Primzahlen

Wir werden uns im Folgenden mit Primzahlen beschäftigen und dafür erst einige zahlentheoretische Begriffe wiederholen, die vielen schon aus der Schule bekannt sein werden.

1 Teilbarkeit

Seien a und b ganze Zahlen, wir schreiben dafür $a, b \in \mathbb{Z}$.
Wir sagen a teilt b, wenn es eine ganze Zahl q gibt, sodass $b = q \cdot a$. Wir schreiben dafür $a \mid b$.
Wir nennen a dann einen Teiler von b, q ist der Komplementärteiler von b zu a.
Ist a kein Teiler von b so schreiben wir $a \nmid b$.

Beispiele:

$4 \mid 12$, denn $3 \cdot 4 = 12$. Der Komplementärteiler von 12 zu 4 ist 3. Die Menge der Teiler von 12 ist $\{1, (-1), 2, (-2), 3, (-3), 4(-4), 6, (-6), 12, (-12)\}$.

$(-3) \mid 27$, denn $(-9) \cdot (-3) = 27$. Der Komplementärteiler von 27 zu (-3) ist also (-9).

$4 \nmid 11$, denn ansonsten müsste es, wie oben verlangt, eine ganze Zahl q geben, sodass gilt: $11 = q \cdot 4$. Diese Gleichung können wir umformen zu $q = \frac{11}{4}$, was keiner ganze Zahl entspricht. Wir könne also das gesuchte q nicht finden und daher ist 4 kein Teiler von 11.

Beachte:
Jede Zahl $b \in \mathbb{Z}$ hat $1, (-1), b, (-b)$ als Teiler. Ein Teiler a von b, für den gilt $a \notin \{1, (-1), b, (-b)\}$ heißt echter Teiler von b.

Jede ganze Zahl a teilt 0, denn es gilt stets $0 \cdot a = 0$.

Ist b eine ganze Zahl ungleich 0 und a ein Teiler von b, so folgt $|a| \leq |b|$.

Teilbarkeitsregeln :
Die folgenden Reglen erweisen sich als nützlich um schnell die Teiler einer Zahl zu finden.
Sei n eine natürliche Zahl mit der Darstellung $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots a_1 \cdot 10 + a_0$ im Zehnersystem. Zum Beispiel $n = 4212 = 4 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10^1 + 2$.
Dann gilt:

(i) $2 \mid n \Leftrightarrow 2 \mid a_0$, n ist also genau dann durch 2 teilbar, wenn die 'Einerstelle' von n durch 2 teilbar ist.

(ii) $3 \mid n \Leftrightarrow 3 \mid (a_0 + a_1 + \ldots + a_k)$, n ist also genau dann durch 3 teilbar, wenn die Ziffernsumme von n durch 3 teilbar ist.

(iii) $4 \mid n \Leftrightarrow 4 \mid (a_0 + 10 \cdot a_1)$

(iv) $5 \mid n \Leftrightarrow 5 \mid a_0$

(v) $8 \mid n \Leftrightarrow 8 \mid (a_0 + 10 \cdot a_1 + 10^2 \cdot a_2)$

(vi) $9 \mid n \Leftrightarrow 9 \mid (a_0 + a_1 + \ldots + a_k)$

(vii) $11 \mid n \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - + \ldots + (-1)^k \cdot a_k)$

Beispiel: Sei $n = 4212$: $2 \mid n$, $3 \mid n$, $4 \nmid n$, $5 \nmid n$, $6 \mid n$, $8 \nmid n$, $9 \mid n$, $11 \nmid n$

2 Größter geimeinsamer Teiler

Seien a und b ganze Zahlen ungleich 0.
Eine ganze Zahl c, die $c \mid a$ und $c \mid b$ erfüllt heißt gemeinsamer Teiler von a und b.

Zwei ganzen Zahlen a und b besitzen stets gemeinsame Teiler ($1 \mid a$, $1 \mid b$). Außerdem muss, wie wir oben gesehen haben ein Teiler c von a (bzw b) betragsmäßig kleiner oder gleich a (bzw b) sein.
Die Menge der gemeinsamen Teiler von a und b ist also nicht leer und nach oben beschränkt. Sie besitzt daher ein größtes Element d. Wir nennen d den *größten gemeinsamen Teiler* von a und b und schreiben dafür $ggT(a, b)$.

Beispiel: Die Menge der gemeinsamen Teiler von 12 und (-18) ist $\{1, (-1), 2, (-2), 3, (-3), 6, (-6)\}$. Daher ist $ggT(12, -18) = 6$.

Es gilt:

(i) $ggT(a, b) = ggT(b, a)$

(ii) $ggT(a, b) \geq 1$, ist $ggT(a, b) = 1$, so heißen a und b *relativ prim* oder *teilerfremd*.

(iii) Für jeden gemeinsamen Teiler c von a und b gilt: $c \mid ggT(a, b)$.

3 Kleinstes gemeinsames Vielfaches

Seien $a, b \in \mathbb{Z}$. a heißt Vielfaches von b, wenn es ein $k \in \mathbb{Z}$ gibt, sodass $a = k \cdot b$, wenn also $b \mid a$ gilt.
$c \in \mathbb{Z}$ heißt gemeinsames Vielfaches von a und b, wenn c ein Vielfaches von a und b ist.

Seien $a, b \in \mathbb{Z}$, $a, b \neq 0$. Die Menge der positiven, gemeinsamen Vielfachen von a und b ist nicht leer (sie enthält $|a| \cdot |b|$) und nach unten beschränkt. Sie entält also ein kleinstes Element g. Wir nennen g das *kleinste gemeinsame Vielfache* von a und b und schreiben dafür $kgV(a, b)$.

Beispiel:

$$kgV(12, 18) = 36 \qquad kgV(-10, 200) = 200 \qquad kgV(a, a^n) = a^n$$

4 Primzahlen

Definition. *Eine natürliche Zahl $p \geq 2$ heißt Primzahl, wenn sie keine echten Teiler besitzt, das heißt p wird nur von $1, (-1), p, (-p)$ geteilt.*

Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.
Achtung: 1 ist keine Primzahl!
Die Folge der Primzahlen beginnt wie folgt: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$.
Sie ist unendlich(wird später bewiesen).
2 ist die einzige gerade Primzahl, jede andere gerade Zahl ist durch 2 teilbar.

Primzahlen kann man sich als 'unzerlegbare Bausteine' der natürlichen Zahlen vorstellen, wie der folgende Satz zeigt:

Satz von der Primfaktorzerlegung: *Sei $a \in \mathbb{N}$, $a \geq 2$. Dann kann a in (bis auf Reihenfolge) eindeutiger Weise als Produkt von Primzahlen dargestellt werden. Das heißt es gibt Primzahlen $p_1, p_2, \ldots, p_n$ (nicht notwendigerweise verschieden) sodass, $a = p_1 \cdot p_2 \cdots p_n$.*

Die Existenz einer solchen Zerlegung ist leicht zu sehen: Falls a eine Primzahl ist setze $n = 1$, $p_1 = a$. Falls a keine Primzahl ist, so besitzt a einen echten Teiler, es gibt also $p, q \in \mathbb{N} : 1 < p, q < a$, $a = p \cdot q$. Wir können a also in Faktoren zerlegen die kleiner als a und größer als 1 sind. Ist nun etwa p keine Primzahl, so können wir mit obigem Argument p in zwei Faktoren, kleiner als p und größer als 1 zerlegen usw... Da die Faktoren in jedem Schritt echt kleiner werden landen wir schlussendlich bei einer Zerlegung in Primzahlen. Ein illustrierendes Beispiel:

$$72 = 6 \cdot 12 = (2 \cdot 3) \cdot (3 \cdot 4) = (2 \cdot 3) \cdot (3 \cdot (2 \cdot 2)) = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2$$

Die Eindeutigkeit ist etwas schwieriger zu sehen und wird in der Zahlentheorie bewiesen.

Finden von Primfaktorzerlegungen

Um die Primfaktorzerlegung einer ganzen Zahl n zu finden geht man am besten methodisch vor. Beginnend mit 2, der niedrigsten Primzahl, überprüft man der Reihe nach welche Primzahlen n teilen und dividiert diese gegebenenfalls 'weg'.

Sei beispielsweise $n = 693$
n ist nicht durch 2 teilbar (siehe Teilbarkeitsregeln oben).
Die Ziffernsumme von n ist $6+9+3 = 18$. Also ist 3 ein Teiler von n, genauer: $n = 3 \cdot 231$.
Auch 231 ist durch 3 teilbar, insgesamt also $n = 3^2 \cdot 77$.
77 ist nicht mehr durch 3 teilbar, ebensowenig durch 5, allerdings gilt $7 \mid 77$. Es folgt $n = 3^2 \cdot 7 \cdot 11$.
Da 11 eine Primzahl ist, haben wir die Primfaktorzerlegung von n gefunden.

Diese Methode des 'Durchprobierens' wird bei großen Zahlen natürlich schnell mühsam. Es wurde aber bisher kein wesentlich effektiveres Verfahren zu Bestimmung der Primfaktorzerlegung gefunden.

Bestimmen des ggTs und kgVs

Mir Hilfe der Primfaktorzerlegung kann man leicht den ggT zweier ganzer Zahlen a und b bestimmen: Der $ggT(a, b)$ setzt sich aus jenen Primzahlen zusammen, die in den Zerlegungen von a und von b auftauchen, und zwar treten sie im ggT in der niedrigsten vorkommenden Potenz auf.

Beispiel: Sei $a = 72 = 2^3 \cdot 3^2$, $b = 60 = 2^2 \cdot 3^1 \cdot 5^1$

$$ggT(72, 60) = 2^2 \cdot 3^1 = 12$$

Das kgV von a und b ist das Produkt aller Primfaktoren, die in a oder b auftreten (oder in beiden) und zwar jeweils zur höchsten auftretenden Potenz.

Beispiel: Sei wieder $a = 72 = 2^3 \cdot 3^2$, $b = 60 = 2^2 \cdot 3^1 \cdot 5^1$

$$kgV(72, 60) = 2^3 \cdot 3^2 \cdot 5^1 = 360$$

Alternativ verwnendet man die Formel

$$|a| \cdot |b| = ggT(a, b) \cdot kgV(a, b)$$

für $a, b \in \mathbb{Z}$, $a, b \neq 0$.
Damit lässr sich aus dem ggT das kgV berechnen oder umgekehrt.