Kap. IV: Der Satz von Euler/Fermat

In diesem Kapitel werden die mathematischen Grundlagen für weitere Verschlüsselungsverfahren bereitgestellt.

§ 8. Der größte gemeinsame Teiler

Es werden hier noch einmal kurz schon **bekannte** Begriffe und Ergebnisse zusammengestellt.

(8.1) DEF: a und b seien zwei beliebige ganze Zahlen. a heißt ein **Teiler** von b (in Zeichen $a \mid b$), wenn es eine ganze Zahl k gibt mit $a \cdot k = b$.
Man sagt dann auch: "**a teilt b**" oder "**b ist ein (ganzzahliges) Vielfaches von a**".

(8.2) BEM: **a)** $a \mid b \iff$ es gibt ein $k \in \mathbb{Z}$ mit $a \cdot k = b$

b) Bei der Definition der Teilbarkeit kommt die Division **nicht** vor.

c) Es gilt: $a \mid 0$ für jede ganze Zahl a, insbesondere also $0 \mid 0$.

d) Ist 0 ein Teiler einer ganzen Zahl a, so folgt $a = 0$.

e) Für $a \in \mathbb{Z}$ bezeichne $T(a)$ die **Menge aller Teiler** von a, d.h.

$$T(a) \;=\; \{\, t \mid t \in \mathbb{Z}\,,\; t|a \}$$

Für $a \neq 0$ ist $T(a)$ eine endliche Menge, und es gilt $T(0) = \mathbb{Z}$.

f) Für $a, b \in \mathbb{Z}$ ist $T(a) \cap T(b)$ die **Menge der gemeinsamen Teiler** von a und b.
Es gilt $1 \in T(a) \cap T(b)$, d.h. $T(a) \cap T(b) \neq \emptyset$.

(8.3) SATZ und DEF:
Seien a und b zwei ganze Zahlen, die **nicht beide** Null sind. Dann ist $T(a) \cap T(b)$ eine endliche nichtleere Menge, in der es ein größtes Element g gibt. g heißt **größter gemeinsamer Teiler** von a und b, in Zeichen

$$g \;=\; \mathrm{ggT}(a,b)\,.$$

(8.4) SATZ: Seien a und b zwei ganze Zahlen, die nicht beide Null sind. Eine ganze Zahl g ist genau dann der größte gemeinsame Teiler von a und b, wenn gilt:

GGT_0) $g \geq 0$

GGT_1) $g \mid a$ und $g \mid b$

GGT_2) Für alle $t \in \mathbb{Z}$ mit $t \mid a$ und $t \mid b$ folgt $t \mid g$.

(8.5) SATZ: Seien $m, n \in \mathbb{N}$. Dann gilt:

a) Der ggT von m und n läßt sich mit Hilfe des **euklidischen Algorithmus** (EA) berechnen.

b) Mit Hilfe des **erweiterten euklidischen Algorithmus** (EEA) lassen sich Zahlen $x, y \in \mathbb{Z}$ berechnen, so dass gilt

$$\mathbf{ggT}(m,n) \;=\; x \cdot m + y \cdot n\,,$$

d.h. $\mathbf{ggT}(m,n)$ läßt sich als **ganzzahlige Linearkombination** von m und n darstellen.

(8.6) DEF: Zwei ganze Zahlen a und b heißen **teilerfremd**, wenn $\mathbf{ggT}(a,b) = 1$ gilt.

(8.7) BEM: Zwei ganze Zahlen a und b sind genau dann **teilerfremd**, wenn es ganze Zahlen x und y gibt mit

$$xa + yb \;=\; 1\,.$$

(8.8) SATZ: Für $a, b, c \in \mathbb{Z}$ gelten die folgenden Aussagen:

a) $a \mid c$ und $b \mid c$ und $\mathbf{ggT}(a,b) = 1 \quad\Longrightarrow\quad (a \cdot b) \mid c$

b) $a \mid (b \cdot c)$ und $\mathbf{ggT}(a,b) = 1 \quad\Longrightarrow\quad a \mid c$.

BEM: Ohne die Voraussetzung, dass die Zahlen a und b teilerfremd sind, gelten die obigen Aussagen i.a. nicht:

Gegenbeispiel zu **a)** : $4 \mid 12$ und $6 \mid 12$, aber $4 \cdot 6 = 24$ ist kein Teiler von 12.

b) $6 \mid (4 \cdot 9)$, aber $6 \nmid 4$ und $6 \nmid 9$.

Zwei Anwendungen:

(8.9) SATZ: **Kürzungsregel**

Seien $a, b, c \in \mathbb{Z}$ und $n \in \mathbb{N}$. Sind dann c und n teilerfremd, so gilt:

$$(a \cdot c) \bmod n = (b \cdot c) \bmod n \quad\Longrightarrow\quad a \bmod n = b \bmod n$$

BEM: Auch hier kann man auf die Voraussetzung $\mathbf{ggT}(c,n) = 1$ nicht verzichten.

(8.10) SATZ: Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:

a) Es gibt ein $x \in \mathbb{Z}$ mit $(a \cdot x) \bmod n = 1$ (d.h. a besitzt ein **Inverses modulo n**)

b) $\mathbf{ggT}(a,n) = 1$.

(8.11) BEM: Der Beweisteil b) $\Longrightarrow$ a) enthält ein Verfahren zur Berechnung des Inversen von a modulo n, falls a und n teilerfremd sind.

Zusatz zu (8.5) **A) Formelmäßige Beschreibung des EA:**

Im Falle $n \mid m$ ist $\mathbf{ggT}(m,n) = n$, so dass wir im folgenden $n \nmid m$ voraussetzen können. Wir führen eine Kette von Divisionen mit Rest aus:

$$\begin{array}{lrcrcll}
(1) & m & = & q_1 \cdot n & + & r_2 & (0 < r_2 < n) \\
(2) & n & = & q_2 \cdot r_2 & + & r_3 & (0 < r_3 < r_2) \\
(3) & r_2 & = & q_3 \cdot r_3 & + & r_4 & (0 < r_4 < r_3) \\
(4) & r_3 & = & q_4 \cdot r_4 & + & r_5 & (0 < r_5 < r_4) \\
\vdots & & \vdots & & & & \\
(k-1) & r_{k-2} & = & q_{k-1} \cdot r_{k-1} & + & r_k & (0 < r_k < r_{k-1})
\end{array}$$

d.h. r_k ist der Rest und q_{k-1} der Quotient bei Division von r_{k-2} durch r_{k-1}.

Wir haben begründet, dass der Rest irgendwann einmal 0 werden muss, d.h. es gibt ein $s \geq 2$ mit

$$r_s \neq 0 \text{ und } r_{s+1} = 0$$

Die letzten drei Zeilen des obigen Rechenschemas lauten dann

$$\begin{array}{lrcrcll}
(s-2) & r_{s-3} & = & q_{s-2} \cdot r_{s-2} & + & r_{s-1} & (0 < r_{s-1} < r_{s-2}) \\
(s-1) & r_{s-2} & = & q_{s-1} \cdot r_{s-1} & + & r_s & (0 < r_s < r_{s-1}) \\
(s) & r_{s-1} & = & q_s \cdot r_s & & &
\end{array}$$

Für diesen letzten von 0 verschiedenen Rest r_s gilt dann $r_s = \mathbf{ggT}(m,n)$.

EEA: Löst man die Gleichung $(s-1)$ nach r_s auf, so erhält man

$$r_s = r_{s-2} - q_{s-1} \cdot r_{s-1}$$

Man setzt jetzt für r_{s-1} den Wert ein, der sich aus der Gleichung $(s-2)$ ergibt:

$$\begin{aligned}
r_s = r_{s-2} - q_{s-1} \cdot \underline{r_{s-1}} &= r_{s-2} - q_{s-1} \cdot (\underline{r_{s-3} - q_{s-2} \cdot r_{s-2}}) \\
&= r_{s-2} - q_{s-1} \cdot r_{s-3} + q_{s-1} \cdot q_{s-2} \cdot r_{s-2} \\
&= (1 - q_{s-2}) \cdot r_{s-2} - q_{s-1} \cdot r_{s-3}
\end{aligned}$$

Damit ist r_s eine Linearkombination der beiden vorherigen Reste r_{s-2} und r_{s-3}. Als nächstes wird r_{s-2} aus der Gleichung $(s-3)$ berechnet und der Wert für r_{s-2} in die letzte Gleichung eingesetzt. Damit wird r_s als Linearkombination der beiden Reste r_{s-3} und r_{s-4} dargestellt. Setzt man dieses Verfahren fort, erhält man am Ende eine Darstellung von r_s als Linearkombination von m und n.

B) Berechnung des ggT's von zwei ganzen Zahlen:

Mit Hilfe des EA läßt sich der ggT zunächst nur von zwei natürlichen Zahlen ≥ 1 berechnen. Wir können den EA aber auch benutzen, um den ggT von zwei ganzen Zahlen a und b zu berechnen, die beide ungleich Null sind: es gilt nämlich $\mathbf{ggT}(a,b) = \mathbf{ggT}(|a|,|b|)$ und $|a|, |b| \in \mathbb{N}$. Ist eine der beiden Zahlen Null, etwa $b = 0$, so ist $\mathbf{ggT}(a,0) = |a|$ für alle $a \in \mathbb{Z}, a \neq 0$. Damit können wir also den ggT von zwei ganzen Zahlen, die nicht beide Null sind, berechnen.
Auch (8.5b) läßt sich übertragen. Sind die ganzen Zahlen a und b beide nicht Null, so kann man mit Hilfe des EEA $\mathbf{ggT}(|a|,|b|)$ als Linearkombination von $|a|$ und $|b|$ darstellen, so dass es auch Zahlen $x, y \in \mathbb{Z}$ gibt mit

$$\mathbf{ggT}(a,b) = x \cdot a + y \cdot b\,.$$