§ 2 Elementare Zahlentheorie

Definition 2.1:

Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$. Die Zahl a heißt ein Teiler von b, falls $\frac{b}{a} \in \mathbb{Z}$ ist.

In dem Fall sagen wir auch:

b ist ein Vielfaches von a oder

b ist durch a teilbar oder

a teilt b.

Wir schreiben dann auch: $a | b$.

Ist a kein Teiler von b, so schreiben wir: $a \nmid b$.

Beispiele:

$3 | 6$; $7 | 91$; $-13 | 39$.

Bemerkungen 2.2:

i) Für alle $a \in \mathbb{Z} \setminus \{0\}$ gilt:

$a | a$, $-a | a$, $1 | a$, $-1 | a$, $a | 0$.

ii) Sind $a, b \in \mathbb{Z} \setminus \{0\}$ und $c \in \mathbb{Z}$ mit $a | b$ und $b | c$, so folgt auch: $a | c$.

iii) Sind $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$ und $b_1, b_2 \in \mathbb{Z}$ mit $a_1 | b_1$ und $a_2 | b_2$, so folgt auch: $(a_1 \cdot a_2) | (b_1 \cdot b_2)$.

iv) Sind $a, b \in \mathbb{Z} \setminus \{0\}$ mit $a | b$ und $b | a$, so ist $a = b$ oder $a = -b$.

v) Jede Zahl $b \in \mathbb{Z} \setminus \{0\}$ hat nur endlich viele Teiler; diese liegen alle im Intervall $[-b, b]$.

vi) Sind $b, c \in \mathbb{Z}$ und $a \in \mathbb{Z} \setminus \{0\}$ mit $a | b$ und $a | c$, so folgt für alle $m, n \in \mathbb{Z}$:

$$a | (m \cdot b + n \cdot c).$$

<u>Definition 2.3:</u>

Sei M eine nichtleere Menge und R eine Relation auf M. R heißt eine <u>Äquivalenzrelation</u>, falls gilt:

(I) R ist <u>reflexiv</u>; das heißt, für alle $x \in M$ gilt: $x R x$.

(II) R ist <u>symmetrisch</u>; das heißt: Sind $x, y \in M$ mit $x R y$, so gilt auch: $y R x$.

(III) R ist <u>transitiv</u>; das heißt: Sind $x, y, z \in M$ mit $x R y$ und $y R z$, so gilt auch: $x R z$.

<u>Beispiele:</u>

i) Die <u>Gleichheitsrelation</u> auf einer nichtleeren Menge M ist eine Äquivalenzrelation; die ist gegeben durch

$$R := \{(x, y) \in M^2 \mid x = y\}.$$

ii) Die volle Menge M^2 ist ebenfalls eine Äquivalenzrelation, das heißt, für <u>alle</u> $x, y \in M$ gilt:

$$x R y.$$

iii) Sei $f: M \to N$ eine Abbildung, und setze

$$R := \{(x, y) \in M^2 \mid f(x) = f(y)\}.$$

Dann ist R eine Äquivalenzrelation.

Definition 2.4:

Sei $m \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent modulo m**, falls $b-a$ durch m teilbar ist, falls also gilt: $m \mid (b-a)$.

Wir schreiben dann auch: $a \equiv b \mod m$.

Beispiele:

$3 \equiv 7 \mod 2$, $2 \equiv 5 \mod 3$, $-3 \equiv 7 \mod 10$

Satz 2.5:

Ist $m \in \mathbb{N}$ fest, so ist die Relation „$\equiv$" eine Äquivalenzrelation auf $\mathbb{Z}$.

Nachweis der Transitivität:

Seien $a, b, c \in \mathbb{Z}$ mit $a \equiv b \mod m$ und $b \equiv c \mod m$. Dann ist sowohl $b-a$ als auch $c-b$ ein Vielfaches von m. Folglich ist auch $c-a = (c-b)+(b-a)$ ein Vielfaches von m; das heißt: $a \equiv c \mod m$. $\square$

Satz 2.6:

Sei $m \in \mathbb{N}$, und seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit

$$a_1 \equiv b_1 \mod m \quad , \quad a_2 \equiv b_2 \mod m.$$

Dann gilt auch:

i) $a_1 + a_2 \equiv b_1 + b_2 \mod m$,

ii) $a_1 - a_2 \equiv b_1 - b_2 \mod m$,

iii) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod m$.

Kongruenzen können also addiert, subtrahiert und multipliziert werden.

Beweis von iii):

Wir erhalten:

$$b_1 \cdot b_2 - a_1 \cdot a_2 = b_1 \cdot (b_2 - a_2) + (b_1 - a_1) \cdot a_2 .$$

Die rechte Seite ist durch m teilbar, weil $b_2 - a_2$ und $b_1 - a_1$ durch m teilbar sind. $\square$

Satz 2.7, Die Division mit Rest:

Seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann gibt es genau eine Zahl $q \in \mathbb{Z}$ und genau eine Zahl $r \in \mathbb{Z}$ mit:

$$a = q \cdot m + r \quad , \quad 0 \leq r \leq m-1.$$

Das bedeutet:

a kann auf eindeutige Weise durch m mit einem Rest r, $0 \leq r \leq m-1$, dividiert werden.

Beweis:

Nachweis der Eindeutigkeit:

Seien $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ mit $0 \leq r_1, r_2 \leq m-1$ und

$$a = q_1 \cdot m + r_1 = q_2 \cdot m + r_2 .$$

Dann folgt einerseits $|r_1 - r_2| < m$ und andererseits $r_1 - r_2 = m \cdot (q_2 - q_1)$, also $r_1 \equiv r_2 \bmod m$.

Das ist nur möglich, wenn $r_1 = r_2$ ist.

Wegen $m \neq 0$ folgt dann auch: $q_1 = q_2$.

Nachweis der Existenz:

Sei $q \in \mathbb{Z}$ die größte Zahl mit $q \cdot m \leq a$, und setze $r := a - q \cdot m$.

Dann ist $r \geq 0$. Laut Wahl von q ist weiter $(q+1) \cdot m > a$, also $r = a - q \cdot m < m$ und folglich $r \leq m-1$. $\square$

Definition 2.8:

Für $n, m \in \mathbb{Z}$ mit $(n, m) \neq (0, 0)$ bezeichnet $ggT(n, m)$ den größten gemeinsamen Teiler von n und m, also die größte Zahl $t \in \mathbb{N}$ mit $t | n$ und $t | m$.
Ist $ggT(n, m) = 1$, so heißen n und m teilerfremd.

Bemerkung 2.9:

Sind $n, m, q \in \mathbb{Z}$ mit $(n, m) \neq (0, 0)$, so ist eine Zahl $t \in \mathbb{N}$ genau dann ein gemeinsamer Teiler von n und m, wenn sie ein gemeinsamer Teiler von m und $q \cdot m + n$ ist.
Man beachte dazu: $n = -q \cdot m + (q \cdot m + n)$.
Insbesondere gilt:

$$ggT(n, m) = ggT(q \cdot m + n, m).$$

Satz 2.10, Der Euklidische Algorithmus zur Berechnung des ggT

Es seien $a_0, a_1 \in \mathbb{N}$ mit $a_1 \leq a_0$. Dann kann $d := ggT(a_0, a_1)$ nach dem folgenden Euklidischen Algorithmus berechnet werden:

Schritt 0:

Falls $a_1 | a_0$, setze $d := a_1$.
Stopp!

Schritt 1:

Bestimme $q_1 \in \mathbb{Z}$ und $a_2 \in \mathbb{N}$ mit

(EA 1) $\quad a_0 = q_1 \cdot a_1 + a_2 \quad , \quad 0 < a_2 \leq a_1 - 1.$

Falls $a_2 | a_1$, setze $d := a_2$.
Stopp!

Schritt i, i > 1:

Wähle $q_i \in \mathbb{Z}$ und $a_{i+1} \in \mathbb{N}$ mit

(EA i) $\quad a_{i-1} = q_i \cdot a_i + a_{i+1} \quad , \quad 0 < a_{i+1} \leq a_i - 1.$

Falls $a_{i+1} | a_i$, setze $d := a_{i+1}$.

Stopp!

Beweis:

Dass der Algorithmus abbricht, folgt sofort aus der Tatsache, dass die natürlichen Zahlen $a_0, a_1, a_2, \ldots$ immer echt kleiner werden.

Weiter liefert Bemerkung 2.9 für alle möglichen i:

$$ggT(a_{i-1}, a_i) = ggT(q_i \cdot a_i + a_{i+1}, a_i) = ggT(a_{i+1}, a_i).$$

Bricht der Algorithmus nach j Schritten ab, so gilt $a_{j+1} | a_j$, und für $d := a_{j+1}$ folgt induktiv:

$$d = ggT(a_j, a_{j+1}) = ggT(a_{j-1}, a_j) = \ldots = ggT(a_0, a_1). \qquad \square$$

Weiter gilt

Satz 2.11:

Sind $a_0, a_1 \in \mathbb{N}$, so folgt für $d := ggT(a_0, a_1)$:

Es gibt $b, c \in \mathbb{Z}$ mit

$$d = b \cdot a_0 + c \cdot a_1 .$$

Der Beweis folgt induktiv direkt aus den obigen Formeln (EA i).

Beispiel:

Zu berechnen ist $ggT(182, 325)$.

Wiederholte Division mit Rest liefert:

$$325 = 1 \cdot 182 + 143,$$
$$182 = 1 \cdot 143 + 39,$$
$$143 = 3 \cdot 39 + 26,$$
$$39 = 1 \cdot 26 + 13,$$
$$26 = 2 \cdot 13.$$

Damit folgt: $13 = ggT(182, 325)$.

Lesen wir die letzten Gleichungen von unten nach oben, so erhalten wir:

$$\begin{aligned} 13 &= 39 - 1 \cdot 26 = 39 - (143 - 3 \cdot 39) = 4 \cdot 39 - 143 \\ &= 4 \cdot (182 - 143) - 143 = 4 \cdot 182 - 5 \cdot 143 \\ &= 4 \cdot 182 - 5 \cdot (325 - 182) \\ &= 9 \cdot 182 - 5 \cdot 325 . \end{aligned}$$

Definition 2.12:

Eine natürliche Zahl $p \in \mathbb{N}$ mit $p \geq 2$ heißt eine **Primzahl**, falls kein $k \in \mathbb{N}$ mit $1 < k < p$ und $k | p$ existiert. $\mathbb{P}$ bezeichne die Menge der Primzahlen.

Bemerkung:

Die kleinsten Primzahlen sind:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$

<u>Satz 2.13:</u>

Es seien $n, m \in \mathbb{N}$, und es sei p eine Primzahl mit $p \mid (n \cdot m)$. Dann gilt $p \mid n$ oder $p \mid m$.

<u>Beweis:</u>

Wir nehmen an, es gelte $p \nmid n$ und $p \nmid m$.

Wegen $p \in \mathbb{P}$ gilt dann: $\quad 1 = ggT(p,n) = ggT(p,m)$.

Nach zweimaliger Anwendung von Satz 2.11 existieren $a, b, c, d \in \mathbb{Z}$ mit:

$$a \cdot p + b \cdot n = 1 \quad , \quad c \cdot p + d \cdot m = 1 \ .$$

Laut Voraussetzung ist weiter $k := \frac{n \cdot m}{p} \in \mathbb{N}$.

Damit folgt:

$$\begin{aligned} & 1 \\ = & (a \cdot p + b \cdot n) \cdot (c \cdot p + d \cdot m) \\ = & p \cdot (a \cdot c \cdot p + a \cdot d \cdot m + b \cdot c \cdot n + b \cdot d \cdot k). \end{aligned}$$

Das ist ein Widerspruch, denn 1 ist kein Vielfaches von p.

$\square$

<u>Satz 2.14, Fundamentalsatz der Elementaren Zahlentheorie:</u>

Zu jeder natürlichen Zahl $n \geq 2$ gibt es Primzahlen $p_1, \dots, p_s$ mit $p_1 \leq \dots \leq p_s$ und

$$\text{(Z)} \qquad n = p_1 \cdots p_s = \prod_{i=1}^{s} p_i \ .$$

Sind auch $q_1, \dots, q_t$ Primzahlen mit $q_1 \leq \dots \leq q_t$ und

$$\text{(Z2)} \qquad n = q_1 \cdots q_t = \prod_{j=1}^{t} q_j \ ,$$

so ist $s = t$ und $p_i = q_i$ für $1 \leq i \leq s$.

Beweis:

Wir führen Induktion nach n.
Für $n=2$ und $n=3$ ist nichts zu zeigen, weil 2 und 3 selbst Primzahlen sind.
Sei nun $n \geq 4$, und sei p_1 der kleinste Primteiler von n; das ist die kleinste Primzahl mit $p_1 | n$.

Nachweis der Existenz:
Nach Induktionsannahme ist

$$\frac{n}{p_1} = p_2 \cdots p_s$$

für gewisse Primzahlen $p_2, \dots, p_s$ mit $p_2 \leq \dots \leq p_s$.
Damit folgt auch (Z).

Nachweis der Eindeutigkeit:
Gelten (Z) und (Z2), so liefert Satz 2.13
wegen $p_1 \in \mathbb{P}$: $p_1 | q_i$ für ein i mit $1 \leq i \leq t$.
Wegen $q_i \in \mathbb{P}$ ist das nur möglich, wenn $p_1 = q_i$ ist.
Weil p_1 der kleinste Primteiler von n ist, folgt: $p_1 = q_1$.
(Z) und (Z2) liefern also:

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t .$$

Anwendung der Induktionsannahme auf die Zahl $\frac{n}{p_1}$ liefert die Behauptung.

$\square$

Bemerkung 2.15:

Satz 2.14 besagt auch:

Jede natürliche Zahl $n \geq 2$ hat eine eindeutig bestimmte Primfaktorzerlegung der Gestalt

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

mit $p_1, \dots, p_k \in \mathbb{P}$, $p_1 < \dots < p_k$, $\alpha_1, \dots, \alpha_k \in \mathbb{N}$.

Bemerkungen 2.16:

Gegeben seien $n, m \in \mathbb{N}$ mit

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad , \quad m = \prod_{i=1}^{k} p_i^{\beta_i} \quad ,$$

wobei gelte:

$p_1, \dots, p_k \in \mathbb{P}$, $p_1 < \dots < p_k$;
$\alpha_i, \beta_i \geq 0$, $\max(\alpha_i, \beta_i) > 0$ für $1 \leq i \leq k$.

i) Eine Zahl $t \in \mathbb{N}$ ist genau dann ein gemeinsamer Teiler von n und m, wenn t die Gestalt

$$t = \prod_{i=1}^{k} p_i^{\gamma_i}$$

hat mit $0 \leq \gamma_i \leq \min(\alpha_i, \beta_i)$ für $1 \leq i \leq k$.

Insbesondere ist

$$ggT(n, m) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)} \quad ,$$

und jeder gemeinsame Teiler von n und m ist auch ein Teiler von $ggT(n, m)$.

ii) Das kleinste gemeinsame Vielfache von n und m ist die Zahl

$$kgV(n,m) = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} .$$

Jedes andere gemeinsame Vielfache von n und m ist nach Satz 2.14 auch ein Vielfaches von $kgV(n,m)$.

iii) Aus i) und ii) folgt:

$$ggT(n,m)\cdot kgV(n,m) = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = n\cdot m .$$

Insbesondere gilt folgende Äquivalenz:

$$ggT(n,m) = 1 \Leftrightarrow kgV(n,m) = n\cdot m.$$

Sind n und m teilerfremd, so sind die gemeinsamen Vielfachen von n und m also genau die Vielfachen von $n\cdot m$.

<u>Satz 2.17, der Chinesische Restsatz für 2 simultane Kongruenzen:</u>

Die natürlichen Zahlen m_1, m_2 seien teilerfremd, und setze $m := m_1 \cdot m_2$. Weiterhin seien $a_1, a_2 \in \mathbb{Z}$ gegeben. Dann gibt es genau eine Zahl $a \in \mathbb{Z}$ mit $0 \leq a \leq m-1$, die die beiden folgenden Kongruenzen löst:

(CR 0) $\qquad a \equiv a_i \mod m_i$ für $i \in \{1,2\}$.

a kann wie folgt ermittelt werden:

Wähle $c_1, c_2 \in \mathbb{Z}$ mit

(CR 1) $\qquad c_1 \cdot m_1 + c_2 \cdot m_2 = 1$

und setze

(CR2) $\quad q := c_1 \cdot m_1 \cdot a_2 + c_2 \cdot m_2 \cdot a_1$.

Dann ist a die eindeutig bestimmte ganze Zahl mit

(CR3) $\quad a \equiv q \bmod m$ und $0 \leq a \leq m-1$.

Beweis:

Nachweis der Eindeutigkeit:

Seien $a, a' \in \mathbb{Z}$ mit $0 \leq a, a' \leq m-1$ und
$$a \equiv a' \equiv a_i \bmod m_i \quad \text{für } i \in \{1,2\}.$$
Dann ist $a - a'$ ein gemeinsames Vielfaches von m_1 und m_2 - und damit nach Bemerkung 2.16 iii) auch von $m = m_1 \cdot m_2$.

Aus $a \equiv a' \bmod m$ und $0 \leq a, a' \leq m-1$ folgt nun $a = a'$.

Nachweis der Existenz:

Nach Satz 2.11 gibt es $c_1, c_2 \in \mathbb{Z}$, die (CR1) erfüllen.
Für q, a wie in (CR2) bzw. (CR3) folgt dann
$$a \equiv q \equiv c_2 \cdot m_2 \cdot a_1 \equiv (1 - c_1 \cdot m_1) \cdot a_1 \equiv a_1 \bmod m_1$$
und analog $a \equiv a_2 \bmod m_2$. $\square$

Bemerkung 2.18:

Ein ähnliches Ergebnis läßt sich für v, $v \geq 2$ beliebig, paarweise teilerfremde natürliche Zahlen $m_1, \dots, m_v$ - etwa durch Induktion - beweisen:

Ist $m := m_1 \cdots m_v$, und sind $a_1, \dots, a_v \in \mathbb{Z}$ gegeben, so gibt es genau eine Zahl $a \in \mathbb{Z}$ mit $0 \leq a \leq m-1$, die jede der folgenden Kongruenzen löst:
$$a \equiv a_i \bmod m_i \quad \text{für } 1 \leq i \leq v.$$

Beispiel:

Bestimme die eindeutig bestimmte Zahl $a \in \mathbb{Z}$ mit $0 \leq a \leq 133 \cdot 92 - 1 = 12235$, die die folgenden Kongruenzen löst:

$$a \equiv 25 \mod 133, \quad a \equiv 17 \mod 92.$$

Zunächst gilt - etwa nach Anwendung des Euklidischen Algorithmus:

$$9 \cdot 133 - 13 \cdot 92 = 1.$$

Gemäß (CR2) setzen wir also

$$q := 9 \cdot 133 \cdot 17 - 13 \cdot 92 \cdot 25 = 20349 - 29900 = -9551.$$

Dann ist $a := -9551 + 12236 = 2685$ zu setzen.

Satz 2.19:

Sei $m \in \mathbb{N}$, und sei $a \in \mathbb{Z}$ mit $ggT(a, m) = 1$. Dann gibt es ein $b \in \mathbb{Z}$ mit $a \cdot b \equiv 1 \mod m$.

Beweis:

Nach Satz 2.11 gibt es $b, c \in \mathbb{Z}$ mit $a \cdot b + m \cdot c = 1$.

Damit folgt sofort: $\quad a \cdot b \equiv 1 \mod m$.

$\square$

Satz 2.20, Der kleine Satz von Fermat für Primzahlen:

Sei p eine Primzahl, und sei $a \in \mathbb{Z}$ mit $ggT(a, p) = 1$.

Dann gilt:

$$a^{p-1} \equiv 1 \mod p.$$

Beweis:

Nach Satz 2.19, angewandt auf $m = p$, gibt es ein $b \in \mathbb{Z}$ mit $a \cdot b \equiv 1 \mod p$.

Nach Aufgabe 11(iii) gilt weiter:

$$a^p \equiv a \mod p.$$

Multiplikation dieser Kongruenz mit b liefert:

$$a^{p-1} \equiv (b \cdot a) \cdot a^{p-1} \equiv b \cdot a^p \equiv b \cdot a \equiv 1 \mod p.$$

$\square$

<u>Definition 2.21:</u>

Die <u>Eulersche φ-Funktion</u> $\varphi : \mathbb{N} \to \mathbb{N}$ ist definiert durch

$$\varphi(n) := \# \{ k \in \mathbb{N} \mid 1 \leq k \leq n, \, ggT(k,n) = 1 \}.$$

<u>Wertetabelle</u>

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

<u>Satz 2.22:</u>

Für jede Primzahl p und jedes $n \in \mathbb{N}$ gilt:

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1} \cdot (p-1).$$

Insbesondere ist $\varphi(p) = p-1$.

<u>Beweis:</u>

Wir erhalten:

$$\begin{aligned} &\varphi(p^n) \\ &= p^n - \# \{ k \in \mathbb{N} \mid 1 \leq k \leq p^n, \, ggT(p^n, k) > 1 \} \\ &= p^n - \# \{ k \in \mathbb{N} \mid 1 \leq k \leq p^n, \, p \mid k \} \\ &= p^n - p^{n-1}. \end{aligned}$$

$\square$

Satz 2.23:

Seien p und q zwei <u>verschiedene</u> Primzahlen.
Dann gilt:

$$\varphi(p\cdot q) = (p-1)\cdot(q-1) = \varphi(p)\cdot\varphi(q).$$

Beweis:

Nach Satz 2.22 braucht nur die erste Gleichung bewiesen zu werden. – Dazu zählen wir alle Zahlen k mit $1 \leq k < p\cdot q$, die <u>nicht</u> teilerfremd zu $p\cdot q$ sind. Das sind einerseits die Vielfachen

$$p, 2p, \ldots, (q-1)\cdot p \qquad (q-1 \text{ Stück})$$

von p sowie andererseits die Vielfachen

$$q, 2q, \ldots, (p-1)\cdot q \qquad (p-1 \text{ Stück})$$

von q. Somit folgt:

$$\varphi(p\cdot q) = (p\cdot q-1) - ((q-1)+(p-1))$$
$$= p\cdot q - q - p + 1 = (p-1)\cdot(q-1).$$

$\square$

Allgemeiner kann man – etwa mit Hilfe des Chinesischen Restsatzes – beweisen:

Satz 2.24:

Für je zwei <u>teilerfremde</u> Zahlen $n, m \in \mathbb{N}$ gilt:

$$\varphi(n\cdot m) = \varphi(n)\cdot\varphi(m).$$

Satz 2.25:

Seien p und q zwei verschiedene Primzahlen.
Dann gilt für alle $m, k \in \mathbb{N}$:

$$m^{k\cdot(p-1)\cdot(q-1)+1} \equiv m \mod p\cdot q.$$

Beweis:
Weil p und q teilerfremd sind, reicht es aus Symmetriegründen, zu zeigen:

$$m^{k\cdot(p-1)\cdot(q-1)+1} \equiv m \mod p.$$

Dies ist trivial im Falle $p | m$.
Andernfalls ist $ggT(m,p)=1$, und dann liefert Satz 2.20:

$$m^{p-1} \equiv 1 \mod p$$

$$\Rightarrow \quad (m^{(p-1)})^{k\cdot(q-1)} \equiv 1 \mod p$$

$$\Rightarrow \quad m^{k\cdot(p-1)\cdot(q-1)+1} \equiv m \mod p. \qquad \square$$

Satz 2.25 wird im folgenden Abschnitt „Kryptologie" wichtig; dort werden Verschlüsselungsvorschriften vorgestellt, die „leicht" durchzuführen sind, wogegen die inverse Entschlüsselung – ohne zusätzliche Kenntnisse – „schwer" ist.