§ 2. Teilbarkeit. Euklidischer Algorithmus

2.1. Wir benutzen die folgenden Bezeichnungen:

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$	Menge aller ganzen Zahlen
$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$	Menge der natürlichen Zahlen (einschließlich 0)
$\mathbb{N}_1 = \{1, 2, 3, 4, \ldots\}$	Menge der natürlichen Zahlen $\geqslant 1$
$\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}, m \neq 0\}$	Körper der rationalen Zahlen
$\mathbb{R} =$ Körper der reellen Zahlen	
$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$	Körper der komplexen Zahlen

2.2. Definition (Teilbarkeit). Für ganze Zahlen $x, y \in \mathbb{Z}$ definiert man

$$x \mid y \qquad \text{(gesprochen: } x \text{ teilt } y\text{)}$$

genau dann, wenn eine ganze Zahl $q \in \mathbb{Z}$ existiert mit $y = qx$.

2.3. Einfache Eigenschaften der Teilbarkeit.
In den folgenden Aussagen seien $x, y, z, a, b, \lambda, \mu$ stets Elemente von $\mathbb{Z}$.

a) (Transitivität) $x \mid y$ und $y \mid z \implies x \mid z$

b) $x \mid a$ und $x \mid b \implies x \mid (\lambda a + \mu b)$ für alle $\lambda, \mu \in \mathbb{Z}$.

c) $x \mid 0$ für alle $x \in \mathbb{Z}$

d) $0 \mid x \implies x = 0$

e) $\pm 1 \mid x$ für alle $x \in \mathbb{Z}$

f) $x \mid \pm 1 \implies x = \pm 1$

g) $x \mid y$ und $y \mid x \iff x = \varepsilon y$ mit $\varepsilon = \pm 1$.

Beweis. Fast alle Aussagen sind trivial. Wir geben einen Beweis für die Implikation "⇒" von g).
Falls $x = 0$, folgt wegen $x \mid y$ und d), dass $y = 0$, also $x = y$.
Wir können also jetzt $x \neq 0$ annehmen. Nach Voraussetzung ist $y = q_1 x$ und $x = q_2 y$ mit ganzen Zahlen q_1, q_2. Einsetzen der ersten Gleichung in die zweite ergibt

$$x = q_2 q_1 x \implies 1 = q_2 q_1 \quad \text{(wegen } x \neq 0 \text{ ist Kürzung erlaubt)}$$

Die Gleichung $q_2 q_1 = 1$ ist aber innerhalb von $\mathbb{Z}$ nur möglich, wenn $q_1 = q_2 = \pm 1$, q.e.d.

Bezeichnung. Die Zahlen ± 1 heißen die *Einheiten* von $\mathbb{Z}$. Sie sind die einzigen ganzen Zahlen, die in $\mathbb{Z}$ ein Inverses besitzen.

2.4. Definition (Größter gemeinsamer Teiler). Seien $x, y \in \mathbb{Z}$. Dann heißt $d \in \mathbb{Z}$ größter gemeinsamer Teiler von x und y, wenn folgende zwei Bedingungen erfüllt sind:

(1) d ist gemeinsamer Teiler von x und y, d.h. $d \mid x$ und $d \mid y$.

(2) Für jeden weiteren gemeinsamen Teiler d' von x und y gilt $d' \mid d$.

Zur Eindeutigkeit. Seien d_1 und d_2 zwei größte gemeinsame Teiler von x und y. Nach Bedingung (2) gilt dann einerseits $d_1 \mid d_2$ und andrerseits $d_2 \mid d_1$. Nach 2.3g) folgt daraus $d_1 = \varepsilon d_2$ mit $\varepsilon = \pm 1$. Der größte gemeinsame Teiler ist also im Falle der Existenz bis auf eine Einheit eindeutig bestimmt. (Die Existenz wird in Kürze bewiesen.)

Bezeichnung. Ist $d \geqslant 0$ größter gemeinsamer Teiler von $x, y \in \mathbb{Z}$, so schreiben wir

$$d = \gcd(x, y).$$

Nach den obigen Bemerkungen ist d eindeutig durch x, y bestimmt. (Die Bezeichnung kommt von *greatest common divisor*). In der zahlentheoretischen Literatur findet sich stattdessen auch häufig die Bezeichnung $d = (x, y)$.

Zwei ganze Zahlen x, y heißen *teilerfremd*, wenn

$$\gcd(x, y) = 1.$$

Es folgt unmittelbar aus der Definition $\gcd(\pm x, \pm y) = \gcd(x, y)$. Weiter ist

$$\gcd(0, 0) = 0.$$

Zwar ist nach 2.3c) jede ganze Zahl Teiler von 0, aber nur die 0 erfüllt auch die Bedingung (2), denn $0 \mid d \;\Rightarrow\; d = 0$.
Ebenso zeigt man $\gcd(x, 0) = |x|$ für alle $x \in \mathbb{Z}$.

2.5. Satz (Teilen mit Rest). *Seien $x, y \in \mathbb{Z}$, $y \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit*

$$x = qy + r \quad \textit{und} \quad 0 \leqslant r < |y|.$$

Beweis.
Eindeutigkeit. Seien $x = q_1 y + r_1$ und $x = q_2 + r_2$ zwei solche Darstellungen. Wir können $r_1 \geqslant r_2$ annehmen. Subtraktion der zweiten Gleichung von der ersten ergibt

$$0 = (q_1 - q_2)y + (r_1 - r_2).$$

Da $0 \leqslant r_1 - r_2 < |y|$, ist dies nur möglich, wenn $q_1 - q_2 = 0$, also auch $r_1 - r_2 = 0$.

Existenz. Wegen $qy = (-q)(-y)$ genügt es, den Fall $y > 0$ zu behandeln.
1. Fall: $x \geqslant 0$. Wir beweisen die Behauptung durch Induktion nach x. Der Induktions-Anfang $x = 0$ ist trivial.

Induktionsschritt $x \to x+1$. Nach Induktions-Voraussetzung haben wir eine Darstellung $x = qy + r$, $0 \leqslant r < y$. Daraus folgt

$$x + 1 = qy + (r + 1).$$

Falls $r + 1 < y$, sind wir fertig. Andernfalls ist $r + 1 = y$ und

$$x + 1 = (q + 1)y + 0$$

die gesuchte Darstellung.
2. Der Fall $x < 0$ wird auf den 1. Fall zurückgeführt. Da $-x > 0$, gibt es eine Darstellung

$$-x = qy + r \quad \text{mit } 0 \leqslant r < y,$$

also $x = (-q)y + (-r)$. Ist $r = 0$, sind wir fertig. Falls $r > 0$, ist

$$x = (-q - 1)y + (y - r)$$

die gesuchte Darstellung, q.e.d.

2.6. Euklidischer Algorithmus. Wir beweisen jetzt, dass der größte gemeinsame Teiler zweier ganzer Zahlen x, y stets existiert und geben gleichzeitig eine Methode zu seiner Berechnung an. Es ist dies der über 2000 Jahre alte Euklidische Algorithmus.
Es genügt offenbar, den Fall $y > 0$ zu behandeln. Wir setzen

$$x_0 := x \quad \text{und} \quad x_1 := y$$

und führen nach folgendem Schema sukzessive Teilungen mit Rest gemäß Satz 2.5 durch, bis sich der Rest 0 ergibt

$$\left\{\begin{array}{ll} x_0 = q_1 x_1 + x_2, & 0 < x_2 < x_1, \\ x_1 = q_2 x_2 + x_3, & 0 < x_3 < x_2, \\ \quad \dots & \\ x_{n-2} = q_{n-1} x_{n-1} + x_n, & 0 < x_n < x_{n-1}, \\ x_{n-1} = q_n x_n + 0. & \end{array}\right. \tag{$*$}$$

Da die Reihe der Zahlen $x_1, x_2, \dots$ streng monoton abnimmt, wird nach endlich vielen Schritten der Rest 0 erreicht.
Behauptung. Der letzte Divisor $d := x_n$ ist der größte gemeinsame Teiler von $x = x_0$ und $y = x_1$.
Dazu haben wir nach Definition zweierlei zu zeigen:

(1) d ist gemeinsamer Teiler von x und y.

Wir betrachten die Gleichungen von $(*)$ der Reihe nach von der letzten zur ersten. Aus der letzten Gleichung folgt, dass $d = x_n$ ein Teiler von x_{n-1} ist. Da also d ein Teiler von x_n und x_{n-1} ist, folgt aus der vorletzten Gleichung, dass d auch x_{n-2} teilt.

So fortfahrend erhält man, dass d alle x_k, $k = n, n-1, \ldots, 1, 0$ teilt. Insbesondere ist d ein gemeinsamer Teiler von $x_0 = x$ und $x_1 = y$.

(2) Jeder Teiler d' von $x = x_0$ und $y = x_1$ ist auch ein Teiler von $d = x_n$.
Hierzu betrachten wir die Gleichungen von $(*)$ von der ersten bis zur letzten. Aus der ersten Gleichung folgt zunächst, dass d' auch ein Teiler von x_2 ist. Da also d' ein gemeinsamer Teiler von x_1 und x_2 ist, folgt aus der zweiten Gleichung, dass d' auch ein Teiler von x_3 ist, usw. Schließlich erhält man, dass d' auch ein Teiler von x_n ist, q.e.d.

2.7. Beispiele. Wir berechnen als Beispiele $\gcd(238, 35)$ und $\gcd(239, 35)$.

$$\begin{aligned} 238 &= 6 \cdot 35 + 28, \\ 35 &= 1 \cdot 28 + 7, \\ 28 &= 4 \cdot 7 + 0. \end{aligned} \qquad \begin{aligned} 239 &= 6 \cdot 35 + 29, \\ 35 &= 1 \cdot 29 + 6, \\ 29 &= 4 \cdot 6 + 5, \\ 6 &= 1 \cdot 5 + 1, \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Also ist $\gcd(238, 35) = 7$ und $\gcd(239, 35) = 1$.

Als nächstes Beispiel betrachten wir zwei aufeinander folgende Fibonacci-Zahlen f_n und f_{n+1}. Aus der Rekursionsgleichung der Fibonacci-Zahlen folgt unmittelbar

$$\begin{aligned} f_{n+1} &= 1 \cdot f_n + f_{n-1}, \\ f_n &= 1 \cdot f_{n-1} + f_{n-2}, \\ &\ldots \\ f_3 &= 1 \cdot f_2 + f_1, \\ f_2 &= 1 \cdot f_1 + 0. \end{aligned}$$

Da $f_1 = 1$ folgt also: *Je zwei aufeinander folgende Fibonacci-Zahlen sind teilerfremd.*

An dieses Beispiel schließen wir noch folgende Bemerkung an: Im Euklidischen Algorithmus $(*)$ werden die Reste x_{k+1} umso schneller kein, je höher die Quotienten q_k sind. Im Falle der Fibonacci-Zahlen sind alle $q_k = 1$, d.h. dies ist der ungünstigste Fall, was die Anzahl der nötigen Schritte in Abhängigkeit von der Größe der Ausgangszahlen betrifft. Beim Euklidischen Algorithmus für f_n und f_{n+1} sind wie gesehen n Schritte nötig. Da f_n in Abhängigkeit von n exponentiell wächst, folgt, dass die Anzahl der Schritte beim Euklidischen Algorithmus zur Berechnung von $\gcd(x, y)$ höchstens logarithmisch mit x, y, d.h. linear mit der Stellenzahl der Argumente wächst. Der Euklidische Algorithmus ist also eine sehr effiziente Methode zur Berechnung des größten gemeinsamen Teilers großer Zahlen. Er benötigt nicht die Primfaktorzerlegung der Argumente.

2.8. Satz (Bézout). *Seien $x, y \in \mathbb{Z}$ und $d = \gcd(x, y)$ ihr größter gemeinsamer Teiler. Dann gibt es Zahlen $\lambda, \mu \in \mathbb{Z}$, so dass*

$$d = \lambda x + \mu y.$$

Bevor wir den Satz beweisen, leiten wir noch eine sehr nützliche Folgerung ab.

Corollar. *Zwei ganze Zahlen x, y sind genau dann teilerfremd, wenn ganze Zahlen λ, μ existieren mit*

$$\lambda x + \mu y = 1.$$

Beweis. Die eine Richtung folgt aus 2.8. Umgekehrt folgt aus $\lambda x + \mu y = 1$ natürlich, dass der größte gemeinsame Teiler von x und y gleich 1 ist.

Bemerkung. Das Corollar ist zu folgender Aussage äquivalent:
Ein ganzzahliger Vektor (a, b) lässt sich genau dann zu einer ganzzahligen Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1$$

ergänzen, wenn a und b teilerfremd sind.

2.9. Erweiterter Euklidischer Algorithmus. Wir kommen jetzt zum Beweis des Satzes 2.8. Die Existenz der Koeffizienten λ, μ zeigen wir konstruktiv mit einer Erweiterung des Euklidischen Algorithmus. Wir setzen wieder $x_0 := x$, $x_1 := y$ und schreiben den Algorithmus $(*)$ noch einmal an:

$$\begin{cases} x_0 &= q_1 x_1 - x_2, \\ x_1 &= q_2 x_2 - x_3, \\ & \cdots \\ x_{k-1} &= q_k x_k + x_{k+1}, \\ & \cdots \\ x_{n-2} &= q_{n-1} x_{n-1} + x_n, \\ x_{n-1} &= q_n x_n + 0. \end{cases}$$

Wir konstruieren der Reihe nach Zahlen $\lambda_k, \mu_k \in \mathbb{Z}$, so dass

$$x_k = \lambda_k x + \mu_k y \quad \text{für } k = 0, 1, 2, \ldots, n.$$

Da $x = x_0$ und $y = x_1$, kann man

$$(\lambda_0, \mu_0) := (1, 0) \quad \text{und} \quad (\lambda_1, \mu_1) := (0, 1)$$

wählen. Sei (λ_i, μ_i) schon für $i \leqslant k$ konstruiert. Dann bekommen wir $(\lambda_{k+1}, \mu_{k+1})$ wegen der Gleichung $x_{k+1} = x_{k-1} - q_k x_k$ durch die Rekursionsformel

$$(\lambda_{k+1}, \mu_{k+1}) := (\lambda_{k-1}, \mu_{k-1}) - q_k(\lambda_k, \mu_k).$$

Da $d = \gcd(x, y) = x_n$, erfüllt $(\lambda, \mu) := (\lambda_n, \mu_n)$ die gewünschte Gleichung

$$d = \lambda x + \mu y, \quad \text{q.e.d.}$$

Beispiel. Wir führen den erweiterten Euklidischen Algorithmus an dem schon in 2.7 behandelten Fall $x = 239$, $y = 35$ durch.

	$(\lambda_0, \mu_0) = (1, 0), \quad (\lambda_1, \mu_1) = (0, 1)$
$239 = 6 \cdot 35 + 29$	$(\lambda_2, \mu_2) = (1, 0) - 6 \cdot (0, 1) = (1, -6)$
$35 = 1 \cdot 29 + 6$	$(\lambda_3, \mu_3) = (0, 1) - 1 \cdot (1, -6) = (-1, 7)$
$29 = 4 \cdot 6 + 5$	$(\lambda_4, \mu_4) = (1, -6) - 4 \cdot (-1, 7) = (5, -34)$
$6 = 1 \cdot 5 + 1$	$(\lambda_5, \mu_5) = (-1, 7) - 1 \cdot (5, -34) = (-6, 41)$
$5 = 5 \cdot 1 + 0$	

Es gilt also

$$1 = \gcd(x, y) = -6x + 41y = -6 \cdot 239 + 41 \cdot 35.$$