3.6. *Es gibt unendlich viele Primzahlen.*

BEWEIS. Widerspruchsbeweis: Wir nehmen an, es gibt nur endlich viele (=k) Primzahlen $p_1, \ldots, p_k$. Nun betrachtet man die Zahl $n = (p_1 \ldots p_k) + 1$. Da keine der Primzahlen $p_1, \ldots, p_k$ Teiler ist (sie haben alle Rest 1 bei der Division mit Rest), kann keine in der nach Satz 2.3.5 vorhanden Primzahlzerlegung vorkommen. Also gibt es weitere Primzahlen. □

Der Satz von der eindeutigen Primfaktorzerlegungen hat mehrere wichtige Anwendungen. Man erhält einen Datentyp zur Speicherung von natürlichen Zahlen > 0. Dazu nummeriert man die Primzahlen $p_1, p_2, \ldots$ und betrachtet die eindeutige Primfaktorzerlegung

$$n = p_1^{e_1} p_2^{e_2} \ldots$$

Als Datentyp für eine natürliche Zahl wählt man ein Feld welches an der Stelle i den Exponenten e_i enthält. Da ein Exponent $e_i = 0$ einem Faktor 1 entspricht, kann nach dem letzten Exponenten $\neq 0$ aufgehört werden. Diese Darstellung der natürlichen Zahlen> 0 wird ***Primexponentendarstellung*** genannt und ist bis auf Nullen am Ende eindeutig.

EXAMPLE 2.3.7. Primexponentendarstellung
Wir nehmen an, die Primzahlen werden aufsteigend sortiert, d.h. $2 = p_1 < p_2 = 3 < p_3 < \ldots$. Dann ist z.B.

$$10 = 2 \times 5 = [1, 0, 1].$$

Dem Vektor $[2, 4, 0, 0, 0, 0, 1]$ entspricht die Zahl $2^2 \times 3^4 \times 17$.

Mit der Primexponentendarstellung kann im Gegensatz zur üblichen Dezimalnotation $(123 = 1\times10^2+2\times10^1+3\times10^0)$ schnell multipliziert werden, aber die Addition ist sehr langsam. Leicht ist auch die Berechnung von ggT und kgV.

COROLLARY 2.3.8. *kgV und ggT in der Primexponentendarstellung*
Seien $a = p_1^{e_1} p_2^{e_2} \ldots$ *und* $b = p_1^{f_1} p_2^{f_2} \ldots$ *zwei positive ganze Zahlen in Primexponentendarstellung. Dann ist*

$$ggT(a, b) = p_1^{min\{e_1,f_1\}} p_2^{min\{e_2,f_2\}} \ldots$$

und

$$kgV(a, b) = p_1^{max\{e_1,f_1\}} p_2^{max\{e_2,f_2\}} \ldots$$

BEWEIS. langweilig □

Damit hat man natürlich einen anderen Algorithmus zur Berechnung des ggT zweier Zahlen zur Verfügung. Man berechnet beide Primexponentendarstellungen und wendet obiges Lemma an. Man bekommt damit allerdings nicht die Linearkombination des ggT.

2.3.1. Verallgemeinerung von den natürlichen Zahlen auf alle ganzen Zahlen. Bei der Division mit Rest teilen wir auch negative ganze Zahlen, man erlaubt aber weiterhin nur positive Teiler. Dann ist der Rest immer eine positive Zahl. So zum Beispiel:

$$-7 = -3 \times 3 + 2.$$